金融證券商零信任導入後續規劃及步驟說明

一月 2025

pwc

Agenda

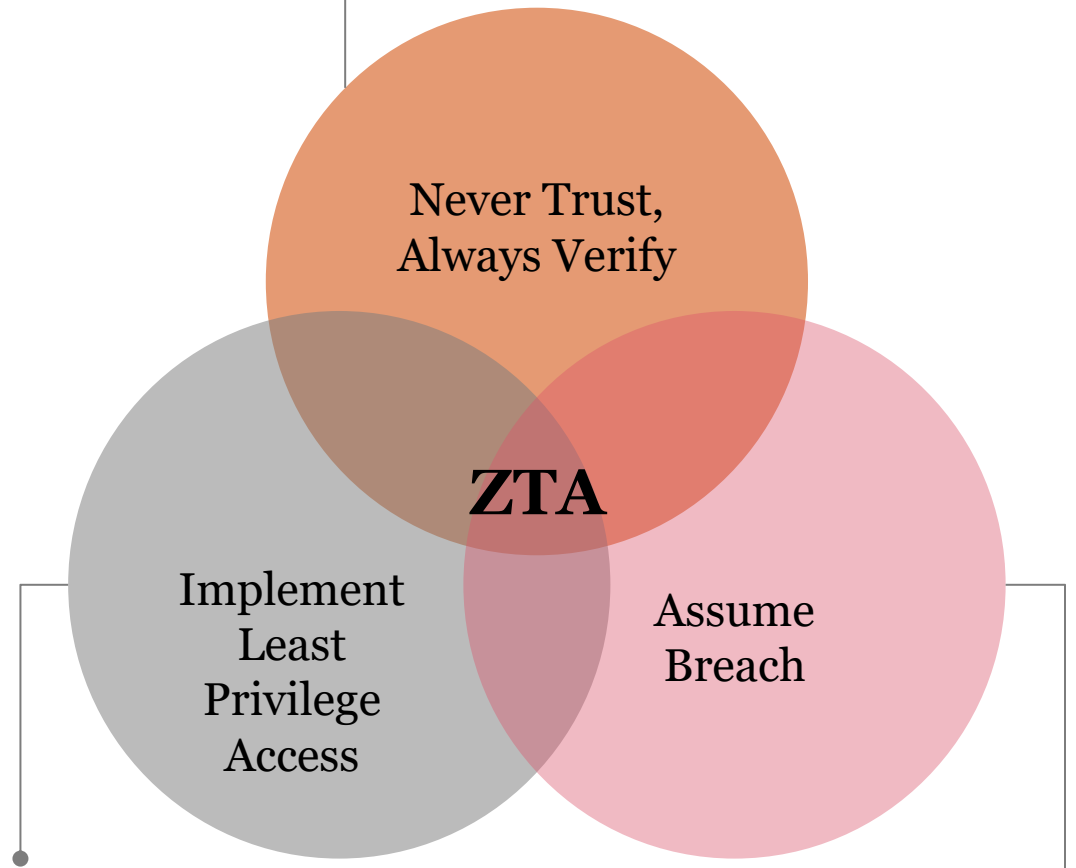
1. 零信任簡介
2. 零信任六大場域說明
3. 後續時程規劃
4. 問題與討論

1

零信任簡介

探索零信任架構

零信任架構是企業的網路安全計劃，其當中概念包含元件關係、工作流程規劃和存取策略。

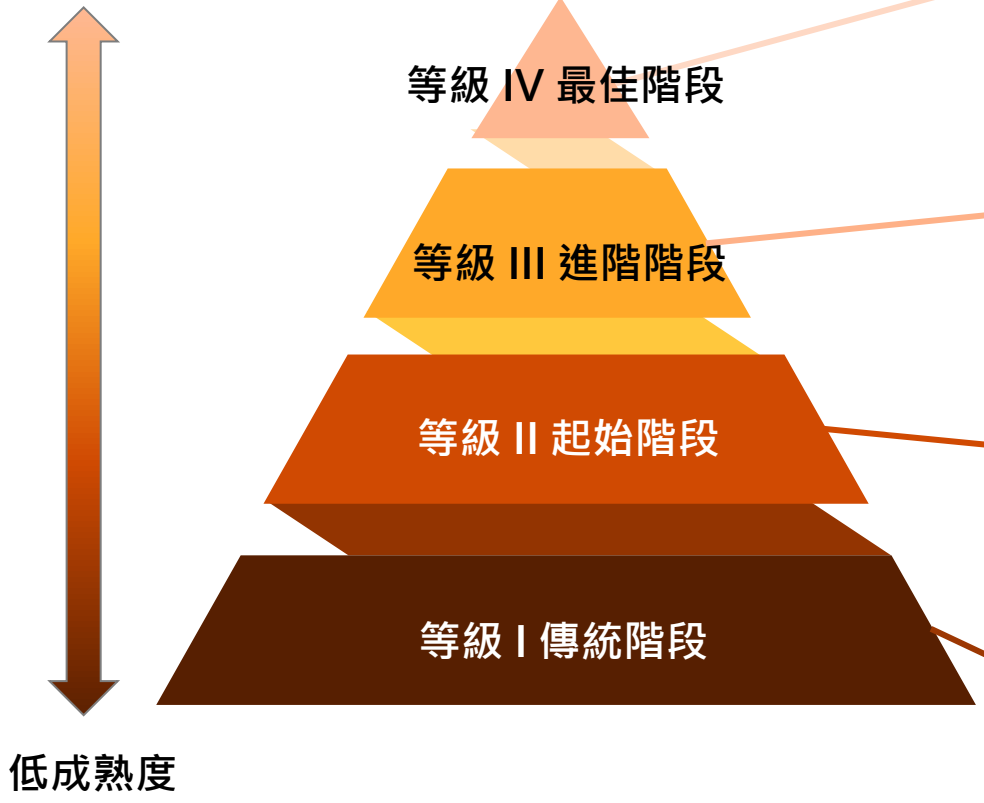


要求組織驗證每個使用者的身份並持續監控使用者行為是否有惡意活動

使用者和設備僅被授予執行任務所需的權限

透過假設資料外洩已經發生，ZTA 為最壞的情況做好準備，並在攻擊確實發生時相應地保護敏感資料

零信任架構實作參考原則分級 – 等級



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。

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。

零信任架構實作參考原則分級 – 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

2

零信任六大場域說明

擇高風險場域先行實作零信任架構

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。

舉例

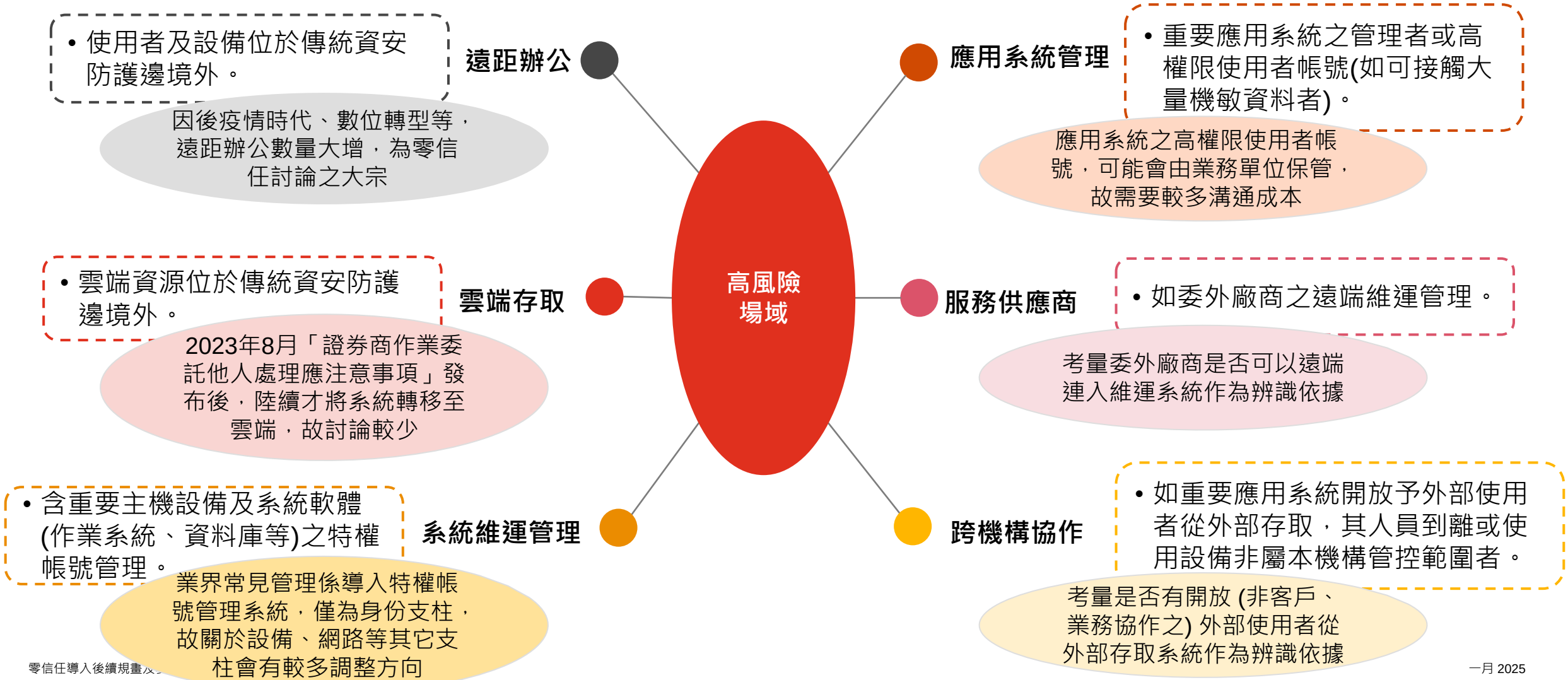
- **存有高度資安風險**
  - 有客戶或員工個資
  - 存有客戶交易資料

高風險

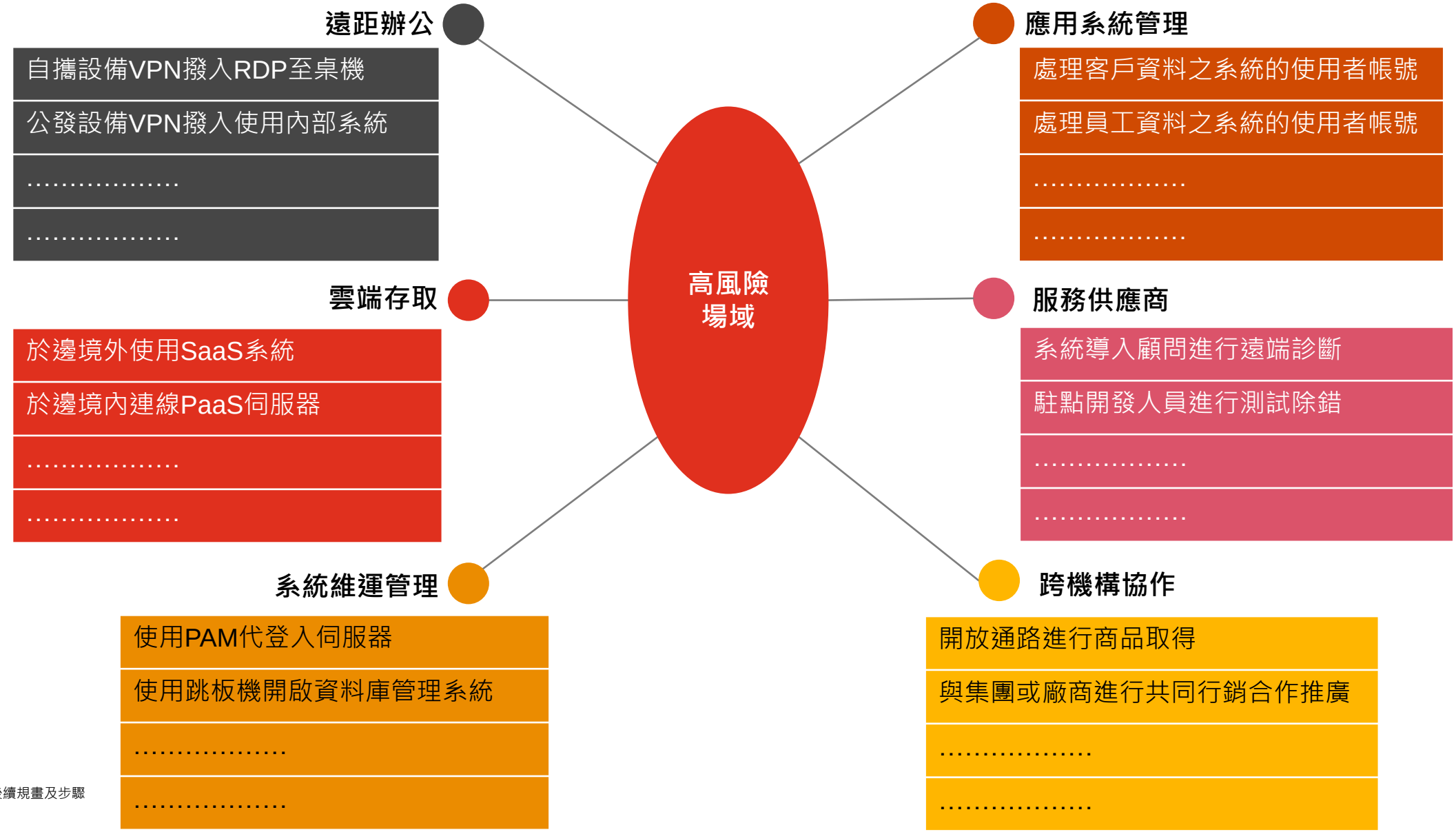
- **對營運的衝擊小**
  - 屬於非自動化提供客戶服務
  - RTO超過8小時
  - 授權機制為集中管理

低衝擊

導入零信任架構參考指引之六大場域



高風險場域情境挑選範例



3

後續時程規劃

先行機構導入分享研討會與說明會介紹

先行機構零信任架構導入分享研討會

- 邀請證交所於2024年挑選之導入零信任先行示範單位，將零信任架構導入經驗與其他證券商分享。

零信任架構參考指引解析說明會

依據金管會發布之「金融業導入零信任架構參考指引」內容，針對零信任架構框架概念、導入策略、零信任架構實作建議實作參考原則分級進行說明。

落實零信任系列說明會

根據五大支柱共36個參考原則，分享導入實務及案例，並提供導入零信任架構相關諮詢常見問題及解決方向。

落實零信任系列說明會 – 各場主題

身分

- 身分認證
- 身分互通
- 權限存取
- 可視性分析
- 自動化治理

設備

- 設備合規
- 供應鏈風險
- 資源存取
- 威脅防護
- 可視化分析
- 自動化治理

網路

- 網路區隔
- 流量管理
- 流量加密
- 網路韌性
- 可視化分析
- 自動化治理

應用程式

- 存取授權
- 威脅防護
- 程式安全
- 程式部署
- 可視化分析
- 自動化治理

資料

- 外洩防護
- 資料分類
- 資料可用性
- 資料存取
- 資料加密
- 可視化分析
- 自動化治理

零信任架構導入進度調查問卷

- 預計於3月寄發「零信任架構導入進度調查問卷」，並於4月回收，以了解各證券業者零信任架構導入之現況。
- 「零信任架構導入進度調查問卷」預計將會以「零信任架構實作參考原則分級表」為主題，區分不同支柱及等級的問題。

調查問卷及說明會時程

三月

寄發「零信任架構導入進度調查問卷」

四月

1. 回收「零信任架構導入進度調查問卷」
2. 零信任架構參考指引解析說明會

五月

落實零信任系列說明會
第一場 身分

六月

落實零信任系列說明會
第二場 設備

七月

1. 落實零信任系列說明會 第三場 網路
2. 先行機構零信任架構導入分享研討會 第二場

八月

落實零信任系列說明會
第四場
應用程式

九月

落實零信任系列說明會
第五場 資料

4

問題與討論

Thank you

pwc.com