保險業資訊作業專案檢查

主要檢查缺失態樣

金融監督管理委員會檢查局

目錄

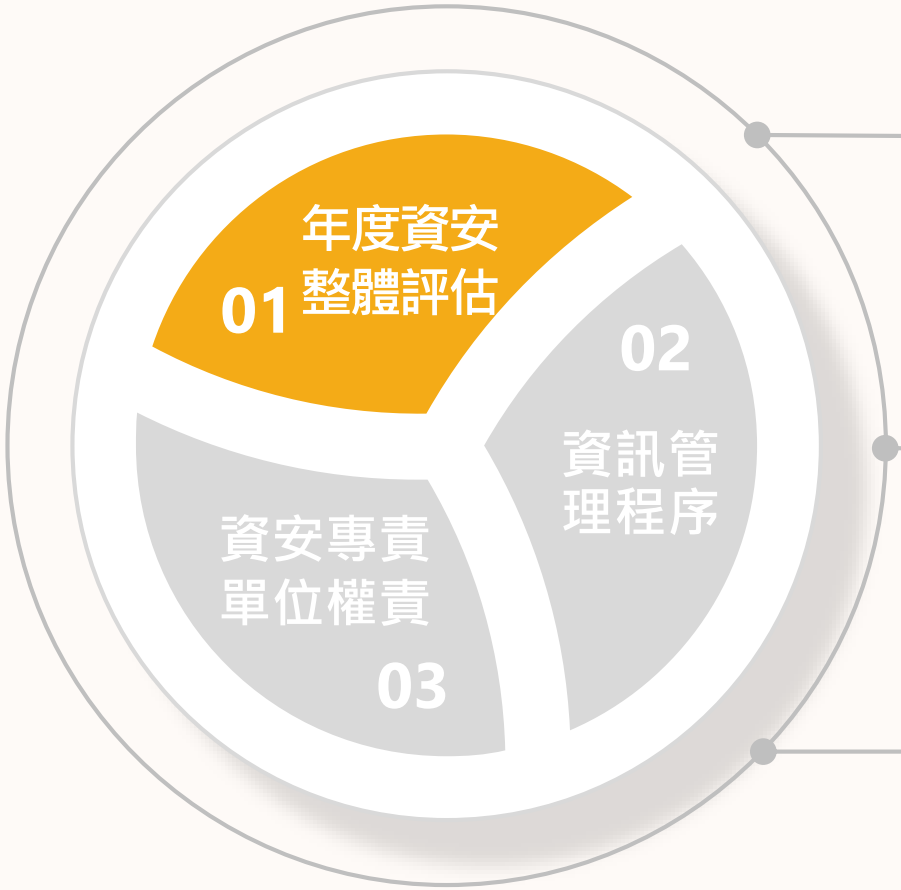
資安治理

1.資安整體執行情形報告
2.電腦系統資訊安全評估

1.資訊安全政策
2.整體資安管理作業程序

1.員額、資歷
2.與資訊單位的分工
3.資安單位權責發揮

資安治理



1.資安整體執行情形報告
2.電腦系統資訊安全評估

資安整體執行情形之報告內容
(「保險業內部控制及稽核制度實施辦法」第6條第10款、第11款及第13款所定防範機制與復原或備援計畫等執行情形，及相關同業公會所定資訊安全規範之遵循情形)

資安治理

1.資安整體執行情形報告
2.電腦系統資訊安全評估

策
理作業程序

的分工
責發揮

電腦系統資訊安全評估作業欠落實

1.電腦系統分類 (重要性及風險程度)
2.評估範圍完整度
3.檢視報告完整性與正確性之落實度
4.評估報告發現事項之後續處理情形
(含送稽核追蹤、改善及覆查落實度)
5.文件保留完整性

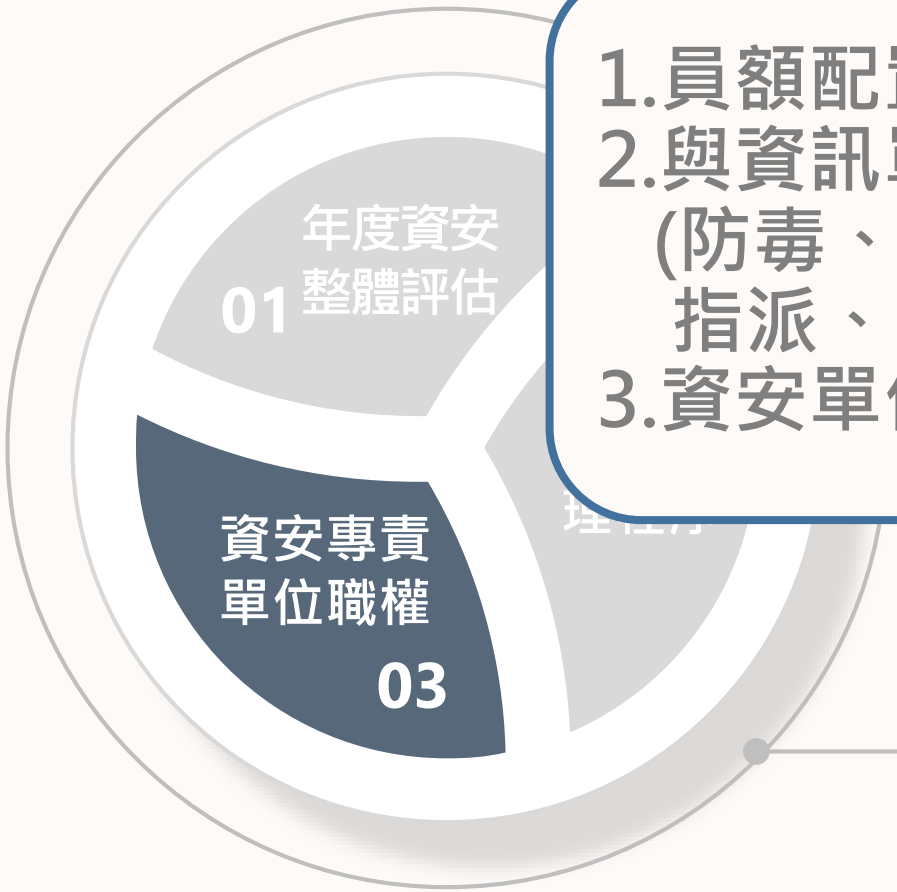
資安治理

1.資安整體執行情形報告
2.電腦系統資訊安全評估

1.資訊安全政策
2.整體資安管理作業程序

1.資安政策核定層級欠妥
2.規範適用範圍欠完整、標準不一致
3.資安事件分級及通報與應變程序欠妥
4.資安專責單位於資安事件通報及應變處理、原始碼掃描等相關程序，尚無權責角色，不利其職責之發揮

資安治理



1.員額配置、資歷欠妥
2.與資訊單位的分工欠妥
(防毒、應用系統使用者權限
指派、個人電腦端點設備管控)
3.資安單位職能未能妥適發揮

整體執行情形報告
系統資訊安全評估

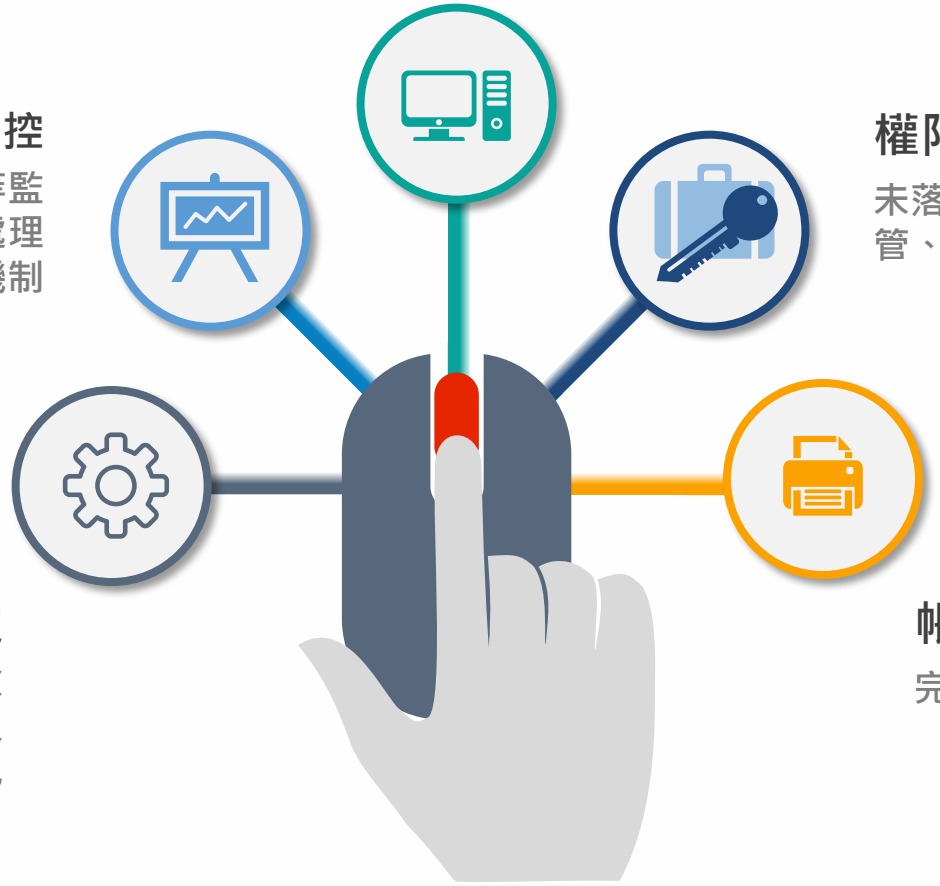
安全政策
資安管理作業程序

1.員額、資歷
2.與資訊單位的分工
3.資安單位職能發揮

主機安全管理

作業系統(含資料庫更新)

未有定期評估及更新機制



主機效能監控

未訂定 cpu、 disk 、memory 等監控指標，未建立告警及後續追蹤處理機制

權限管理

未落實最小授權、特權帳號未回收納管、未建立申請使用及覆核機制

主機安裝及設定

未建立妥適之主機設定參數檢核表(含安裝版本、安全參數及服務啟用等)，且未定期檢視

帳號及權限清查

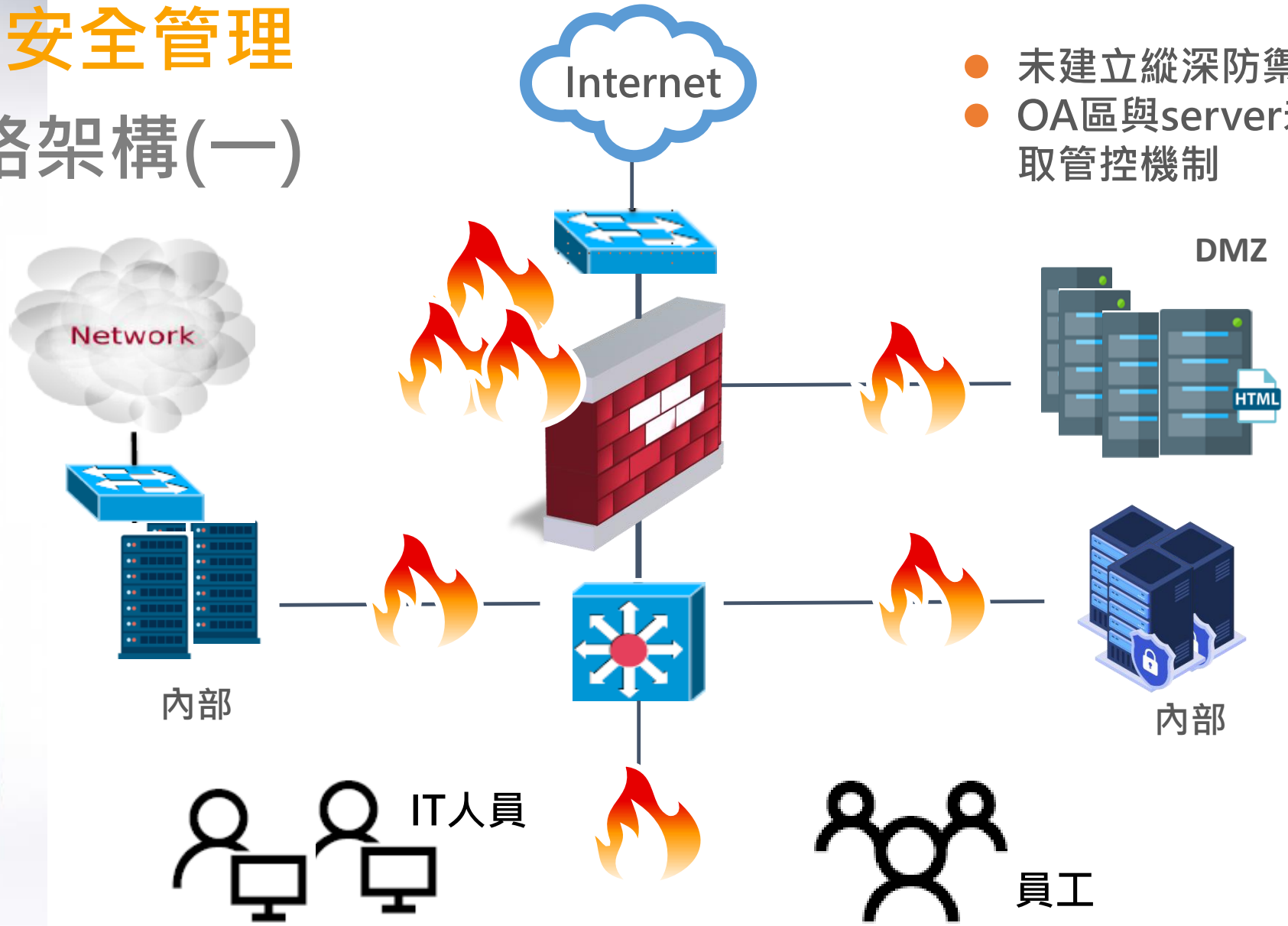
完整性欠妥、未落實權限清查

網路安全管理

1. 網路架構(一)
2. 網路架構(二)
3. 防火牆管理
4. 弱點掃描
5. 滲透測試
6. SIEM
7. 外部遠端連線管理
8. 正式主機連線管理

網路安全管理

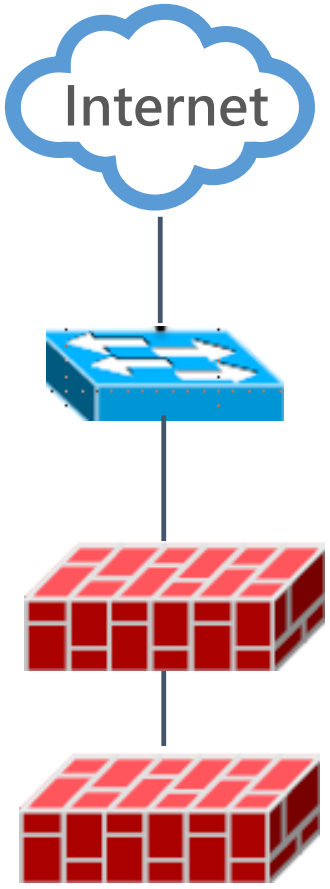
網路架構(一)



- 未建立縱深防禦機制
- OA區與server未有存取管控機制

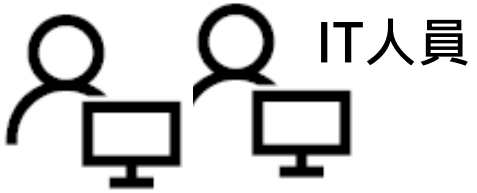
網路安全管理

網路架構(二)



- 主機未依伺服器業務特性(保險業務類或行政管理類)區隔管理
- 正式機與測試機同一網段
- 正式營運主機與辦公區同一網段
- 有系統建置於DMZ區，未妥適評估資安風險及其必要性
- 資料庫建置於DMZ區

伺服器



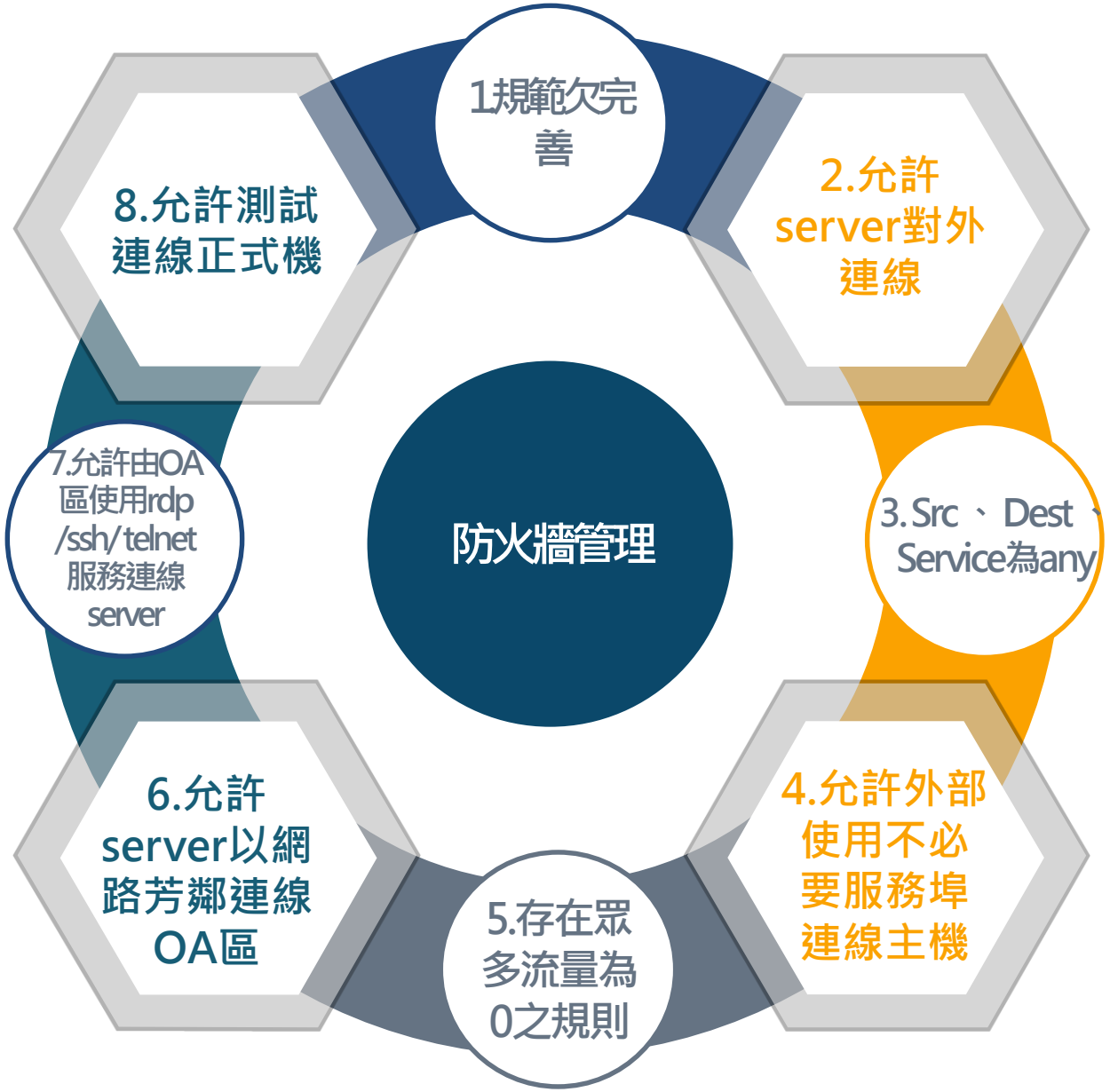
IT人員

員工

網路安全管理

個人資料保護

資安風險



規範：應定義高風險規則，洽會資安單位審核條件，定期檢視

最小授權原則，落實檢視

網路安全管理

弱點掃描

- 規範欠完整：週期、範圍、修補時程、追蹤管控修補機制及陳核層級
- 掃描範圍未全面涵蓋所有伺服器
- 僅對高風險以上弱點進行修補，後續追蹤管控欠妥
- 對暫不修補弱點之補償措施及管控機制不足
- 白名單審查機制欠妥

滲透測試

- 規範欠完整：週期、範圍、修補時程、追蹤管控修補機制及陳核層級
- 檢測範圍未全面涵蓋對外開放any連線之伺服器
- 僅對高風險以上弱點進行修補，後續追蹤管控欠妥
- 對暫不修補弱點之補償措施及管控機制不足

SIEM

- 規範欠完整：未規定範圍、監控態樣及告警機制、追蹤管控程序
- 日誌蒐集及監控態樣範圍不足
- 發生事件，未有即時告警及後續追蹤處理機制

外部遠端連線管理

- 規範欠完整：未規定依職務角色規範授權範圍、未建立後續覆核程序
- 身分驗證機制不足，僅以固定帳密進行驗證
- 未限制資料上下載
- 未留存操作行為軌跡

正式主機連線管理

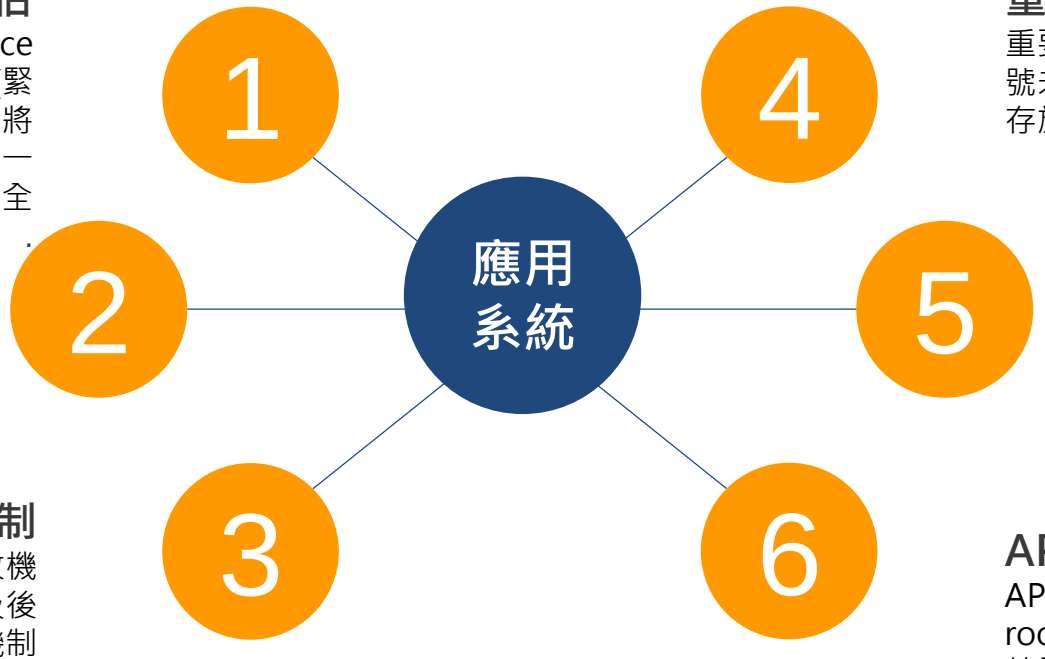
- 未於安全環境下，連線正式營運環境(如辦公區可連線網路環境)
- 身分驗證機制不足，僅以辦公室日常使用之固定帳密進行驗證
- 未限制資料上下載
- 未留存操作行為軌跡

電子商務系統安全管理

系統建置風險評估
風險評估作業欠妥，未包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)，且有未依功能需求不同，將提供內部及外部人員使用功能，設計為同一套系統，不利資訊安全

測試及安全檢測作業
應用系統測試欠落實 ，程式安全檢測對弱點修補作業欠妥，含例外管理及補償措施。

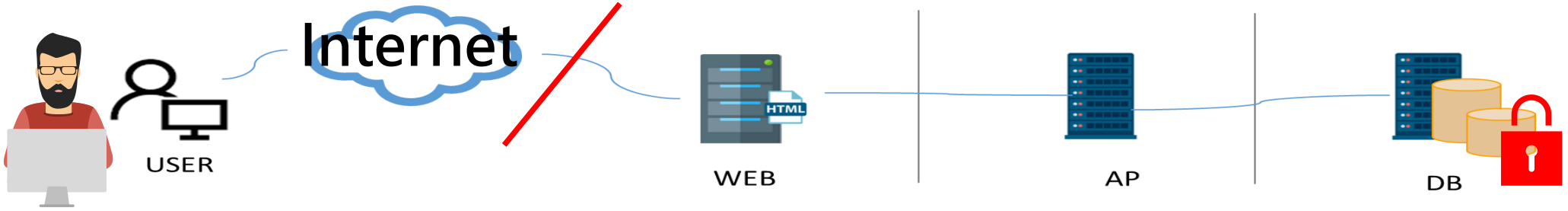
網站及APP安全監控機制
未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制



重要資料保護機制
重要資料如信用卡號有效年月及銀行帳號未加密存放；連線資料庫使用之密碼存放於DMZ區且明碼存放

個資應用安全設計
由外部連線應用系統可查詢大量個資，僅以固定帳密進行管控，提供對外服務網站之資料顯示涉及個人資料，未評估妥適隱碼

APP安全設計
APP設計及檢測作業欠妥，未偵測root ，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視



Fsc

電子商務系統安全管理

系統建置風險評估

風險評估作業欠妥，未包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)，且有未依功能需求不同，將提供內部及外部人員使用功能，設計為同一套系統，不利資訊安全

測試及安全檢測作業

應用系統測試欠落實，程式安全檢測對弱點修補作業欠妥，含例外管理及補償措施。

網站及APP安全監控機制

未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制

1

新系統建置，風險評估作業欠妥，應包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)；另有未依功能需求不同，將提供內部及外部人員使用功能，設計為同一套系統之情形，不利資訊安全

2

3

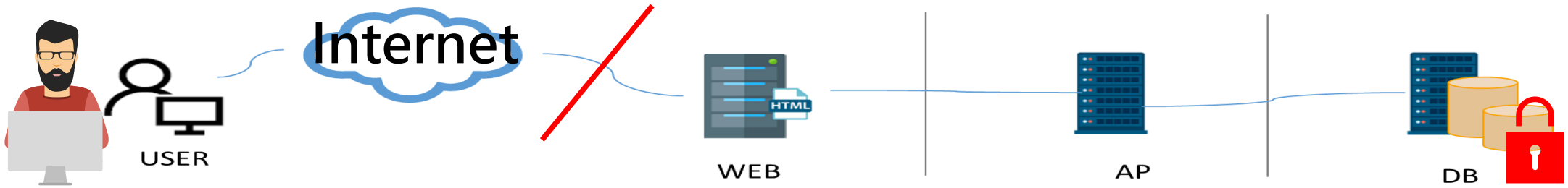
6

帳
碼

詢大量個資，
提供對外服務
資料，未評估

APP安全設計

APP設計及檢測作業欠妥，未偵測root，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視



電子商務系統安全管理

系統建置風險評估
風險評估作業欠妥，未包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)，且有未依功能需求不同，將提供內部及外部人員使用功能，設計為同一套系統，不利資訊安全

測試及安全檢測作業
應用系統測試欠落實，程式安全檢測對弱點修補作業欠妥，含例外管理及補償措施及後續追蹤管理

網站及APP安全監控機制
未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制

1

2

3

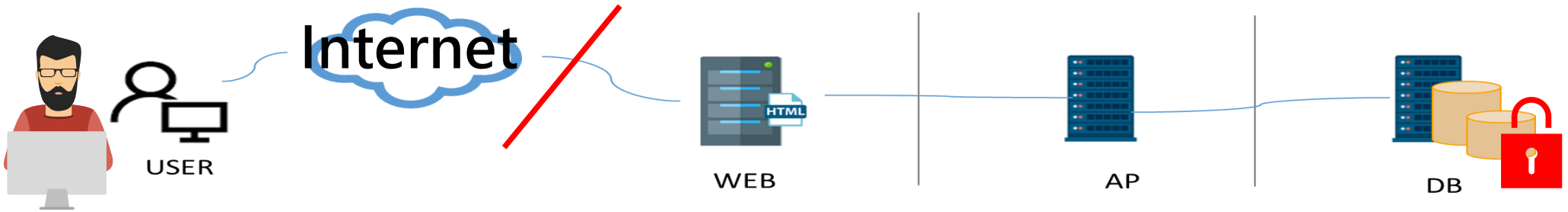
6

應用系統測試欠落實，對程式原始碼安全檢測所發現弱點修補作業亦欠妥，含例外管理、補償措施及後續追蹤管理

重要資料保護機制
重要資料如信用卡號有效年月及銀行帳[illegible]之密碼

設計
可查詢大量個資，[illegible]控，提供對外服務網站之資料類未涉及個人資料，未評估妥適隱碼

APP安全設計
APP設計及檢測作業欠妥，未偵測root，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視



電子商務系統安全管理

系統建置風險評估
風險評估作業欠妥，未包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)，且有未依功能需求不同，將提供內部及外部人員使用功能，設計為同一套系統，不利資訊安全。

測試及安全檢測作業
應用系統測試欠落實，程式安全檢測對弱點修補作業欠妥，含例外管理及補償措施。

網站及APP安全監控機制
未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制

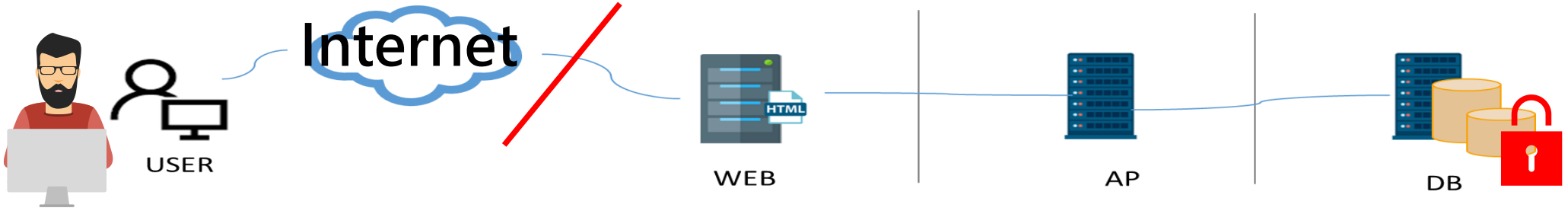
1
2
3
6

未建立網頁或檔案防置換或竄改機制，且未建立 APP防偽冒監控及後續處理機制

重要資料保護機制
重要資料如信用卡號有效年月及銀行帳[illegible]資料庫使用之密碼[illegible]存放

用安全設計
[illegible]線應用系統可查詢大量個資，[illegible]帳密進行管控，提供對外服務網站之資料顯示涉及個人資料，未評估妥適隱碼

APP安全設計
APP設計及檢測作業欠妥，未偵測root，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視



Fsc

電子商務系統安全管理

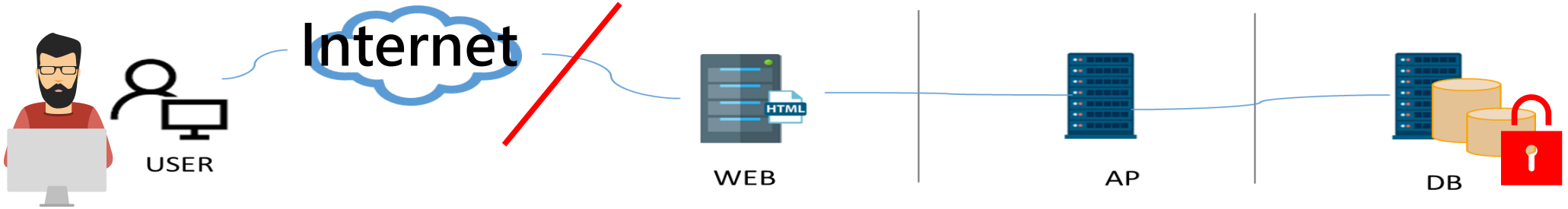
重要資料如信用卡號有效年月及銀行帳號未加密存放；連線資料庫使用之**密碼**存放於**DMZ區且明碼**存放

重要資料保護機制
重要資料如信用卡號有效年月及銀行帳號未加密存放；連線資料庫使用之密碼存放於DMZ區且明碼存放

個資應用安全設計
由外部連線應用系統可查詢大量個資，僅以固定帳密進行管控，提供對外服務網站之資料顯示涉及個人資料，未評估妥適隱碼

網站及APP安全監控機制
未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制

APP安全設計
APP設計及檢測作業欠妥，未偵測root，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視



電子商務系統安全管理

系統建置風險評估
風險評估作業欠妥，未包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)，且未提供內部及外部人

測試及安
應用系統測試欠落實對弱點修補作業欠妥

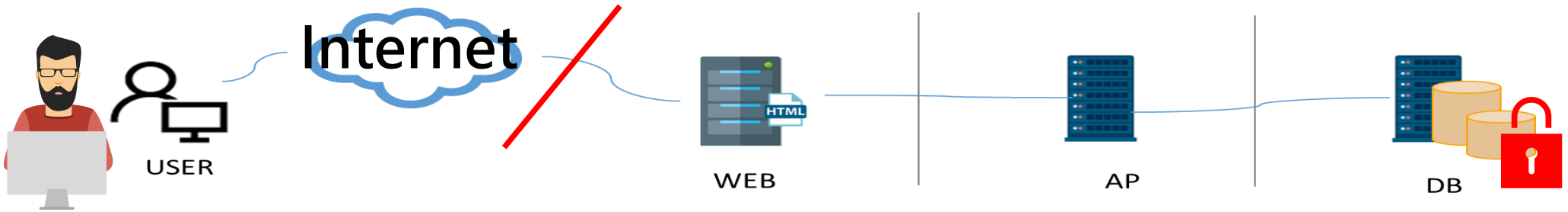
網站及
未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制

由外部連線應用系統可查詢大量個資，僅以固定帳密進行管控，另提供對外服務網站之資料顯示涉及個人資料，未評估妥適隱碼

重要資料保護機制
重要資料如信用卡號有效年月及銀行帳號未加密存放；連線資料庫使用之密碼存放於DMZ區且明碼存放

個資應用安全設計
由外部連線應用系統可查詢大量個資，僅以固定帳密進行管控，提供對外服務網站之資料顯示涉及個人資料，未評估妥適隱碼

APP安全設計
APP設計及檢測作業欠妥，未偵測root，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視



電子商務系統安全管理

系統建置風險評估
風險評估作業欠妥，未包含技術、Source所有權、網路架構等，及後續配套措施(緊急應變計畫)提供內部及

測試
應用系統測試欠對弱點修補作業

網
未建立網頁或檔案防置換或竄改機制，且未建立APP防偽冒監控及後續處理機制

APP設計及檢測作業欠妥，未偵測root ，可以模擬環境執行，對源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視

重要資料保護機制
重要資料如信用卡號有效年月及銀行帳號未加密存放；連線資料庫使用之密碼存放於DMZ區且明碼存放

個資應用安全設計
由外部連線應用系統可查詢大量個資，僅以固定帳密進行管控，提供對外服務網站之資料顯示涉及個人資料，未評估妥適隱碼

APP安全設計
APP設計及檢測作業欠妥，未偵測root ，可以模擬環境執行，源碼檢測結果之弱點修補作業欠妥，檢測報告未落實檢視

Fsc

個人資料保護

個資清冊

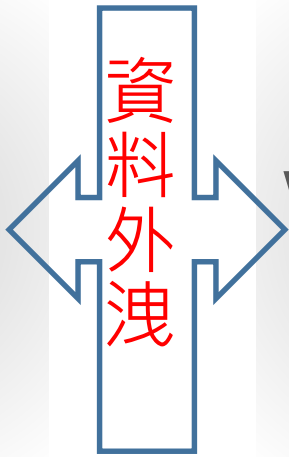
個資盤點
欠完整

存取軌跡

個資檔案及資料庫存取軌跡稽核欠完整

電子郵件管控

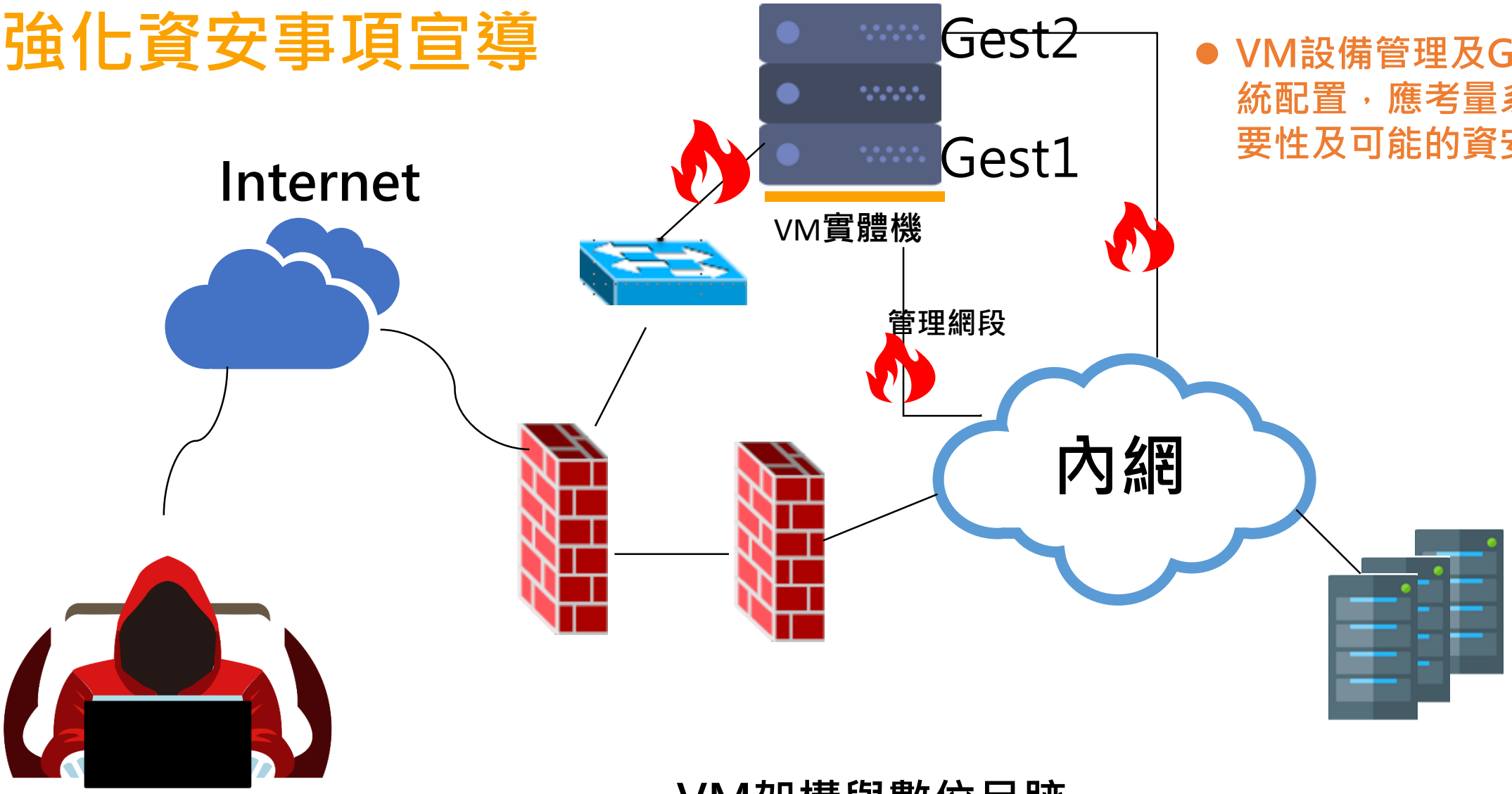
開放使用webmail



筆記型電腦管控

硬碟加密機制、usb、wifi及藍芽等

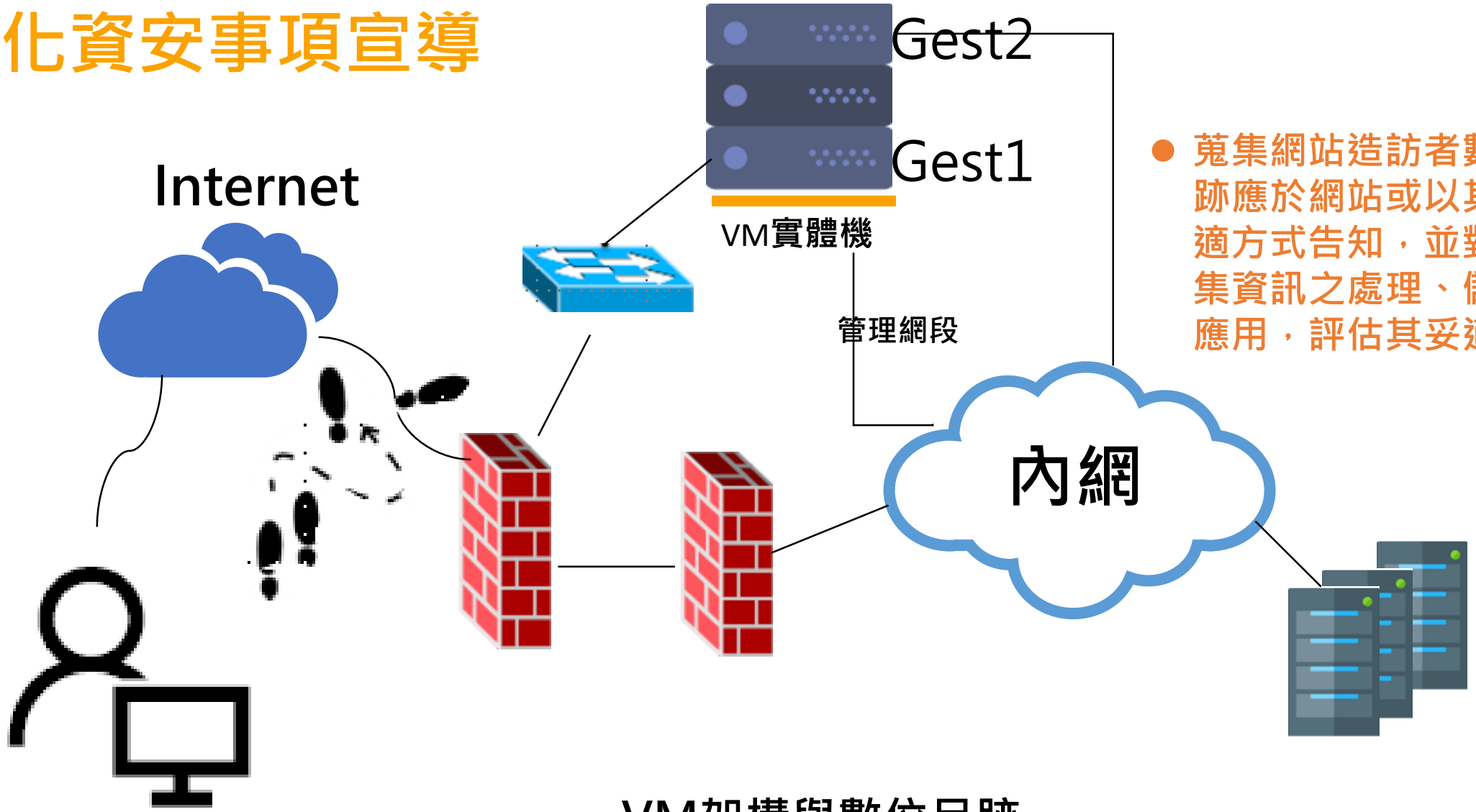
強化資安事項宣導



VM架構與數位足跡

- VM設備管理及Guest系統配置，應考量系統重要性及可能的資安風險

強化資安事項宣導



VM架構與數位足跡

- 蒐集網站造訪者數位足跡應於網站或以其他妥適方式告知，並對所蒐集資訊之處理、儲存與應用，評估其妥適性


Thank You