2.3. 風險管控

依據營運產生的各種風險特性與影響程度，本公司有關營運重大政策、背書保證、資金貸與、銀行融資等重大議案皆經適當權責部門評估分析及依董事會決議執行，稽核室亦依風險評估結果擬訂其年度稽核計劃，並確實執行；以落實監督機制及控管各項風險管理之執行。

重要風險項目	風險管理權責單位（第一機制）	風險審議及控管機制（第二機制）	風險決策與監督（第三機制）	因應對策
公司整體策略及目標風險	一級主管	經營檢討會議	● 因應及處理最高決策機構：董事會 ● 負責風險事項之監控及追蹤單位：稽核室	● 每年年底透過策略營檢視當年度實績及隔年之策略目標訂定實施方向。 ● 每月經營檢討會審核及控管公司整體策略目標之達成狀況及風險對應措施。 ● 透過每週之主管會議即時反應可能影響目標達成之風險處理。 ● 每季至少召開一次董事會，檢視公司整體策略目標之達成狀況，對於各項目標無法達成之風險，決定因應及處理決策。
市場風險	業務部	經營檢討會議		● 新產品開發市場競爭行動：掌握及配合現有顧客發展方向，以增加新產品線的銷售機會。 ● 依據本公司之內控制度之銷售循環規範各相關部門作業，以降低接單及應收帳款流程風險管理、顧客之信用風險評估及控管作業。
法規遵循控管	管理部	經營檢討會議 董事會		● 本公司訂有「環境安全衛生法規及要求鑑別管理辦法」，每月由法規查核人員進行環安衛有關之法規查核，105 年起已推展到財務、工商、個資及勞動等相關法令之查核，以確認法令之符合度及即時改善作業。 ● 本公司訂有「合約審查管理辦法」，明訂核決權限以及審查程序。 ● 本公司聘有法律顧問加上隸屬之全興集團設立法務專責人員，對於各項契約、協議及法律事務提供諮詢服務。
資訊風險	總經理室	經營檢討會議	● 因應及處理最高決策機構：董事會	● 本公司訂定「資訊作業管理辦法」等作業標準，如：應用系統開發與維護、資料存取、備份機制、病毒與網路入侵防護、機房設置不斷電系統、門禁系統等。依據公司標準採取管制措施，並落實權限控管。 ● 資訊安全管理之管理架構、資訊安全政策、具體管理方案及投入資通安全管理之資源等完整說明如第 34~37 頁。

重要風險項目	風險管理權責單位（第一機制）	風險審議及控管機制（第二機制）	風險決策與監督（第三機制）	因應對策
財務風險	預算委員會 管理部	經營檢討會議 董事會	● 負責風險事項之監控及追蹤單位：稽核室	● 流動性風險：本公司獲利穩定、營運資金充足，尚無重大銀行借款，未來持續維持不低於月營收之約當現金及定存。 ● 利率風險：公司主要以營運資金收入即時償還長期及短期借款。在有短期資金時，公司主要投資於高流動性之短期票券及定存，以保障本金安全及維持流動性。 ● 匯率變動風險：隨時注意匯率波動情形外增減進口鋼材之外幣短期借款額度使用，做為外匯避險工具，與波動影響較大顧客協商隨匯率變動幅度調整價格機制。 ● 通貨膨脹風險：未來本公司會隨時注意通貨膨脹變化情形，調整當地原物料的採購庫存，並配合改善提案的推行降低成本及增加效率效益等。 ● 其他財務風險：本公司無從事高風險、高槓桿投資及衍生性商品等交易，本公司 110 年無再為他人背書保證，及無資金貸與他人事項。 本公司訂有「資金貸與及背書保證處理程序」，相關作業依其規定作業。
人員風險	管理部	經營檢討會議		因應人口結構改變、移工風險及少子化風險： ● 本公司持續與大專院校產學合作提供新進培訓人員。 ● 持續推展優化生產動線、推行 TPS 及 TPM 以提升生產效率。 ● 評估進行各設備及生產線自動化減少人員需求。
環境、安全衛生之災害風險	安管室 環安系統委員會	經營檢討會議 職業安全衛生委員會	● 因應及處理最高決策機構：董事會	● 本公司通過 ISO 14001、CNS 45001(ISO 45001) 等環安衛管理系統驗證，並進行內部 TPM 環安分科會之推展，透過系統運作及設定各項目標、方案持續推展中，以降低環境、安全衛生之災害風險。 ● 新興傳染病應變風險 (例如：COVID-19 等) 因應對策說明如第 76 頁。

重要風險項目	風險管理權責單位（第一機制）	風險審議及控管機制（第二機制）	風險決策與監督（第三機制）	因應對策
氣候變遷風險	能源系統委員會 溫室氣體盤查委員會	經營檢討會議 職業安全衛生委員會	● 負責風險事項之監控及追蹤單位：稽核室	● 110/12/21 董事會通過在「永續委員會」下設置氣候變遷治理組織「TCFD 推行委員會」，利用 TCFD 架構建構本公司的氣候風險辨識流程。經推行委員及種子成員等討論氣候風險與機會結果，彙總編製「至興精機 2021 年氣候相關風險財務揭露報告書」，詳如 6.2. 氣候變遷因應。 ● 本公司雖尚未被列入溫室氣體減量法規範對象，因本公司一廠及三廠為能源大戶，主要之溫室氣體為能源間接溫室氣體 (類別 2)- 電力約 85%，本公司自 104 年起導入 ISO 50001 能源管理系統，並成立能源推行委員會，推行過程實施多個能源管理行動方案，以每年至少節能 1% 以上為目標，同時進行溫室氣體排放量盤查，透過 ISO 50001 能源專案的推展，間接減少溫室氣體的排放量，以減緩氣候變遷風險。 ● 許多政府正在研議開徵碳稅或能源稅，對於生產所需原物料與能源的價格也逐年提高，而這些因素都將提高企業的生產成本。本公司將持續關注國內外法規變化，了解法規趨勢，做好及早因應之準備，以降低可能之財務成本。

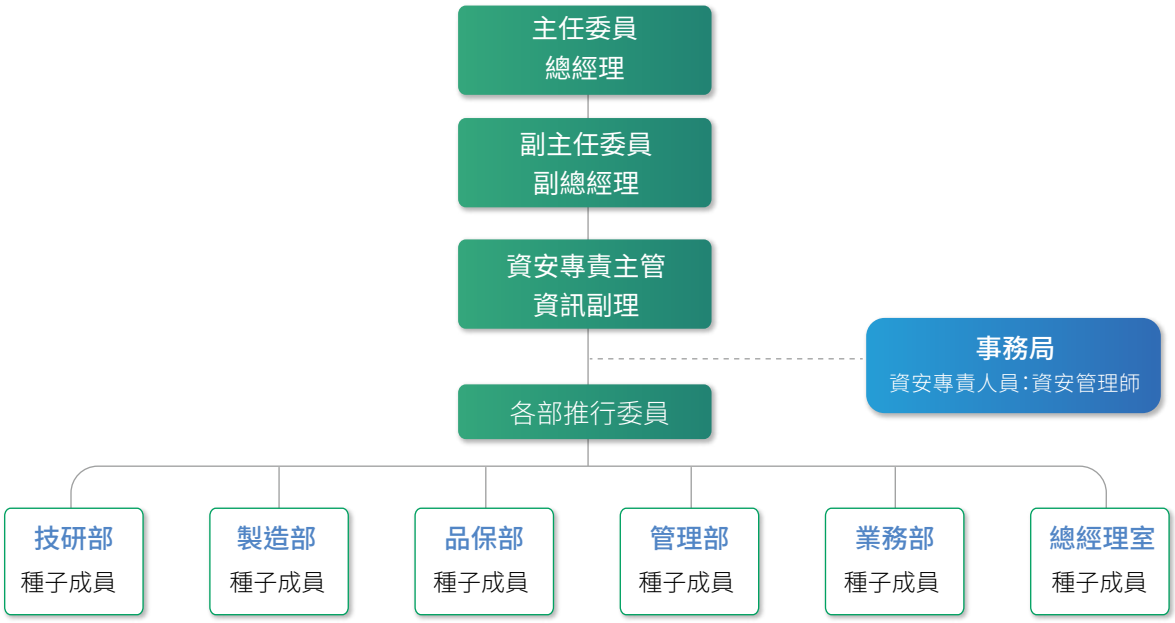
資訊安全管理

1. 資訊安全風險管理架構

本公司成立有風險管理委員會，每年定期進行風險評估，107 年 8 月起因應資訊系統設備可能故障或遭受入侵影響製造營運及會計等風險，加上因應措施也會增加額外成本，由資訊部門安排資訊設備預前檢修保養管理計畫，並加強各項資訊安全防護措施，訂定管理目標：提升資訊管理服務率 (MTTR)，管理目標於每月定期之主管經營會報進行績效檢討管控。

本公司訂定「資訊作業管理辦法」、「可攜式儲存媒體管理辦法」、「電子郵件作業」等相關作業標準，包括如 : 應用系統開發與維護資料存取、備份機制、病毒與網路入侵防護、機房設置不斷電系統、門禁系統、攜帶式硬碟及隨身碟管理、電子郵件使用權限管理等。依據公司標準採取管制措施，並落實權限控管，以確保資訊安全的活動及服務。

111 年 1 月為使資訊安全管理系統化修訂「組織資源管理辦法」成立資訊安全管理委員會，由總經理、副總經理擔任主任委員、副主任委員，並指定總經理室資訊副理及管理師擔任資安專責主管及資安專責人員，資訊安全管理委員會組織圖如下：

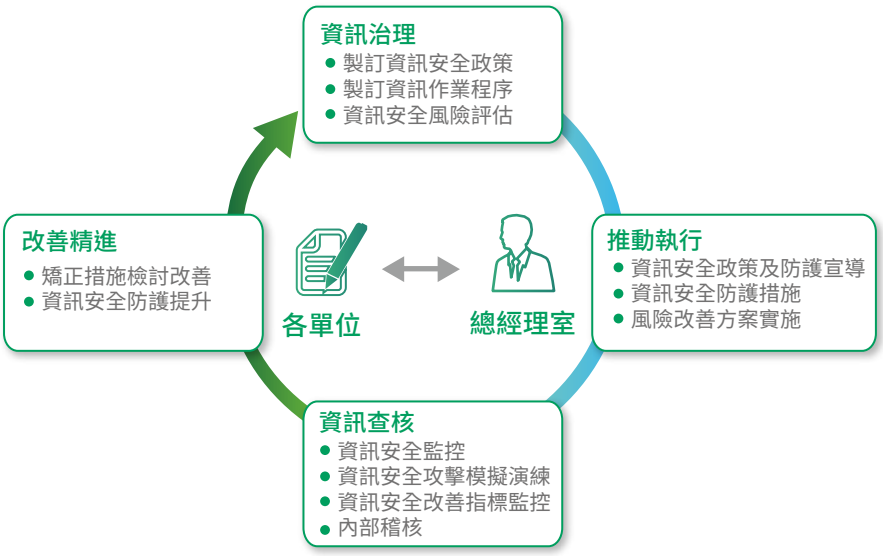


2. 本公司「資訊作業管理辦法」訂定資訊安全政策如下：

本公司為從事汽、機車零件及自行車零件製造之企業，為防止資訊系統受未經授權之存取、控制或其他侵害，並確保資訊機密性、完整性及可用性，制訂本政策如下，供全體同仁共同遵循：

- 符合政府資訊安全相關法規之要求。
- 建立系統及網路的權限，防止未經授權之使用。
- 提供合適的資訊軟硬體，維持公司之正常運作。
- 建立系統資料備份機制，驗證資料回復的可行性及正確性。
- 建立資訊安全防護措施，預防病毒及駭客入侵。
- 建立資訊安全通報機制，降低公司營運的影響。
- 員工資訊安全教育訓練，強化資訊安全的認知。

3. 資訊安全風險管理與持續改善流程圖



管理方案		110 年執行狀況
網路安全	• 強化網路防火牆與網路控管，防止電腦病毒跨機台及跨廠區擴散	• 建置防火牆進行即時監控，異常即時回報、排除
裝置安全	• 每兩年至少 1 次弱點偵測與滲透測試 • 依電腦類型建置端點防毒措施，強化惡意軟體行為偵測	• 109 年 7 月已實施，下次實施日期為 111 年 7 月 • 每周一啟動病毒碼更新與掃描
資訊安全保護技術強化	• 文件及資料加密控管及有效追蹤	• 依部門職務設定存取權限 • 電子郵件使用權限管理 • 攜帶式硬體及隨身碟管理 • 電腦系統主機報廢，進行破壞處理，確保機體不被他用，資料不被擷取與外流。
教育訓練與宣導	• 各單位每年至少 1 次實施資訊安全宣導 • 每年至少 1 次實施資訊安全緊急應變演練	• 110 年資訊安全宣導共 169 人次 • 110 年 6 月已實施資訊系統遭受入侵應變演練，下次實施日期為 111 年 5 月

5. 投入資通安全管理之資源

(1) 人力資源：本公司資訊安全作業執行人力包括主任委員、副主任委員、資安專責主管、資安專責人員、各部門推行委員及種子共 23 人。

(2) 資安設備：防火牆、防毒軟體、網路自動防禦系統、郵件過濾系統、應用系統開發與維護資料存取、行動媒體管理、存取管控及密碼管理、備份系統及雲端備存管理等。

(3) 實體環境建置機房門禁與不斷電系統等。

6. 即使本公司已建立上述管理作業流程、與許多資安防護措施，但無法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。

本公司將透過持續檢視和評估資訊相關的作業標準，以確保其適當性和有效性；透過內部每年各單位至少進行 1 次之資訊安全訓練宣導，以提高各單位使用者養成資訊安全守則的良好使用習慣，教育使用者不開啟來路不明檔案、不隨意安裝不明程式、勿任意連結網站；定期進行模擬資訊系統遭受入侵災害復原演練，並進行演練結果檢討，必要時檢討修訂原管理作業流程及增加必要設施，以降低可能發生不法入侵資訊系統的風險。

因應 COVID-19 疫情影響，大量使用視訊會議軟體可能存在的風險，進行管控如下：

1. 視訊會議軟體漏洞追蹤

由於駭客技術日益增進，視訊會議軟體之漏洞會持續遭到利用，因此定期追蹤相關漏洞新聞，確保安裝最新且已完成漏洞修補的版本。

2. 員工使用電腦之安全性

為確保視訊會議軟體安裝之安全性，進行作業系統安全性更新、登入使用密碼機制，並安裝防毒軟體與最新病毒碼等。

3. 連線之加密保護

視訊會議軟體連線，使用加密與金鑰方式，建立加密通道，連線至企業內網，確保資料安全與防護。

4. 高度資安意識與防範

強化整體資安意識，利用至興數位學習平台，宣導相關資安政策，落實資安措施與流程。

5. 視訊軟體之使用

本公司視訊會議以具有端點對端點加密 Cisco webex 視訊軟體為主，其他軟體安裝使用必須經申請同意後才能下載使用。