



# 公部門與企業 數位韌性指南

從備援、災難復原到資安防護的實務框架

# 您的組織準備好了嗎？

組織的關鍵系統可以  
承受多長時間的停機？

遇到勒索軟體攻擊時，  
您的備份是否與主系統隔離？

您的團隊上一次緊急應變  
/ DR 演練是什麼時候？

DR = 災難復原

您知道各系統的  
RTO / RPO 目標嗎？

RTO = 可接受的最長停機時間

RPO = 可接受的最大資料遺失量

如果海底電纜中斷，  
您的服務還能運作嗎？

您是否已經有 IT 緊急  
應變人力規劃？

如果以上問題讓您猶豫，這本指南就是為您準備的。

# 01 我們可能遇到的威脅

「知彼知己，百戰不殆」。了解資訊系統會遭遇到的威脅，才能打造具有高韌性的數位服務。



## 局部區域性災害

天災 (地震、颱風、水災)、設施故障、電力中斷、供水異常、實體設備損壞等，影響單一機房或單一可用區 (Availability Zone, AZ, 即大型獨立資料中心)。



## 全區域基礎設施故障

大規模天災或基礎設施連鎖故障，導致整個區域的資料中心同時不可用。



## 對外連線中斷

海底電纜中斷、骨幹網路癱瘓，導致無法對外提供服務或存取境外備援資源。



## 網路攻擊與資安事件

無論是勒索軟體、DDoS、社交工程攻擊、APT 進階持續性威脅、內部人員惡意行為、供應鏈攻擊等，都可能癱瘓整個機關運作。



## 新型威脅類型

新興風險已從「服務中斷」、「資料失效」延伸至「量子攻擊」、「認知與信任操弄」：先竊取、後解密；假訊息、Deepfake 與內容竄改直接攻擊服務可信度等。基礎設施須具備自動偵測與反應機制，同時得以應對 AI 誤用等風險。

# 韌性規劃四大原則

- 1 先假定災害規模，再選擇對應架構
- 2 依系統重要性，採用不同等級的韌性策略
- 3 為不同等級的韌性策略，規劃對應預算
- 4 定期演練驗證，確保韌性規劃持續有效

# 02 如何提升韌性

數位韌性的建設，需要從六個關鍵面向同步推進。每個面向環環相扣，缺一不可。

# 韌性六大支柱



# 2.1

## 備援架構

備援架構是韌性的基石。當主要系統無法運作時，備援架構能讓服務在最短時間內恢復。

我們假定的最大災害規模是什麼？

各系統可接受的最長停機時間 (RTO) 是多少？

各系統可接受的最大資料遺失量 (RPO) 是多少？

我們的預算能支撐什麼等級的備援架構？

| 策略                           | 恢復時間 | 資料遺失 | 成本       | 適用場景    |
|------------------------------|------|------|----------|---------|
| 備份與還原<br>Backup & Restore    | 數日   | 數小時  | 低 (1.1x) | 非關鍵系統   |
| 即時複寫<br>Pilot Light          | 數小時  | 分鐘級  | 低 (1.2x) | 中等重要性系統 |
| 暖備援 (縮容運行)<br>Warm Standby   | 數小時內 | 秒~分鐘 | 中 (1.5x) | 重要業務系統  |
| 熱備援 (全量運行)<br>Hot Standby    | 數分鐘  | 近即時  | 高 (1.8x) | 關鍵任務系統  |
| 雙主中心 (全量運行)<br>Active-Active | 數秒   | 近零   | 最高 (2x+) | 零停機要求   |

# 2.1

## 備援架構

備援架構是韌性的基石。當主要系統無法運作時，備援架構能讓服務在最短時間內恢復。

### 實務實踐

#### 多可用區部署

- 將系統部署於同一區域 (如台灣) 內，具有三座以上相隔一定距離、實體隔離的可用區 (AZ)，確保單一可用區故障不影響服務。
- 使用負載平衡器自動分配流量至運作中的可用區
- 資料庫採多可用區同步複寫，確保資料一致性
- 可用區應具備獨立電力、冷卻與實體建築

#### 跨區域備援

- 關鍵系統的備份資料，應存放於不同地理區域 (如台灣、日本)，若涉及個人資料、機敏資料或依法受管制資料時，應依主管機關規範及組織資料治理政策辦理
- 依據系統重要性，選擇適當的跨區域備援策略
- 建議選擇於台灣設有本地區域的公有雲，搭配跨區域複寫，兼顧資料主權與異地備援

#### 基礎設施即程式碼 (IaC)

- 所有基礎設施配置應以程式碼管理 (可用熟悉的程式語言)，確保可重複部署
- 災害發生時，可在備援區域快速重建完整環境
- 定期驗證 IaC 腳本的正确性

#### 多維度備援

- 備援不僅限於基礎設施，亦應考量：
  - 通訊路徑
  - 計算資源
  - 資料存取
  - AI 推論能力

# 2.2

## 災難復原

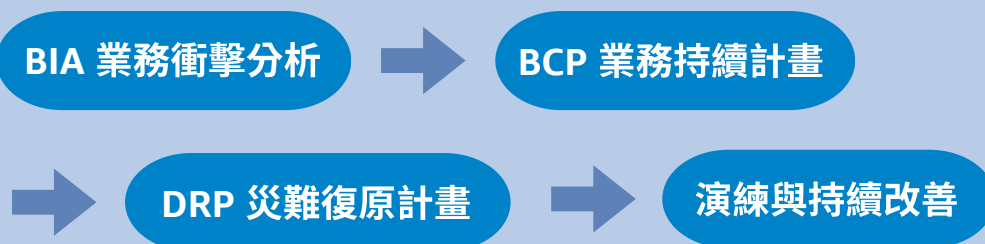
災難復原 (DR) 不是一次性專案，而是持續改善的循環流程。

### 韌性生命週期



## 建立業務持續管理體系 (BCM)

BCM 是一套完整的管理框架，確保組織在面對各種中斷事件時，能夠持續運作關鍵業務。BCM 涵蓋從分析、規劃到演練的完整循環。

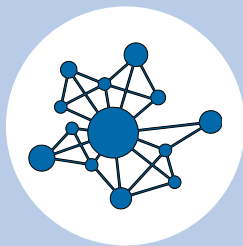


參考標準：ISO 22301 (BCM 管理系統)、ISO 22317 (BIA 指引)

# 2.3

## 網路韌性

網路是所有數位服務的命脈。  
網路中斷意味著服務中斷。



### 多路徑連線

- 關鍵系統應具備至少兩條獨立的網路路徑
- 建議採用多重骨幹網路，避免單一線路成為單點故障
- 考慮使用不同技術的備援線路 (光纖 + 無線)



### 對外連線備援

- 主要對外連線中斷時，有備援連線可自動接手
- 考慮使用全域任播 IP 與高可用 DNS 服務及多重 DNS 備援機制，提升網路韌性及服務可用性
- 針對關鍵或實體線路風險較大之地理區域，**導入海地星空全域強韌通訊網方案結合雲端作為備援**



### 內部網路分段

- 將內部網路依功能與安全等級進行分段
- 限制不同網段之間的存取權限
- 確保單一網段的問題不會擴散至整個網路

# 2.3

## 網路韌性

網路是所有數位服務的命脈。  
網路中斷意味著服務中斷。

### 實務實踐

| 項目      | 建議做法                       |
|---------|----------------------------|
| DNS 韌性  | 使用多個 DNS 服務提供者，避免 DNS 單點故障 |
| DDoS 防護 | 部署 DDoS 緩解服務，保護對外服務入口      |
| CDN 加速  | 使用內容傳遞網路分散流量，降低單點壓力        |
| VPN 備援  | 遠端存取應有備援 VPN 通道            |
| 頻寬監控    | 持續監控網路頻寬使用率，提前擴充資源         |

### 網路韌性組織檢核

- ☐ 是否有至少兩條獨立的對外網路連線？
- ☐ DNS 是否有備援機制？
- ☐ 是否部署 DDoS 防護？
- ☐ 內部網路是否已做適當分段？
- ☐ 遠端存取是否有備援方案？
- ☐ 是否有網路連線中斷的應變程序？

# 2.4

## 安全防護

資安事件是現代企業面臨的最大威脅之一。  
勒索軟體可以在數分鐘內癱瘓整個組織。

### 組織應該如何強化資安防護

#### 身分與存取管理

- 實施最小權限原則，僅授予必要的存取權限
- 所有管理帳號啟用多重要素驗證 (MFA)
- 定期審查帳號權限，移除不再需要的存取權限
- 使用集中式身分管理，統一管控所有系統存取

#### 資料保護

- 敏感資料在傳輸與儲存時均應加密
- 實施資料分級制度，依等級採取不同保護措施
- 定期備份關鍵資料，並確保備份與主系統隔離
- 備份資料應加密且定期驗證可還原性

#### 端點防護

- 所有端點設備部署防毒與端點偵測回應 (EDR)
- 作業系統與應用程式保持最新安全更新
- 限制使用者安裝未經核准的軟體
- 實施裝置管理政策，確保設備合規

#### 加密機制演進

- 組織應關注加密技術的長期演進風險
- 確保在新型運算能力出現時仍能維持資料安全

# 2.4

## 安全防護

資安事件是現代企業面臨的最大威脅之一。  
勒索軟體可以在數分鐘內癱瘓整個組織。

### 資安四不六要

#### 四不

- 1** 不點選不明連結或附件
- 2** 不使用未經核准的軟體與服務
- 3** 不共用帳號密碼
- 4** 不在公共網路傳輸敏感資料

#### 六要

- 1** 要啟用多重要素驗證
- 2** 要定期更新密碼，使用強密碼或密碼管理器
- 3** 要定期備份重要資料
- 4** 要保持系統與軟體更新
- 5** 要通報可疑的資安事件
- 6** 要定期參加資安教育訓練

# 2.5

## 監控告警

沒有監控的系統，就像沒有儀表板的飛機，直到墜機才知道問題在哪。

### 基礎設施

- CPU、記憶體、磁碟、網路等資源使用率
- 伺服器與服務的健康狀態
- 資料庫連線數、查詢效能、複寫延遲
- 備份任務執行狀態與成功率

### 應用程式

- 服務回應時間與錯誤率
- API 呼叫量與成功率
- 使用者體驗指標（頁面載入時間、交易完成率）
- 應用程式日誌的異常模式

### 安全監控

- 異常登入行為（非上班時間、異常地點）
- 權限變更與敏感操作
- 網路流量異常（大量外傳資料、異常連線）
- 弱點掃描結果與修補進度

## 告警分級

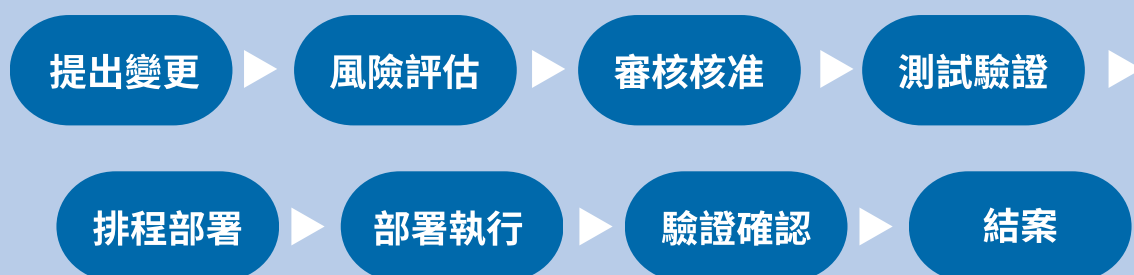
| 等級 | 嚴重度 | 回應時間     | 影響範圍           |
|----|-----|----------|----------------|
| P1 | 緊急  | 15 分鐘內回應 | 核心服務中斷，影響所有使用者 |
| P2 | 高   | 1 小時內回應  | 重要功能異常，影響部分使用者 |
| P3 | 中   | 4 小時內回應  | 非核心功能異常，影響有限   |
| P4 | 低   | 下個工作日    | 輕微問題，不影響業務運作   |

# 2.6

## 變更管理

多數系統故障並非來自外部威脅，而是來自內部變更。良好的變更管理是韌性的重要防線。

### 變更流程



### 部署安全網

| 部署方式                            | 風險程度 | 部署說明             |
|---------------------------------|------|------------------|
| 藍綠部署<br>(Blue/Green Deployment) | 低風險  | 維護兩套環境，切換流量至新版本  |
| 金絲雀部署<br>(Canary Deployment)    | 低風險  | 先將少量流量導向新版本，逐步擴大 |
| 滾動更新<br>(Rolling Update)        | 中風險  | 逐批更新實例，確保服務不中斷   |
| 一次性部署<br>(One-Click Deployment) | 高風險  | 同時更新所有實例         |

### 回滾機制

- 每次部署前確認回滾步驟與所需時間
- 自動化回滾流程，縮短回滾時間
- 設定明確的回滾觸發條件 (錯誤率超過閾值、回應時間異常)
- 保留前一版本的部署包與配置，確保可快速回滾

# 2.6

## 變更管理

多數系統故障並非來自外部威脅，而是來自內部變更。良好的變更管理是韌性的重要防線。

### 非程式變更管理

#### 資料結構變更

---

- **向下相容策略**：逐步增減欄位，避免一次性破壞性變更
- **資料遷移驗證**：變更後自動比對新舊結構的資料完整性

#### AI 模型更新

---

- **模型版本管理**：追蹤版本、資料集、效能指標，確保可回溯
- **A/B 測試**：新舊模型平行運行，確認新版優於舊版後再全面切換

#### 推論邏輯變化

---

- **影子模式**：新邏輯與現行邏輯並行運作，只記錄結果差異，不回傳給使用者
- **輸入輸出契約測試**：定義 API 預期輸入輸出規格，每次變更後自動驗證是否符合

# 03 韌性成熟度 自我檢核

請依據以下檢核表，評估貴組織目前的韌性成熟度。

### 備援架構

- ☐ 已識別所有關鍵業務系統
- ☐ 已為各系統定義 RTO/RPO 目標
- ☐ 關鍵系統已部署多可用區架構
- ☐ 已建立跨區域備援機制
- ☐ 基礎設施已採用程式碼管理 (IaC)

### 業務持續管理 (BCM) 與災難復原

- ☐ 已建立業務持續管理 (BCM) 體系
- ☐ 已完成業務衝擊分析 (BIA)，  
識別關鍵業務與系統分級
- ☐ 已制定業務持續計畫 (BCP)，  
涵蓋人員、流程、技術、場地
- ☐ 已制定災難復原計畫 (DRP)，  
包含各系統復原程序書 (Runbook)
- ☐ 已定義危機通報流程、指揮體系與決策權限
- ☐ 每年至少執行一次 DR 演練
- ☐ 備份資料定期驗證可還原性

### 網路韌性

- ☐ 對外連線具備至少兩條獨立路徑
- ☐ 已部署 DDoS 防護機制
- ☐ DNS 具備備援機制
- ☐ 內部網路已做適當分段
- ☐ 已建立網路中斷應變程序

請依據以下檢核表，評估貴組織目前的韌性成熟度。

### 安全防護

- ☐ 所有管理帳號已啟用 MFA
- ☐ 已實施最小權限原則
- ☐ 敏感資料已加密保護
- ☐ 已建立資安事件應變程序
- ☐ 定期執行資安教育訓練

### 監控告警

- ☐ 已建立基礎設施與應用程式監控
- ☐ 已定義告警分級與回應時間
- ☐ 已建立值班與告警升級機制
- ☐ 關鍵指標有儀表板可視化
- ☐ 日誌集中管理且可搜尋

### 變更管理

- ☐ 所有變更經過正式審核流程
- ☐ 採用漸進式部署策略
- ☐ 每次部署都有回滾計畫
- ☐ 變更紀錄完整可追溯
- ☐ 測試環境與正式環境一致



完成檢核後，針對未達標項目制定改善計畫，並定期重新評估。

# 04 下一歩行動

# 運用 AWS 強化企業韌性

AWS 根據備援架構、網路韌性，提供三種共契產品方案，可依 RTO / RPO / 成本 選擇對應方案

## 備援架構 SYSDR - System Disaster Recovery

|                |                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SYSDRL1</b> | <b>資料備份還原 (Backup &amp; Restore)</b><br>AWS Backup, S3 CRR, EBS Snapshots<br>RTO 數日      RPO 數小時      成本 低 1.1x      適用場景 非關鍵系統、開發測試          |
| <b>SYSDRL2</b> | <b>系統資料抄寫 (Pilot Light)</b><br>RDS Read Replica, Aurora Global DB, EC2 AMI<br>RTO 數小時      RPO 分鐘級      成本 低 1.2x      適用場景 中等重要性系統           |
| <b>SYSDRL3</b> | <b>暖備援 (Warm Standby)</b><br>Auto Scaling, Route 53, ELB<br>RTO 數小時內      RPO 秒 ~ 分鐘      成本 中 1.5x      適用場景 重要業務系統                          |
| <b>SYSDRL4</b> | <b>熱備援 (Hot Standby)</b><br>Multi-AZ RDS, ElastiCache, ELB<br>RTO 數分鐘      RPO 近即時      成本 高 1.8x      適用場景 關鍵任務（金融、醫療）                       |
| <b>SYSDRL5</b> | <b>雙主中心 (Active-Active)</b><br>Aurora Global DB, DynamoDB Global, Global Accelerator<br>RTO 數秒      RPO 近零      成本 最高 2x+      適用場景 零停機、全球化服務 |

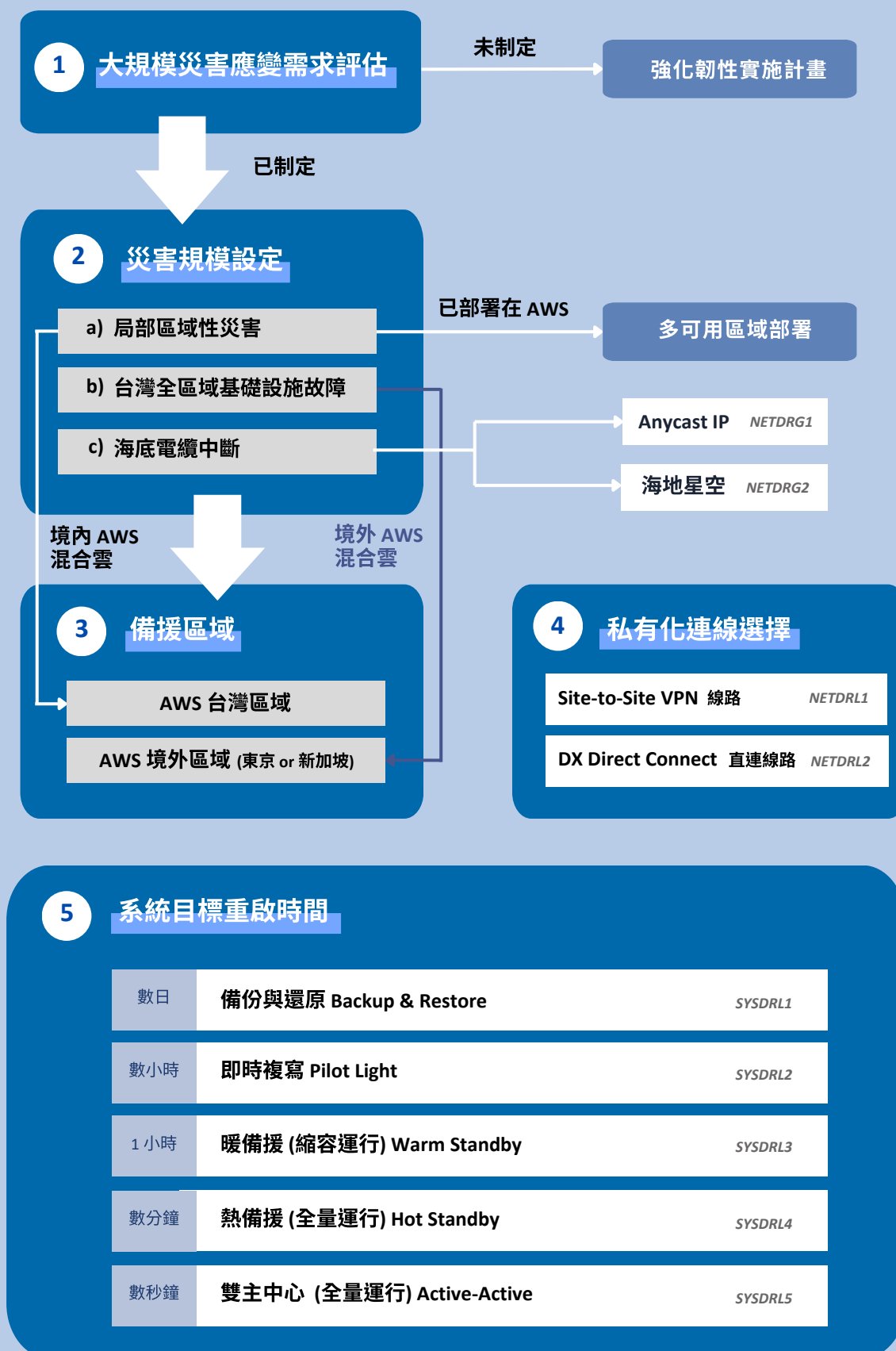
## 島內網路韌性 NETDR - Network Disaster Recovery Local

|                |                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------|
| <b>NETDRL1</b> | <b>Site-to-Site VPN 線路 (AWS Site-to-Site VPN)</b><br>IPSec 加密通道，可作為 Direct Connect 備援<br>適用場景 備援連線、中小型企業 |
| <b>NETDRL2</b> | <b>DX Direct Connect 直連線路 (AWS Direct Connect)</b><br>透過專用光纖線路直連 AWS，穩定低延遲的私有連線<br>適用場景 穩定頻寬、低延遲的核心系統    |

## 海外網路韌性 NETDR - Network Disaster Recovery Global

|                |                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------|
| <b>NETDRG1</b> | <b>Anycast IP 方案 (AWS Global 450+ POP)</b><br>Global Accelerator + CloudFront；經 AWS 骨幹網路傳輸<br>適用場景 海外使用者、跨境傳輸 |
| <b>NETDRG2</b> | <b>海地星空全域強韌通訊網方案</b><br>整合「海纜（海）、行動/固網/微波（地）、低中高多軌道衛星（星/空）」<br>適用場景 建構多層次防護網；海纜異常時維持關鍵通訊                      |

# 大規模災害架構選擇流程



## 提升數位韌性是持續改善的過程， 建議從以下步驟開始：

1

### 假定災害規模

與業務單位共同定義需應對的災害情境

2

### 定義各系統 RTO/RPO

依系統重要性分級設定恢復目標

3

### 盤點現況差距

使用本指南的檢核表評估現有韌性水準

4

### 制定改善計畫

依優先順序排定改善項目與時程

5

### 實施、演練、持續改善

定期 DR 演練，驗證 RTO/RPO 達標

## 善用公有雲 (雲網整合) 或境外機房提升韌性

若您需與具備境內/外機房的專業顧問團隊討論，歡迎隨時  
與 中華電信 AWS 團隊聯繫 ([aws\\_mkt@cht.com.tw](mailto:aws_mkt@cht.com.tw))

多可用區部署

跨區域備援

自動擴展

託管式服務

基礎設施即程式碼

混沌工程工具



# AWS 亞太 (台北) 區域現已開放

## 在台灣安全地儲存資料並推動創新

AWS 亞太 (台北) 區域將使具有資料落地需求的客戶在台灣安全地儲存資料，同時提供更低的延遲。此區域將使各行業的客戶從安全、可擴展和可靠的雲端基礎設施中受益，進而推動數位轉型和創新。

## AWS 在台灣的投資

台灣的 AWS 亞太 (台北) 區域將扮演重要角色，協助當地客戶運用雲端運算和人工智慧 (AI) 等先進技術，加速創新和數位轉型，同時提升生產力。亞馬遜在 AWS 亞太 (台北) 區域的投資將為台灣經濟與在地社群帶來漣漪效應，創造就業機會、促進社區參與、以及提升企業人才實力。

## 關於 Amazon Web Services

自 2006 年來，Amazon Web Services 一直提供服務豐富、應用廣泛的雲端服務。AWS 不斷擴展可支持幾乎任何雲端工作負載的服務，為客戶提供超過 240 種功能全面的雲端服務，包括運算、儲存、資料庫、網路、分析、機器學習與人工智慧、物聯網、行動、安全、混合雲、媒體，以及應用開發、部署和管理等方面，遍及 39 個 AWS 區域內的 123 個可用區域 (Availability Zones)，並已公布計畫在智利、紐西蘭、沙烏地阿拉伯及 AWS 歐洲主權雲端建立 4 個 AWS 區域、13 個可用區域。全球超過百萬客戶信任 AWS，包含發展迅速的新創公司、大型企業和政府機構。AWS 協助客戶強化自身基礎設施，提高營運上的彈性與應變能力，同時降低成本。



**了解更多全球公部門轉型案例**

# 有準備，更安全

本指南適用於公家機關與大型企業，旨在提供提升數位韌性的通用框架與實務實踐。  
各組織應依據自身業務特性、法規要求與預算限制，調整具體實施方案。

