臺灣證券交易所股份有限公司

金融業導入零信任架構參考指引解析說明會

三月 2025

pwc 資誠

Agenda

項次	內容
1	零信任架構的背景與核心概念
2	高風險、低衝擊場域的優先導入策略
3	實作案例與持續評估

1

零信任架構的背景與核心概念

國際零信任政策趨勢

Aug. 2021

美國首次公布「聯邦零信任戰略」（Federal Zero Trust Strategy）

Oct. 2021

新加坡發布「網路安全戰略2021」，指出零信任網路安全策略是未來五年發展重點

Jun. 2022

日本數位廳針對政府資訊系統，發布零信任架構適用方針

Nov. 2022

美國國防部揭露該部零信任政策與藍圖

Apr. 2023

美國公布「聯邦零信任戰略」（Federal Zero Trust Strategy）第二版

Jul. 2023

NIST-1800-35公布第二版草稿

資料來源:
https://www.ithome.com.tw/news/149103
https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J21056588511107072 3&sid=0L330518966956925447&sq=
https://www.openfind.com.tw/taiwan/zero-trust.html
https://www.ithome.com.tw/news/149103
https://itw01.com/8TSGGEF.html

零信任想要解決的痛點與現象

傳統的邊界保護
逐漸式微
(Traditional perimeter-based defenses declining)

分散的資訊中心型態漸多
(Decentralized IT Environments)

E.g. 逐漸增多的資訊中心，如雲端服務

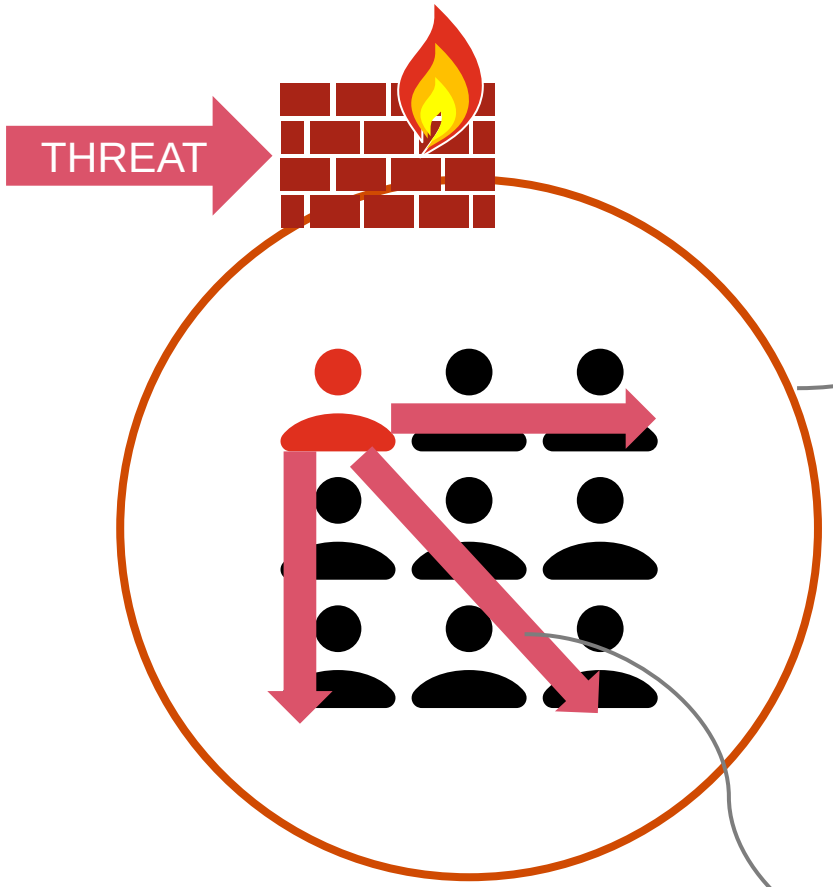
內部威脅漸漸地增加
(Insider Threat)

E.g. 逐漸多樣的聯網設備，如自攜裝置

敏感性資料洩漏狀況激增
(Sensitive Data Breaches)

E.g. 逐漸多元的科技服務，如行動服務

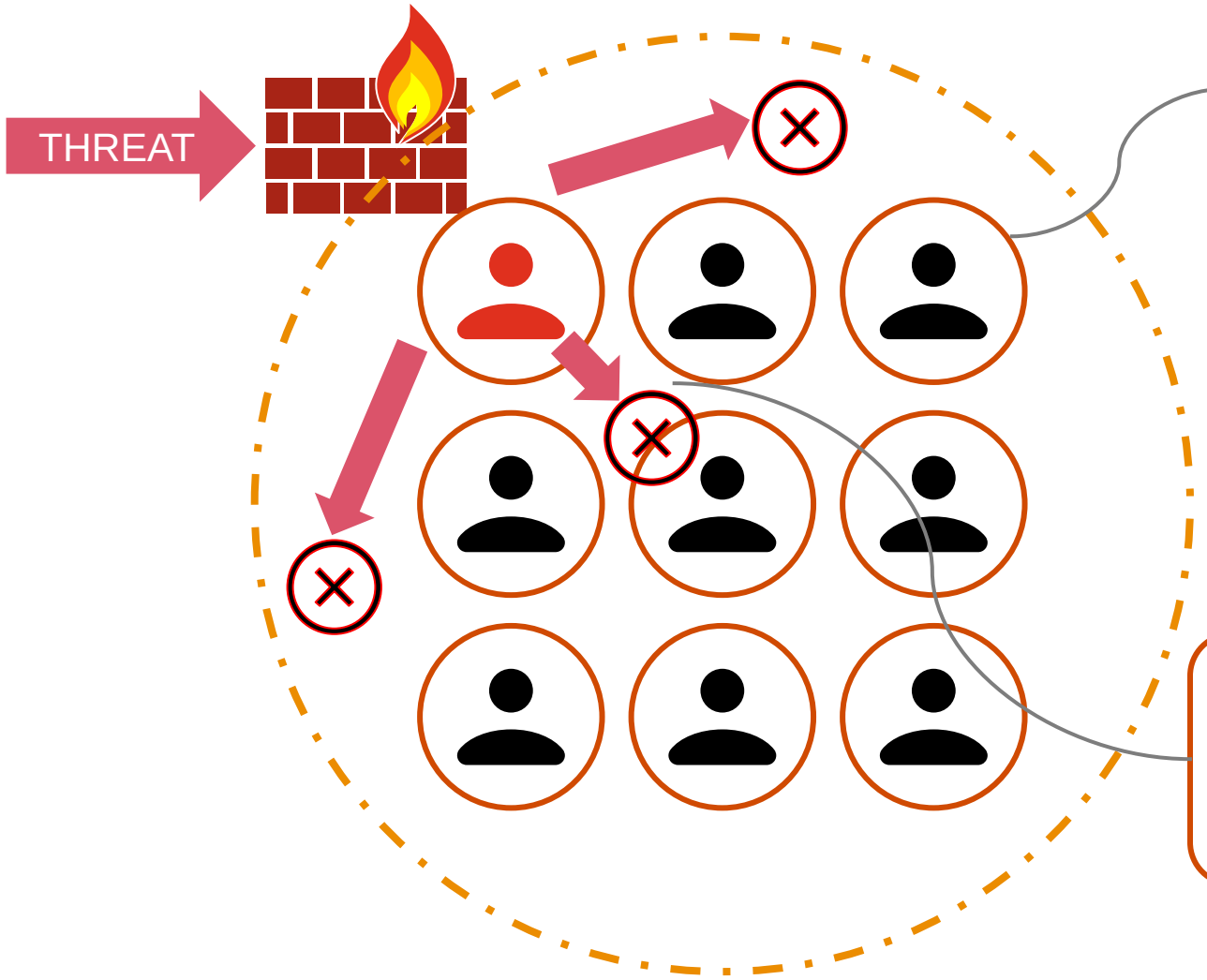
傳統邊界保護架構逐漸式微之狀況



- 傳統一層式保護架構，多半仰靠邊界防火牆，以進行組織內部資產資安保護。

- 一旦牆內某成員遭受感染，在固若金湯的城牆內，病毒會通行無阻。

零信任架構之補強



- 邊界牆內各重要資產另築內防禦層，以避免橫向感染發生。

- 一旦邊界牆內某成員遭受感染，既使病毒流竄，防禦層起作用保護。

專案緣起

金融業導入零信任架構參考指引

2024.7.15

一、緣起

因應疫情帶動異地/居家辦公模式，亦隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已難以滿足新形態工作需求。國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略；我國

新聞稿

金管會發布「金融業導入零信任架構參考指引」，鼓勵深化資安防護

2024-07-18

金融監督管理委員會（以下稱金管會）近期發布「金融業導入零信任架構參考指引」(以下稱參考指引)，鼓勵金融業以零信任思維深化資安防護。

金管會前於111年12月發布「金融資安行動方案 2.0」時，為因應後疫情時期及數位轉型之資安防護需求，參考國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略，我國「國家資通安全發展方案」亦推動政府機關導入零信任網路，爰將「鼓勵零信任網路部署，強化連線驗證與授權管控」納為精進重點之一。

金管會表示，考量零信任架構涵蓋整體資安防護框架，導入過程不可能一次到位，而

五、零信任架構推動路徑

本參考指引為漸進導入零信任架構路徑之一，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。本會並將依據金融機構導入進程，滾動修訂整體推動策略及分階段推動指標，主要推動路徑如下：

(一) 鼓勵分享實務案例，帶動持續深化及擴散

本會鼓勵金融機構導入零信任架構，於 113 年研擬導入規劃，本會並將自各業別擇金融機構先行，分享導入經驗作為示範，供金融同業交流研討最佳實務。

金融業導入零信任架構參考指引-指引參考資料

政府因應國際資安政策，制定「金融業導入零信任架構參考指引」。

主要參考文件如下：

(一) NIST SP 800-207：美國國家標準技術研究院定義零信任，並提供部署模型和案例。政府依此提出身分鑑別、設備鑑別、信任推斷三大核心組件。

(二) 美國總統指令：要求聯邦政府採用零信任架構作為資安現代化策略，並於 2024年達成身分識別、設備、網路等五面向的安全標準；另美國國防部也發布零信任架構參考指引，提供各種SP 800-207實踐方式說明。

(三) CISA零信任成熟度模型：根據五個支柱以及逐步導入的四個等級，推動零信任架構。

(四) 國家資通安全發展方案：資安數計畫推動零信任架構，從身分鑑別、設備鑑別與信任推斷逐步實施，並建立相關產品標準及測驗機制。

NIST SP800-207-零信任架構概述

什麼是零信任?

- **不假設信任、必須持續評估的網路安全範例**
- **不因網路或設備位置而自動授予信任**

主要目標

1. **減少未經授權的數據和服務訪問**
2. **執行每次請求的最小訪問權限**

基本原則

- 所有的資料與服務都被當作資源。
- 無論裝置的網路位置，都需確保安全。
- 對於資源存取，應以連線判斷是否許可。
- 訪問基於動態策略，涵蓋用戶、設備與環境屬性。
- 持續監控與衡量完整性與安全狀況。
- 嚴格落實身分鑑別與授權機制，依監控結果動態決定。
- 盡可能收集資訊現況，以增進安全狀態。

NIST SP800-207-零信任邏輯元件

零信任的邏輯元件

- 零信任部署由許多邏輯元件組成，可為本地服務或雲端服務

存取控制核心

- **政策落實點(PEP)**：在主體(如用戶或設備)存取資源前，PEP會根據存取控制策略決定是否授予權限
- **政策決策點(PDP)**：在PEP背後由控制層面支援，由政策引擎(PE)和政策管理者(PA)組成

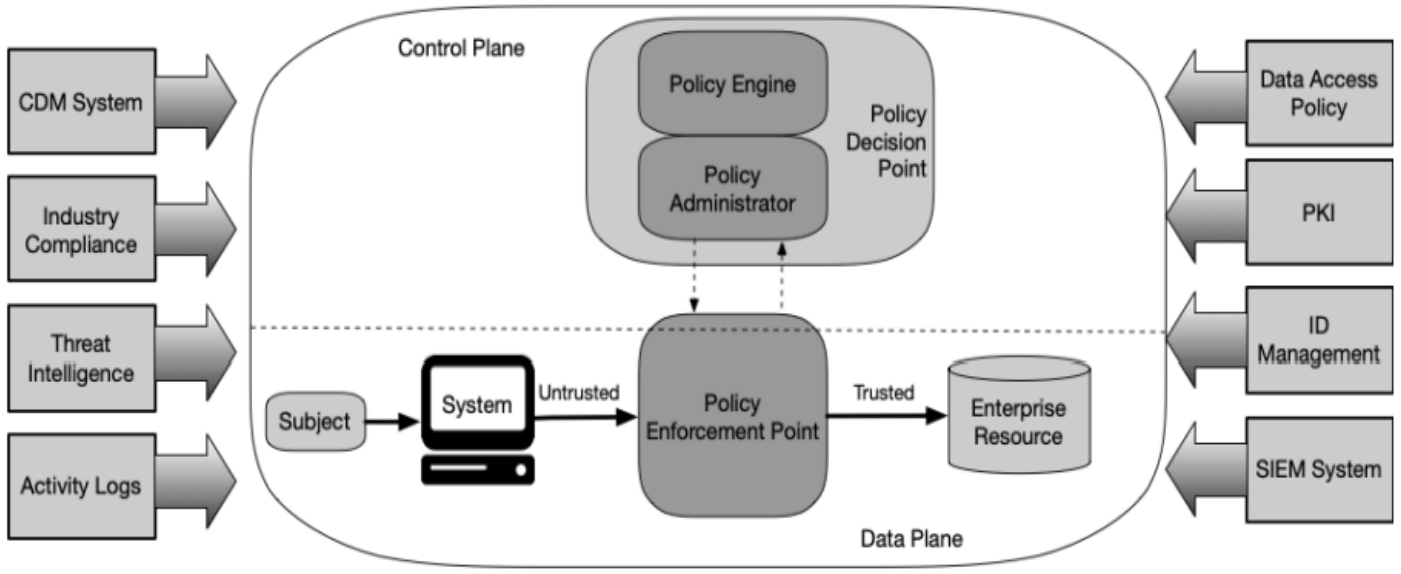


Figure 2: Core Zero Trust Logical Components

NIST SP800-207-零信任的應用場景與挑戰

應用場景

- 多地辦公企業
- 多雲環境
- 外部存取
- 企業協作
- 提供公眾服務

常見威脅

- 破壞決策過程
- Dos攻擊或網路中斷
- 盜取帳密/內部威脅
- 網路可視性
- 系統與網路資訊的儲存
- 過度依賴單一服務商
- 核心元件採非人實體的風險

導入流程

1. 識別企業內部角色
2. 識別企業資產
3. 識別關鍵流程，並評估風險
4. 擬定政策
5. 識別解決方案
6. 初期部署與監控
7. 擴展零信任架構

美國國防部零信任架構參考
DoD Zero Trust Reference Architecture Principle (July 2022)

Principle 01

Assume no implicit or explicit trusted zone in networks.

Principle 02

Identity-based authentication and authorization are strictly enforced for all connections and access to infrastructure, data, and services.

Principle 03

Machine to machine (M2M) authentication and authorization are strictly enforced for communication between servers and the applications.

Principle 04

Risk profiles, generated in near-real-time from monitoring and assessment of both user and devices behaviors, are used in authorizing users and devices to resources.

Principle 05

All sensitive data is encrypted both in transit and at rest.

Principle 06

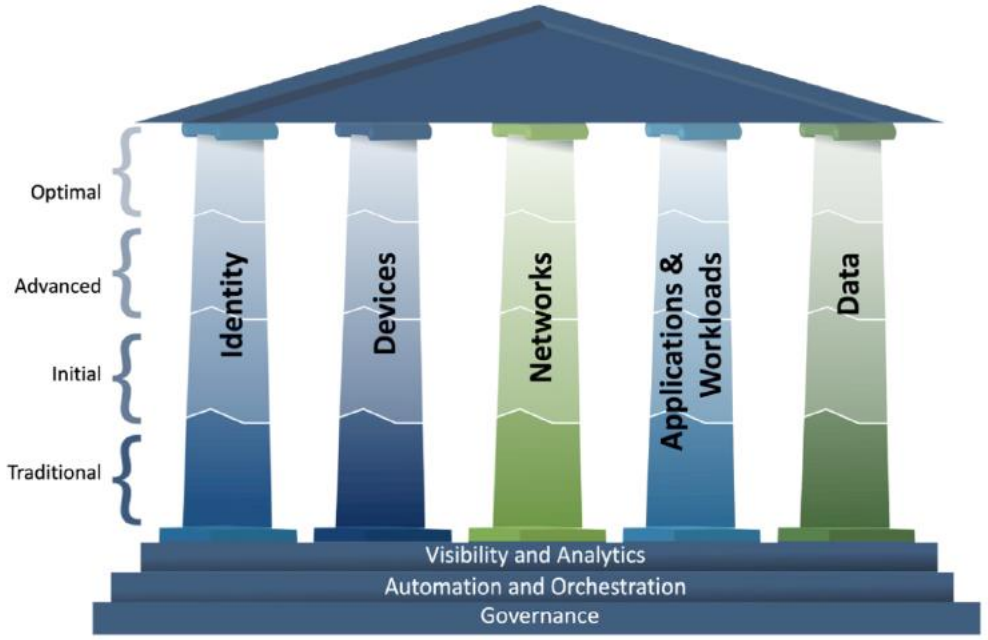
All events are to be continuously monitored, collected, stored, and analyzed to assess compliance with security policies.

Principle 07

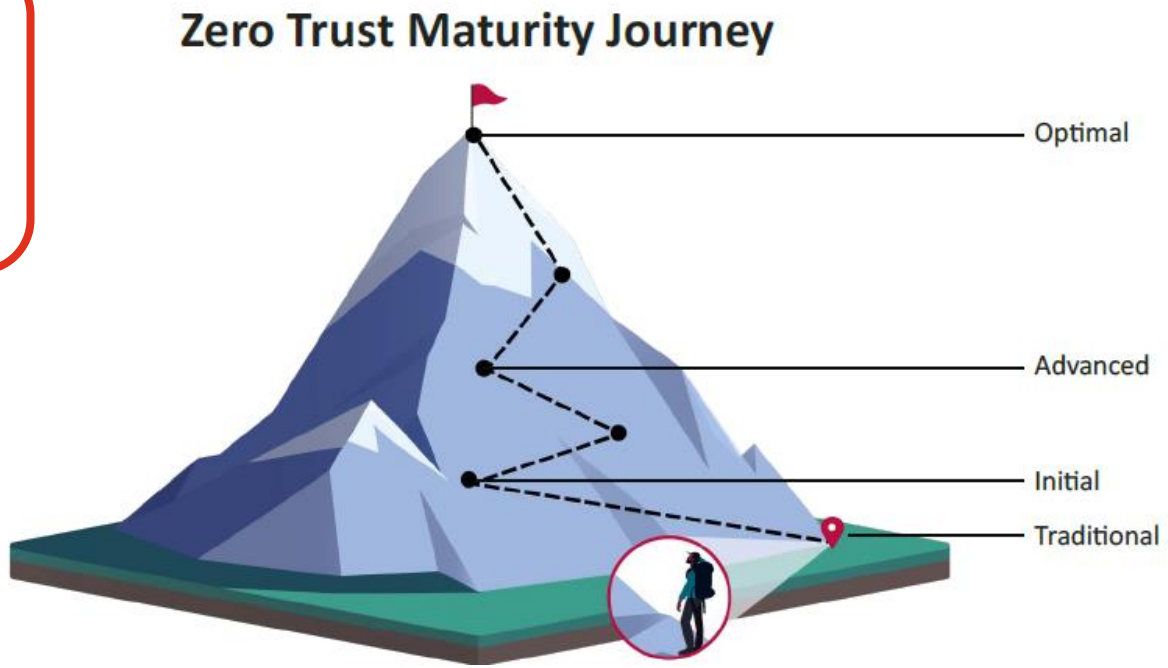
Policy management and distribution is centralized.

CISA零信任成熟度模型

登峰規劃：
零信任成熟度模型提供五大支柱與三面基礎共200種成熟度狀態敘述，供企業評估自身成熟度（傳統、初始、進階及理想階段），以利未來資安藍圖繪製與投資規畫。



Zero Trust Maturity Model



造極心法：
逐步強化，分散投入成本，避免直上的瞬間高成本
Gradual evolution to Zero Trust、Distributing costs over time rather than entirely upfront

零信任架構導入對於金融業各業別可能影響面向

銀行業

- ✓ 與大量支付網路串接（ Integration with Payment Networks ）
- ✓ 非常強調高可用性（Emphasis on system uptime）

保險業

- ✓ 作業需密集彙整多系統資訊（Highly Integration with muti-systems）
- ✓ 大量的資料保存需求（ Large volumes of documents preservation）

證券業

- ✓ 交易低延遲要求（Minimalize latency）
- ✓ 前、中、後台系統資料拋轉高效要求（Interface Efficiency）

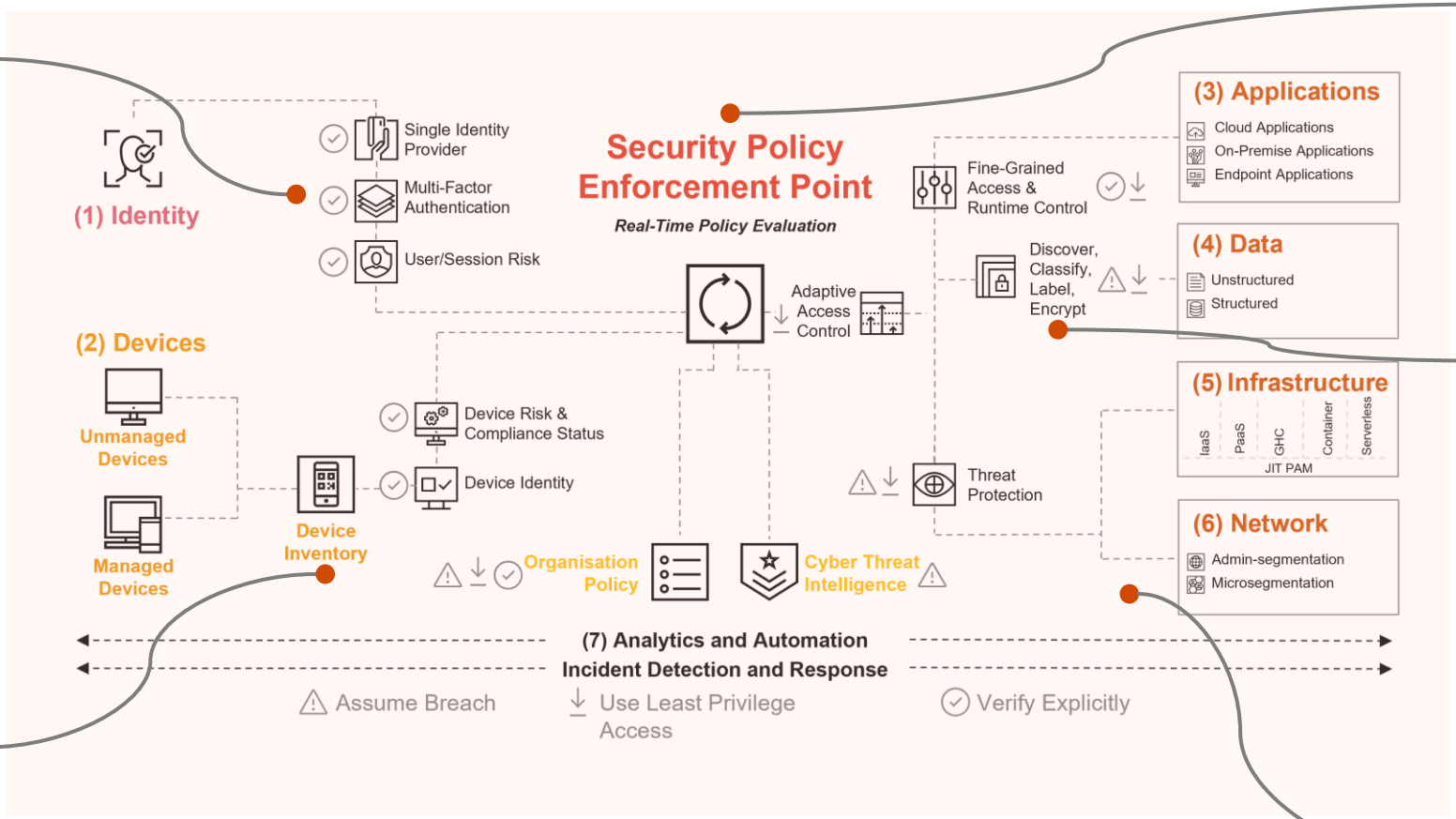
欲達零信任架構所需的各項資訊架構調整、建設

多層次身分驗證

登入採多因子驗證、系統內活動套用權限檢查。

設備識別

快速識別後，自動化加入監控網，並因應狀態給予不同存取權限。



信任推斷

持續性監控下，自動化且實時調整政策並適用規則。

資料保護

自動化上標籤識別，並給予對應保護等級，且加密。

細緻區隔

網路設備軟體化，將整個場域以單一功能、單一群組切分。

由於零信任架構是資訊架構強化的方式，IT是架構調整及建設中的建築家

2

高風險、低衝擊場域的優先導入策略

金融業導入零信任架構參考指引-方法論一(方法論為參考)

高風險 (符合任一情境)

- 是否存有客戶個資？
- 是否存有客戶交易資料？
- 是否存有員工個資？

低衝擊 (符合任一情境)

- 是否為非自動化提供客戶服務？
- 回復時間目標 (RTO) 是否超過8小時？

高風險且低衝擊的系統

金融業導入零信任架構參考指引-方法論二(方法論為參考)

風險因子

分數	資源所在地	使用者	權限	設備	系統與資料	連線方式
3	資源在第三方託管區域或雲端環境(非組織內部環境)/資源在組織DMZ區以內之內部環境	使用者為外部人員	所使用權限為最高權限、管理者權限與特殊權限	所使用設備非為組織分配設備且於組織之外	所涉及系統與資料為重要系統或涉及個人資料	透過網際網路進行連線
2	資源在組織內部環境DMZ區	使用者為內部資訊人員	所使用權限為一般使用者權限(能做日常維運特定活動)	所使用設備為組織分配設備且為可攜式設備(可位於組織之外)	所涉及系統與資料為非重要系統或非涉及個人資料，但為非公開資料	透過VPN或專用網路進行連線
1	資源在一般可公開環境	使用者為內部業務單位人員	所使用權限為一般查詢權限	所使用設備為組織分配設備且位置於內部環境	所涉及系統為公開資料之系統	透過內部網路直接連線

各風險因子加總後分數高者為高風險場域

金融業導入零信任架構參考指引-方法論二(方法論為參考)

衝擊因子

分數	營運中斷衝擊面	作業流程改變衝擊面	人力訓練衝擊面	技術差異衝擊面	財務支出衝擊面
3	可能會造成與營運直接相關系統中斷	導入會造成業務流程重大改變，需要透過試運行來推動	教育訓練不足會造成關鍵流程或整體運行中斷	組織目前無相關技術或資源，必須導入全新技術或進行大幅度的技術改造方能執行	需額外投入超出既有預算2500萬元(含)以上之情境
2	可能會造成與營運間接相關系統中斷	導入僅影響特定部門或操作步驟，可透過教育訓練與宣導來推動	教育訓練不足會造成少部分流程運行較緩慢	組織目前有部分相關技術與解決方案，僅需要購買或擴充即可應用	需額外投入超出既有預算500萬元(含)~2500萬元以下之情境
1	僅有極少機率造成與營運相關系統中斷	該場景存在既有機制無需調整作業流程	教育訓練執行情況較不影響整體導入	導入不輸要額外引進解決方案，僅需微調設定即可應用	無需額外投入預算或低於500萬元之情境

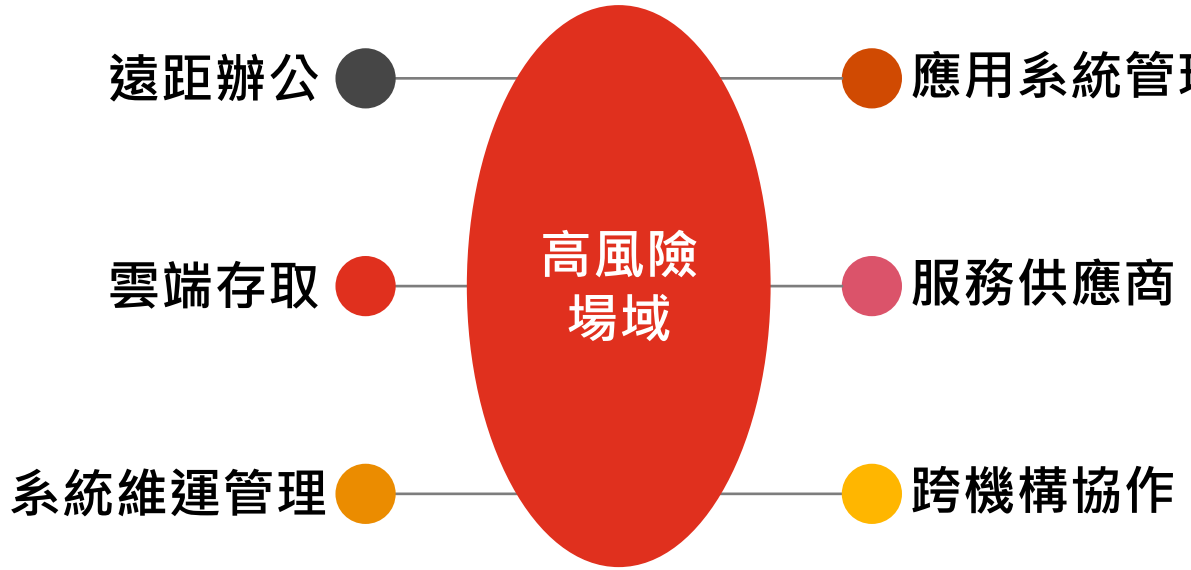
各衝擊因子加總後分數低者為低風險場域

金融業導入零信任架構參考指引-場域

風險導向，擇高風險場域、低營運衝擊先行

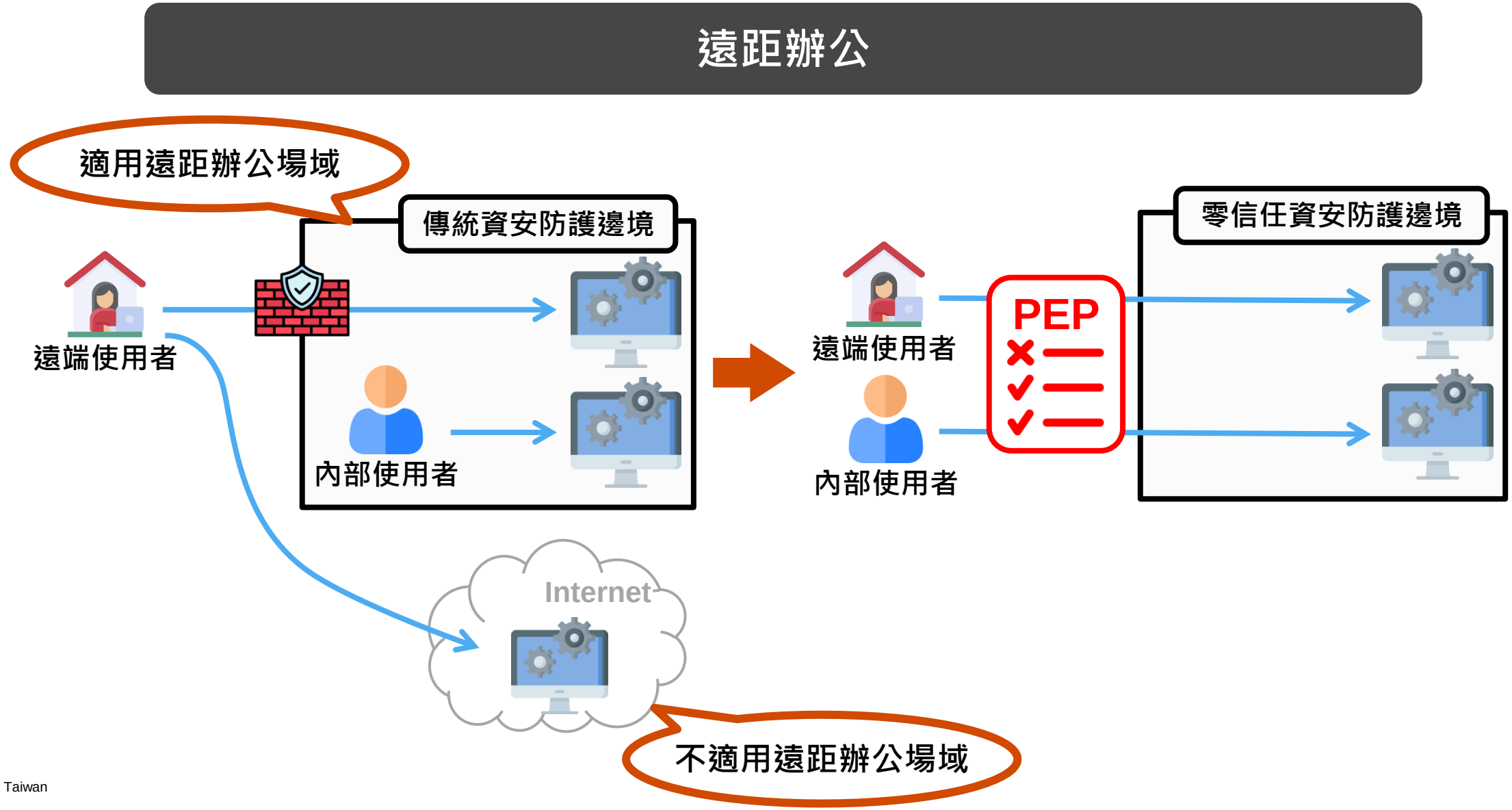
原則
- 可控範圍內、減少影響面。
- 可獲致實質補強效益。

建議
- 依風險基礎方法進行適當評估，擇定其導入優先序及範圍。



- 使用者及設備位於傳統資安防護邊境外。
- 雲端資源位於傳統資安防護邊境外。
- 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。
- 重要應用系統之管理者或高權限使用者帳號(如可接觸大量機敏資料者)。
- 如委外廠商之遠端維運管理。
- 如重要應用系統開放予外部使用者從外部存取，其人員到離或使用設備非屬本機構管控範圍者。

金融業導入零信任架構參考指引-場域



金融業導入零信任架構參考指引-場域

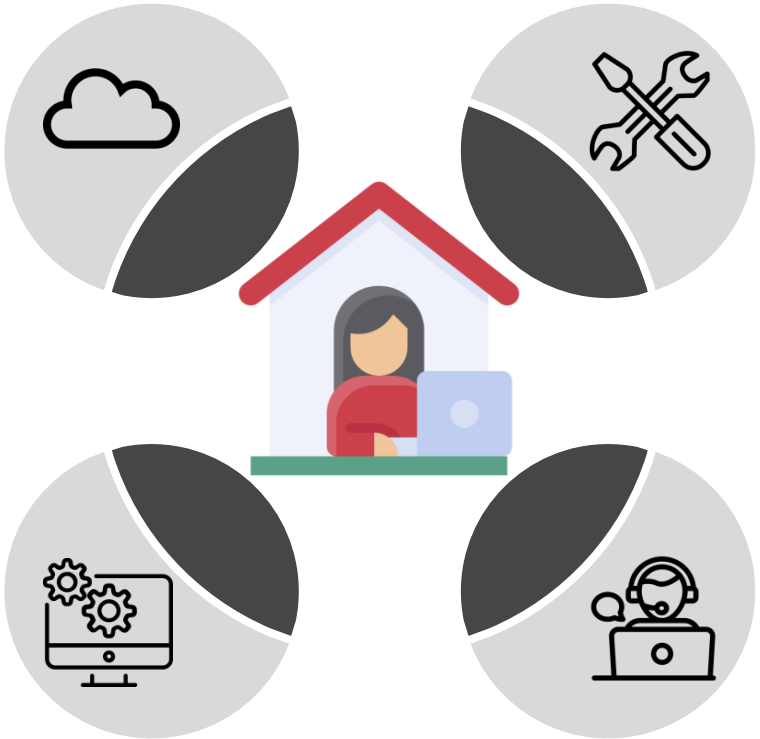
遠距辦公

雲端存取

透過遠距辦公方式存取雲端

系統維運管理

透過遠距辦公方式進行系統維運管理



應用系統管理

透過遠距辦公方式存取重要應用系統和高權限使用者帳號

服務供應商

服務供應商透過遠距辦公方式進行維運管理

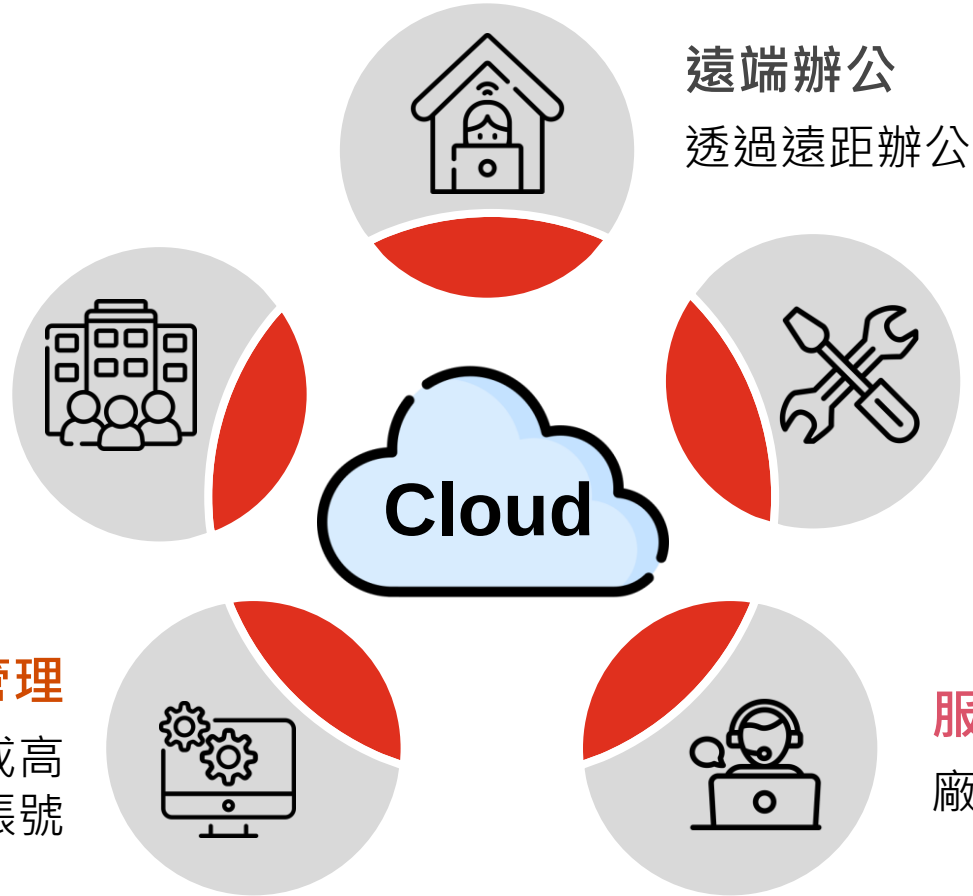
金融業導入零信任架構參考指引-場域

雲端存取

支柱	參考原則項次	IaaS	PaaS	SaaS
身分	1.1~1.6	V	V	V
設備	2.1~2.6	V	V	V
網路	3.1~3.2	V		
	3.3~3.6	V	V	V
應用程式	4.1~4.3、4.6	V	V	V
	4.4~4.5	V	V	
資料	5.1~5.7	V	V	V

金融業導入零信任架構參考指引-場域

雲端存取



遠端辦公

透過遠距辦公方式存取雲端

跨機構協作

外部使用者從外部存取雲端重要應用系統

系統維運管理

雲端網路設備、作業系統、資料庫等系統軟體的特權帳號管理

應用系統管理

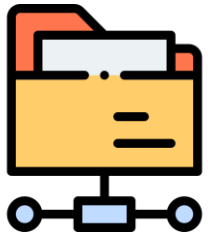
重要雲端應用系統的管理者或高權限使用者帳號

服務供應商

廠商進行雲端基礎設施維運管理

金融業導入零信任架構參考指引-場域

系統維運管理



AD

作業系統

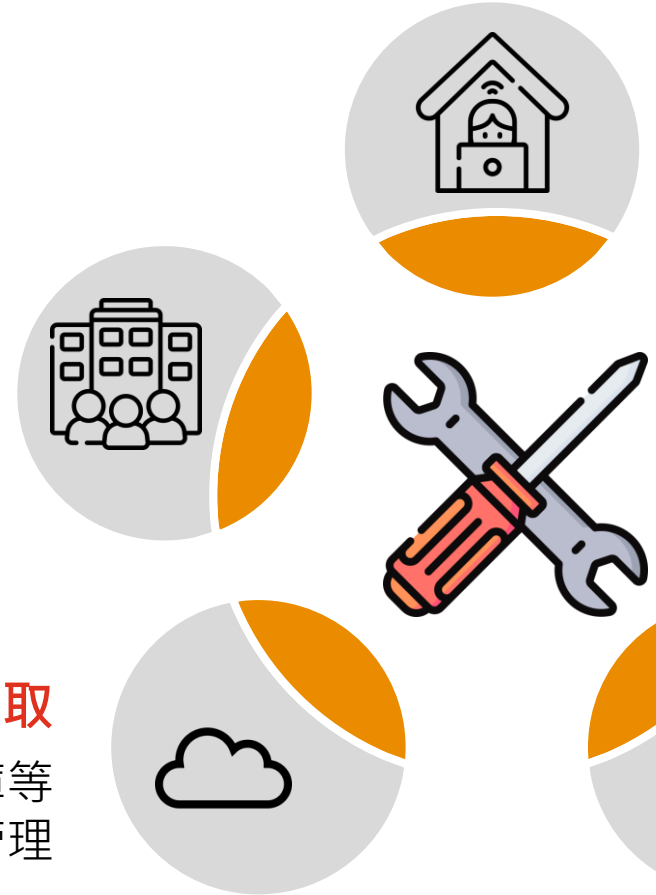
資料庫

網路設備

AD、網路設備、作業系統、資料庫等重要主機設備及系統軟體之特權帳號管理皆屬系統維運管理場域之範圍

金融業導入零信任架構參考指引-場域

系統維運管理



遠端辦公

透過遠距辦公方式進行系統維運管理

跨機構協作

外部使用者使用的應用系統之作業系統、資料庫的維運管理

應用系統管理

應用系統之作業系統、資料庫的特權帳號管理

雲端存取

位於雲端之作業系統、資料庫等系統軟體的特權帳號管理

服務供應商

服務供應商進行系統維運管理

金融業導入零信任架構參考指引-場域

應用系統管理

大量個資或機敏資料

區分一般使用者及管理員帳號

應用系統含有大量個資或機敏資料，且同時有一般使用者帳號及管理員帳號，屬應用系統管理場域之範圍

金融業導入零信任架構參考指引-場域

應用系統管理

遠端辦公

透過遠距辦公方式存取重要應用系統和高權限使用者帳號

服務供應商

廠商進行應用系統之底層作業系統、資料庫等系統軟體維護

系統維運管理

應用系統之底層作業系統、資料庫等系統軟體的特權帳號管理

雲端存取

重要應用系統位於雲端

跨機構協作

外部使用者擁有管理者或高權限使用者帳號

金融業導入零信任架構參考指引-場域

服務供應商

以遠端方式維運

使用外部設備維運

範圍不含應用系統

委外廠商以遠端方式或駐點時使用外部設備進行維運管理，屬服務供應商場域之範圍

金融業導入零信任架構參考指引-場域

服務供應商

遠端辦公

服務供應商透過遠距辦公方式進行維運管理

跨機構協作

外部使用者使用的應用系統之作業系統、資料庫的維運管理

應用系統管理

應用系統之作業系統、資料庫的特權帳號管理

雲端存取

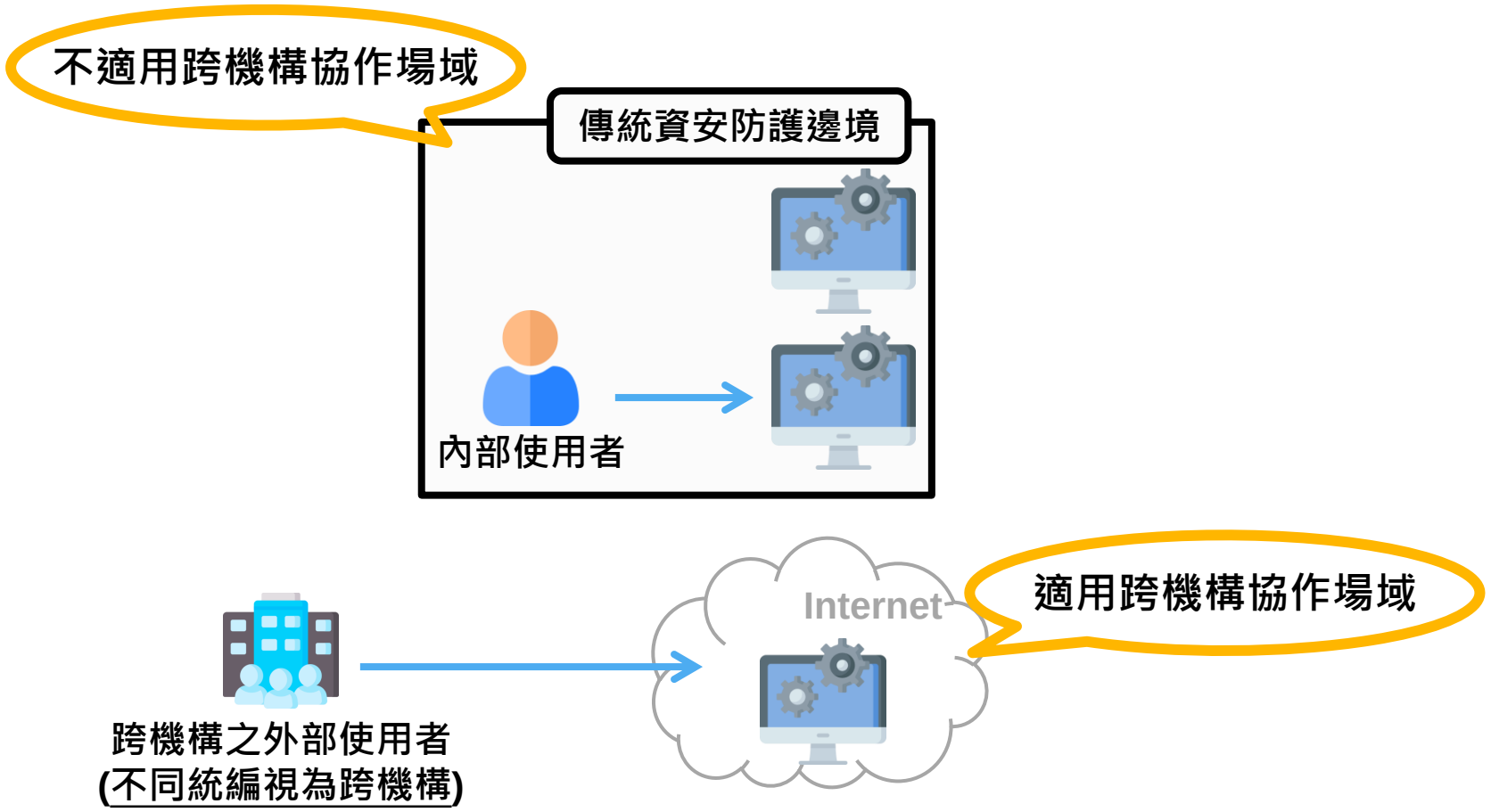
服務供應商進行雲端系統維運管理

系統維運管理

服務供應商負責重要主機設備或作業系統、資料庫等系統軟體的特權帳號管理

金融業導入零信任架構參考指引-場域

跨機構協作

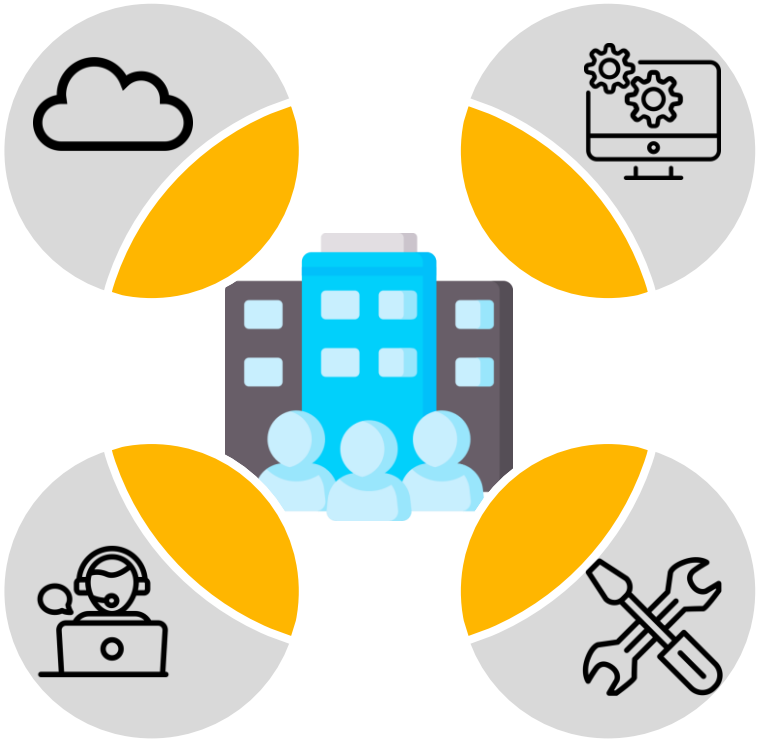


金融業導入零信任架構參考指引-場域

跨機構協作

雲端存取

外部使用者可存取雲端資源



應用系統管理

外部使用者擁有管理者或高權限使用者帳號

服務供應商

跨機構協作連線之應用系統之底層作業系統、資料庫等系統軟體維護

系統維運管理

跨機構協作連線之應用系統之底層作業系統、資料庫等系統軟體的特權帳號管理

金融業導入零信任架構參考指引-範例

情境1

A系統允許員工透過VPN遠端存取系統。

→ ✓ 適用遠距辦公場域

情境2

A系統已與雲端服務提供者簽訂PaaS服務。

→ ✓ 適用雲端存取場域，場域內某些項次不適用

情境3

A系統之資料庫的特權帳號由組織內部管理，作業系統及網路設備則由雲端服務提供者維護管理。

→ ✓ 適用系統維運管理及雲端存取場域

金融業導入零信任架構參考指引-範例

情境4

A系統含有機敏資料，且應用系統帳號之權責已區分一般使用者與管理者帳號。

→ ✓ **適用應用系統管理場域**

情境5

A系統之作業系統、網路設備等基礎設施皆由服務供應商進行維運。

→ ✓ **適用服務供應商場域**

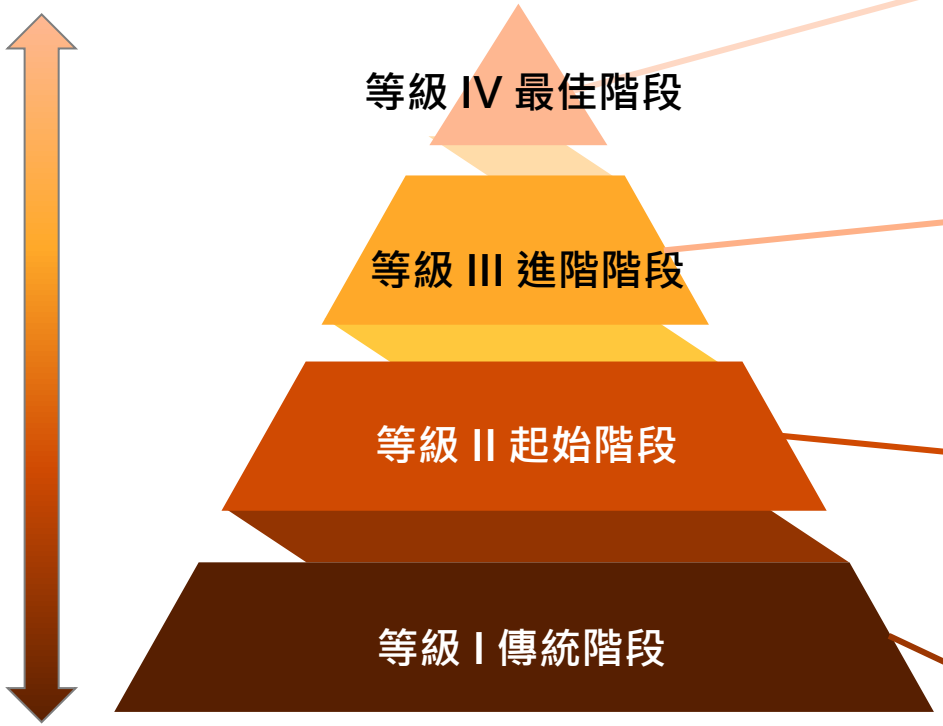
情境6

A系統僅開放外部使用者透過VPN存取應用系統，無法從網際網路存取應用系統。

→ X **不適用跨機構協作場域**

金融業導入零信任架構參考指引-等級

高成熟度



低成熟度

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。

以即時指標為主，整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制。事件日誌應涵蓋依據起始階段定義之動態屬性及零信任政策產生之行為紀錄。相關日誌可集中收容於 SIEM 平台並與資安監控機制（SOC ）整合。

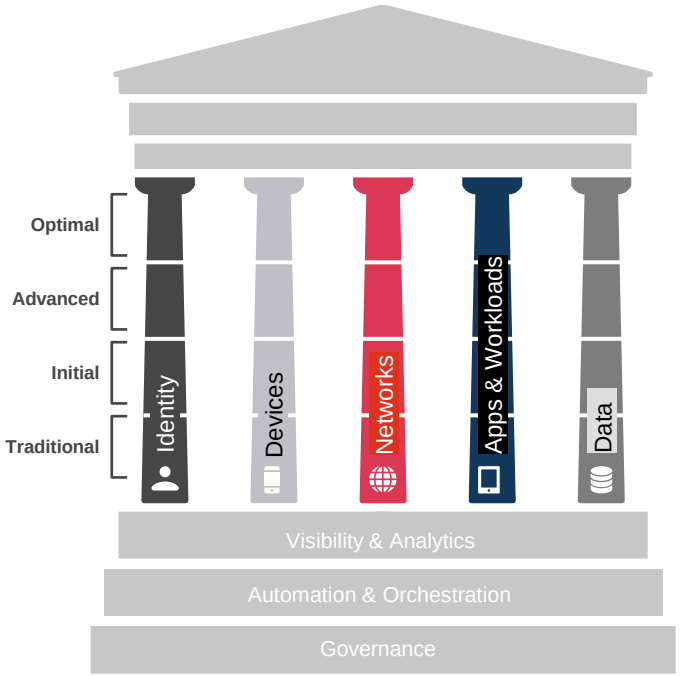
以動態指標為主，建立具基於屬性存取控制（ABAC）機制，可將每個工作階段（Session） 之動態屬性（如時間、地點、健康狀況、合規性等）納為授權審核條件，動態撤銷、限縮存取授權或即時告警；並應辨識存取標的之關鍵數據與資源，及其被存取之交易流程。

以靜態指標為主 ，建議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，不以導入新產品 / 解決方案為必要。

金融業導入零信任架構參考指引-實作參考原則

身分(7)
- 身分認證（I*1、II*1）
- 身分互通（I*1、II*1）
- 權限存取（II*1）
- 可視性分析（III*1）
- 自動化治理（IV*1）

設備(7)
- **設備合規**（I*1、II*1）
- **供應鏈風險**（I*1）
- **資源存取**（II*1）
- **威脅防護**（III*1）
- **可視化分析**（III*1）
- **自動化治理**（IV*1）



網路(7)
- 網路區隔（I*1、II*1）
- 流量管理（I*1、II*1）
- 流量加密（I*1）
- 網路韌性（III*1）
- 可視性分析（III*1）
- 自動化治理（IV*1）

資料(8)
- **外洩防護**（I*1、III*1）
- **資料分類**（I*1）
- **資料可用性**（I*1）
- **資料存取**（II*1）
- **資料加密**（I*1）
- **可視化分析**（III*1）
- **自動化治理**（IV*1）

應用程式(7)
- **存取授權**（I*1、II*1）
- **威脅防護**（III*1）
- **程式安全**（II*1）
- **程式部署**（II*1）
- **可視化分析**（III*1）
- **自動化治理**（IV*1）

金融業導入零信任架構參考指引-實作參考原則

身分驗證是保護數位資源的第一道防線，零信任強調每次存取重新認證

1. 身分
2. 設備
3. 網路
4. 應用程式
5. 資料

I 靜態指標

- **1-1 身分認證**：採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險
- **1-3 身分互通**：對外部使用者提供不低於內部使用者信賴等級之身分鑑別機制。(參照 ISO 29115三階段驗證)
- **1-4 身分互通**：如具多元身分鑑別機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115三階段驗證)

II 動態指標

- **1-2 身分認證**：採用包含綁定實體載具(如FIDO、晶片卡、OTP)的多因子驗證機制，可抗網路釣魚風險。
- **1-5 權限存取**：完成身分鑑別後，依角色屬性存取控制並加入動態屬性審核條件，具動態撤銷及限縮存取功能。

III 即時指標

- **1-6 可視性分析**：整合事件日誌，建立定期審查及偵測異常行為機制，並與資安監控機制整合進行即時判斷。

IV 整合指標

- **1-7 自動化治理**：建立自動化管理機制，確保帳號生命週期的安全性及合規性。

金融業導入零信任架構參考指引-實作參考原則

保障連線設備的合規和安全性，確保每個設備都是可信賴的

I 靜態指標

- **2-1 設備合規**：具有效盤點且可唯一識別之納管設備機制，對未納管設備具風險控管機制。
- **2-3 供應鏈風險**：對外部設備建立不低於內部設備防護基準之管控措施，或限制透過合規中繼閘道存取。

II 動態指標

- **2-2 設備合規**：具合規檢測及弱點管理機制，並持續監控不合規設備，採行風險控管措施。
- **2-4 資源存取**：將設備動態屬性納為授權審核條件，具動態撤銷、限縮存取及隔離未合規設備之能力。

III 即時指標

- **2-5 威脅防護**：對設備活動紀錄具即時偵測及回應機制，偵測到威脅時可自動隔離或即時應處。
- **2-6 可視化分析**：整合事件日誌，建立定期審查及偵測異常行為機制，並與資安監控機制整合進行即時判斷。

IV 整合指標

- **2-7 自動化治理**：可依資安政策快速調適之自動化管理機制，確保設備生命週期的安全性及合規性。

金融業導入零信任架構參考指引-實作參考原則

1. 身分
2. 設備
3. 網路
4. 應用程式
5. 資料

網路被切分為最小的區段，防止未授權的存取與橫向擴散

I 靜態指標

- **3-1 網路區隔**：具網段隔離機制，限制同網段主機間連線及資源存取。
- **3-4 流量加密**：於資源存取路徑進行資料傳輸加密(如 https 加密協定)。

II 動態指標

- **3-2 網路區隔**：具軟體定義網路或網路微分段機制，可依據業務需求調整防護邊界。
- **3-3 流量管理**：可視化設備與系統、端點、網路間的相依性，並具流量異常監控及應處機制。

III 即時指標

- **3-5 網路韌性**：具即時偵測及回應機制，動態調整網路設定以維持服務並最小化業務影響。
- **3-6 可視性分析**：整合事件日誌並建立定期審查及異常行為偵測與回應機制。

IV 整合指標

- **3-7 自動化治理**：具依資安政策及網路態勢快速調適的自動化管理機制。

金融業導入零信任架構參考指引-實作參考原則

應用程式是數位基礎設施主要存取點，透過角色和作業屬性進行授權控制

I 靜態指標

- **4-1 存取授權**：以作業屬性及風險區隔角色，採最小授權原則並針對特權作業採獨立授權。

II 動態指標

- **4-2 存取授權**：將帳號動態屬性納為每個工作階段的授權審核條件，並針對特權作業採即時存取機制。
- **4-4 程式安全**：對應用程式進行資安檢測，確保應用程式本身的安全性。
- **4-5 程式部署**：為應用程式建立持續整合及部署通道，並減少人員介入誤失。

III 即時指標

- **4-3 威脅防護**：對應用程式活動紀錄具有即時偵測及回應機制，並動態撤銷不符常規操作的授權。
- **4-6 可視性分析**：整合事件日誌並建立定期審查及異常行為偵測與回應機制。

IV 整合指標

- **4-7 自動化治理**：建立自動化管理機制，確保應用程式生命週期的安全性及合規性。

金融業導入零信任架構參考指引-實作參考原則

資料在存儲與傳輸上的保護在零信任架構中非常重要

I 靜態指標

- **5-1 外洩防護**：針對機敏資料部署資料外洩防護機制，如DLP。
- **5-3 資料分類**：建立資料盤點、分類及標籤機制，確保資料保護政策。
- **5-4 資料可用性**：建立本地端高可用性及異地端備份，確保資料有效保護及還原。
- **5-6 資料加密**：依資料分級對機敏性資料加密儲存，並確保金鑰管理安全。

II 動態指標

- **5-5 資料存取**：將資料存取的動態屬性納為授權審核條件，並具重新驗證機制。

III 即時指標

- **5-2 外洩防護**：具監控資料存取及使用情況機制，偵測並阻止疑似資料外洩行為。
- **5-7 可視性分析**：整合事件日誌，建立定期審查及偵測異常行為機制。

IV 整合指標

- **5-8 自動化治理**：建立自動化管理機制，確保資料生命週期的安全性及合規性。

3

實作案例與持續評估

具體案例介紹 – A金融機構

	風險導向盤點方法		
	步驟一：適用場景	步驟二：高風險	步驟三：低衝擊
遠距辦公	83	48	4
雲端存取	0	0	0
系統維運管理	9	9	1
應用系統管理	9	9	1
服務供應商	0	0	0
跨機構協作	8	7	1

場域選擇

- 「遠距辦公」、「系統維運管理」、「應用系統管理」、「跨機構協作」

系統選擇

- 「健康檢查系統」、「客戶資料整合系統」、「櫃檯e化系統」、「遠距服務系統」...等 (系統名稱已去識別化)

具體案例介紹 – B金融機構

	風險導向盤點方法		
	步驟一：適用場景	步驟二：高風險	步驟三：低衝擊
遠距辦公	93	55	10
雲端存取	1	1	1
系統維運管理	28	15	1
應用系統管理	28	15	1
服務供應商	0	0	0
跨機構協作	6	3	0

場域選擇

- 「遠距辦公」、「雲端存取」、「系統維運管理」、「應用系統管理」

系統選擇

- 「行銷平台」、「錄音檔調聽系統」、「語音查詢系統 」、「電銷外撥系統」、「人資系統」...等 (系統名稱已去識別化)

具體案例介紹 – C金融機構

	風險導向盤點方法		
	步驟一：適用場景	步驟二：高風險	步驟三：低衝擊
遠距辦公			
雲端存取			
系統維運管理			
應用系統管理			
服務供應商			
跨機構協作			

係使用不同方法論

場域選擇

- 「服務供應商」

系統選擇

- 「客服系統」、「數位報表系統」、「數位契約系統」、「錄音錄影系統」(系統名稱已去識別化)

金融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

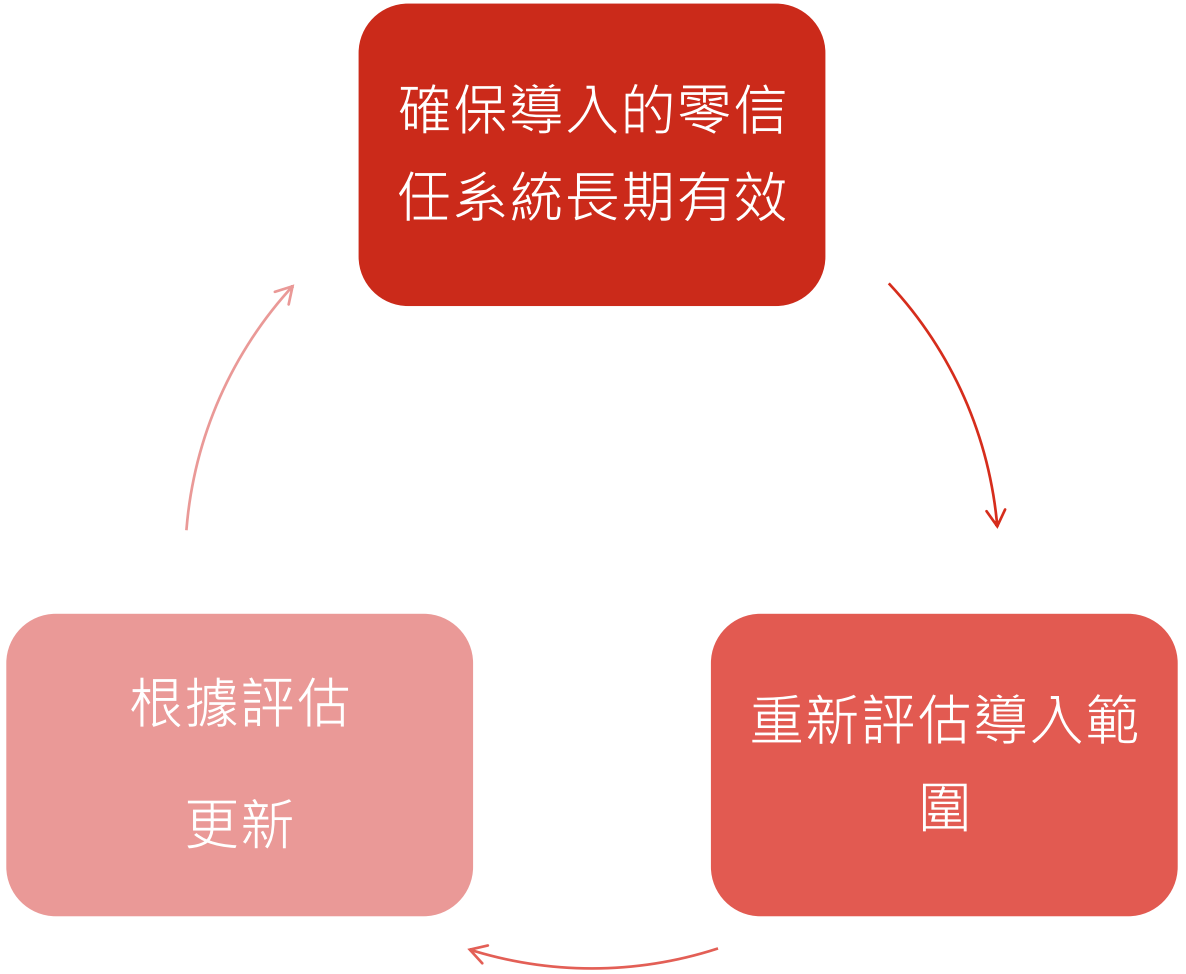
實務案例分享

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

持續評估



結語

- 零信任架構在導入過程中，應以高風險、低衝擊場域為優先部署策略，以減少安全威脅同時降低業務影響。
- 對導入的對象系統進行持續評估，確保安全控制措施的有效性和適應性，以應對不斷變化的安全威脅。
- 隨著科技的進步，零信任架構在未來的資訊安全中將更顯重要，我們鼓勵各機構積極探索與應用此策略，確保業務的持續安全性。

Q & A

pwc.tw