pwc 資誠

推動證券商導入金融零信任說明會

-資料保護

資誠智能風險諮詢管理有限公司

2025.9

Agenda

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

1

實作參考原則分級解析-資料保護

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

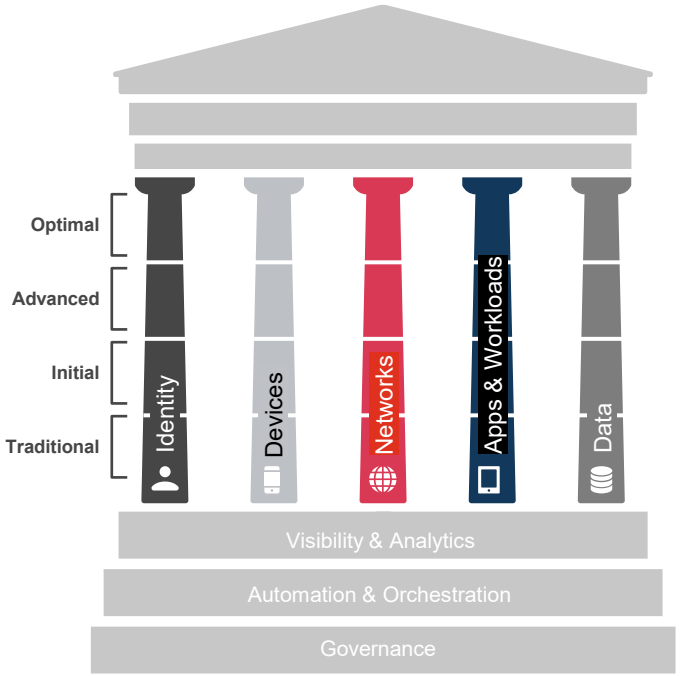
等級 IV

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（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

5. 資料

資料在存儲與傳輸上的保護在零信任架構中非常重要

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**：針對機敏資料部署防止資料外洩防護機制，如依據資料特徵之DLP、資料不落地等。
- **5-3 資料分類**：建立資料盤點、分類及、標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。
- **5-4 資料可用性**：建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如離線備份、儲存於隔離環境、防止寫入等)及有效還原。
- **5-6 資料加密**：依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。

II 動態指標

- **5-5 資料存取**：可將資料存取的動態屬性(如MFA強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警。

III 即時指標

- **5-2 外洩防護**：具監控資料存取和使用情況機制，可依據資料存取行為或資料處理模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行。
- **5-7 可視性分析**：整合事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，並與資安監控機制整合，針對入侵指標或攻擊行為樣態進行即時的判斷與應處。

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。

金融業導入零信任架構參考指引-實作參考原則

5-1 外洩防護

針對機敏資料部署防止資料外洩防護機制，如依據資料特徵之DLP、資料不落地等。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

基於資料特徵的機敏資料防護機制

1. **DLP(資料外洩防護)**
   - 基於資料特徵(如敏感字詞、格式或標籤)，進行識別與控管，防止未經授權的存取、傳輸或複製。
2. **資料不落地**
   - 透過即時訪問技術(如虛擬桌面、雲端應用程式)，防止資料存於外部裝置。

金融業導入零信任架構參考指引-問答

Question:
根據零信任參考指引，下列何者可進行資料外洩防護？

選項A

員工簽署NDA

→ ✗ 不適用

選項B

DLP與資料不落地政策

→ ✓ **存取閘道應建置機敏資料外洩防護(如DLP、資料不落地)機制**

選項C

VPN

→ ✗ 不適用

5-2 外洩防護

具監控資料存取和使用情況機制，可依據資料存取行為或資料處理模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行為。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

外洩防護機制範例

1. **行為的風險評估**
   - 機密資料存取過於頻繁
   - 偏離一般操作習慣
2. **動態調整授權**
   - 針對高風險操作 –> 限制或撤銷存取
3. **即時告警與阻止**
   - 判定資料外洩時，系統可立即阻止，並發出警報

金融業導入零信任架構參考指引-問答

Question:
根據零信任參考指引，若使用者在不尋常時間存取資料，即使擁有權限，應如何處理？

選項A

動態評估風險並可能即時撤銷授權

✓ 如有異於使用者以往或已定義之高風險異常存取行為時執行

選項B

封鎖帳號直到人工審查完成

✗ 不適用

選項C

允許其存取後再追蹤

✗ 不適用

金融業導入零信任架構參考指引-實作參考原則

5-3 資料分類

建立資料盤點、分類及、標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

最小授權原則

- 限制存取範圍，確保使用者僅接觸必要資料

1. 資料盤點與分類

- 盤點資料，並依敏感度、用途等方式進行分類

2. 資料標籤

- 將資料添加標籤(如”VVIP”、”PHI”等)，以便識別

金融業導入零信任架構參考指引-問答

Question:
根據零信任參考指引，資料分類與標籤機制最主要的作用是？

選項A

協助落實最小授權規則，依敏感度管控存取

✓ **資料存取應採角色基礎存取控制(RBAC)原則**

選項B

方便使用者自由分享

✗ **不適用**

選項C

減少資料中心空間

✗ **不適用**

金融業導入零信任架構參考指引-實作參考原則

5-4 資料可用性

建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如離線備份、儲存於隔離環境、防止寫入等)及有效還原。

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

➢ **可用性：確保經授權的使用者要對系統進行操作時，能確實的存取與使用。**

- 本地端：使用雲端或備援技術等方法提高可用性。
- 異地端：資料備份儲存於不同地理位置。

資料保護：離線備份、隔離儲存、防止寫入

資料還原：定期測試備份還原流程，確保能快速復原。

金融業導入零信任架構參考指引-問答

Question:
根據零信任參考指引，如何強化備份資料的可用性與安全？

選項A

僅儲存在雲端

→ ✗ 不適用

選項B

每週備份至行動硬碟

→ ✗ 不適用

選項C

採異地備份、離線隔離與還原測試

→ ✓ **根據異常操作行為，動態撤銷、限縮存取授權或即時告警**

金融業導入零信任架構參考指引-實作參考原則

5-5 資料存取

可將資料存取的動態屬性(如 MFA 強度、設備合規、時間、地點等) 納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、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

動態授權審核條件

- 審核動態屬性
  (如MFA強度、合規、位置、時間)
- 實施動態撤銷或限制存取授權
- 即時警告/阻斷/隔離

範例：

- **操作應用系統查詢資料時遇到VVIP**：
  員工A再執行OTP驗證且該納管設備通過合規、健康度檢查
  —> 允許存取資料
- **維運資料庫針對遮罩欄位資料異動**：
  員工B透過PAM申請使用代登方式
  —> 發出即時告警

金融業導入零信任架構參考指引–問答

Question:
根據零信任參考指引，部署 MFA 是否足以符合資料存取原則？

選項A

缺乏持續驗證與設備合規檢查，無法動態調整授權

透過相關機制依資料存取的動態屬性(ABAC)作為授權審核條件，並具啟動重新驗證之機制

金融業導入零信任架構參考指引-實作參考原則

5-6 資料加密

依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。

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

什麼是加密/金鑰?

- 加密是將「明文」編碼為「密文」的過程。
- 金鑰是一組代碼，用來加密或解密資料。
- 只有持有對應金鑰才能將「密文」轉換回 「明文」。

加密金鑰安全管理

- 管理金鑰的產生、儲存、分發、輪換(更換)、銷毀
- 企業使用金鑰管理系統(KMS)-產生、分發、更換
- 企業使用硬體加密模組(HSM)-儲存

金融業導入零信任架構參考指引-問答

Question:
在金鑰管理方面，下列哪一作法最符合零信任原則要求？

選項A

將金鑰與資料寫在同一檔案中以便快速存取

→ X 不適用

選項B

採人工方式傳遞金鑰給使用者

→ X 不適用

選項C

使用專業 KMS (Key Management System) 集中控管

→ ✓ 金鑰應具安全管理機制

金融業導入零信任架構參考指引-實作參考原則

5-7 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、SOAR Playbook)。

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，可作為人工處理的備案。

金融業導入零信任架構參考指引-實作參考原則

5-8 自動化治理

可依資安政策快速調適之一致性且自動化管理機制，確保於資料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	•手動執行資料生命週期與安全政策 資料生命週期：存取、使用、儲存、加密、配置、保護、備份、分類、淨化等
最佳化	**•全面自動化資料生命週期與安全政策，涵蓋企業所有資料 ***資料治理Data Governance(DG)、 資料安全Data Security(DS)*****

資料支柱之應用–資料保護架構圖(釋例)

傳統

網路為中心
彼此孤立

零信任

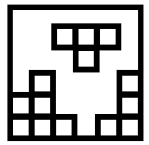
資料為中心
相互整合

使用者帳號、密碼存取

基於使用者(檔案基礎)存取

基於設備存取

使用者角色存取



靜態密碼

機敏性資料加密

資料傳輸加密

資料外洩防護機制(DLP)

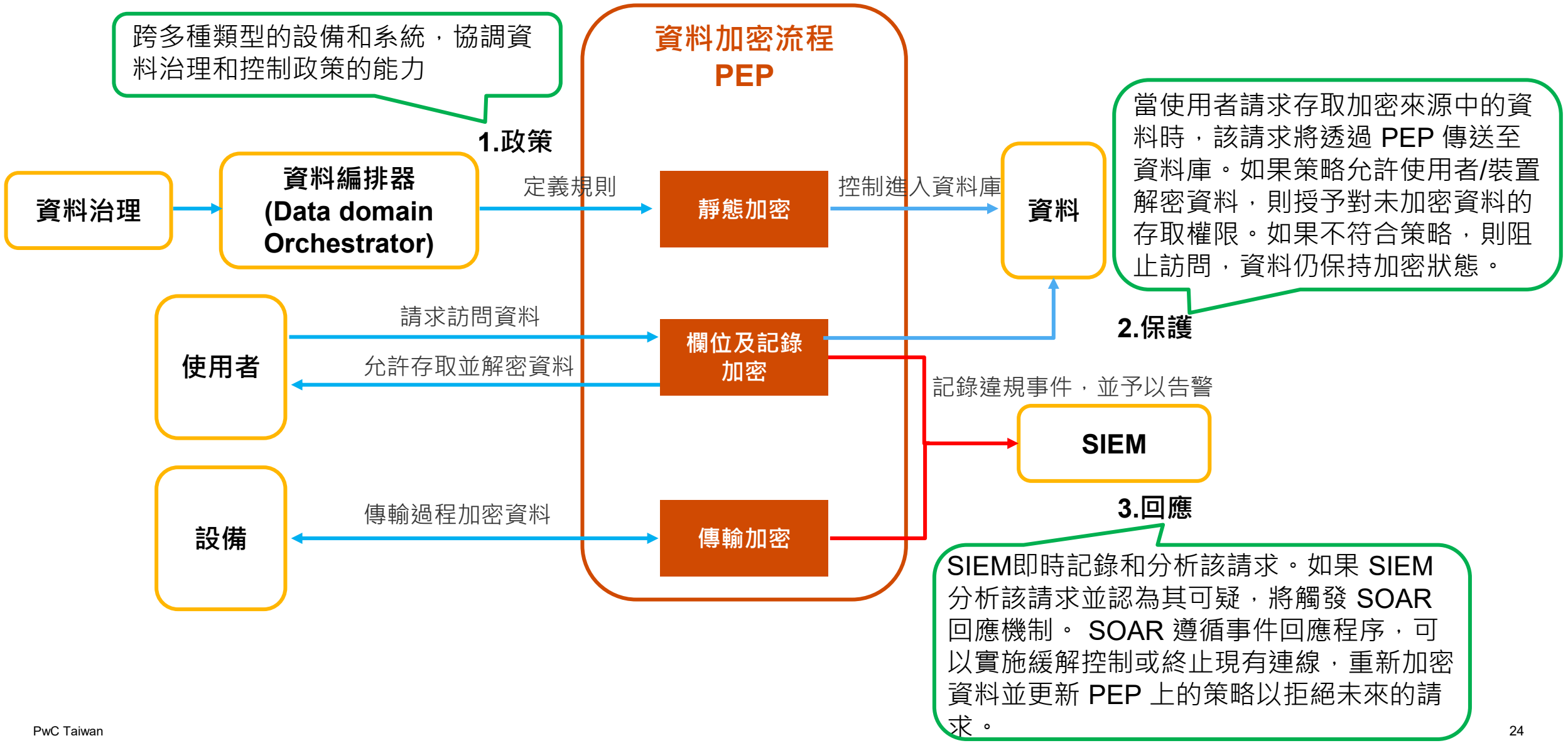
數位版權管理 (DRM)

資料標籤機制

過往資料安全方法是彼此孤立的、並採取以網路為中心策略。在以前的安全模型中，資料容易受到攻擊，因為資料僅受基本安全的保護，例如：使用者名稱/密碼、基於使用者/裝置的存取以及靜態加密，並且採用很少更新或驗證的存取控制-基於角色(RBAC)。

未來的資料安全方法將採用統一的零信任框架，透過以資料為中心的策略，持續評估和彼此相互協調的保護措施。採取資料為中心的技術將透過在欄位和記錄中增加額外的加密控制來幫助保護靜態資料。傳輸中的資料也必須加密。資料標籤將為數位權限管理 (DRM) 和資料外洩防護 (DLP) 解決方案提供支援，從而允許利用基於屬性的存取控制 (ABAC)作為動態授權的審核條件。

資料支柱之應用-資料加密參考流程(釋例)



資料支柱之應用-資料加密參考流程(釋例)

資料編排器(Data domain Orchestrator)

負責在資料治理(Data Governance)和加密流程(Data Encrypted Process)之間架起橋梁。

功能

1. 政策轉換：資料治理層會制定許多保護資料政策，並由資料編排器翻譯成技術性指令，發送至PEP。

2. 協調和管理：檢查資料保護需求，確保政策規範落實至各系統。

加密流程介紹

- **靜態加密(Encryption at Rest)**：將資料在設備或伺服器上加密，防止資料在未傳輸狀態被用戶訪問。
- **欄位和紀錄加密(Field and Record Encryption)**：針對資料庫中所有欄位與紀錄進行加密(取得資料庫不見得取得機密資料)。
- **傳輸加密(Encryption in Transit)**：加密資料傳輸過程，以防過程中遭受竄改。

應用場景：

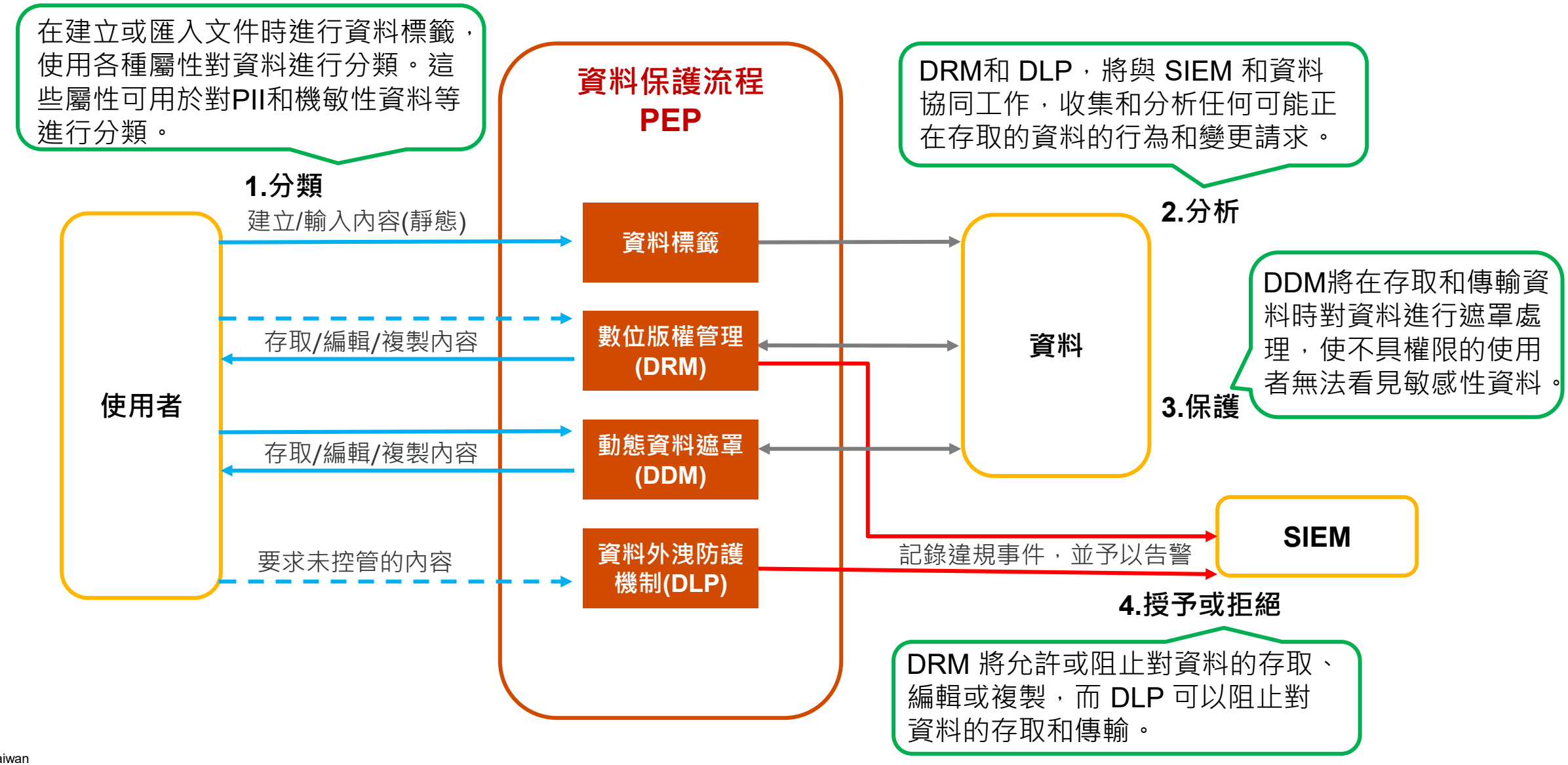
情境一：理專查詢高資產客戶資料

- 查詢過程中只有被授權的欄位會解密顯示，其他保持加密
- 若嘗試下載整批未授權資料 → 系統封鎖並通報 SIEM

情境二：API 傳輸報表資料給第三方機構

- 資料在 API 傳輸過程中啟用 TLS，防止中間人攻擊
- 記錄所有傳輸事件並進行風險分析

資料支柱之應用-資料保護參考流程(釋例)



資料支柱之應用-資料保護參考流程(釋例)

資料保護流程介紹

- **資料標籤(Data Tagging)**：在資料建立或匯入時，使用屬性對文件進行標籤分類，Ex: 機密程度。
- **資料權限管理(Data Right Management)**：根據使用者的權限，監控資料訪問、編輯、複製。
- **動態資料遮蔽(Dynamic Data Masking)**：授予敏感資料訪問權限時，DDM即時隱藏特定資料欄位。
- **資料外洩防護(Data Loss Protection)**：處理敏感性資料的移動或異動之阻擋。

運作方式

1. DRM、DLP監控資料的訪問與變更，並將異常狀況回報SIEM；透過SIEM彙總與分析異常狀況，並予以告警。
2. 透過PEP管控存取，由SIEM監測可疑活動，SOAR即時回報異常。

應用場景：員工誤將投資報表寄至私人信箱

• 資料外洩防護(DLP) 偵測到報表含機密標記，自動封鎖信件傳送

• 同步記錄事件、警示資安人員

資料支柱之應用-動態資料遮蔽(Dynamic Data Masking)(釋例)

動態資料遮蔽

(Dynamic Data Masking)

功能

動態資料遮罩可藉由遮罩處理，使不具權限的使用者無法看見敏感性資料。

優勢

增強的安全性：保護敏感資料免遭未經授權的訪問，同時仍允許必要的資料使用。合規性：幫助組織遵守資料保護法規，確保敏感資訊不會被不必要地洩漏。

案例

開發和測試：允許開發人員和測試人員處理真實資料，而不會洩露敏感資訊。

資料共享：在保護敏感資料的同時，促進與第三方的安全資料共享。

加密

使用加密演算法來加密敏感資料，並且只有具有解密金鑰的授權使用者才能存取原始資料

重排

隨機重排資料欄的資料，使個別記錄無法辨識並用於保留資料內的關係

Postcode		Postcode
SW1 1AA	->	AS1W1A
LS3 5UB	->	S5BL3U
W3 4RT	->	4WR3T
B11 6PA	->	6PB1A1

替代

替代遮罩涉及用類似但虛構的資料來取代敏感資料，如:使用預先定義清單中的名稱來取代實際名稱

Name		Name
Alice	->	Bmjdf
Bob	->	Cpc
Carol	->	Dbspm
Carlos	->	Dbsmpt

字符化

用隨機產生的字符或參考值來取代正式資料，從而保持資料完整性，並將敏感資訊公開的風險降至最低

Credit Card		Credit Card
1234-2234-3234-4234	->	XXXX-XXXX-XXXX-4234

2

零信任架構導入常見問題-資料保護

零信任架構導入常見問題一覽表-資料保護(1/3)

PwC 整理常見導入零信任架構之資料保護時，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
如何平衡資料保護和員工工作效率?有些部門反映DLP政策過於嚴格影響工作	建議採用分級分類的DLP政策，根據資料敏感度和業務需求制定不同級別的規則。同時，可以考慮實施自適應DLP，根據用戶行為和風險評分動態調整政策嚴格度。
監控資料存取是否只需要收集存取日誌即可？	單純收集日誌只能事後稽核，無法達成「即時防護」，零信任即時可視性與動態授權調整 例如：當使用者的存取行為異常時（如短時間內大量下載、跨國登入、非上班時段匯出資料），必須立即採取限制措施。 建議可包含以下幾個關鍵面向： 1.將存取日誌整合至 SIEM / UEBA，即時進行異常行為分析。 2.對於高風險行為，觸發動態授權（例如自動降低權限、要求 MFA 或暫時阻斷存取）。 3.建立即時告警與 SOC 回應流程，確保異常事件能被快速處理，而不是事後才發現。

零信任架構導入常見問題一覽表-資料保護(2/3)

PwC 整理常見導入零信任架構之資料保護時，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
公司已經有人員進行資料盤點，為什麼仍然很難落實最小授權?	單純依靠人工盤點，資料分類往往不完整或無法即時更新，導致授權政策失真。 例如，某些檔案雖屬敏感，但因未標註而被錯誤開放存取。這會讓「最小授權」流於形式。 建議可包含以下幾個關鍵面向： 1.導入自動化資料發現工具（Data Discovery / Classification），持續掃描資料庫、檔案伺服器、雲端存放區。 2.針對資料加上標籤（Tagging / Metadata），並與 IAM/RBAC/ABAC 政策綁定，確保授權精準。 3.建立持續更新的資料目錄（Data Catalog），確保新產生的資料也能即時分類分級，避免落空。

零信任架構導入常見問題一覽表-資料保護(3/3)

PwC 整理常見導入零信任架構之資料保護時，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
資料可用性，在備份作業上有什麼建議?	建議可包含以下作法： 實施 3-2-1 備份原則：至少三份備份、儲存在二種不同媒介，其中一份異地或離線保存。 部署不可變備份（Immutable Backup） 或 WORM（Write Once Read Many）技術，避免被竄改。 定期演練災難復原（DR Drill），確保在異常事件發生時能快速恢復服務。 納入零信任流程，限制誰可以存取備份系統，並要求 MFA + 行為監控，避免惡意刪除或誤操作。

Q & A

pwc.tw