風險管理 GRI 2-13

尖點風險管理政策目標

尖點風險管理之目標旨在透過完善的風險管理架構，考量可能影響公司目標達成之各類風險加以管理，並透過將風險管理融入營運活動及日常管理過程，達成以下四大目標：實現企業目標、提升管理效能、提供可靠資訊、有效分配資源。

尖點科技風險管理政策與程序

尖點科技自成立至今，一直秉持嚴謹的風險管理來確保公司的正常運作，正視風險的存在。我們強化風險管理，並以積極的態度轉化風險為機會，定期透過風險的監控、辨識、衝擊評估與擬訂因應對策來降低風險。

為強化公司治理並健全風險管理作業，尖點於 2023 年 8 月董事會通過將隸屬於董事會之「企業永續發展委員會」更名為「企業永續暨風險管理委員會」，本委員會由 2 位獨立董事及 1 位董事所組成。

同日，董事會亦審議通過尖點之「風險管理政策與程序」，作為推動企業永續發展及風險管控之管理依據。透過「企業永續暨風險管理委員會」轄下功能推動小組每季定期會議檢視企業永續及風險管理推動成效。

尖點「企業永續暨風險管理委員會」職責及運作情形簡述如下：

- 審查永續發展政策、目標、策略與執行方案。
- 審查整體之風險管理政策、架構、組織、機制及管理標準。
- 關注各利害關係人，包括股東、客戶、供應商、員工、政府、非營利組織、社區、媒體所關切之議題及督導溝通計畫。
- 提出必要之改善建議，定期向董事會報告永續發展之運作及風險管理之情形。

2024 年度共召開 2 次「企業永續暨風險管理委員會」會議及 4 次轄下功能推動小組會議。

風險管理層級

董事會

企業永續暨風險管理委員會 董事 / 獨立董事

轄下功能推動小組

	公司治理	夥伴關係	幸福職場	綠色永續	社會關懷
議題	・永續管理 ・公司治理 ・法規遵循 ・技術創新 ・風險管理	・客戶關係 ・供應鏈管理 ・產品責任	・員工照顧 ・育才發展 ・職業安全 ・人權管理	・氣候變遷與環境政策 ・水資源管理 ・廢棄物管理	・在地關懷 ・環境保護 ・積極參與
權責單位	・經管室 ・財務處 ・研發處 ・管理部 ・稽核室、法務	・營業處 ・品保處 ・資材部	・管理部 ・安衛室	・管理部 ・資材部 ・製造部 ・營業處	・管理部 ・安衛室

風險評估項目

環境面	・溫室氣體排放管理 ・能源管理 ・空水廢毒噪排放管理 ・氣候變遷 ・循環生產
社會面	・職業安全衛生風險 ・人力資源風險
治理面暨經濟面	・市場風險 ・投資風險 ・財務風險 ・營運風險 ・智慧財產 ・資訊安全 ・供應鏈 ・法律風險 ・合規風險
其他面	・重大外部危害事件 ・極端事件引發之風險

風險管理程序三階段

第一階段 ／ 辨識與分析
・分析風險發生機率及影響程度
01

第二階段 ／ 評量與回應
・依據風險等級決定需優先處理之風險事件
・針對風險回應訂定相關處理計畫及執行
02

第三階段 ／ 監督與審查
・功能推動小組會同各營運單位監督執行情況
・企業永續暨風險管理委員會每年定期向董事會報告風險管理執行情形
03

當公司營運風險超出了例行性的控制（如：天然災害、人為因素、系統故障等事故），立即依風險管理政策與程序啟動公司危機管理機制。確保在急難狀況下仍能確保組織持續運作，並藉由實施風險管理程序，將事故發生時所帶來的衝擊和中斷時間降至最低。公司將持續鑑別潛在的風險並採取必要的管控，使發生事故時所帶來的衝擊降到最低程度，以確保尖點的永續營運。

2024 年風險緩解計畫執行情形

尖點依循年度風險管理作業時程，於每年下半年由高階主管針對內外部營運環境進行風險鑑別與評估，聚焦於對企業營運具高度影響性與可能性的潛在風險議題。針對評估結果中判定為「高風險」的項目，進一步擬定風險緩解計畫，包含預防性措施、監控機制與責任單位。相關計畫將納入次年度行動方案中執行，以降低風險發生之可能性與衝擊程度，確保營運穩定與永續發展目標之實現。

以下為因應 2023 年下半年鑑別出之高風險議題，所執行的風險緩解與監控計畫：

【資訊安全風險】緩解計畫執行情形	
致災源	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	2024 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 2024 年 12 月底，總計阻擋了網路攻擊 452,167 次及網頁攻擊 86,041 次，未有任何資料損毀之情事發生。

【財務風險】監控計畫執行情形	
風險面向	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 2023 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	集團財務處
執行成果	1. 2024 年 12 月 31 日現金為新台幣 20.13 億元，流動比率為 264%，速動比率為 219%。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. 2024 年 11 月發生某歐系客戶申請破產保護事件，考量應收帳款約台幣 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. 2024 年 12 月 31 日淨外幣部位為資產美金 300 萬元，匯率波動 1% 對損益表之影響數為新台幣 23 萬元，目前因避險需求，已承作衍生性商品淨額為美元 230 萬元，與淨外幣部位相當。

2024 年風險鑑別及其策略

2024 年 10 月「企業永續暨風險管理委員會」轄下功能推動小組，依「環境面」、「社會面」、「治理面暨經濟面」、「其他面」四大構面，鑑別出 2024 年主要風險議題為「資訊安全風險」及「人資面向風險」，並提出對應的風險緩解計畫如下：

【資訊安全風險】 緩解計畫

風險面向	風險因應策略
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. 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. 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、法務、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。
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。	
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。	
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。	

【人資面向風險】 緩解計畫

風險面向	風險因應策略
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，例如合約管理、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」，保障員工權益並減少違法風險。 2. 提升員工滿意度 ・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. 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. 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. 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。
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。 ・員工滿意度調查反映的內部管理問題。	
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。	
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。	
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。	

藉由危害鑑別與風險評估工具，將公司潛在可能威脅進行評估，依「風險管理程序」予以分級，針對風險等級為高風險者，擬訂目標及管理措施，並予以實施，確保公司得以持續維持營運。

展望 2025 年，尖點將持續依循政府法律及法規、企業永續暨風險管理委員會風險管理程序、公司內控機制之各項流程，確保公司業務持續營運，並以資訊工具提供預警機制輔助，強化公司對於各項風險之管理。