



## 2.3 風險管理

### 風險治理組織

為強化公司穩健經營的韌性與永續發展，飛宏成立風險治理組織由集團總經理擔任執行長，透過跨單位編制針對風險管理相關事務，建置系統化運作機制，並依據風險管理手冊，進行與公司營運相關之環境、社會及公司治理議題之風險評估與鑑別，每年定期向董事會報告風險治理執行情形與結果，俾使董事會得以監督風險治理機制運作及整體落實情形。

風險治理範圍涵蓋集團內各公司，風險治理成員由各事業單位之最高主管擔任，風險治理執行人員則由各事業單位指派專人執行日常營運中的各項風險治理相關作業。

### 風險管理政策與目標

建置並維持有效之風險管理系統且持續改善，使公司得以保障對客戶之承諾，維護股東權益、關注員工工作環境與健康及朝向永續經營。完整政策請參見本公司[風險管理手冊](#)。

### 風險管理目標



### 風險管理程序

#### 風險識別與監控

飛宏辨識及確認內、外部環境的潛在風險與衝擊，針對公司營運、技術、資安、設施、供應鏈、財務及人員等面向，於 2024 年鑑別出 10 項風險，較前一年新增全球地緣政治風險及總體經濟風險，同時針對不同風險項目制定了衝擊因應減緩措施與管理專責，建立從預警、應變、危機管理、以及復原行動等程序，確保營運永續。



面向	風險辨識	營運衝擊影響	減緩措施	營運契機
 環境面 (E)	電力、水中斷	電力、水資源等公共設施中斷營運受到衝擊。	<ul style="list-style-type: none"> <li>制訂緊急應變方案，降低電力、水中斷的衝擊。</li> <li>設置發電機、不斷電系統、評估儲能設施導入等。</li> <li>建置廠內儲水及外部水源支援機制；施行節水、節電措施。</li> </ul>	加速提升能、資源使用效率，導入再生能源使用，建置能資源應急機制。
	環境與氣候變遷	溫室氣體排放管理。 能資源管理。 空水廢毒噪管理。	<ul style="list-style-type: none"> <li>檢視國際環保趨勢制定符合營運需求之環境保護對策。</li> <li>進行災害預防監控，並演練緊急應變及復原能力。</li> <li>衝擊或威脅與因應策略詳見「氣候變遷風險與機會」章節。</li> </ul>	潛在機會詳請見「氣候變遷因應」章節。
 社會面 (S)	重大傳染病的威脅	因傳染病擴散，公司員工無法上班、材料無法準時運輸到公司，導致生產線停線，公司無法符合客戶需求。	<ul style="list-style-type: none"> <li>啟動防疫組織與SOP機制，確保人員安全上線，重啟運作。</li> <li>分流、異地上班，以分散風險。</li> <li>強化供應鏈夥伴關係，互享並配合供應鏈防疫機制。</li> </ul>	迅速且審慎計畫逐步恢復正常產出，以展現危機處理能力，爭取客戶信任與更多業務機會。
	職業安全風險	職業傷害與公共安全事件會衝擊到公司的正常營運，因嚴重程度的差異，甚至可能導致人員、財產的損耗與工廠停工。	<ul style="list-style-type: none"> <li>盤點職業病危害因素作業，避免員工接觸危害因素機會。</li> <li>加深日常維安意識及演練，如遇緊急災害、公安事故，立即啟動任務編組執行救助。</li> <li>強化勞資協商管道，建立和諧的勞資關係。</li> <li>落實員工健康檢查。</li> </ul>	降低並防範職災發生機會，確保人員財產安全，以增進利害關係人對公司持續營運的信心。
 治理面 (G)	全球地緣政治風險	政治衝突不穩定對公司營運及供應鏈帶來潛在威脅；連帶導致在地勞工市場混亂、匯率波動貨幣貶值等風險。	<ul style="list-style-type: none"> <li>定期檢視大陸廠區及合作夥伴營運據點地緣政治相關議題。</li> <li>擬定完整指揮體系及生產移轉計劃，並與主要客戶達成共識。</li> </ul>	加強供應鏈韌性，減少對單一國家或供應商的依賴，評估分散生產基地至政治穩定國家之供應商合作。
	總體經濟風險 (市場需求)	2024年全球經濟下行風險升高，特別是歐美市場經濟成長力道呈現負值持續疲軟影響企業整體銷售。	<ul style="list-style-type: none"> <li>定期與客戶持續溝通對於銷售數量之預期。</li> <li>審視資本支出合理性與控制工廠生產成本。</li> </ul>	鞏固及延伸核心競爭力，展現差異化優勢，超前部署綠色低碳品與循環經濟雙轉型。
	道德風險	因違反誠信經營與行為準則，導致公司損失。2024年針對各廠進行腐敗風險評估，識別出重大風險在於採購領域的不適當接受餽贈、金錢，或以交際費用支出換取供應商物品和服務投標優惠待遇的回報。	<ul style="list-style-type: none"> <li>飛宏新進員工報到須接受「企業道德與商業行為準則」訓練，並於訓練後簽名認可。</li> <li>不定期透過教育訓練及全員宣導，以推動誠信經營之重要與實踐。</li> </ul>	全員恪守企業道德與商業行為準則，並落實誠信經營。
	資通安全風險	因洩漏、竊取、破壞……等人為因素，或天然災害損害，所導致之公司、個人資訊及內外通訊系統異常，造成公司營運損失，甚至導致公司信譽的損害。	<ul style="list-style-type: none"> <li>每年二次資訊系統異地還原演練，模擬任何天災或人為因素導致資料損毀時，確保最短時間內恢復系統運作。</li> <li>維持兩家電信業者專線備援，確保對外營運正常。加強系統加密能力與密碼管理。</li> <li>落實員工訓練宣導，強化資安管理及員工守法觀念。</li> </ul>	建構高可靠度資訊安全管理系統，來防堵任何通訊中斷、資料遺失及洩漏的可能性，以取得所有利害關係人對公司的信任與支持。
	財務風險	<ul style="list-style-type: none"> <li>利率、匯率變動影響財務收入與支出，衝擊財務槓桿、通貨膨脹風險。</li> <li>關稅壁壘造成客戶下單意願及生產成本增加，供應鏈供貨受阻。</li> </ul>	<ul style="list-style-type: none"> <li>評估利率曝險項目及浮動利率之影響程度。</li> <li>匯率風險採取自然避險方式，短期資金投資以具流動性、本金和收益兼具安全性之銀行保本理財商品和定存為主。不從事高風險、高槓桿的投資活動。</li> <li>處分閒置資產現金流入和向金融機構申請之融資額度支應營運資金和長期資本支出。</li> <li>積極布局越南生產基地以有效彈性調動，減少貿易關稅的影響。</li> </ul>	<ul style="list-style-type: none"> <li>管理利率、匯率的變動對資產及現金流的影響，穩健公司的財務運作。</li> <li>強化營運與生產模式之應變能力、擴大供應鏈的夥伴關係及永續經營能力。</li> <li>配合政府投資優惠，持續強化台灣總部研發能力與科技人才，布局中國以外生產基地。</li> </ul>
	供應商風險	供應商無法如期提供原物料，影響正常營運及出貨。	<ul style="list-style-type: none"> <li>檢視庫存管理機制與「供料及時預警系統」。</li> <li>替代料供應商備援機制，確保物料來源穩定，無斷鏈風險。</li> <li>定期執行供應商之BCP稽核，協助供應商建立風險管理機制。</li> </ul>	強化與供應商的永續夥伴關係，以達成客戶需求與期望，共同創造雙贏共榮。



## 組織風險預警

本公司密切關注國內外經營環境的變化與風險，嚴格遵守政府法規及內部制度，並持續強化風險控管。具體措施如下：

### 財務風險控管

本公司堅持穩健經營原則，不參與高風險或高槓桿投資。匯率風險方面，採取自然避險策略，並透過舉借美元負債降低曝險部位。短期閒置資金則優先投資於具流動性且兼顧本金與收益安全性的銀行保本理財商品與定存。此外，透過私募普通股增資、發行五年期固定利率公司債，以及金融機構融資額度，確保營運資金與長期資本支出的穩定性。

### 營運風險控管

本公司深知天災與意外事故可能對生產運營及員工安全造成重大影響，因此採取積極預防管理策略，並嚴格執行風險管理計畫與安全規範，以確保達成電源產業的最高安全標準。

為應對災難（如火災、地震、颱風、停水、停電、戰爭、政治動亂、恐怖攻擊、食物中毒、法定傳染病、環境污染等），本公司建立完整的應變機制，確保在突發事件後能迅速恢復正常運作，降低公司與客戶財產損失，並維護企業聲譽及員工安全。此外，我們透過完善的保險規劃與固定保險費支出，轉移營運風險，將可能損失降至最低，以確保企業穩定發展。

## 2.4 資通安全

飛宏不斷精進資訊安全管理制度與強化防護能力，透過資訊安全管理委員會，推動並落實各項資訊安全管理措施，以保護公司智慧財產、客戶資料及提升員工資安意識，持續完備風險管控機制，以強化公司的資訊安全。

### 資安策略與治理

為落實資訊安全管理機制，確保資訊資產之機密性、完整性及可用性，飛宏於 2023 年底導入並建立資訊安全管理系統 (Information Security Management System, ISMS)，並於 2024 年 10 月取得國際標準 ISO/IEC 27001:2022 認證。透過 P-D-C-A (Plan-Do-Check-Act) 循環管理模式，持續精進各項安全措施，落實資訊安全政策，強化員工資安意識，並導入專業資安技術，藉此降低資安威脅所帶來的營運與財務風險，提升公司整體資通通訊防護強度，進而取得客戶信任。

#### 資安風險管理

- 資訊安全風險識別與評估
- 資安風險管理與對策制定
- 遵循資安法規與國際標準

#### 多層資安防護

- 人員與實體安全
- 帳號與權限管理
- 資安監控與維運
- 雲端安全



#### 檢討與持續改善

- 資訊安全措施檢討與改善
- 資訊安全教育訓練與宣導
- 資安威脅及技術掌握

#### 監控資安管理成效

- 資訊安全持續監控
- 資訊安全指標量化評估
- 資訊安全威脅演練
- 通過外部資安國際稽核認證

