資訊安全風險管理執行情形

(業於 113 年 11 月 04 日第 14 屆第 16 次董事會報告)

資訊處報告

資訊安全風險管理報告議程

1. 2024年度資安已執行項目

1.1 ISMS 管理面
1.2 ISMS 實作面
1.3 PIMS 管理面
1.4 技術面

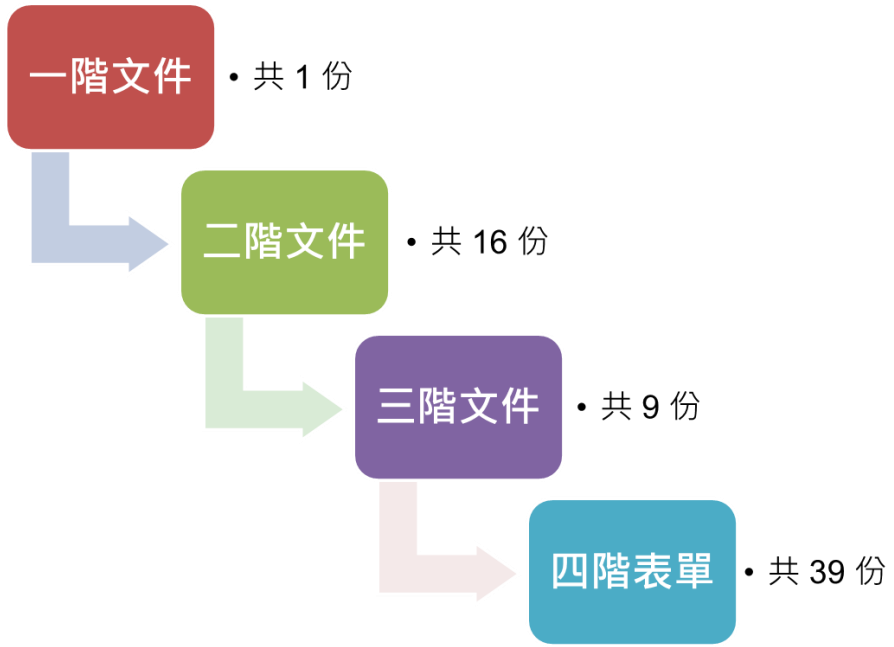
2. 資安計畫預計執行項目

2.1 ISMS 管理面
2.2 PIMS 管理面
2.3 技術面

2024 年度
資安已執行項目

1.1 ISMS 管理面

- 四階程序/表單文件修改及發佈 2024/04/23



一階文件

- ISMS-L1-01 資訊安全政策

二階文件

- ISMS-L2-01 組織全景分析評鑑辦法
- ISMS-L2-02 資訊安全組織設置辦法
- ISMS-L2-03 資訊安全文件暨紀錄管理辦法
- ISMS-L2-04 人力資源安全管理辦法
- ISMS-L2-05 資訊資產管理辦法
- ISMS-L2-06 資訊安全風險評鑑與管理辦法
- ISMS-L2-07 實體安全管理作業辦法
- ISMS-L2-08 通信與作業管理辦法
- ISMS-L2-09 存取控制管理作業辦法
- ISMS-L2-10 資訊作業委外管理作業辦法
- ISMS-L2-11 應用系統安全管理作業辦法
- ISMS-L2-12 資訊安全事件通報處理管理辦法
- ISMS-L2-13 資訊業務持續營運管理辦法
- ISMS-L2-14 資訊安全稽核暨矯正管理作業辦法
- ISMS-L2-15 資訊安全實施管理辦法
- ISMS-L2-16 適用性聲明書

三階文件

- ISMS-L3-01 資訊機房安全管理作業規範
- ISMS-L3-02 主機與伺服器安全管理作業規範
- ISMS-L3-03 防火牆建置與管理作業規範
- ISMS-L3-04 弱點管理作業規範
- ISMS-L3-05 備份管理作業規範
- ISMS-L3-06 營運持續計畫
- ISMS-L3-07 軟體資產管理作業規範
- ISMS-L3-08 雲端服務作業規範
- ISMS-L3-09 情資分享管理作業規範

四階表單

- ISMS-L2-01-01 組織全景評鑑表
- ISMS-L2-02-01 資訊安全組織成員表
- ISMS-L2-02-02 外部單位聯絡表
- ISMS-L2-02-03 利害關係人溝通一覽表
- ISMS-L2-03-01 資訊安全管理文件列表
- ISMS-L2-03-02 資訊安全文件修訂建議表
- ISMS-L2-03-03 外來文件一覽表
- ISMS-L2-04-01 委外人員保密切結書
- ISMS-L2-05-01 資訊資產清冊
- ISMS-L2-05-02 資訊資產變更申請單
- ISMS-L2-05-03 資訊資產分級管制措施對照表
- ISMS-L2-05-04 組態安全管理表
- ISMS-L2-05-05 組態例外管理表
- ISMS-L2-05-06 資料刪除紀錄表
- ISMS-L2-06-01 風險評鑑彙整表
- ISMS-L2-06-02 風險評鑑報告
- ISMS-L2-06-03 風險處理計畫表
- ISMS-L2-09-01 帳號清查紀錄表
- ISMS-L2-09-02 資料庫作業申請表
- ISMS-L2-11-01 系統開發暨驗收及上線申請表
- ISMS-L2-12-01 資訊安全事件通報單
- ISMS-L2-14-01 資訊安全內部稽核計畫
- ISMS-L2-14-02 資訊安全管理制度內部稽核表
- ISMS-L2-14-03 資訊安全內部稽核報告
- ISMS-L2-14-04 資訊安全矯正處理表
- ISMS-L2-15-01 資訊安全目標有效性量測表
- ISMS-L3-01-01 資訊機房人員進出登記表
- ISMS-L3-01-02 資訊機房工作日誌
- ISMS-L3-01-03 資訊機房工作月誌
- ISMS-L3-01-04 資訊設備維修攜出入申請表
- ISMS-L3-03-01 防火牆規則管制表
- ISMS-L3-05-01 備份異地備份媒體管理表
- ISMS-L3-05-02 備份測試查核表
- ISMS-L3-06-01 營運衝擊分析表
- ISMS-L3-06-02 營運持續演練計畫
- ISMS-L3-06-03 營運持續演練報告
- ISMS-L3-07-01 軟體使用管理表
- ISMS-L3-08-01 雲服務專案管理表
- ISMS-L3-09-01 威脅情資收集分析管理表

1.1 ISMS管理面

- **最新攻擊詐騙及資安通識教育訓練**

攻擊詐騙威脅知識分享

Jan.- Mar.
- ChatGPT詐騙新法
- 駭客針對Booking.com用戶展開攻擊
- 你有被騙嗎？LINE公布2023年 5 大熱門假訊息
- 新的惡意軟體Xamalicious 在Google Play上下載超過 33 萬次

Apr.- June
- LockBit勒索軟體被查封
- 知名遠端桌面連線軟體AnyDesk證實伺服器遭駭

July- Sep.
- Facebook詐騙警報：「無法相信他已經走了」
- 小心LINE輔助認證詐騙手法！5大社群隱私防範守則
- 超過90款惡意程式溜進Google Play

Oct.- Dec.
- 您該如何防範深偽（Deepfake）AI詐騙影片？
- 130萬臺Android電視機上盒遭植入後門程式
- 國內網路攝影機存在5年的漏洞被駭遭植入Mirai變種

資安通識教育訓練

May - June
- 智慧化環境

July - Sep.
- 物聯網安全防護

Oct. - Nov.
- 勒索軟體攻擊流程與防護

1.1 ISMS管理面

- 資安治理及會議

資安治理

July
- 內部稽核 -July 7-8
- 管理審查 -July 23

Aug.
- 辦公室無線網路使用限制公告 -Aug. 14
- 資安事件通報信箱設立 -Aug. 15
- SAP ERP及AD網域登入帳號密碼變更原則公告 -Aug.23
- 資訊安全管理公告 -Aug. 30

Sep.
- 密碼複雜性強化及說明 -Sep. 14

例行季會

Q1
- March 27

Q2
- June 26

Q3
- September 25

1.2 ISMS實作面

-資產盤點：人員16筆、資料30筆、軟體42筆、硬體79筆、服務9筆
-組態盤點：網路設備34項筆、應用系統130筆、非網路設備硬體28筆

本年度將風險值64以上的部分界定為高度風險，共計16項，皆已擬訂風險處理對策

針對SAP及此次驗證範圍內帳號進行全面盤點 (SAP、SAP DB、SAP OS、SAP QAS、SAP介接系統、網路設備、門禁、環控系統…等)

備份媒體列表管理，並完成2項重要備份測試查核

完成6項關鍵業務之營運持續演練。 (電力系統、空調設備、網路、防火牆、儲存設備、SAP系統)

每月確認當月情資，進行影響分析及處理，4~9月已處理7件情資

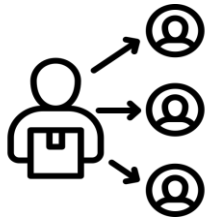
1.2 ISMS實作面

機房管理

May
- 加裝監視器

June
- 新增漏水偵測設備
- 機櫃線路整理

July
- 機房裝卸及報廢區域規劃及劃分



供應商管理

公司
- SFC委外資通安全規範

個人
- 委外人員保密切結書

今年9月通過 ISO27001:2022 驗證

ISO 驗證

文件審查 -Sep.5

- 稽核發現：4項觀察事項(OBS)，皆已完成矯正

實地審查 -Sep.23~24

- 稽核發現：10項觀察事項(OBS)、4項可改進空間(AOI)，矯正進行中
- **正面發現：**
  1. **管理階層支持與重視ISMS，持續擴充資源，強化資安作業**
  2. **蒐集威脅情資，並進行管控及處理**
  3. **建立SOC 資安監控機制**
  4. **部分作業使用雲端服務，並實施資料備份機制**
  5. **使用BPM系統，增進作業效率**
  6. **鼓勵並培訓同仁，持續精進資安專業能力**
  7. **人員正面看待改善機會，即知即行**

1.3 PSMS管理面

- **個資清冊及風險評鑑**

個資盤點及個資清冊

第一梯
數發處/行銷處/永續發展處

第二梯
財會處/人資處/採購處/海外事業發展組

第三梯
大園廠/中壢廠/新竹廠

第四梯
資訊處

風險評鑑

已完成
數發處、行銷處、永續發展處
、海外事業發展組、採購處

進行中
財會處、人資處、資訊處

1.3 PSMS管理面

- 內部稽核與教育訓練

稽核發現

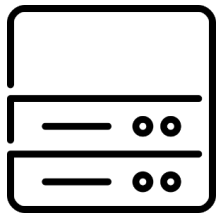
- 數發處 (4項)
- 行銷處 (26項)
- 永續發展處 (7項)
- 財會處 (9項)
- 人資處 (3項)
- 採購處 (1項)
- 海外事業發展組 (1項)
- 資訊處 (5項)
- 共通事項 (4項)

教育訓練

March

- 個資生命週期流程

1.3 技術面



集團檔案伺服器汰換
(2024/08~)

- 新主機群環境
- 同步關係建立
- 結構性差異校正

網站滲透測試
(2024/06~08)

- 對外網站滲透測試及漏洞修補
- ESG相關新上線網站測試

伺服器弱點掃描
(2024/09~)

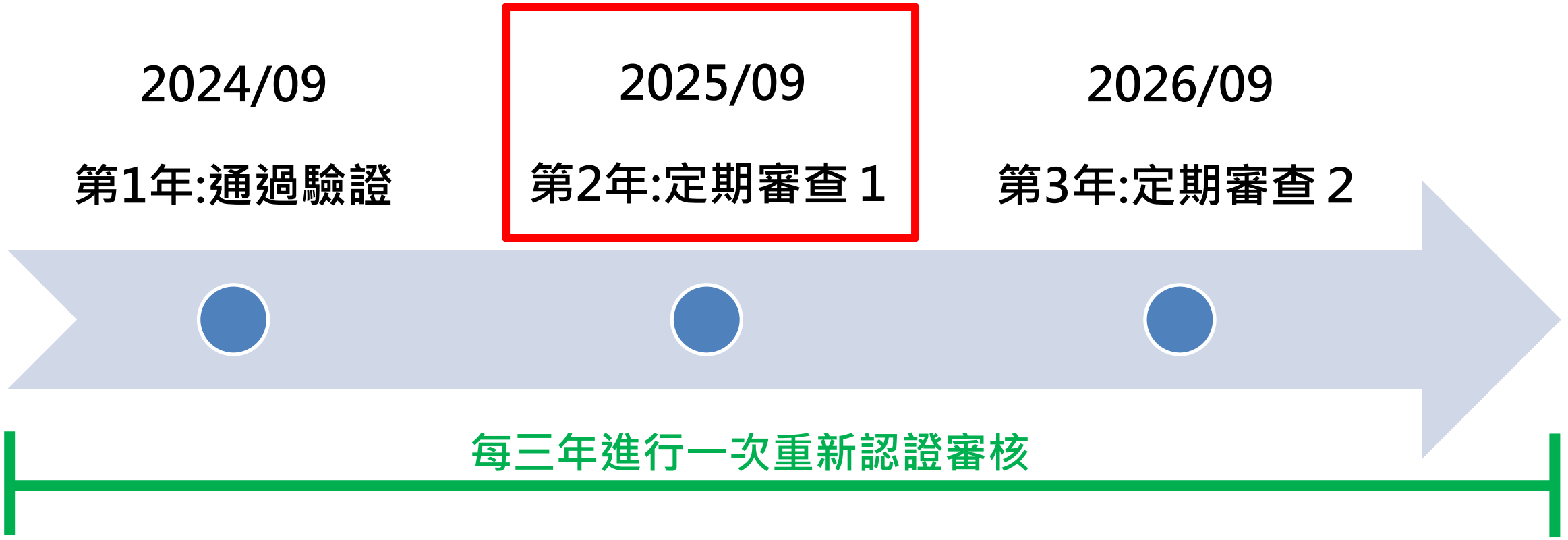
- 系統及伺服器弱點掃描及弱點改善強化
- 依 ISO27001 規範推動風險認列控管及修補重建

資安計畫
預計執行項目

2024/11 ~ 2025

2.1 ISMS 管理面

- 預計執行項目

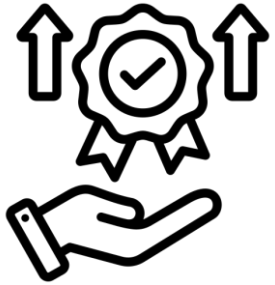


2.2 PIMS 管理面

- 預計執行項目

程序文件制定

- 四階文件及表單新增修改



風險處理及改善

- 高風險個資項目處理
- 降低風險程度

管理審查會議

- 條列各單位內稽發現
- 改善計畫討論

2.3 技術面

- **預計執行項目**

網路可視性強化

- 更有效地監控及識別異常行為及潛在威脅，提升資安防護力

網路微分段

- 切分及實施微分段，限制攻擊者活動範圍，降低內部攻擊風險與加強重要資料保護

SIEM

- 透過日誌管理收集、AI事件分析等功能、即時監控及分析不同來源設備安全事件，快速識回應及阻斷潛在威脅