宜進實業・資安風險評估分析

（十三）資安風險評估分析及其因應措施

本公司的生產事業自台南廠從 2020 年 1 月 1 日起停止生產後，目前主要採委外生產，資訊作業的重心已移轉至行政單位，整體的網路環境更趨於單純化，整體作業風險亦相對降低；在新冠肺炎疫情部份，因一直採取積極的防範措施，對本公司的資訊作業及安全均未受到任何影響。

本公司對資訊環境維護及資安威脅防範方案之投資，均秉持適用、適時、適量之原則，對資安風險之控管亦遵照內部控制制度，及參考外部實例或廠商建議而持續改進；針對資安風險之評估，乃依下列 10 個類別 209 個查核項目(依 ISACA 國際電腦稽核協會台灣分會之"資通安全公司自我檢查表"加以修訂)，定期於每年 12 月至隔年 1 月間進行自我評估及分析，依查核項目之達成度或完整性給予高、中、低評比並予量化統計後，再依據風險性較高的部份進行檢討及擬具改善措施，近期執行的時間為 2020 年 12 月 28 日至 2021 年 1 月 5 日，由資訊工程師及資訊主管執行，報告呈總經理核閱，並提供內、外部稽查。

由於本公司的資訊管理系統均為自行開發，僅限於公司區域網路執行，未開放透過網際網路之連線，本年度自評風險較集中於端點防護及資訊合約中對外部存取權限的約束；而透過資訊設備平日運作的日誌，發現 2020 年外部對公司內郵件主機、端點電腦的攻擊手法及頻率均在增加，評估後擬更換端點的防毒、防駭軟體及加強閘道的防護機制來因應，近期已請資安廠商提供具備偵測及稽核功能的設備進行測試及評估，以結合原有網路管理設備共同防禦，增加控制風險的力道，並請資安廠商提供滲透攻擊、弱點檢測等相關服務，以持續改善資安環境之弱點及增加風險評估之可信度，**總結整體之資安風險程度介於"低-中"之間，無重大營運風險**。

項次	評估類別	風險評比(%)			重要管控措施
		低	中	高	
1	資訊安全政策	70	30	0	1.明定資安組織、權責及事件之通報、處理綱要。 2.定期審查、修訂資訊安全政策。
2	建立資訊安全組織	82	18	0	1.設資安管理小組及個人資料保護小組。 2.訂立資安事件之緊急應變處理及回報程序。
3	人員安全與管理	30	70	0	1.內部控制制度定義資訊人員、使用者之作業權限劃分，及人員異動、離職之作業準則。 2.每半年執行作業權限複核。 3.每年定期普查個人電腦，防止公器私用。
4	資產分類與控管	33	67	0	1.資訊類軟、硬體資產列冊管理。 2.每年定期普查電腦，確認軟、硬體資產。
5	實體及環境安全管理	75	25	0	1.專用電腦機房具溫度、電力自動控管。 2.伺服器及個人電腦安裝防毒軟體，重要職務之電腦，每日定時備份，其備份份數至少二代。 3.營運資料庫採雙主機即時備援，每半年定期模擬事故演練後輪替運作。
6	通訊與操作管理	71	26	3	1.電子郵件主機具自我防護及保存稽核之功能。 2.每日分析防火牆紀錄，並使用上網行為記錄器，即時防堵內、外部異常行為。 3.即時宣導資安事件、通告或案例，提升防護意識。 4.使用 Hinet 資安艦隊之防護方案，擴展防護廣度，防堵內、外之攻擊。
7	存取控制	81	19	0	1.電子檔資料依部門、個人設定存取權限。 2.對外連線作業申請需經部門主管及總經理同意。 3.電子郵件區分內、外部，不須對外連絡之人員僅能內部寄信。 4.人力資源系統於讀取個資時，自動記錄存取軌跡。
8	系統開發與維護	76	18	6	應用系統自行開發、維護，在規劃分析時主動將安全需求納入設計考量，防範外部的侵入篡改。
9	永續運作之計畫管理	67	33	0	1.營運資料庫每半年定期演練、測試。 2.重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。
10	內部稽查及其它	75	25	0	1.每年電腦普查時告知公司軟體所授權之範圍，規範以外之軟體則要求移除或提供授權證明；軟、硬體普查資料，隨時依資產狀況更新。 2.資訊單位每年定期自評資訊作業環境安全。 3.內部稽核人員每年定期稽查資訊控制作業。
風險總評（%）		**72**	**27**	**1**	1.更換端點的防毒、防駭軟體及加強閘道的防護機制 2.與資安廠商合作滲透攻擊及弱點檢測等防護管理