永續經營與風險管理、誠信經營、法規遵循與重大性議題關聯性

基本上，永續經營管理對內應依公司法建立《公司組織章程》，內含法規遵循、誠信經營，利益迴避與倫理道德，這些要藉由建置各項管理系統與制度，並向主管與員工宣導與培訓甚至測驗及格，讓員工們養成良好的職業道德與行為，融入經營理念自然形成【善的循環】企業文化。我們依據 TCFD 的邏輯連結重大性議題的關聯性下表：

管理層級	永續經營管理依據 TCFD 的規定連結重大性議題的關聯性
公司治理 – 誠信經營 – 倫理道德 – 法規遵循	· 依據 GRI 國際標準的規定：公司治理除包含內部治理架構、董事組成與任務等組織人員外，在國內必須遵守公司法等相關法規，若外銷必須遵守當地國家的法規，才能生存與成長的基本條件。 · 在永續經營管理，企業依法建立組織章程、倫理道德政策與制度等行為準則，如誠信經營、利益迴避、反貪腐及賄絡、及市場壟斷等不正當行為，企業應行公平競爭與交易，並教育訓練員工，讓各級主管與員工養成良好的行為。 · 企業財務與 ESG 永續經營資訊公開揭示，是公司治理與永續經營的佐證文件。
營運策略與管理	· 企業常用的經營策略有：財務或成本導向、顧客服務與滿意導向、產品或生產差異化、產品領導的核心作業流程、組織學習與成長構面等策略。配合建立管理系統與制度來管理，運用各類短中長期計畫與指標來達成預計目標。 · 針對氣候變遷對公司資產帶來實質的風險進行評估、分類與排序，建立因應策略以及精準且嚴謹的預防措施與緊急應變計畫；當危機或災難發生時，立即提出最適當的應對措施與恢復計畫，降低災害損害與不穩定性的可能影響。 · 在轉型風險方面，順應能源多元化趨勢，並配合《再生能源發展條例》的規範與目標，進行規劃與購買再生能源及投資綠電憑證之專案。
風險管理	· 依據 TCFD 的氣候風險分類有實質風險與轉型風險，前者如地震、水災、颱風、污水排放、乾旱、停電停水、跳電，後者有氣溫上升、節能減碳與排放量管制、企業形象。 實質風險有歷史案例可供查核與比對，也有緊急應變措施與預案應可有效管控損失；轉型風險係最近 10 餘年受重視的地球平均溫度上升造成極端氣候如豪大雨洪水、颱風多、乾旱頻傳等，故聯合國組織要求歐盟國家 2023 年開始實施【碳關稅】的措施，首波針對石化、鋼鐵與水泥業的高碳排放量的企業。降低碳排放量的設備或措施都會增加企業的成本 · 企業經營的傳統風險的議題有：財務調度與客戶信用、產品不良率高被客戶退貨要求賠償或重工、員工投訴或違反環保、勞動、公司相關法令被政府機關罰款，這些風險議題都會造成公司的財務損失，其大小視該發生案件的嚴重性，才能評估金額的大小與對公司營運後續的影響。
指標與目標	· 公司治理短中長期計畫與指標 · 永續營運短中長期計畫與指標 · 產品創新短中長期計畫與指標 · 社會公益推廣的短中長期計畫與指標 · 綠能、綠色生產、節能減碳與環境保護短中長期計畫與指標 · 友善職場勞動人權與健康安全短中長期計畫與指標

2.3 資訊安全

資通安全風險管理架構

本公司依據主管機關之規定加強資通安全管理，管理架構：由營運副總統籌，組織管理部，資訊室，稽核室，法務室設立資訊安全治理組織，檢視各項安全管理，統整資訊及建議改善計劃，由營運副總決議各項安全管理政策，提報董事長及執行長，指派政策執行專責人員推動與執行。

資訊安全政策

· 進行資訊資產風險評鑑，針對系統架構、網路安全、資源管理，軟硬體授權檢核其與企業環境是否合規性及高可用性，並對風險事項進行調整或納入改善計劃。

· 保密政策與資料保護宣導、檔案及記錄管理、移動設備管控、層級權限管制，以及稽核與法務單位不定時檢核與彙整記錄，協同運作，彙報各項異常資訊，降低資訊外洩風險，維護企業重要資產及競爭力。

· 與時俱進之資訊安全認知宣導，提昇員工資安意識、以落實於日常工作之中。

· 與各家資安公司保持密切合作關係，針對各地不斷發生的資訊安全事件及安全弱點，即時通知、調查及處理，確保弱點及早修復以防範未然。

措施落實

外對內，內對內多層防護

(1) 架構多層且不同廠牌防火牆設備，啟用各優勢功能，進階偵測技術，監控流量，識別應用程式，分析未知惡意軟體，預先阻斷不明連線行為與滲透。

(2) 跨廠區或跨機種網路控管，廠區間增設防火牆設備，防止病毒與攻擊跨廠區擴散。

(3) 增設多道多層式郵件防禦閘道，啟用 Attachment Defense，URL 即時檢測，BEC 詐騙，網路釣魚勒索病毒防護等功能，多維度檢測，反規避偵測，禦防進階式郵件滲透，攔截先進式攻擊威脅。

端點防護

(1)電腦依不同類型安裝一種以上防護軟體，除了增強基本防毒防護，更導入新世代端點APT端點防護，利用行為偵測功能，對於不尋常的操作行為零時差監控，即時阻擋及刪除惡意程式與降低橫向感染，另外，更利用機械學習和行為分析，阻止無檔案惡意軟體與記憶體攻擊。

(2) 購入入侵防護服務，即時警示與回應，阻止大規模入侵。

(3) 建立機台入廠檢測機制，防止惡意軟體伴隨著系統漏洞進入廠內。

(4) 端點裝置控管，禁止可攜式儲存設備或無線設備使用。

(5) 上網行為控管與隔離防護，文書作業與瀏覽外部網頁區分不同作業環境，降低誤觸釣魚網站進而下載惡意軟體至個人電腦中，阻斷駭客外對內潛伏。