113 年度風險運作情形

為落實企業風險管理，本公司於 107 年起完成建置風險管理範疇、組織及架構，隸屬「企業永續委員會」，每年進行風險因子鑑別與風險控管；110 年重新制定「營運持續計劃(BCP)」政策，針對營運持續管理建立公司相關內部程序書，並將相關風險評估報告於同年 11 月 05 日提報董事會通過，後續每年定期向董事會報告運作情形。

112 年起，將「企業永續發展委員會」更名為「企業永續暨風險管理委員會」，每年定期依重大性原則，考量經濟面、社會面及環境面等公司治理議題，對利害關係人產生重大影響者，進行風險評估並擬定風險管理策略與計畫。

一、113 年重大風險議題執行情形

112 年依經濟、環境、社會、治理幾大構面，鑑別出公司主要的風險議題為「資訊安全風險」及「財務風險」，針對此兩項重大議題，於 113 年進行之緩解計畫執行情形說明如下：

■【資訊安全風險】緩解計畫

致災源	地震、火災、水災、資安事件、電力系統、服務器故障
致災點	服務器、磁碟陣列、UPS 不斷電系統
潛在災害分析	1. 因地震、火災、水災，造成服務器損壞無法使用。 2. 駭客入侵服務器導致資料遭到刪除或加密。 3. 病毒感染服務器導致資料遭到刪除或加密。 4. 磁碟陣列硬體故障導致無法使用。 5. 資料外洩導致公司機密資料外流造成損失。
預估災損	1. 服務器系統損毀。 2. 服務器硬體故障。 3. 儲存資料遺失。 4. 機密資料外流。
減災措施	1. 磁碟與移動式硬碟備份以及異地備份。若服務器損壞無法使用，購買新設備後可由備份資料恢復系統；若整個機房發生災害損毀，可於其他地區恢復系統。 2. 公司資料均有磁碟與移動式硬碟備份，另將移動式硬碟做異地備份，

	即便資料遭到刪除或加密，可從迅速從磁碟備份資料恢復。 3. 重要主機均安裝防毒軟體，並具有中央控制台進行管理。 4. 定期汰換老舊服務器或磁碟陣列，減少因設備老舊導致的硬體故障。 5. 重要主機均安裝 Microsoft Defender Endpoint 即時偵測異常行為，可於駭客入侵或病毒感染時第一時間發現。 6. 重要主機均安裝 XFort 端點防護軟體，紀錄資料流向。
物資需求	1. 異地備份用硬碟。 2. 企業用防毒軟體。 3. Microsoft Defender Endpoint。 4. 端點防護軟體。
預算編列	逐年編列維護費
執行單位	集團資訊處
執行成果	113 年總計投入新台幣 322 萬元，主要為相關資安防護的軟硬體建置。截至 113 年 10 月底，總計阻擋了網路攻擊 375,285 次及網頁攻擊 76,285 次，未有任何資料損毀之情事發生。

■【財務風險】監控計畫

主要面向	相關配套措施
現金流/流動性風險	1. 資金需求預測與管控：本公司定期編製滾動資金預估表，掌握未來 6 個月資金需求，以提前準備對應的資金需求。 2. 資金壓力測試：定期進行資金壓力測試，模擬公司在市場情況最差時(如銷售急劇下滑、資金市場緊縮)的現金流變化，並評估公司是否有足夠的現金儲備和應對措施。 3. 保持良好信用評級：本公司 112 年信用評級為 TCRI 4 級，屬於財務健全企業。公司並與往來銀行維持良好關係，並簽立銀行聯貸合約，確保融資管道的暢通及穩定。
應收帳款違約風險	1. 設定信用政策與信用限額：根據客戶的信用狀況，設置適當的信用額度和付款條件。當客戶信用狀況或還款異常時，控制客戶授信額度，以降低發生呆帳風險。 2. 應收帳款管理系統：公司已建立自動化應收帳款管理系統，監控每筆應收帳款的狀態。若有逾期帳款發生，第一時間發送催收郵件，便於及時追蹤和管理，提醒相關人員跟進催收帳款。

	3. **逾期應收帳款催收作業**：對逾期應收帳款進行積極催收，採取電話、電子郵件和正式信函等方式提醒客戶付款。若客戶應收帳款已發生逾期，立即與法務單位進行催收行動，確保公司權益。 4. 應收帳款減值準備：對於已逾期應收帳款，收回可能性低或風險較高的帳款，立即列入呆帳，以反映財務狀況的真實性，並減少未來可能出現的資產損失對財務的影響。
匯率風險	1. 定期進行匯率風險評估：本公司每月評估曝險之外幣資產及負債，分析各貨幣波動可能帶來的風險，以掌握公司財務狀況對匯率變動的敏感性。 2. 避險作業：透過外幣收支互抵及避險交易，以達到外幣部位之平衡，降低匯率波動影響。 3. 定期風險報告：定期向管理層提交衍生性商品交易報告，內容包括曝險部位、避險交易部位、匯率波動風險對財務影響等，確保管理層充分理解財務風險狀況並提供決策參考。
執行單位	財務處
執行成果	1. 113 年 9 月 30 日現金為新台幣 17.9 億元，流動比率為 271%，速動比率為 224%。資金壓力測試結果，在無營收情況下，公司帳上現金可供使用 18 個月。 2. 113 年 11 月發生某客戶申請破產保護事件，造成應收帳款約台幣 1,200 萬元恐無法收回，已全數提列應收帳款減值準備，對財務業務無重大影響。 3. 113 年 9 月 30 日淨外幣部位為資產美金 280 萬元，匯率波動 1%對損益表之影響數為新台幣 27 萬元，目前因避險需求，已承作衍生性商品淨額為美元 200 萬元，與淨外幣部位相當。

二、113 年風險鑑別及風險評估作業

依循金融監督管理委員會「公開發行公司建立內部控制制度處理準則」及證交所「上市上櫃公司風險管理實務守則」相關條文，於 112 年 8 月 4 日董事會決議通過「風險管理政策與程序」，並依此政策與程序規範執行風險評估。

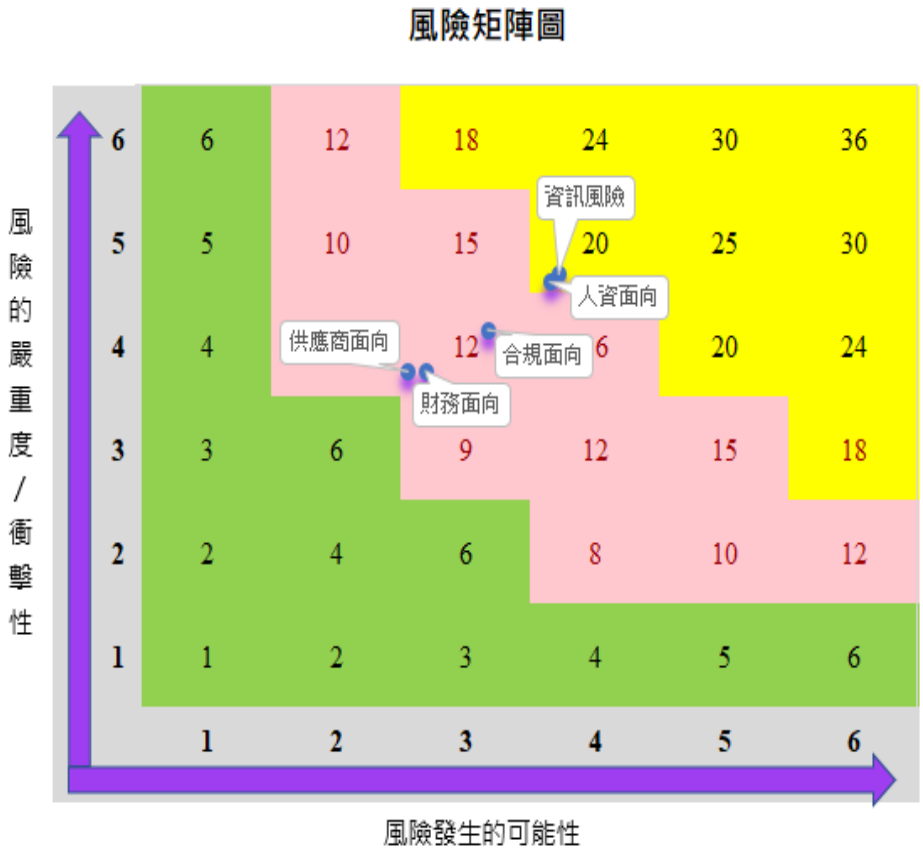
113 年 10 月份由企業永續暨風險管理委員會功能推動小組成員及數位經營管理階層主管，依「經濟(含治理)」、「環境」、「社會」、「其他」四大構面等二十

項風險項目中辨識出風險最高的五項議題。

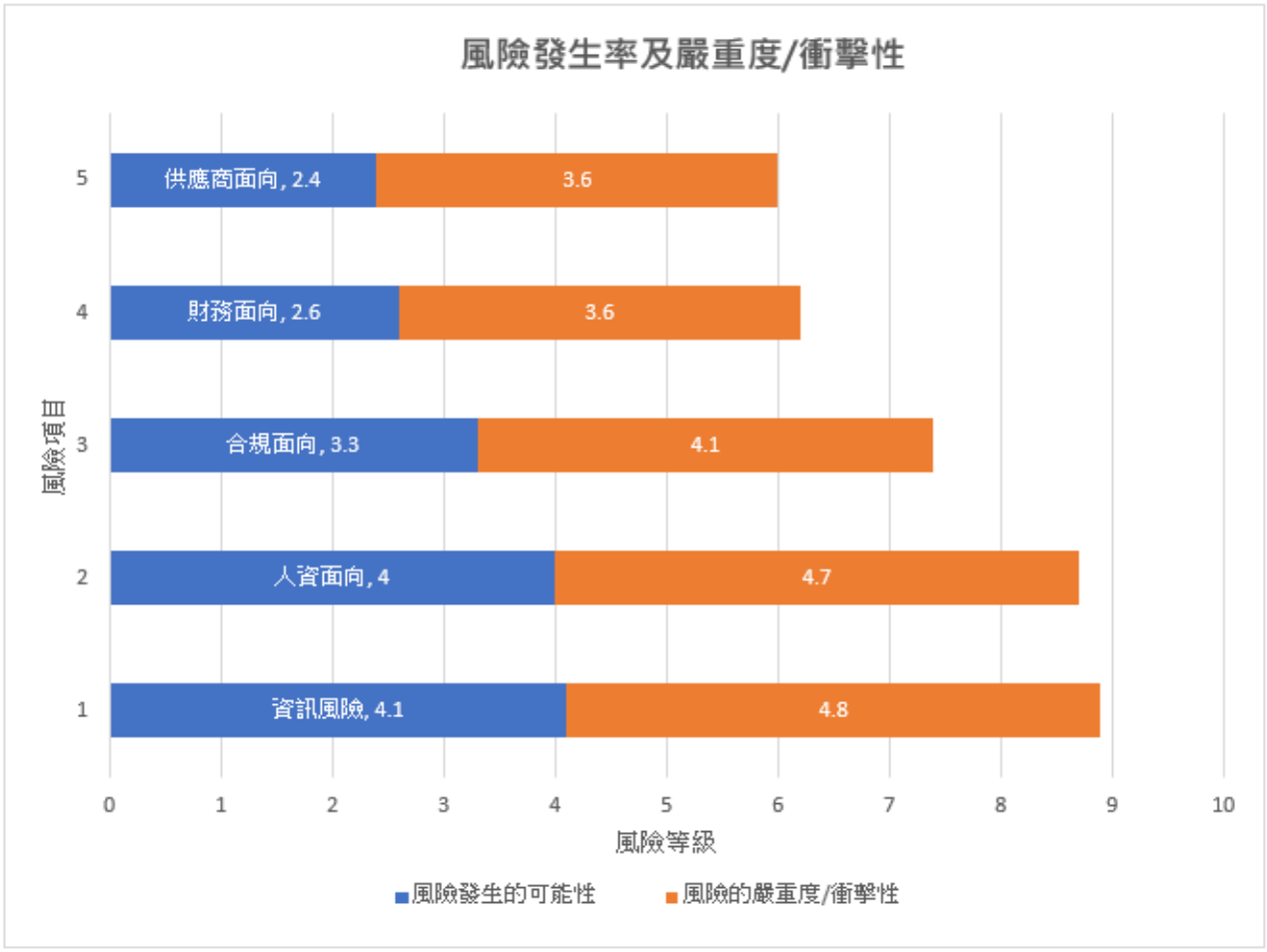
五項議題風險評估結果如下：

題目	風險的嚴重度/衝擊性	風險發生的可能性	風險等級
資訊風險	4.8	4.1	19.68
人資面向	4.7	4.0	18.80
合規面向	4.1	3.3	13.53
財務面向	3.6	2.6	9.36
供應商面向	3.6	2.4	8.64

再依前五項議題進行重大風險評估，最後依總分產生風險高、中、低；高度風險則提出相關緩解計畫、中度風險則維持現有公司營運狀況、低度風險則暫為可接受風險。分析結果如下：



風險分數	風險等級
7≧R	低度風險
8≧R≧17	中度風險
R≧18	高度風險
風險等級=發生可能性*風險嚴重度	



依圖表分析，鑑別出「資訊風險」、「人資面向」屬高度風險，依企業永續暨風險管理委員會功能推動小組評估後，提出對應的風險緩解計畫如下：

三、114 年重大風險議題之緩解計畫

■【資訊安全風險】緩解計畫

主要面向	風險策略調整
1. 資訊風險的來源與類型 ● 外部威脅：如駭客攻擊、勒索軟體、惡意軟體、供應鏈攻擊。 ● 內部風險：員工疏忽、內部資料洩漏、訪問權限管理不當。 ● 技術性漏洞：系統設計缺陷、未更新的軟體漏洞、基礎設施過時。 ● 自然災害與意外：停電、硬體損壞、火災、洪水等導致系統不可用。	**1. 風險管理策略** ● 風險迴避：停止或調整高風險的業務流程。 ● 風險降低：採取資安技術及流程（如加密、滲透測試、零信任架構）。 ● 風險轉移：透過資訊風險保險分散財務損失風險。 ● 風險接受：在風險影響可接受範圍內，透過備援機制應對。

2. 關鍵利害關係人 ● 內部：高層管理、IT 部門、風險管理部門、全體員工。 ● 外部：客戶、供應商、監管機構、投資者。 需考量這些利害關係人對於資訊安全的期望及責任分配。	**2. 技術層面的應對措施** ● 強化防禦措施： ● 建立入侵防禦系統（IDS）和防火牆。 ● 進行定期的漏洞掃描與系統升級。 ● 數據保護： ● 對敏感資料實施加密。 ● 使用分層存取控制限制未授權存取。 ● 備援計畫： ● 定期進行數據備份並測試災難復原計畫（DRP）。
3. 法規與合規性要求 ● 地區或國家法律規定，如 GDPR（歐盟資料保護法）或 CCPA（加州隱私法）。 ● 資安相關標準的合規性，例如 ISO 27001、SOX 法案（美國），或其他行業規範。	**3. 組織與管理層面應對策略** ● 培訓與教育：提高全體員工的資安意識，尤其是針對釣魚攻擊、密碼管理等常見威脅。 ● 跨部門合作：建立 IT、法律、人資及業務部門之間的協作機制。 ● 資安監控機制：設置全天候監控系統，主動偵測與應對威脅。
4. 資訊風險對業務的影響 ● 財務損失：因勒索軟體支付贖金、系統中斷造成營收損失。 ● 聲譽損害：客戶資料洩漏導致信任降低。 ● 法律責任：因違反隱私法規或未能妥善保護資料而面臨的罰款與訴訟。	**4. 資訊風險的指標與評估** ● 指標範例： ● 每月偵測到的攻擊次數。 ● 發生的資安事件平均應對時間。 ● 備援與復原測試的成功率。 ● 定期審查與改進：透過稽核、風險評估與利害關係人的反饋調整策略。

■【人資面向風險】緩解計畫

主要面向	風險策略調整
1. 勞動法規與合規風險 ● 勞動法規違反風險（如超時工時、薪資不足或不公平待遇）。 ● 勞動基準法與當地就業法律的合規性檢查，例如合同管理、最低工資標準、休假權益等。 ● 與多元化與包容性相關的反歧視規定是否落實。	**1. 強化風險識別與合規監控** ● 建立內部合規監控系統，定期鑑別勞動法規遵循情況。 ● 制定明確的勞動合約與「工作規則」，保障員工權益並降低違法風險。

2. 員工流失與吸引力風險 ● 高員工流失率對業務的影響，包括知識流失、招聘成本增加等。 ● 組織是否具備吸引和留住高素質人才的能力，特別是在競爭激烈的市場中。 ● 員工滿意度與敬業度調查反映的內部管理問題。	**2. 提升員工滿意度與敬業度** ● 定期進行員工滿意度調查，並據此調整工作條件與環境。 ● 提供競爭力的薪酬和福利，吸引及留住人才。
3. 多元化與包容性風險 ● 員工群體中的性別、年齡、種族或其他少數群體是否存在平權問題。 ● 組織是否建立多元文化、包容性管理的措施，以防止歧視和偏見。	**3. 推動多元化與包容性政策** ● 開展反歧視與包容性培訓，提高員工和管理層的意識。
4. 員工技能與學習風險 ● 技術變革或產業轉型可能導致的技能缺口。 ● 員工是否具備與時俱進的技能，特別是在數位化和自動化加速的情境下。	**4. 技能發展與學習計劃** ● 投資於智慧製造轉型的內部培訓計劃，確保員工具備未來所需技能。 ● 鼓勵內部職位輪調與鼓勵提案改善，提升員工跨部門技能。
5. 工作文化與道德風險 ● 是否存在職場霸凌、騷擾或道德問題，影響員工士氣及組織聲譽。 ● 領導層與員工之間的信任關係是否受到影響。	**5. 營造透明與道德的文化** ● 制定反霸凌和騷擾的零容忍政策，建立匿名舉報機制。 ● 領導層示範良好的倫理行為，傳遞正向的組織價值觀。