推動證券商導入金融零信任說明會

–身分驗證

資誠智能風險諮詢管理有限公司
五月 2025

pwc 資誠

Agenda

項次	內容
1	實作參考原則分級解析-身分驗證
2	零信任架構導入常見問題-身分驗證

1

實作參考原則分級解析-身分驗證

CISA零信任架構-五大概念

(一) 假設環境惡劣：環境內外都存在惡意攻擊或潛在威脅，機構採嚴謹的態度將所有使用者、裝置、應用程式、均視為不受信任。

(二) 假設已有安全漏洞：假設惡意攻擊存在於機構環境中，預設系統或網路已遭受攻擊；加強對存取和授權決策的審查，以改善風險。

(三) 永不信任、持續驗證：每個裝置、使用者、應用程式和資料流都依循最小權限原則，透過持續、多種類的驗證手段，進行身份驗證和明確授權審核。

(四) 明確審核：所有對資源的存取是有條件性的，建立具基於屬性存取控制機制(靜態或動態指標)，來授予存取權限。並且存取可根據產生的信任級別進行動態撤銷、限縮存取授權或即時告警，實施自動化資料存取控制。

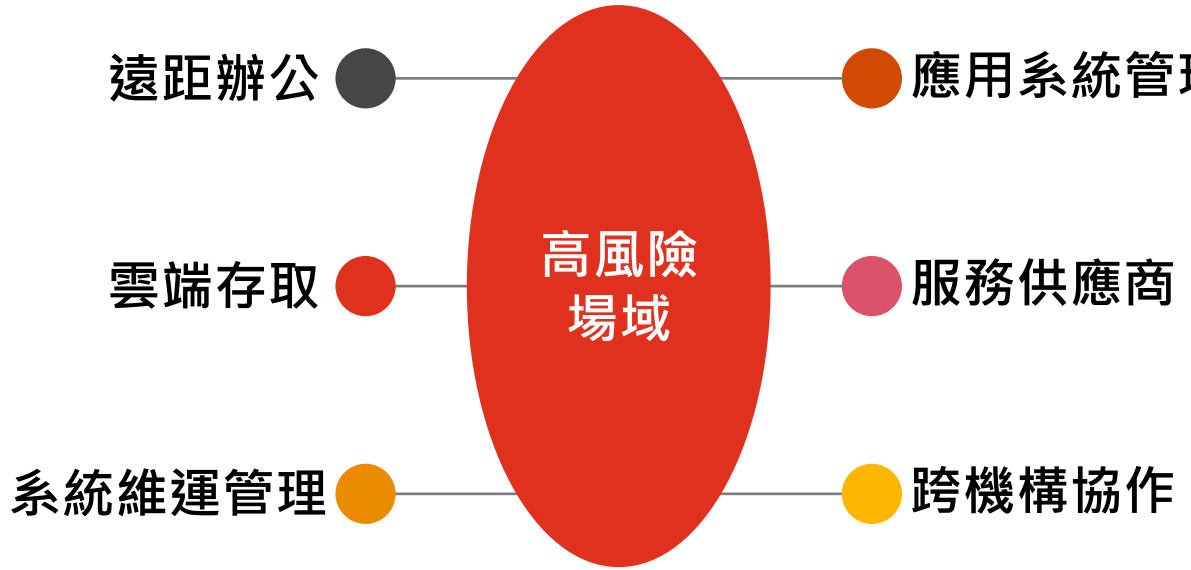
(五) 統一分析：整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，以便於進一步自動化分析。

金融業導入零信任架構參考指引-場域

風險導向，擇高風險、低衝擊之場域先行

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。

零信任架構實作參考原則分級-5大支柱

Identity

身分

是指唯一描述特定使用者或實體（包括非個人實體）的屬性或屬性集。

Devices

設備

是指任何可連接到網路的資產（包括其硬體、軟體、韌體等），包括伺服器、桌上型電腦和筆記型電腦、印表機、行動電話、物聯網設備、網路設備等。

Networks

網路

是指開放的通訊介質，包括典型通道（例如機構內部網路、無線網路），以及其他潛在通道（例如用於蜂巢式網路和應用程式層級通道）。

Applications

應用程式

包括在本機、行動裝置和雲端環境中執行的資通系統、程式和服務。

Data

資料

包括正在訪問或曾經訪問的設備、網路、應用程式、資料庫、基礎設施和備份（包括本機和虛擬環境）中的所有結構化和非結構化檔案和片段。

金融業導入零信任架構參考指引-實作參考原則

等級 I

支柱	功能
身分	身分認證
	身分互通
設備	設備合規
	供應鏈風險
網路	網路區隔
	流量加密
應用程式	存取授權
資料	外洩防護
	資料分類
	資料可用性
	資料加密

等級 II

支柱	功能
身分	身分認證
	權限存取
設備	設備合規
	資源存取
網路	網路區隔
	流量管理
應用程式	存取授權
	程式安全
	程式部署
資料	資料存取

等級 III

支柱	功能
身分	可視性分析
設備	威脅防護
	可視性分析
網路	網路韌性
	可視性分析
應用程式	威脅防護
	可視性分析
資料	外洩防護
	可視性分析

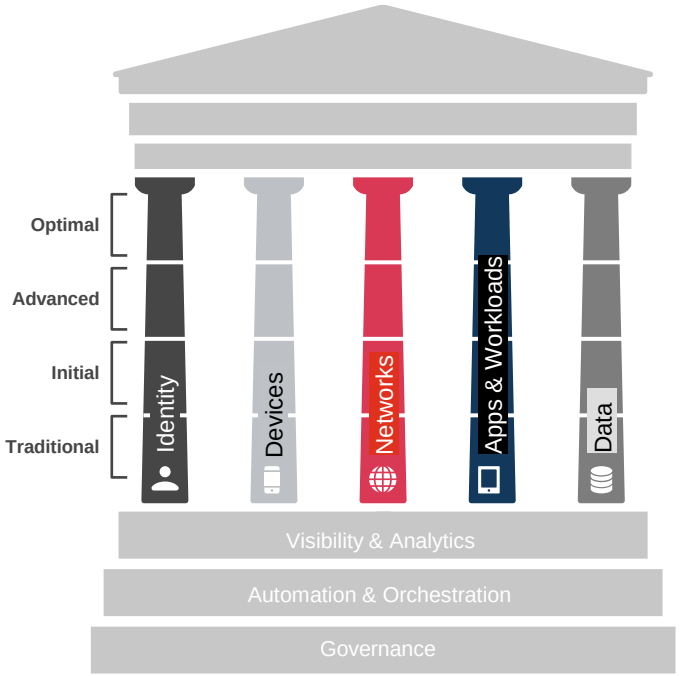
等級 IV

支柱	功能
身分	自動化治理
設備	自動化治理
網路	自動化治理
應用程式	自動化治理
資料	自動化治理

金融業導入零信任架構參考指引-實作參考原則

1 身分(7)
- 身分認證（I*1、II*1）
- 身分互通（I*2）
- 權限存取（II*1）
- 可視性分析（III*1）
- 自動化治理（IV*1）

2 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）



3 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）

5 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）

4 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）

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

金融業導入零信任架構參考指引-實作參考原則

1. 身分

身分驗證是保護數位資源的第一道防線，零信任強調所有存取請求都經過認證

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，零信任強調所有存取請求都經過認證

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等)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，除依角色屬性存取控制落實最小授權原則外，並具基於屬性存取控制機制，可將每個工作階段之動態屬性(如時間、地點等)納為授權審核條件，動態撤銷、限縮存取授權或即時告警。

III 即時指標

- **1-6 可視性分析**：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，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或SOAR Playbook等)。(參照F-ISAC威脅情資及金融資安監控組態基準)。

IV 整合指標

- **1-7 自動化治理**：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，確保於帳號生命週期之安全性及合規性。

金融業導入零信任架構參考指引-實作參考原則

1-1 身分認證

採用**多因子身分鑑別(Multi-Factor Authentication, MFA)**，降低帳號密碼遭破解、竊聽等風險。

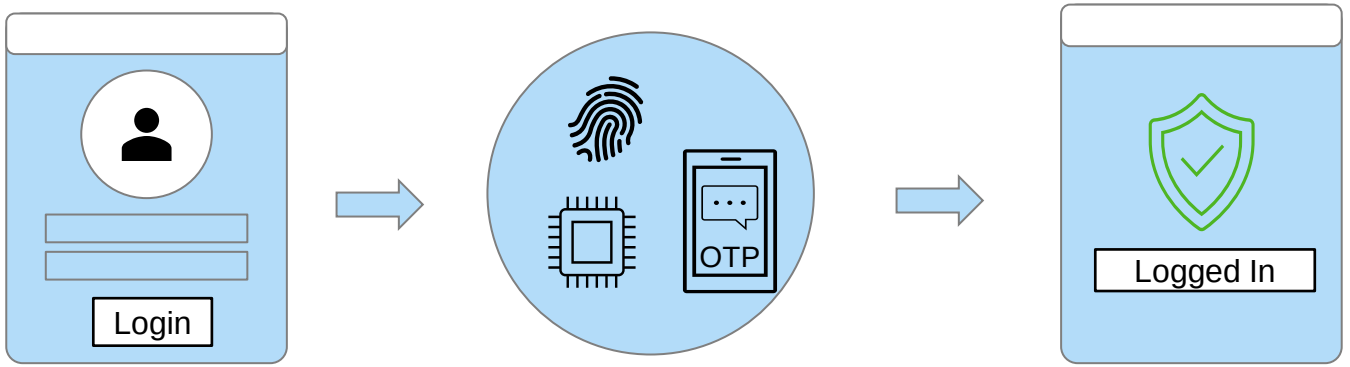
- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

多因子驗證

(一) **something you know**：帳號及密碼、PIN碼、安全問題等。

(二) **something you have**：智慧卡、晶片卡、憑證、動態密碼OTP等。

(三) **something you are** ：臉型、指紋、DNA、虹膜、掌紋等生物特徵。



多因子驗證

金融業導入零信任架構參考指引-實作參考原則

1-2 身分認證

採用包含**綁定實體載具**的多因子驗證機制，可抗網路釣魚風險。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

實體載具範例

- **FIDO**：無密碼，透過生物辨識、第二裝置等驗證
- **晶片卡**
- **動態密碼產生器**
- **綁定手機且具數字配對APP**

排除簡訊、語音、電子郵件中的一次性密碼(OTP)作為驗證方式。

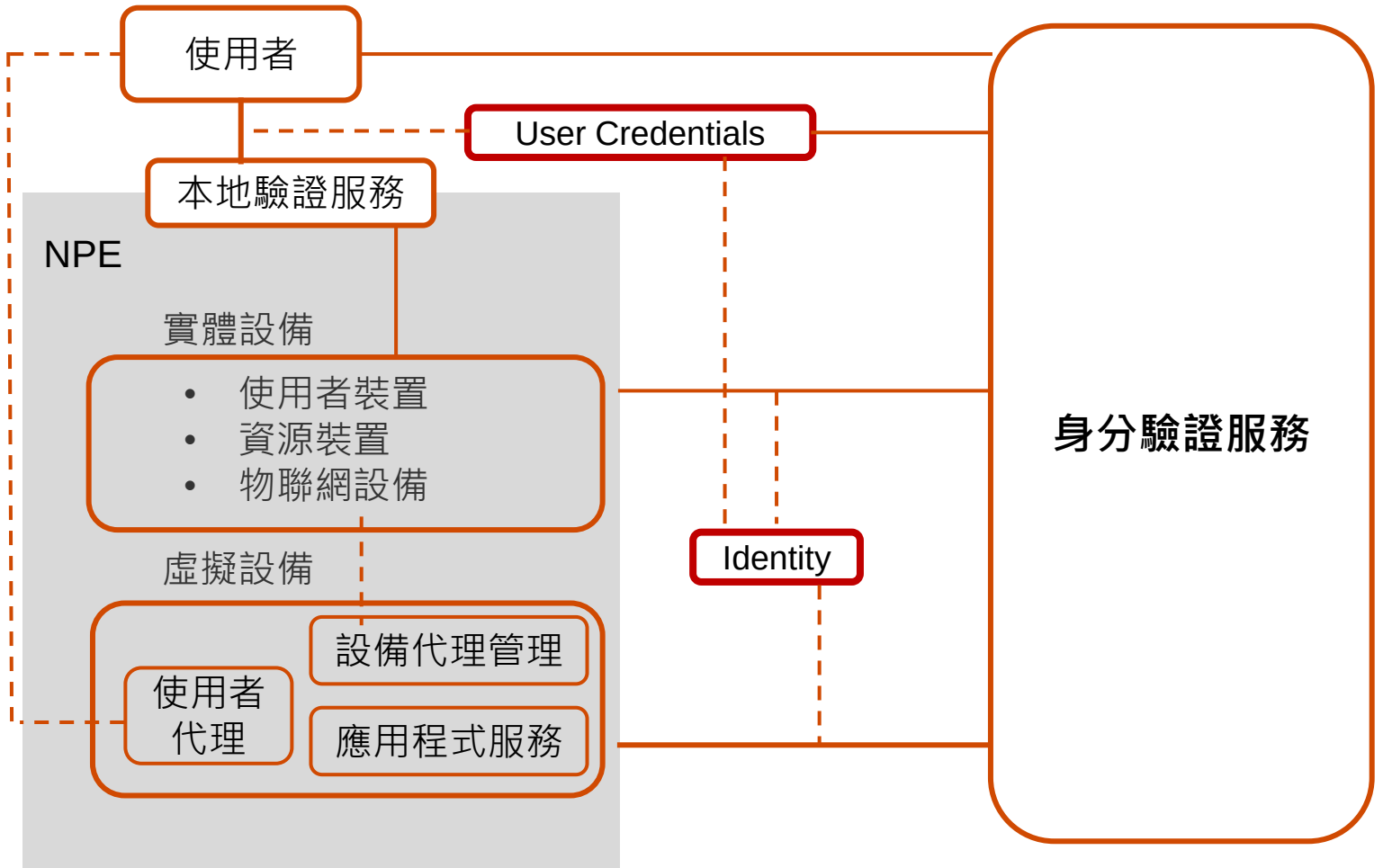
身分認證架構圖(釋例)

1. 身分

圖示: 認證API / 資料交換

身分認證運作方式

1. **主要概念**
   使用者與設備在連接到資源之前，必須先進行身份驗證
2. **身分驗證服務**
   負責驗證這些使用者或裝置的身份，確保獲得授權後才能存取資源。
3. **使用者 & 設備**
   需要身份驗證的人與裝置，如：電腦、手機、提供應用程式或網路服務的設備、 IoT / 感測器
4. **虛擬設備(支援身分驗證)**
   可以安裝至裝置中協助進行完整的設備管理，並由虛擬設備將能更多協助判斷的資訊提供給身分驗證服務



金融業導入零信任架構參考指引-實作參考原則

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

1-3 身分互通

對**外部使用者**(如服務供應商或跨機構協作)提供或採用**不低於內部使用者信賴等級**之身分鑑別機制。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)

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 評估身分登錄、信物管理與身分驗證三階段)

➡ **多種驗證機制之間，信賴等級一致**

零信任概念

零信任安全模型假設所有用戶和裝置在進入系統時均不可信，需經過驗證。

ISO29115 是什麼？

- 在ISO29115中，ISO提供「個體身分驗證信賴框架」方法論。
- 金管會參考ISO29115，於112年10月24日訂定「金融服務業辦理數位身分驗證指引」。
- 本標準定義實體身分驗證信賴等級，協助金融服務業選擇適當驗證機制以應對風險。

「金融服務業辦理數位身分驗證指引」ISO29115標準之身分識別機制

數位身分驗證機制三階段，原則上包含以下作業程序

階段	主要作業內容
身分登錄	• 身分核驗：提供身分資料(如姓名、生物特徵)，由註冊管理者進行核驗。 • 註冊及紀錄保存：核驗通過後，將資料登錄並保存紀錄。
信物管理	• 綁定及核發：信物與客戶資料綁定後，發放信物。 • 啟用及保存：客戶啟用信物並妥善保管，且應避免未授權使用。 • 暫停、撤銷及更換：依據信物使用情形及客戶狀態進行適當處理，如暫停、撤銷、更換等措施。
身分驗證	• 客戶及信物關聯性之驗證：客戶提交信物，驗證其持有者與信物之身分。 • 驗證結果回復及紀錄保存：驗證成功後，回覆結果予驗證者並保存紀錄。

「金融服務業辦理數位身分驗證指引」ISO29115身分驗證的信賴等級參考

信賴等級		客戶身分信賴程度	風險情境	應用示例
LoA1	等級一	少許或無信心	低風險	• 自行建帳號，密碼由用戶定義或自動產生 • 登入時使用密碼即可
LoA2	等級二	中等信心	中風險	• 帳號由機構預定 • 登入程序可採多因子驗證或密碼加一次性密碼(OTP)
LoA3	等級三	高度信心	高風險	• 帳號需經過驗證(可遠端，通道須加密) • 採用多因子登入驗證
LoA4	等級四	極高信心	極高風險	• 帳號須臨櫃驗證，密碼現場授予 • 使用硬體信物進行登入驗證

身分互通架構圖(釋例)

1. 身分

聯合企業身分服務(Federated Enterprise Identity Service):

整合身分憑證和授權，並在組織群組之間共用，以便使用者及設備可以跨組織存取其他網域中的服務。

作用

- **確保只有授權人員能存取系統**，提高安全性。
- **自動管理帳號與權限**，減少人為錯誤與風險。

架構

1. 身份提供者（Identity Provider）

• 負責建立與管理身份資訊，決定誰能存取哪些資源。

2. 使用者主檔（Master User Record）

•使用者的個人屬性和權利等資訊

3. 憑證保管（Credential Vault）

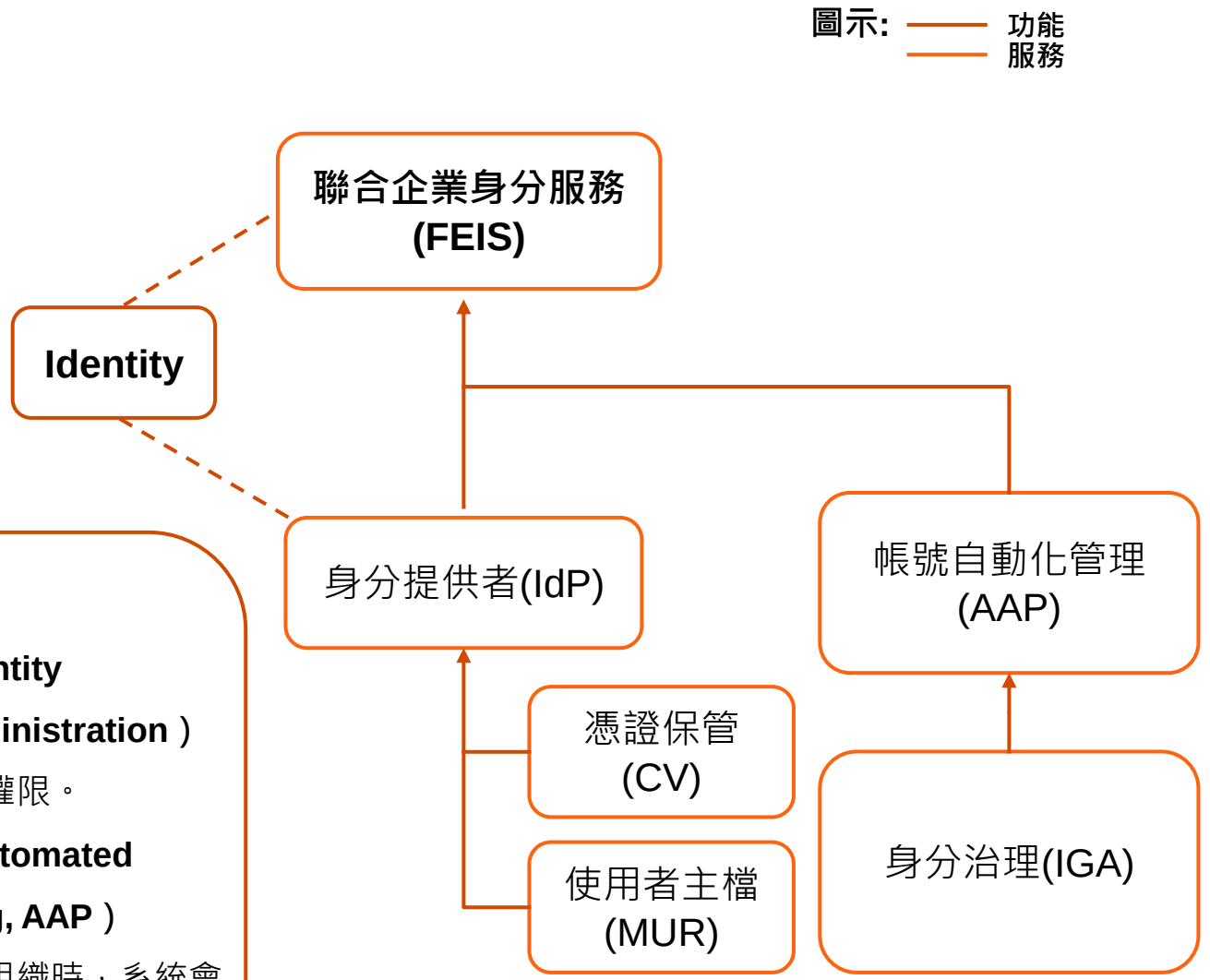
• 安全存放密碼、憑證等重要身份資訊

4. 身份治理（IGA, Identity Governance and Administration）

• 定期審查與管理存取權限。

5.帳號自動化管理（Automated Account Provisioning, AAP）

• 當使用者加入或離開組織時，系統會自動建立或撤銷帳號。



金融業導入零信任架構參考指引-實作參考原則

1-5 權限存取

完成身分鑑別後，除依角色屬性存取控制(RBAC)落實最小授權原則外，並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、地點等)納為授權審核條件，動態撤銷、限縮存取授權或即時告警。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

1. **角色為基礎的控制(RBAC)**
   - 授予角色相應的適當授權
   - 給予工作所需**最低權限**
2. **屬性為基礎的控制(ABAC)**
   - 加入**情境條件**(如時間、地點)，來判斷是否允許存取
   - 讓**存取權限**可以隨情境變化**動態調整**
3. **動態權限管理**
   - 當**偵測異常**情況時，立即撤銷或**縮小權限**
   - 如有異常行為，即時發出**警示**

金融業導入零信任架構參考指引-實作參考原則

屬性為基礎的控制(ABAC)範例

身分(一般來說)

組織適用屬性
工作職能、 部門、許可級別、辦公位置、資歷、身分驗證強度

資源適用屬性
文件分類級別、所有權、內容類型、建立日期、敏感度、資料合規標籤

環境適用屬性
訪問時間、存取位置、裝置類型、網路安全等級、作業系統、會話風險評分

操作適用屬性
執行類型、編輯權限、存取頻率、請求目的

將 ABAC 套用至 VPN 撥入程序時，機構可以使用一系列屬性來確保只有授權使用者，在特定的條件下能夠存取網路。提供一些可應用的實用屬性：

Ex.VPN撥通

組織屬性
如：員工/供應商、 IT/財務、總部/遠端、就業狀態(在職/留停)、管理職、MFA

環境屬性
僅限工作日、公司Wi-Fi、白名單、國家或地區、連線風險評分

操作屬性
唯讀/完全存取、資料傳輸限制

連線屬性
持續時間、閒置時間、存取次數

屬性為基礎的控制(ABAC)範例

身分(一般來說)

組織適用屬性
工作職能、 部門、許可級別、辦公位置、資歷、身分驗證強度

資源適用屬性
文件分類級別、所有權、內容類型、建立日期、敏感度、資料合規標籤

環境適用屬性
訪問時間、存取位置、裝置類型、網路安全等級、作業系統、會話風險評分

操作適用屬性
執行類型、編輯權限、存取頻率、請求目的

將 ABAC 套用至特權帳號管理時，機構可以使用一系列屬性來管理特權帳號存取權限，僅在特定條件下存取並降低風險。提供一些可應用的實用屬性：

Ex. PAM(特權帳號)

組織屬性
如：是否為特定角色、就業狀態(在職/留停)、任期、訓練是否合規、身分驗證強度

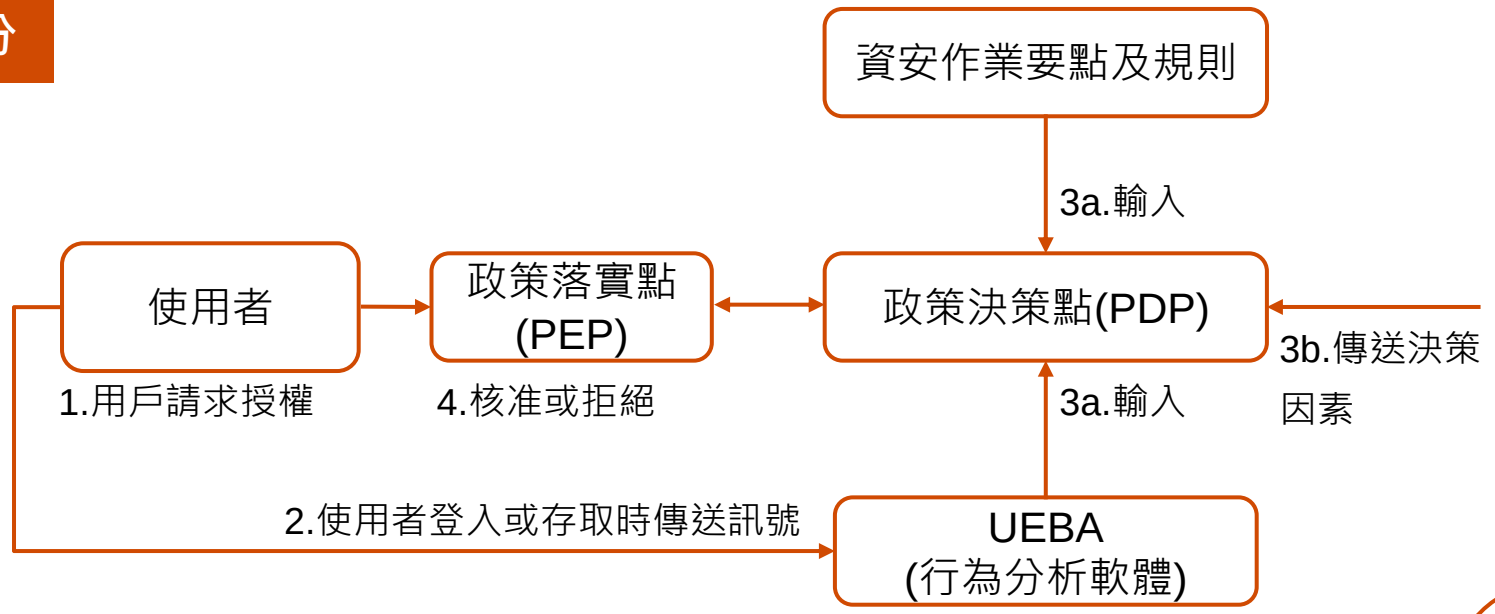
環境屬性
工作日、公司Wi-Fi、IP位置、特定時間或日期

操作屬性
唯讀/完全存取、資料傳輸限制、資料敏感

連線屬性
持續時間、閒置時間、存取次數、同時段的連線

權限存取架構圖(釋例)

1. 身分



- RBAC (角色權限)
- ABAC (屬性、情境)
- Network Access Control(網路存取控制)
- Authorization Factors for Hygiene Diagnostics(安全診斷)
- Application Sensitivity(資料機敏性)
- Data Tags(資料標籤)

條件授權概念

使用者請求授權後，會傳送決策資訊給PDP，讓PDP綜合評估是否給予使用者授權

授權條件因素

1. RBAC角色權限：角色的權限能否存取
2. ABAC屬性：使用者是否在安全的情境
3. 網路存取控制：使用者是否有授權連上特定網路
4. 設備健康：設備是否有潛在風險
5. 應用程式敏感性：根據應用程式敏感度給予風險評級
6. 資料標籤：根據資料敏感度給予風險評級

金融業導入零信任架構參考指引-實作參考原則

1-6 可視性分析

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，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或SOAR Playbook等)。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

1. **集中收容日誌資料至同一平台**(如SIEM)
   - 確保安全事件有完整、可查的紀錄
2. **異常偵測與警告機制**
   - 定期審查並監控日誌，偵測異常行為
   - 發現可疑活動，立刻觸發警示採取應對
3. **資安監控與即時回應**
   - 與資安監控中心(SOC)整合，快速分析入侵指標(IOC)或攻擊行為模式(Mitre ATT&CK TTP)
   - 根據事件自動執行回應動作(如生成事件單或啟動SOAR Playbook)

名詞解釋

- SIEM：安全資訊事件管理系統，集中收集和分析資安日誌，即時偵測異常，協助快速應對安全威脅。
- Mitre ATT&CK TTP：Mitre建立的框架，描述攻擊的戰術、技術、程序(TTP)，幫助團隊識別攻擊行為。
- SOAR Playbook：敘述如何驗證及回應安全事件的文件。若SOAR(資安協作自動化應變系統)失效，可以人工處理作為備案。

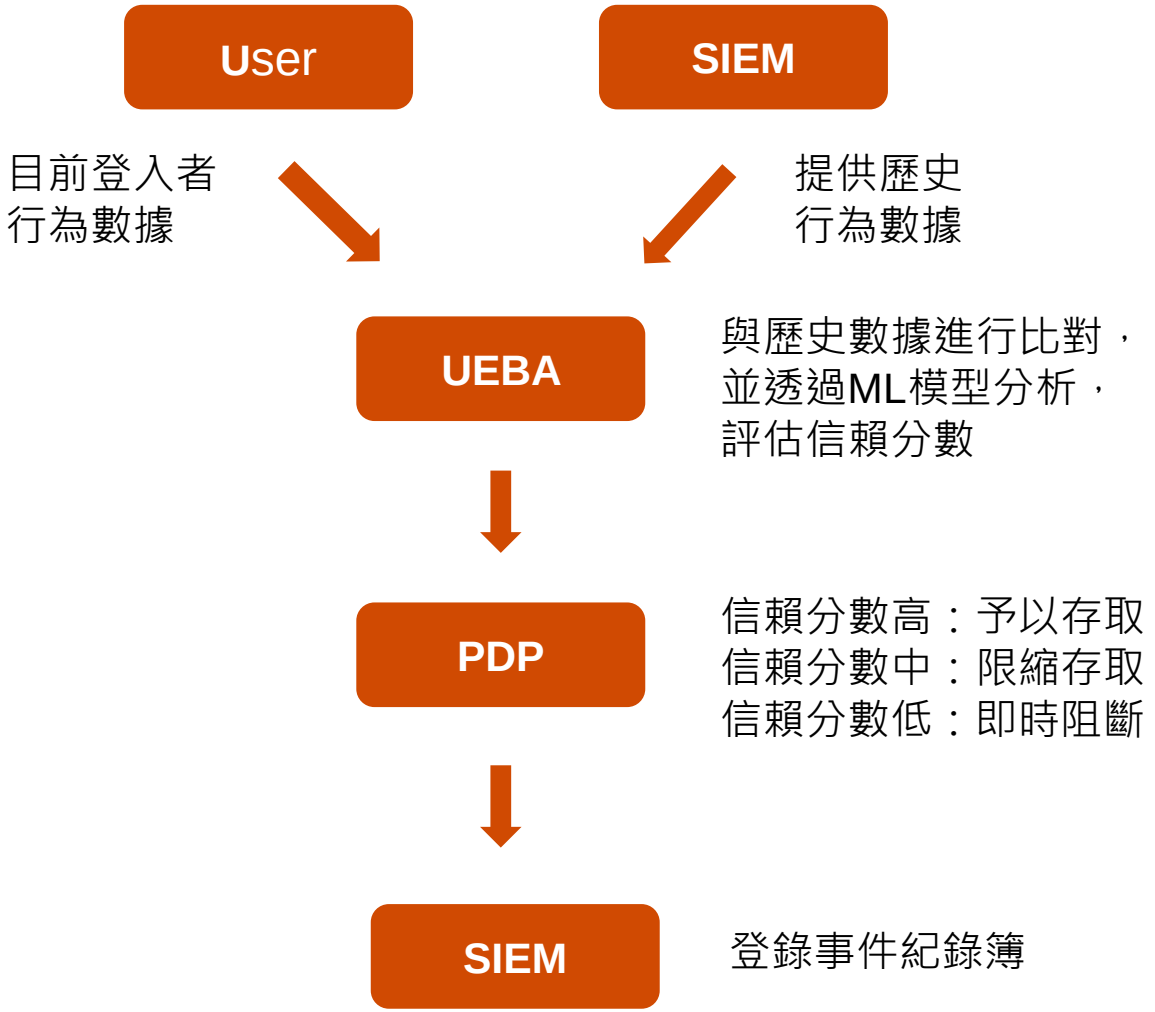
持續驗證及分析(釋例)

1. 身分

使用者與實體分析行為(UEBA)概念

User and Entity Behavior Analytics, UEBA

是一種安全軟體，透過分析使用者與系統設備的行為模式，來識別異常活動和潛在威脅。



持續驗證及分析(釋例)

1. 身分

UEBA運作方式

1. **建立正常行為基準(前置)**
   收集與分析正常使用者行為數據，設定正常行為基準
2. **監控與分析**
   持續觀察用戶和設備行為，並透過機器學習分析變化
3. **風險評估與回應**
   根據行為異常度分配風險分數(信賴分數)，並進行撤銷、限制存取、告警等回應指令。

行為數據範例(可為SIEM資料)

- **登入模式**
  登入的時間、地點、使用設備等，是否符合正常行為。
- **檔案傳輸活動**
  大量或不尋常檔案下載，或頻繁操作特定資料夾。
- **應用程式使用**
  各應用程式使用率、出現不尋常的高風險應用程式使用行為。
- **異常操作模式**
  使用者執行異常指令，或不符合平時操作習慣，如訪問數個從未使用過的系統

金融業導入零信任架構參考指引-實作參考原則

1-7 自動化治理

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，確保於帳號生命週期之安全性及合規性。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

階段	說明
傳統	•手動管理使用者身分帳號(開通、停用、自我管理) •各系統整合程度低 •定期審查
最佳化	•系統能根據行為、需求靈活調整，自動化管理所有身分帳號 •自動化管理身分的生命週期(建立、使用到停用)，使其安全並合規 •全面整合所有環境的身分管理 Enterprise-wide***身分識別與存取管理IAM***

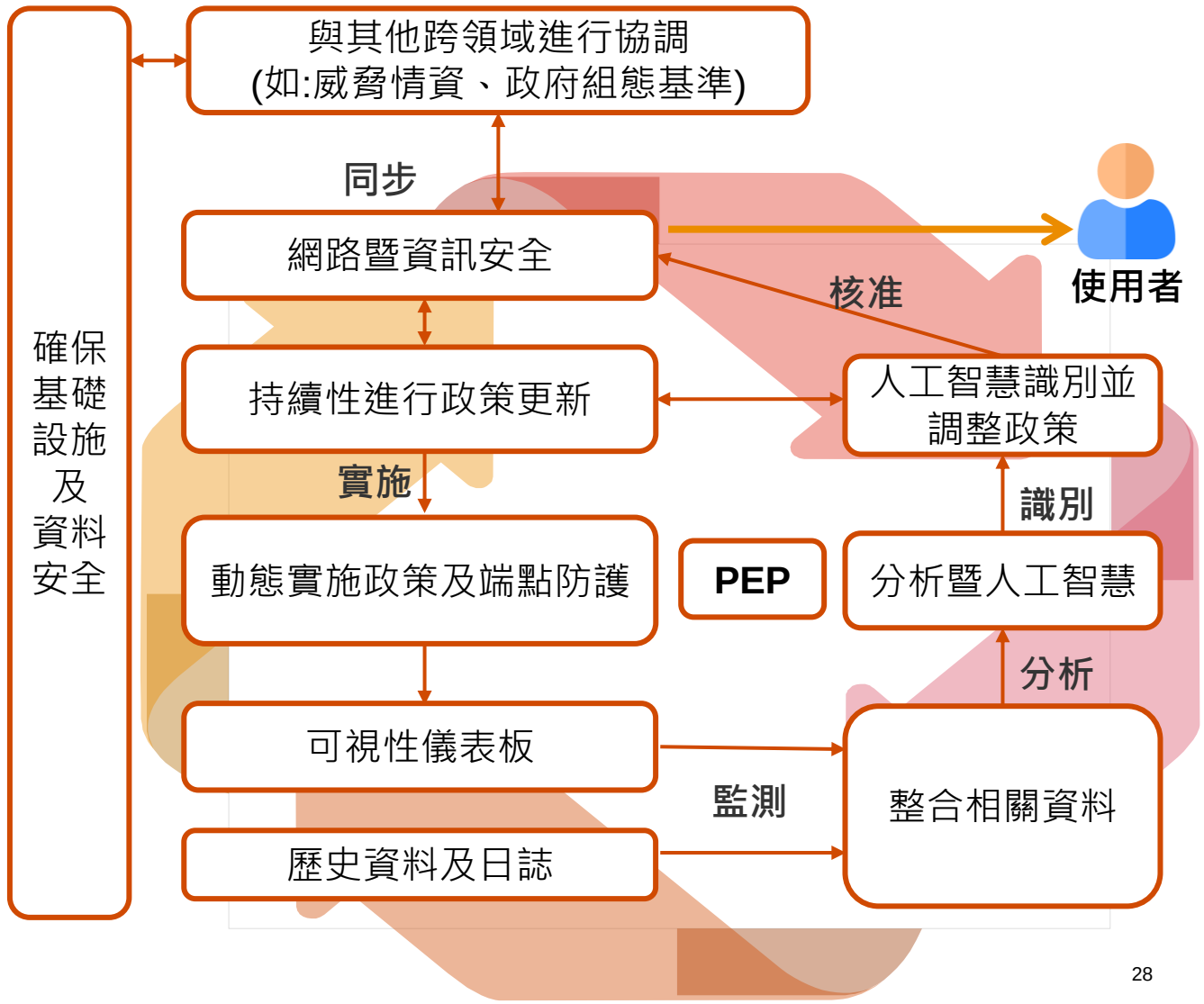
自動化治理架構圖(釋例)

傳統

- 孤立的管理政策
- 不平衡的應用及控制
- 根本原因分析
- 遺漏、誤報
- 人工手動操作

目前傳統框架下，重要且關鍵的資料時常發生遺漏、而防護機制也常誤判或無法理解原因。這需要維運和資安團隊不斷進行人工操作判斷，從而導致對於整體資安環境的應變能力是緩慢且不即時。

零信任



2

零信任架構導入常見問題-身分驗證

零信任架構導入常見問題一覽表–身分驗證(1/3)

PwC 整理常見導入零信任架構時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
想在明年全面導入 SSO，要如何確保符合理想的零信任要求?	為符合零信任原則，導入 SSO 時可： • 啟用多因子鑑別（MFA）強化身分驗證。 • 實施條件式存取控制（如：信賴等級、IP 位置等）。 • 檢視工作職掌與角色，定期審查並檢討使用者權限，落實權限最小化原則。 • 依照資安政策設置合理的存取時間，已管控存取風險。
現行系統相對老舊或採自行設計客製，擬不支持SSO機制怎麼辦?	若系統無法整合進單一登入（SSO）或 IAM 流程，建議採以下處理方式： • 設置補償性控制流程，如使用可選擇透過Private Link（VPN）、來源 IP 限制、跳板機存取，降低存取風險。 • 加強稽核日誌與異常偵測，即便技術無法整合，確保行為可監控、可追溯。 • 納入中長期升級規劃，將無法整合的系統列為藍圖，規劃替換或改善時程。

零信任架構導入常見問題一覽表–身分驗證(2/3)

PwC 整理常見導入零信任架構時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
已導入SSO/IAM 機制，但為什麼仍不符合零信任要求?	首先針對 IAM，需檢視是否做到統一的帳號管理與角色控管，且每一次系統登入是否均需透過 SSO 流程，無繞過情況。其次，對於單一登入（SSO），檢查所有內部、雲端、外部應用是否都整合進 SSO，若有無法整合的系統，是否有正式提出流程的補償性控制，如：跳板機存取。
身分驗證機制有哪些要求需要高階管理層特別介入，以加速落實?	1. 權限政策與例外授權標準： 高階管理層可制定最小權限原則與例外核准機制，避免部門因方便而過度授權。 2. 權限稽核與責任歸屬： 高階管理層可推動督導及權限定期審查，並納入內部稽核制度。

零信任架構導入常見問題一覽表–身分驗證(3/3)

PwC 整理常見導入零信任架構時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
最小權限原則，建議落實的方式?	針對最小權限原則的落實，主要做法是先依照業務需求制定標準化的角色權限設定，透過角色為基礎（RBAC）或屬性為基礎（ABAC）的模型，明確界定每個職務應具備的最小存取範圍。所有權限申請必須經由標準流程，由主管審核確認業務必要性，並設置到期日或定期重新審查機制。
日誌除記錄登入資訊外，還有哪些其他建議?	為確保單純記錄登入資訊能符合身分可視性的稽核要求，關鍵在於資料的完整性、關聯性與可追溯性。常見紀錄資訊，如：使用者身分、身分認證等級(MFA)、連線持續時間、操作行為、錯誤紀錄等。

Q & A

pwc.tw