pwc 資誠

推動證券商導入金融零信任說明會

-應用程式保護

資誠智能風險諮詢管理有限公司

2025.8

Agenda

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

1

實作參考原則分級解析-應用程式保護

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

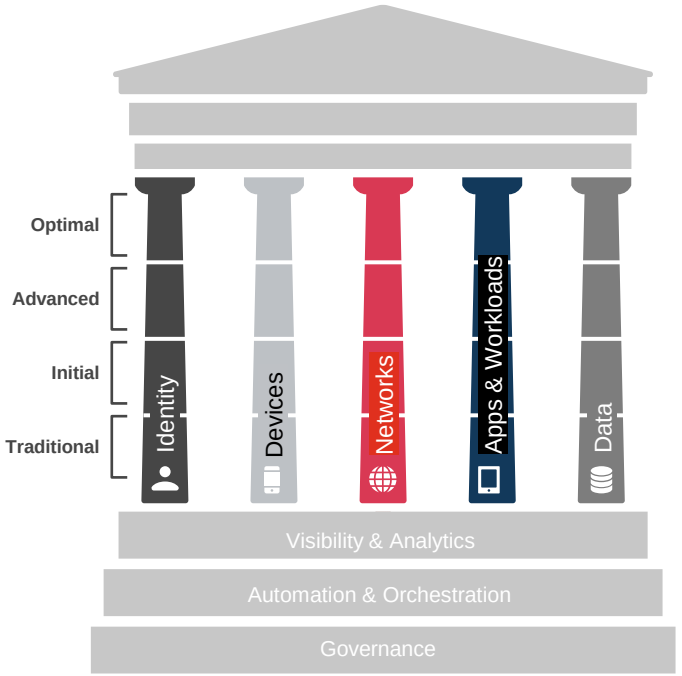
等級 IV

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

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）

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（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）

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

4. 應用程式

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

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

1. 身分
2. 設備
3. 網路
4. 應用程式
5. 資料

I 靜態指標

- **4-1 存取授權**：以作業屬性及風險區隔角色，並依角色風險等級定義授權條件(如身分及設備鑑別之等級)，採最小授權原則定義授權範圍；並針對特權作業採獨立角色授權(不混用於非特權作業)，減少特權帳號之濫用及風險。

II 動態指標

- **4-2 存取授權**：可將帳號動態屬性(如MFA強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。
- **4-4 程式安全**：從網際網路及防護邊界內部對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放經Internet存取之防護能力。
- **4-5 程式部署**：為應用程式開發、測試及部署建立持續整合及部署(CI/CD)通道，分階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行落實權責分離。

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，並可依據使用者行為或使用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。
- **4-6 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

- **4-7 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，確保於應用程式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

4-1 存取授權

以作業屬性及風險區隔角色，並依**角色**風險等級定義授權條件(如身分及設備鑑別之等級)，採**最小授權原則**定義授權範圍；並針對**特權作業採獨立角色授權**(不混用於非特權作業)，減少特權帳號之濫用及風險。

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

<u>角色為基礎的控制(RBAC)</u>

- 授予角色相應的適當授權
- 給予工作所需最低權限

<u>角色作業屬性類型</u>

- 使用者屬性：功能或職位（Ex: ”經理”、”工程師”、”實習生”）
- 部門：所在部門單位（ Ex: ”財務”、”人資”、”IT”）

風險級別
- 高風險
- 中風險
- 低風險

➡ **僅授權使用者職責所需之必要權限**

➡ **特權作業獨立管理，且可採用「臨時特權」**

金融業導入零信任架構參考指引-實作參考原則

4-2 存取授權

可將帳號動態**屬性**(如 **MFA 強度**、**設備合規**、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)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

MFA(多重要素驗證)強度範例

- 低強度MFA：簡單密碼+電子郵件驗證
- 高強度MFA：FIDO+動態密碼

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

設備合規範例

- 符合政策的系統與防毒軟體
- 設備已掃描並修補

合規性檢測

- 確保設備符合安全和管理標準(包括設置、軟體版本、病毒碼規範等)

弱點管制

- 能檢查設備是否更新或有無資安漏洞

監控不合規設備

- 能執行風險控制措施(如強制更新、修補漏洞、即時警告)

金融業導入零信任架構參考指引-實作參考原則

	角色為基礎的控制(RBAC)	屬性為基礎的控制(ABAC)	風險為適應的控制
定義	依照角色設定相應的授權，給予工作所需最低權限	對執行操作的請求根據其屬性或、環境條件，並根據這些屬性和條件讓存取權限隨變化動態進行授予或拒絕。	基於使用者身分、請求以及被存取系統與使用者之間存在的安全風險等級等因素。將使用安全指標（如身分驗證方法的強度、系統與使用者之間連線的保護等級以及使用者的實體位置）來進行風險評估
指標	*I* 靜態指標	*II* 動態指標	*II* 動態指標
技術機制	基於角色，授予使用者一組明確定義的能力或權限	基於使用者屬性，能更精細授予使用者一組權限	使用AI或機器學習，可以檢測異常情況，動態調整安全策略，並確保僅在符合安全政策時，才授予存取權限
優勢	管理使用者權限相對簡單	能依照屬性特徵，更靈活性、精細地管理存取控制	具持續性監控及自動化管理，根據不斷變化的用戶行為、網路狀況和設備運行狀況動態調整安全策略
適用場域	所有企業	需求高度安全的環境，如金融、醫療或跨組織等敏感資料系統	需要靈活配置、並依環境變化調整權限的企業或系統

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，下列何者為特權帳號管理的正確做法？

選項A

特權帳號可與一般帳號混用以簡化作業流程

X 不適用

選項B

所有帳號皆具備同等權限，避免混淆

X 不適用

選項C

特權帳號應獨立授權且與非特權帳號分離

✓ **特權帳號應有獨立角色授權(不混用於非特權作業)**

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，下列哪一項可落實 Just-in-Time Access 控制的做法？

選項A

帳號長期開通

→ ✗ 不適用

選項B

將帳號密碼記錄在記事本中以便快速啟用

→ ✗ 不適用

選項C

採即時授權、回收的存取方式，每次使用前需申請、審核並限定使用時段

→ ✓ **只在需要時開啟，且僅開啟最小權限與最短時間所需連線**

金融業導入零信任架構參考指引-實作參考原則

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，並可依據**使用者行為或使用模式**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。

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

偵測回應機制

- **功能**：即時監控**應用程式活動紀錄**，偵測並回應潛在威脅
- **操作**：發現異常活動時，
  - (1) 發出告警
  - (2) 發出事件單
  - (3) 限縮存取
  - (4) 消除橫向移動

金融業導入零信任架構參考指引–問答

Question:
零信任威脅防護強調「應用程式活動紀錄」下列哪種機制能協助評估？

選項A

雲端資料儲存同步

→ ✗ 不適用

選項B

使用者行為分析(UEBA)

→ ✓ 可評估使用者或應用程式，是否違反了任何原則或行為

選項C

VPN log下載

→ ✗ 不適用

金融業導入零信任架構參考指引–問答

Question:
根據零信任威脅防護，當使用者出現異常操作模式時，建議可以如何應對？

選項A

提升該帳號權限，以利調查

→ ✗ 不適用

選項B

自動封鎖所有其他使用者

→ ✗ 不適用

選項C

產生告警並觸發事件回應流程

→ ✓ **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

4-4 程式安全

從網際網路及防護邊界內部對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放經Internet 存取之防護能力。

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

資安檢測方法：

- **源碼(程式碼)檢測**：分析程式碼以找出潛在安全漏洞
- **弱點掃描**：檢查應用程式漏洞
- **滲透測試**：模擬攻擊行為，檢測應用程式防禦能力

➡ **進行內部、外部(網路)資安檢測，增加應用程式安全性**

金融業導入零信任架構參考指引–問答

Question:
根據程式安全防護原則，強化應用程式的資安防護建議採取哪項措施？

選項A

儲存帳號密碼於應用程式代碼中

→ X 不適用

選項B

只使用內部測試即可上線

→ X 不適用

選項C

定期實施弱點掃描與滲透測試

→ ✓ 適用

金融業導入零信任架構參考指引-實作參考原則

4-5 程式部署

為應用程式開發、測試及部署建立持續整合及部署(CI/CD) 通道，分階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行落實權責分離。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

CI/CD通道

- **持續整合(CI)**：開發人員完成階段性程式碼開發後，提交至版本控制系統，提交後觸發 Pipeline (工作排程)之執行；針對最新程式碼進行編譯及封裝；進行自動化測試及程式碼規範檢查。
- **持續部署(CD)**：透過工具自動交付，最後由人工進行部署，或者自動化進行部署至開發/測試/正式環境。

指引的融通(或由不同團隊執行落實權責分離)

- **最小授權原則**：僅授權必要人員可作業權限

金融業導入零信任架構參考指引-問答

Question:
在 CI/CD 流程中，下列哪一項屬於最佳實踐？

選項A
評估採自動化機制並採最小授權進行權責分離

✓ 不適用

選項B
單人部署並具有全部權限

✗ 不適用

選項C
由開發者直接部署至正式環境

✗ 不適用

金融業導入零信任架構參考指引-實作參考原則

4-6 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、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–問答

Question:
應用程式可視性分析中，指引建議整合哪些安全系統

選項A

SIEM

→ 適用

選項B

SOC

→ 適用

金融業導入零信任架構參考指引-實作參考原則

4-7 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，確保於應用程式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	•手動設置應用程式系統的位置和存取權限，以及有限的維護與審查機制
最佳化	**•全面自動化應用程式配置，持續優化以符合安全和效能需 ***持續整合(CI)/持續部署(CD)、 {建議}執行期間應用系統自我防護RASP Runtime Application Self-Protection**

2

零信任架構導入常見問題-應用程式保護

零信任架構導入常見問題一覽表-應用程式保護(1/2)

PwC 整理常見導入零信任架構之應用程式保護時，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
針對特權作業採獨立角色授權(不混用於非特權作業)的定義是什麼?	• 指應用程式中具有高風險或敏感性的操作功能（如帳號管理、權限變更等），必須設定專門的角色來執行，且不得讓該角色同時具備一般使用者功能，以確保職責區隔、風險可控與行為可稽核。
目前沒有導入特權管理工具，針對特權作業採即時存取(Just-in-Time Access)機制和即時告警，在推動上有什麼建議落實措施？	旨在尚未導入特權管理工具前，首先建議 基本控管與現況盤點 • 盤點應用程式中涉及特權操作的帳號與功能。 • 拆分特權與一般操作權限，落實基本最小權限原則（RBAC）。 • 避免使用常態性高權限帳號。 接者：導入 Just-in-Time 存取與即時告警 • 建立權限申請與核准流程，提供限時授權（如 15 分鐘～1 小時，可視風險情況而定）。 • 使用腳本或流程工具，自動控制帳號啟用與失效。 • 特權操作時發出即時通知與告警。

零信任架構導入常見問題一覽表-應用程式保護(2/2)

PwC 整理常見導入零信任架構之應用程式保護時，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
如何將AP日誌整合分析並具有即時回應機制？	可優先逐步將日誌格式標準化，接者將日誌集中化收容，最後整合分析、建立行為分析基線；可先以 SIEM 建立基礎行為基線，再逐步導入 UEBA（User & Entity Behavior Analytics）工具，透過 Log 或 API 呼叫與應用整合，發現異常行為即觸發權限降級或阻斷。
只要有部署向GitLab、Jenkins等工具，是否就算有達到CI/CD的要求嗎? **針對CI/CD的自動化的部署有那些關鍵考量因素?**	達到 CI/CD 要求，應包含以下幾個關鍵面向： 1. 自動建置與測試流程：當開發人員提交程式碼時，系統會自動觸發建置與各階段測試（單元測試、整合測試等），若測試失敗則中止部署。 2. 環境隔離與變更控管：不同部署環境（如 dev、staging、prod）必須有明確隔離，並透過版本控制系統（如 Git）進行變更管理與審核。 3. 自動部署與回滾機制：部署流程應能自動完成，並具備異常處理與回滾功能，確保系統穩定性與可恢復性。 4. 權限與審查制度：重要部署應由受信任人員審核，並採取最小權限原則避免人為錯誤或資安風險。 5. 安全與稽核整合：整合憑證管理、弱點掃描、行為記錄等資安控制，確保部署流程安全可追蹤。

Q & A

pwc.tw