附表：零信任架構實作參考原則分級表

項次	支柱	功能	原則	等級
1.1	身分	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。	Ⅰ
1.2	身分	身分認證	採用包含綁定實體載具(如 FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對 APP 等，排除簡訊、語音及電子郵件 OTP)的多因子驗證機制，可抗網路釣魚風險。	Ⅱ
1.3	身分	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)	Ⅰ
1.4	身分	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)	Ⅰ
1.5	身分	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。	Ⅱ
1.6	身分	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)	Ⅲ
1.7	身分	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。	Ⅳ

項次	支柱	功能	原則	等級
2.1	設備	設備合規	具有效盤點且可唯一識別(如 TPM 等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。	Ⅰ
2.2	設備	設備合規	具納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。	Ⅱ
2.3	設備	供應鏈風險	對外部設備(如 BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之合規中繼閘道(如 VDI 等)存取。	Ⅰ
2.4	設備	資源存取	可將設備之動態屬性(如是否納管及合規、設備位址、或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼閘道(如 VDI 等)存取。	Ⅱ
2.5	設備	威脅防護	對設備活動紀錄具有即時偵測及回應機制(EDR)，在偵測到威脅指標(IOC)時，可自動隔離或即時應處(如發出事件單即時追蹤處置)。	Ⅲ
2.6	設備	可視化分析	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)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
2.7	設備	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，確保於設備生命週期之安全性及合規性。	Ⅳ

項次	支柱	功能	原則	等級
3.1	網路	網路區隔	具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。	Ⅰ
3.2	網路	網路區隔	具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。	Ⅱ
3.3	網路	流量管理	呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。	II
3.4	網路	流量加密	於資源存取路徑之資料傳輸加密(如採 https 等加密協定)。	Ⅰ
3.5	網路	網路韌性	對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。	Ⅲ
3.6	網路	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)進行即時的判斷與回應(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
3.7	網路	自動化治理	具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。	Ⅳ

項次	支柱	功能	原則	等級
4.1	應用程式	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
4.2	應用程式	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。	Ⅱ
4.3	應用程式	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。	Ⅲ
4.4	應用程式	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。	Ⅱ
4.5	應用程式	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。	Ⅱ
4.6	應用程式	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)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
4.7	應用程式	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。	Ⅳ

項次	支柱	功能	原則	等級
5.1	資料	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
5.2	資料	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。	Ⅲ
5.2	資料	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
5.3	資料	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
5.4	資料	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。	Ⅱ
5.5	資料	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
5.6	資料	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)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
5.7	資料	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。	Ⅳ