資安室第三季報告

Date: 113/10/01

113年第三季 資安報告

報告綱要

- 資訊與網路安全管理團隊
- 風險評估與因應措施
- 安全管理措施
- 資訊安全管理模式
- 資安投資與改善

資訊與網路安全管理團隊

本公司於 111/09/01 起成立資訊安全室，設有專責主管及資訊安全專責人員各一名，並由總經理/執行長擔任資訊與網路安全管理團隊召集人；除資訊安全室外，資訊與網路安全管理團隊包含具專業技術及知識之資訊中心、內部稽核室、人力資源室、法務室及獨立客觀的主管人員（各事業單位及功能單位管理階層），負責統籌、計畫、執行及分析資通安全事件，且每年至少評估一次資通安全政策。

風險評估與因應措施

威健核心資通營運系統	風險評估	因應措施
Email System	1. 使用者帳密被盜，成為垃圾廣告郵件跳板。 2. 郵件主機因被當跳板而被列為黑名單，無法收發郵件。 3. Email主機軟硬體故障之風險。	• 導入Office 365 Outlook(SaaS服務)進行電子郵件收發，並啟用2FA的雙重認證，降低帳密被盜風險及因軟硬體故造成服務中斷。
ERP System	1. 營運資訊資料 C,I,A (Confidentiality, Integrity and Availability) 的管控。 2. ERP 軟硬體的維運。 3. 系統開發維運人員的人才不足。	• 每年進行ERP使用者帳號/權限盤點，由各部門主管覆核。 • 進銷存流程需進行電子簽核達到資料正確性。 • IT部門計畫性更換ERP伺服器，並採用虛擬化方式提高系統完整性與可用性。 • 招募培訓新進從業人員，以利系統開發與維運。

風險評估與因應措施

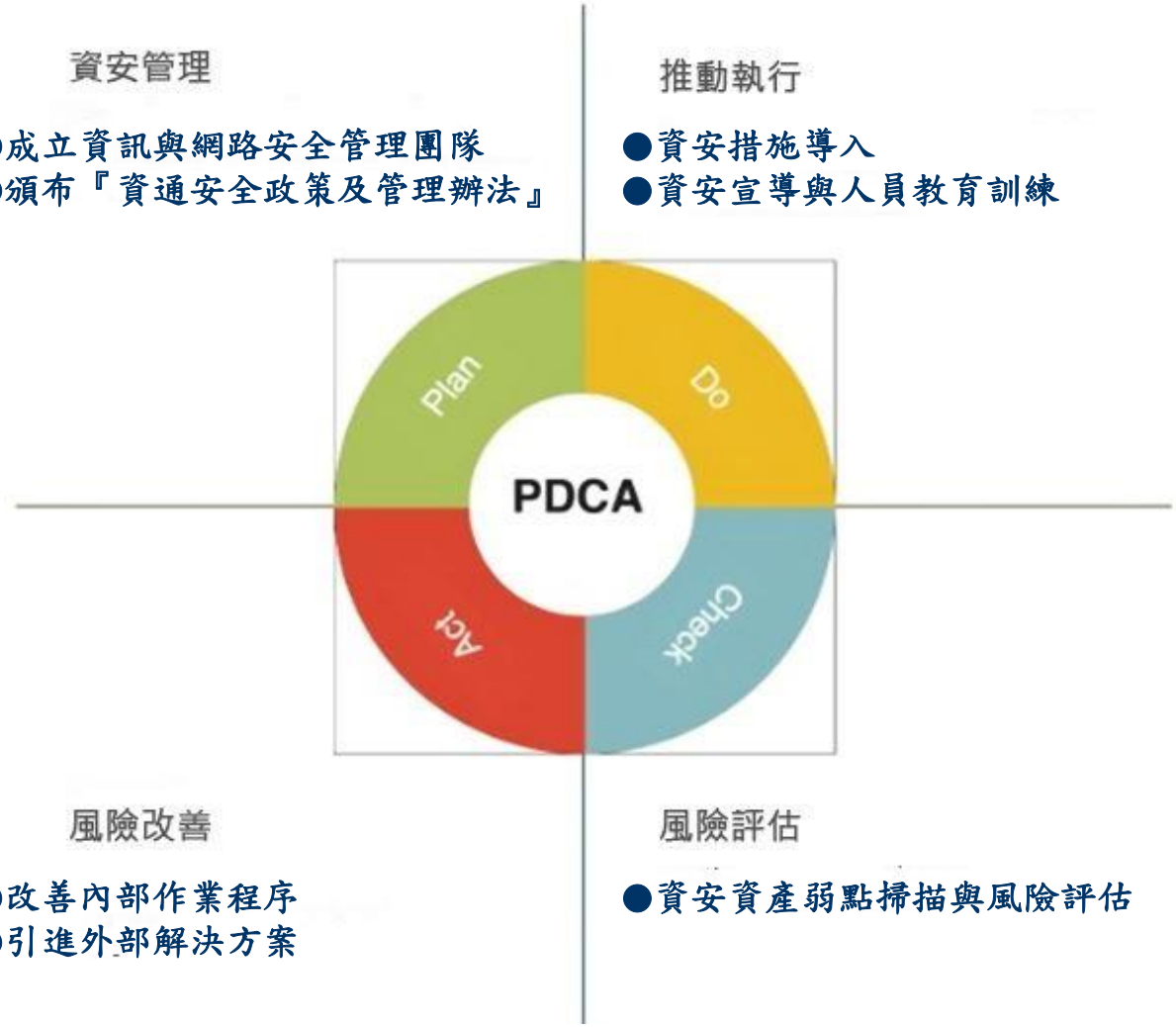
威健核心資通營運系統	風險評估	因應措施
WMS System	1. WMS為自行開發的系統，使用Client/Server的架構，且DB均已虛擬化，故相對於ERP的風險較小較可控。 2. 出錯貨(date code)的人為操作風險。	• WMS伺服器以虛擬化平台建置於中華電信IDC 機房，並計畫性汰舊換新。 • WMS Client 在內部網路使用並未暴露於Internet，且使用者須申請安裝 WMS Client 端軟體方能存取資料。 • 倉庫對從業人員定期進行教育訓練。
WorkFlow	1. 目前使用華苓AgentflowV3.7，華苓已對該版本不進行維護。	• 已規劃執行升級Agentflow V4計畫。
個資法的遵行	1. 「人事系統」由人事部門管理，並委外維護。 2. WKT並無CRM系統或過多的客戶資料對於個資也都採最小資料(僅知原則)保存，故風險相對較小。	• 113年9月12資安室委由中華電信舉辦「個資法教育訓練」，線上出席合併會後觀看影片427人次。 • 「核心系統」之測試環境對個資訊息進行遮蔽。

安全管理措施

管理類別	管理措施	執行項目
權限管理	人員帳號、權限管理與系統操作行為之管理措施。	新進員工帳號申請、定期覆核有效帳號、離職員工帳號失效。
存取控管	人員存取內外部系統及資料之控制措施。	定期覆核使用者系統使用權限。
外部威脅	內部系統潛在弱點、中毒管道與防護措施。	主機弱點檢測及更新措施，病毒防護與惡意程式偵測，基於中華電信HiNet SOC的情資分享加強防火牆的設定。
弱點分析	針對PC與伺服器系統弱點掃描與檢查、修補措施。	定期檢查與修復高風險性弱點，若無法修補則進行補償性措施。
社交工程與資安教育訓練	針對使用者同仁定期宣導資安觀念（email與新人訓練）。	MIS/ICSO(資安室)不定期發送email分享資安新聞、宣導資安注意事項，並於新人訓練時闡明威健資安相關規範與措施。

資訊安全管理模式

採用PDCA 循環流程管理模式，確保資訊安全管理目標之達成並且持續改善。



資訊安全管理模式

資安管理 (Plan)

- **成立資訊與網路安全管理團隊**

  本公司於 111/09/01 起成立資訊安全室，設有專責主管及資訊安全專責人員各一名，並由總經理/執行長擔任資訊與網路安全管理團隊召集人；除資訊安全室外，資訊與網路安全管理團隊包含具專業技術及知識之資訊中心、內部稽核室、人力資源室、法務室及獨立客觀的主管人員（各事業單位及功能單位管理階層），負責統籌、計畫、執行及分析資通安全事件，每年至少評估一次資通安全政策。

- **頒布『資通安全政策及管理辦法』範圍共分十大項**

  一.資通安全政策制定及評估
  二.資通安全組織及權責
  三.資訊資產分類與控管
  四.人員安全管理
  五.實體及環境安全管理
  六.通訊與作業管理
  七.存取控制
  八.系統開發與維護
  九.營運持續管理
  十.資通安全措施符合性之檢核

資訊安全管理模式

推動執行 (Do)

- **資安措施導入**

導入Office 365 Outlook(SaaS服務)，結合中華數位的Mail SPAM SQR攔截過濾垃圾郵件與威脅郵件成果良好。
113年第三季(113/1/01~113/9/30)：
正常郵件: 4,824,159 封
垃圾郵件: 133,878 封
威脅郵件: 43,790 封
攔截精準度：99.81% (統計自 113/01/01 ~ 113/09/30)

- **資安宣導與人員教育訓練**

資安宣導: MIS/ICSO(資安室)每月定期進行「MIS資安宣導 資訊安全與軟體使用」及「資安情報」不定期宣導。(113 第三季 Total 宣導次數: 3次)。
資安教育: 新人訓練- MIS/ICSO(資安室)於新人訓練時針對駭客、病毒、網路釣魚、電腦蠕蟲、社交工程、密碼維護等議題，提出說明與宣導。 2024/09/24計有21位新進同仁(20名參與課程)。
資安教育訓練- 一般人員每年1小時/資訊人員每年3小時。2024/09/12 個資法教育訓練(3小時/427名參與課程，不含被派駐海外同仁，參與率93%)。

資訊安全管理模式

風險評估 (Check)

- **資安資產弱點掃描與風險評估**

防火牆規則盤點及控管。
每年進行伺服器弱點掃描。
每年進行開發程式源碼掃描。
以中華電信HiNet SOC 做為資安情資收集， MIS/ICSO(資安室)會依據所提供的資訊加強防護。

風險改善 (Action)

- **改善內部作業程序**

IT人員於 113/09 更新防毒軟體 WithSecure ,目前如下：

EDR and EPP for Servers	(端點檢測和響應Server)	授權:10	已安裝:10
EDR and EPP for Computers	(端點檢測和響應PC)	授權:100	已安裝:73
EPP for Computers	(端點防護PC)	授權:400	已安裝:397

- **引進外部解決方案**

中華電信輔導ISO27001:2022，預計2025年6月取得認證。

資安投資與改善

- 資安事件與因應：

  駭客病毒入侵： 113年第三季無重大駭客或病毒入侵事件。
  電腦網路故障： 113年第三季無重大網路中斷事件。
  環境設施故障： 113年第三季無重大環境設施(泛指機房冷氣,供電等設施)故障。
  重大資安事件： 113年第三季無因發生重大資通安全事件所遭受之損失或影響營運、商譽等之情事。
  113年第三季無經證實侵犯客戶隱私或遺失客戶資料投訴之情事。

- 113年第三季 資安人員相關教育課程與活動：

主辦單位	課程/活動名稱	日期	時數(小時)	參加人員	證(明)書
中華電信	個資法教育訓練	113/09/12	3	1.林義閔(資安室主管)	無

- **資安投資評估：**

  因應ISMS(ISO27001-2022)導入，經顧問團隊(中華電信)已完成初步評估，包含零信任導入、弱點掃描與SOC(Security Operation Center)監控、多網域SSL憑證購買、DDoS防護租用等，將陸續提出報價，以利後續投資方案選擇。