延宇資訊股份有限公司

115年度 ISO27001資訊安全管理系統(ISMS) 暨 ISO27701個資隱私保護管理系統(PIMS) 管理審查會議

2026年07月23日

會議議程

- 主席致詞
- 討論議題
- 臨時動議

管理審查會議

- **依據 ISO/IEC 27001 標準規範**

  應依已規劃的期間(至少一年一次)，審查本公司的資訊安全管理系統，以確保其持續的適切性、合宜性及有效性，包括上次評鑑改進情形、資訊安全及個資保護之政策及目標。

管理審查會議應考量下列事項

一、過往管理審查之議案的處理狀態
二、與資訊安全管理系統有關之外部及內部議題的變更
三、與資訊安全管理系統相關關注方之需要及期望的變更
四、資訊安全績效之回饋
1. 不符合項目與矯正措施
2. 監督及量測結果
3. 稽核結果
4. 資訊安全目標之達成
五、關注方之回饋
六、風險評鑑結果與風險處理計畫狀態
七、持續改善之機會

一、過往管理審查之議案的處理狀態

- 今年為導入 ISO 27001 及 ISO 27701 第三年，去年(114年度)管理審查會議無追蹤之議案。

二、與資訊安全管理系統有關之內部及外部議題的變更(1/4)

- 今年鑒別出本公司之關注方(interested parties)包括資訊系統維運服務、資訊安全管理系統操作、隱私權保護管理系統、極端氣候議題，溝通方式以公告、公文、E-mail、會議、合約、電話及通訊軟體等。

- 鑒別出資訊安全管理制度之導入範圍以「資訊安全管理系統操作及資訊基礎設施維運作業」為範圍。

二、與資訊安全管理系統有關之內部及外部議題的變更(2/4)

- 今年ISMS/PIMS四階文件新增、修訂、廢止狀況如下：
  - 新增：
    - 一階文件：0 份
    - 二階文件：0 份
    - 三階文件：0 份
    - 四階文件：0 份

二、與資訊安全管理系統有關之內部及外部議題的變更(3/4)

- 今年ISMS/PIMS四階文件新增、修訂、廢止狀況如下：
  - 修訂：
    - 一階文件：0 份
    - 二階文件：2 份
    - 三階文件：2 份
    - 四階文件：12 份
- 詳如： YAN-ISMS-04-06資訊安全管理文件列表

二、與資訊安全管理系統有關之內部及外部議題的變更(4/4)

- 今年 ISMS/PIMS 四階文件新增、修訂、廢止狀況如下：
  - 廢止：
    - 一階文件：0 份
    - 二階文件：0 份
    - 三階文件：0 份
    - 四階文件：0 份

三、與資訊安全管理系統相關關注方之需要及期望的變更

- 今年導入 ISMS ，尚無收到相關關注方之需要及期望的變更需求。

四、資訊安全績效之回饋

4.1. 不符合項目與矯正措施

4.2. 監督及量測結果

4.3. 稽核結果

4.4. 資訊安全目標之達成

4.1.不符合項目與矯正措施

- 不符合項目之來源
  - 資訊安全內、外部稽核結果。
  - YAN-ISMS-04-03 ISMS_PIMS 有效性量測表
  - 資訊安全事件
- 本年度內部稽核於 2025年 06 月 16 日完成，共列計 7 個不符合事項；矯正作業持續進行中，矯正措施請參考「YAN-ISMS-04-29矯正與預防處理單」。
- 統計 2025 年 06 月至 2026年 06 月 29 日止，共有 2 件資安事件。

4.2.監督及量測結果

- 2026年度「YAN-ISMS-04-03 ISMS_PIMS 有效性量測表」已涵蓋 ISMS及PIMS 標準要求，包含組織控制措施、人員控制措施、實體控制措施、技術控制措施、個人資料蒐集、個人資料處理、個人資料利用、個人資料傳輸、個人資料儲存與銷毀、個人資料存取控制、隱私權公告聲明、個人資料事故管理、個人資料檔案管理、個人資料檔案風險評鑑，共 14 項。
- 2026年第二季量測項目無不符合項目。

4.3.稽核結果 (1/4)

- 本年度內部稽核於 2026年 06 月 29 日完成，共列計 7 個不符合事項；矯正作業持續進行中，矯正措施請參考「YAN-ISMS-04-29矯正與預防處理單」。

- 今年外部稽核預計於 2026 年 08 月 07 日實施，請各單位持續維持系統之有效行。

4.3.稽核結果 (2/4)

- 內部稽核不符合事項一覽表：

項次	查核項目 ISMS PIMS	觀察事項
1	組織全景 4.2 5.2.2	本公司同仁對差勤系統之影響說明，已於113年完成更換104 Pro差勤系統，關注者識別及期望與需求分析之內容應就目前使用之差勤系統之反應進行分析。
2	身分管理 A.5.16 6.6.2.1	同仁吳○景於115/2/28離職，YAN-ISMS-04-37系統使用權限管理名冊(日期115/6/14未註記停用日期)。
3	遠距工作 A.6.7 6.3.2.2	組織應審慎評估授權失效之重要設備持續使用SSLVPN可能會產生憑證與帳號外洩之風險考量。

4.3.稽核結果 (3/4)

- 內部稽核不符合事項一覽表：

項次	查核項目 ISMS PIMS	觀察事項
4	密碼技術之使用 A.8.24 6.7.1.1 6.7.1.2	M365 Admin Center授權管理工具故障，未即時通報及開立「YAN-ISMS-04-22資訊-個資安全事件通報單」。
5	組態管理 A.8.9	組態項目資料(環境類)YAN-ISMS-G-57-11506-12，組態編號不應沿用前任設備之編號。

4.3.稽核結果 (4/4)

- 內部稽核不符合事項一覽表：

項次	查核項目 ISMS PIMS	觀察事項
6	網路安全 A.8.20 6.10.1.1 網路服務之安全 A.8.21 6.10.1.2	Forti防火牆授權已到期(2020/09/05)，替換之防火牆PA-440因營運業務考量短暫下線。Forti防火牆無法持續取得原廠安全更新、技術支援及漏洞修補，增加對外服務之資訊安全風險，建議重新評估風險可接受性及後續部署規劃。
7	PII控制者告知第三方之義務 A.7.3.7 PII傳輸控制措施 A.7.4.9	「YAN-PIMS-04-03個人資料處理同意書」內容未說明個資當事人同意提供PII給第三方組織，或因專案業務需求，同意移轉PII與第三方揭露對象。

4.4.資訊安全目標之達成 (1/8)

- 本年度資訊安全目標計 14 項，均符合，資訊安全目標均於「YAN-ISMS-04-03 ISMS_PIMS 有效性量測表」呈現。

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
A.5	(1)資訊安全政策審查次數	4.1.4	≧1 次/年	1	0			
	(2)資訊安全政策宣導	4.1.4	≧1 次/年	1	0			
	(3)衝突之職務是否有做區隔	4.1.2	不符≦2 件	0	0			
	(4)有否確實簽署保密協議	4.1.1/4.1.2	不符≦2 件	0	0			
	(5)外部單位聯絡清單是否定期更新		不符≦1 件	0	0			
	(6)威脅情資否是定期更新		不符≦1 件	0	0			
	(7)資訊資產清冊更新		不符≦2 件	0	0			
	(8)資訊資產清冊符合分級與標示規定		不符≦2 件	0	0			
	(9)定期審查重要系統存取權限（管理者帳號清查）	4.1.1/4.1.2	不符≦1 件	0	0			

4.4.資訊安全目標之達成 (2/8)

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
A.5	(10)密碼長度及複雜度應符合規範	4.1.1/4.1.2	不符≦1 件	0	0			
	(11)管理者帳號申請是否依規定填寫表單		不符≦1 件	0	0			
	(12)是否依契約定期稽核委外作業供應者服務交付		不符≦2 件	0	0			
	(13)是否定期審查委外作業供應者管理程序或政策		不符≦2 件	0	0			
	(14)檢討營運持續計畫演練執行情形	4.1.5	≧1次/年	0	1			06/29執行營運持續演練計畫
	(15)法律法規鑒別是否每年檢視	4.1.7	≧1 次/年	1	1			
	(16)合法軟體之安裝	4.1.7	不符≦0件	0	0			
	(17)矯正預防措施於規定時間內改善完成	4.1.6	逾期≦2件	0	0			

4.4.資訊安全目標之達成 (3/8)

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
A.6	(1)是否有年度教育訓練計畫	4.1.4/6.1	不符≦1 件	0	0			
	(2)教育訓練若未依據計畫執行，是否說明原因，並經權責主管同意	4.1.4/6.1	不符≦2 件	0	0			
	(3)員工離退帳號是否確實停用或刪除		不符≦1 件	0	1			離職人員吳嘉璟未及時關閉郵件帳號
	(4)遠距工作連線申請是否依規定管制	4.1.1/4.1.2	不符≦1 件	0	0			
	(5)發生資訊安全事故時，是否依據規定之時程進行通報及處理，並保存佐證紀錄。		不符≦5件	0	0			
	(6)檢查資通安全事件通報單，是否重複發生相同資安事故件數		重複≦1件	0	0			

4.4.資訊安全目標之達成 (4/8)

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
A.7	(1)檢查有否遵守機房門禁規定		不符≦2 件	0	0			
	(2)檢查消防器材		≧2 次/年	1	0			
	(3) UPS 是否定期保養		不符≦2 件	0	0			
	(4)是否實施桌面淨空與螢幕淨空		不符≦2 件	0	0			
	(5)媒體汰除是否按規定執行		不符≦2 件	0	0			
A.8	(1)系統稽核日誌是否已依據規劃，進行保存及審查	4.1.1/4.1.2	不符≦1 件	0	0			
	(2)監控網路重要伺服器執行作業之系統容量（例如CPU、RAM、硬碟），若超過閥值是否進行處理		不符≦2 件	0	0			
	(3)定期備份及還原重要系統資料		不符≦3件	0	0			
	(4)發生中毒事件，是否依據作業要求進行處理		≦3 次/年	0	0			
	(5)檢查病毒碼是否即時更新		不符≦2 件	0	0			
	(6)弱點掃瞄後，未依據規定時間完成弱點處理之件數		≧1次/年	0	0			

4.4.資訊安全目標之達成 (5/8)

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
A.8	(7)檢查重要系統時間是否同步		不符≦2 件	0	0			
	(8)檢查防火牆設定是否與防火牆進出規則不相符次數	4.1.1/4.1.2	≦3次/年	0	0			
	(9)資訊系統變更，是否依據變更作業之要求，進行變更申請、評估、處理及審查?		不符≦2 件	0	0			
	(10)發生組態變更事件，且未更新組態項目資料表。		不符≦2 件	0	0			
個人資料蒐集	(1)蒐集前是否確認蒐集目的與範圍	6.3	不符≦1件	0	0			
	(2)蒐集個資時是否告知個資法要求事項	6.3	不符≦2件	0	0			
	(3)抽查個人資料蒐集是否逾越特定目的之必要範圍	6.3	不符＜1件	0	0			

4.4.資訊安全目標之達成（6/8）

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
個人資料處理	(1)抽查個人資料處理是否逾越蒐集目的	6.3	不符＜1件	0	0			
	(2)抽查個人資料使用若與原目的不同，是否針對新處理目的取得當事人同意，並保留紀錄	6.3	不符＜1件	0	0			
個人資料利用	(1)抽查個人資料利用是否逾越蒐集目的	6.3	不符＜1件	0	0			
個人資料傳輸	(1)抽查個人資料進行傳輸過程中是否具備安全控管	6.3	不符＜1件	0	0			
個人資料儲存與銷毀	(1)抽查之個人資料是否落實保存、銷毀或監督程序	6.3	不符≦1件	0	0			
	(2)每年至少 1 次進行保存期限資料盤點與到期評估	7.4.6	≧1 次/年	0	1			7月份執行已達保存期限之資料盤點
	(3)銷毀期限到期之個人資料，明確訂定預計銷毀日期。	7.4.6	≧1次/年	0	1			7/6執行資料銷毀

4.4.資訊安全目標之達成 (7/8)

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
個人資料儲存與銷毀	(4)預備銷毀的個人資料按照預計行程執行銷毀，且留下銷毀紀錄。	A.7.4.8	≧1次/年	0	1			7/6執行資料銷毀
個人資料存取控制	(1)含個人資料之紙本文件是否置於上鎖櫃子保存	6.2/6.4	不符≦1件	0	0			
	(2)已集中放置等待銷毀的個人資料，有妥善存放上鎖保管處。	A.7.4.6/ A.7.47	不符≦0件	0	0			
隱私權公告聲明	(1)抽查組織是否針對隱私權管理進行公告或具備相關聲明	6.1	不符≦1件	0	0			
個人資料事故管理	(1)發生個資事故未依規定通報與處理，並保存相關佐證紀錄	6.3	不符≦1件	0	0			

4.4.資訊安全目標之達成 (8/8)

項次	量測項目	對應政策目標	目標水準	量測結果(季)				差異說明
				一	二	三	四	
個人資料檔案管理	(1)個人資料檔案清冊是否定期更新	6.3	≧1 次/年	0	0			
	(2)系統或服務負責人是否於完成識別與維護個人資料檔案作業後，擬定或更新個人資料檔案之作業流程圖	6.3	不符≦1件	0	0			
個人資料檔案風險評鑑	(2)高於可接受風險值之個人資料檔案，是否於風險改善之時程內完成風險改善?	6.3	不符≦1件	0	0			

年度目標達成率 = (對應政策目標達成數量/對應政策目標達成數量(54*4季)*100%)
(如達成率低於89%需填寫YAN-ISMS-04-29矯正與預防處理單，實施矯正措施)

➢2026年第二季量測項目無不符合項目。

五、關注方之回饋

- 今年度資訊安全管理系統及個人隱私保護系統導入後，尚無收到新增的關注方之回饋。

六、風險評鑑結果與風險處理計畫狀態(1/2)

- 資訊資產辨識與價值評估結果此次風險評估階段，相關業務之資訊資產權責單位依據「YAN-ISMS-02-03資訊資產暨個資資產管理程序書」執行風險評估，辨識出資訊室共盤點出 93 項資訊資產， 納入組態管理共 18 項，並由資安長審核。請參考「YAN-ISMS-04-08資訊資產清單」。
- 依據「YAN-ISMS-03-10資訊安全風險評鑑說明書」執行風險評鑑，資訊資產價值為「中」以上(含)者共 38 項。
- 本年度風險評鑑作業，「安控後」風險等級為「中」 1 項，風險處理策略為「接受」，不需擬定「YAN-ISMS-04-11資訊作業風險改善計畫」，規劃風險改善措施。

六、風險評鑑結果與風險處理計畫狀態 (2/2)

- 依據「YAN-ISMS-03-10資訊安全風險評鑑說明書」執行「YAN-ISMS-04-09資通系統盤點及分級表」，資通系統共盤點出 12 項，其中核心系統 6 項。
- 本年度風險評鑑作業後，共 5 項核心系統評鑑風險均為「中」級、 1 項核心系統評鑑風險為「普」級，不需擬定「YAN-ISMS-04-11資訊作業風險改善計畫」，規劃風險改善措施。

七、持續改善之機會

- 無。

臨時動議



結語(主席指示)