金融監督管理委員會
Financial Supervisory Commission

金融業導入零信任架構參考指引

金管會

2024.7.18

金融資安行動方案 2.0 (2022.12)

- 客戶
  - 2.1 eKYC與業務風險對照
- 第三方服務商
  - 2.2 第三方風險評估與管理
- 居家/異地辦公
  - 2.3 因應新型態資安攻擊

政策面

1.擴大資安長設置，定期召開資安長聯繫會議

管理面

4.1 擴大推動導入國際資安管理標準	7.鼓勵配置多元專長資安人才，擴大演訓量能

技術面

事前-資安部署	事中-資安監控	事後-營運持續

深化	**6. 鼓勵零信任網路部署**	4.2 擴大推動資安監控機制	3.1 金融核心資料保全
有效	5. 鼓勵資安監控與防護之有效性評估		3.2 對外服務營運持續實演練
聯防	8.1 提升資安情資分享動能	8.2 增進資安聯防運作效能	9 攻防演練及重大事件支援演訓

為什麼需要導入零信任架構？

NIST 800–27 Operative Definition:
Zero trust (ZT) provides **a collection of concepts and ideas** designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised.

1 企業邊界模糊，場域外人員及設備安全控管不易

- 居家辦公、遠端工作
- 供應商、合作商
- 雲端平台

2 假設資安有缺口，攻擊者一定會進入內網

- 內網是資安防禦最脆弱的一環，已獲授權人員、設備等不可信
- 內網探測、滲透、橫向擴散

身分 → 設備 → 網路 → 應用程式 → 資料

零信任思維重新檢視資安政策

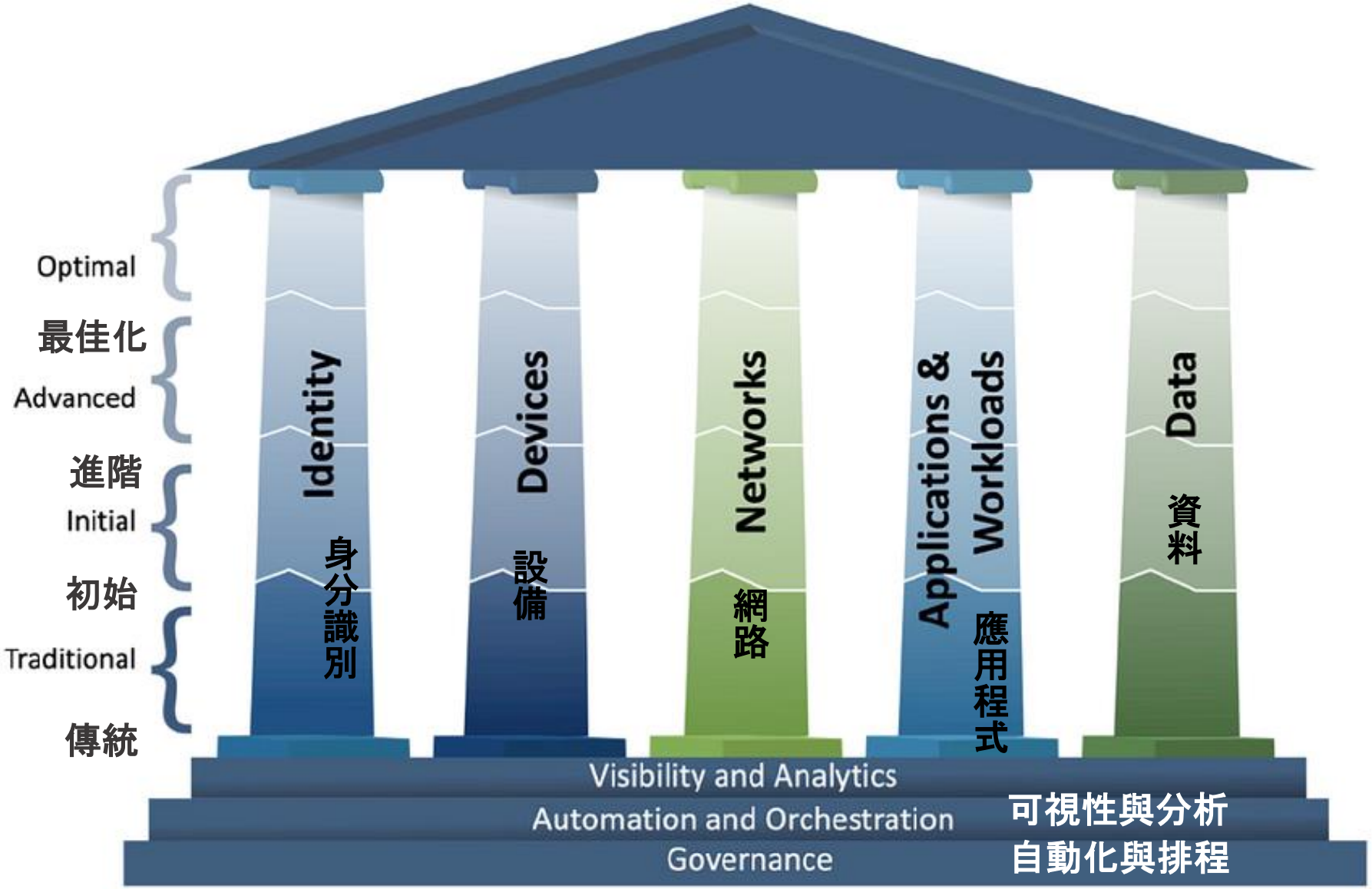
- ☐ 整體資安防護框架
- ☐ 既有資安防護基礎

- 由外而內
  - ➢ 縮小攻擊表面、增加防禦深度
- 由內而外
  - ➢ 擴大防護表面、限縮損害衝擊
- 提高可視性
  - ➢ 持續監控與驗證

風險導向->擇高風險場域先行[例舉]

遠距辦公	• 使用者及設備位於**傳統資安防護邊境外**
雲端存取	• 雲端資源位於**傳統資安防護邊境外**
系統維運管理	• 含重要**主機設備及系統軟體**(作業系統、資料庫等)之**特權帳號**管理
應用系統管理	• 重要**應用系統之管理者**(如帳號管理員)或**高權限使用者帳號**(如可接觸大量個資或機敏資料使用者)
服務供應商	• 如委外廠商之**遠端維運**管理
跨機構協作	• 如重要應用系統之**外部使用者**

美國網路安全暨基礎設施安全局(CISA)
——— 零信任成熟度模型2.0 (2023.4發布)



循序漸進->依分級指標分階段導入

Ⅰ 傳統

靜態指標

- **RBAC 基於角色存取控制**
- 優先盤點既有資安防護機制之完整性，規劃**防禦深度之優化及整合**。

Ⅱ 起始

動態指標

- **ABAC 基於屬性存取控制**
- 將**動態屬性(如時間、地點, 設備合規性等)**納為授權審核條件，動態撤銷、限縮存取授權或發出告警。

Ⅲ 進階

即時指標

- **SIEM/SOC**
- 整合或收容事件日誌，建立定期審查及異常行為**(IOC、Mitre ATT&CK TTP)**之偵測、告警及回應機制。
- **UEBA** 使用者和實體行為分析。

Ⅳ最佳

整合指標

- 建立可依資安政策快速調適之一致性且自動化之管理機制，確保安全性及合規性。
- **點►線►面**

永不信任、持續驗證

盤點資源存取途徑->以零信任思維深化資安防護

身分	設備	網路	應用程式	資料
● **雙因子**身分驗證 ● 優先選擇**安全強度較高、可抗網路釣魚者** ➢具數字配對APP ➢FidO ➢晶片卡 ● **動態屬性存取授權** ⋮	● 可識別為**已納管之設備** ● 具設備**健康合規性**管理 ➢作業系統更新 ➢防毒軟體病毒碼更新 ● **動態屬性存取授權** ● **設備活動即時偵測及回應** ⋮	● 全程**加密傳輸** ● 具適當**網段分割，採最小需求原則的網路連線** ➢建議採各系統獨立之網段區隔 ● **網路活動即時偵測及回應** ⋮	● 包含源自內**部與外部的安全性檢測** ● 採**最小授權原則** ● **動態屬性存取授權** ● **應用程式活動即時偵測及回應** ⋮	• 機敏性**資料加密儲存** • 支援最小授權規則 • **資料外洩防護** • **動態屬性存取授權** • **資料存取活動即時偵測及回應** ⋮

日誌收集 → 日誌與事件管理 → 資安監控/事件應處

零信任架構推動路徑

導入參考指引

行政指導：金融機構於導入實務仍得考量既有資訊與資安環境、資安防護水準、資源及人力、業務風險、相關解決方案成熟度等因素調適；或另為適切之規劃，不以本參考指引為限。

實務案例分享

鼓勵金融機構分享實務案例，供金融同業交流研討最佳實務，帶動持續深化及擴散。

資安基礎規範

定期調查導入規劃及進程，與各同業公會、周邊單位共同依據對各金融業別屬性、規模及業務風險等，衡量實際資安防護需求及執行可達性，適時納入資安規範，提升整體資安防禦水準。

簡報完畢

敬請指教