鴻碩精密電工股份有限公司
2023 年度風險管理報告

2023 年 12 月 12 日

企業經營面對瞬息萬變、充滿營運挑戰的外在環境，建構風險應變機制暨強化風險管理能力已成為企業永續經營的必要條件。鴻碩公司為穩健營運、降低經營風險，在經營管理、環境、資訊方面皆有當責單位負責管理，經董事會通過擬訂風險管理辦法及擬訂企業風險管理政策。

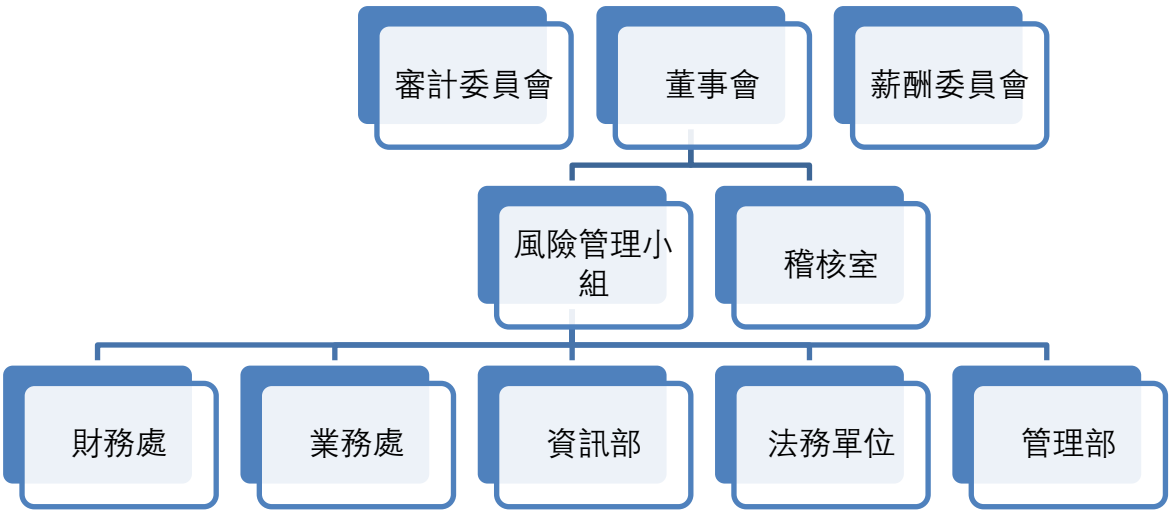
一、風險管理辦法

為促進本公司穩健經營與永續發展，建立健全之風險管理機制，於 111 年 12 月 14 日經董事會通過訂定風險管理辦法，作為本公司風險管理之依據。本辦法係為有效辨識、分析衡量、控制處理、持續監測各項風險，提升全體員工之風險意識，期將風險控制於可承受之程度內，達到風險控管之目標。

二、企業風險管理政策

1. 秉持企業永續經營及社會責任，建置企業風險管理機制，為公司所有的利害關係人提供適當的風險管理。
2. 針對重要的風險事件，進行事前風險評估，訂定危機處理程序及復原計劃，降低營運衝擊的嚴重度
3. 持續改善風險管理機制及縮短應變時間，提升風險管理的完整性及風險控制的有效性。

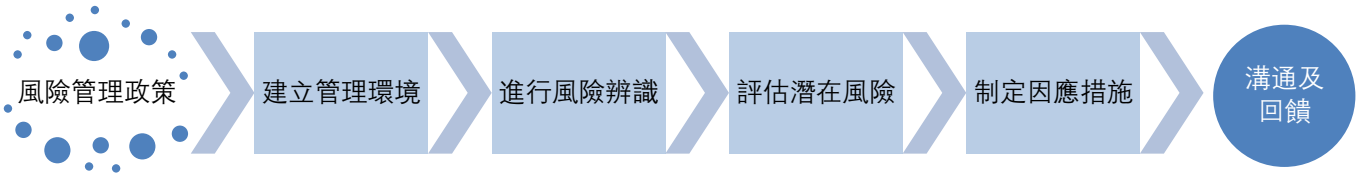
三、風險管理組織



本公司風險管理相關組織及權責如下:

1. 董事會: 核定整體之風險管理政策與重大決策，為本公司風險管理之最高決策單位，並負本公司整體風險管理之最終責任。
2. 風險管理小組: 永續發展專（兼）職單位下設風險管理小組，進行公司風險的綜合評估並向永續發展專（兼）職單位提出風險管理報告。永續發展專（兼）職單位每年定期向董事會報告。
3. 稽核室: 依據風險管理政策及風險評估結果擬訂年度稽核計畫並執行稽核作業，協助董事會監督決策之執行，確保各項作業風險均獲得有效管控，並適時提出改善建議。
4. 各風險管理單位: 本公司各部門為風險管理單位，應落實執行風險管理，部門主管負有風險管理之責，分析及監控所轄業務之相關風險，確保風險控管機制與程序能有效執行。

四、風險管理程序



本公司風險管理小組，由各單位主管負責風險管理計劃之推動及運作，並由各部門主管及同仁共同參與推動執行。每年至少一次向董事會進行報告運作狀況。本公司之風險及風險因應如下:

1. 災害風險管理: 地震、火災保險持續每年進行廠區投保事宜及人員進行防災教育訓練。
2. 策略風險管理: 客戶信用管理，依照授信管理辦法落實。
3. 營運風險管理: 隨時追蹤客戶貨款支付情形，每月針對逾期之帳齡進行檢討以及供應商履約與品質控管重要供應商執行供應商考核與評鑑並要求供應商提供品質保證合約及廉潔聲明書。
4. 財務風險管理: 隨時關注匯率、利率之變動，以減少財務費用。
5. 法律風險管理: 不定期針國內外重要政策及法律變動進行辨識與因應，以及針對重要合約與法律顧問及具備法律專業背景獨立董事進行審查，以確保足以保障公司權益及符合公司利益。

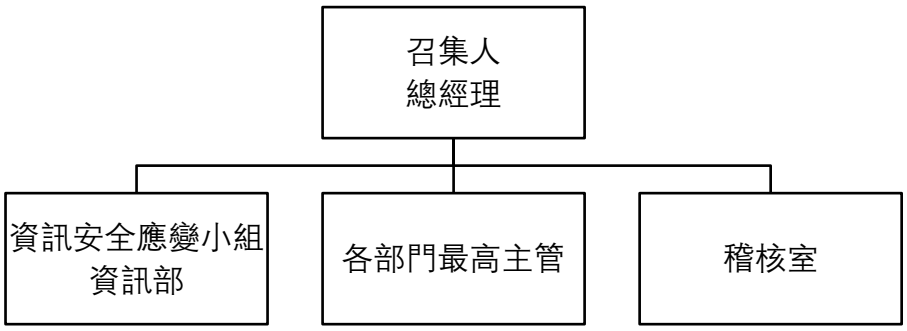
6. 資訊安全風險管理: 各項作業系統登入人員進行密碼管理，設置防毒軟體與控制外網使用及進行系統與資料的備份，機房使用電力備援系統，確保資料傳輸穩定，降低外部干擾造成資料存取中斷。

五、風險辨識及因應對策

項次	風險辨識	因應對策
1	利率風險	利率波動風險，美國為因應通膨危機，採取緊縮貨幣政策，持續升息。 本公司及海外各子公司支應營運周轉之銀行借款，大都以新台幣為主，中國大陸子公司則以人民幣借款為主，越南子公司則是以美元借款為主，因此，美元利率變動雖影響借款成本，但影響仍屬有限。惟應收帳款中約有 50%以上係以美元計價，除支付大陸子公司貨款外，大都承作定存，賺取台幣、人民幣與美元利差。因為利率的波動，對公司營運成本存在相當程度的影響，本公司也採取以下因應對策: 1. 分別於 2023 年 2 月份及 7 月份辦理現金增資及發行可轉換公司債，共募集約台幣 5.3 億元可轉換公司債，全數償還銀行借款，以調整財務結構。 2. 本公司 112 年 11 月底合併銀行借款(含應付短期票券及長期借款)為 1,294,883 仟元，合併利息費用為 35,709 仟元，占合併營業收入淨額比率為 1.79%，利息費用所占比率不高，故利率變動對本公司損益之影響尚屬有限，但為降低利率風險，持續與金融機構密切保持聯繫，隨時注意金融市場狀態，以取得較低之銀行優惠融資利率以支應營運所需資金，降低利息支出。
2	匯率風險	除中國大陸以人民幣計價外，本公司主要外幣仍以美元為主，而影響美元匯率波動的因素如下: 1.美國經濟 若美國經濟保持強勁，美元會升值，相反則美元會貶值。隨著重要的衰退指標為 2 年期和 10 年期美債收益率曲綫倒掛程度加劇，市場一致認爲美國經濟未來會陷入衰退，只是程度大小問題。自 2022 年 7 月初開始，2 年期美債收益率高於 10 年期美債收益率，兩者之間的利差為負數，並且不斷擴大，此一現象一直被視爲經濟衰退的前兆。 2.通貨膨脹 美國通脹居高不下，個人消費支出物價指數（PCE）目前在 5%附近，遠高於聯準會設定的 2%長期目標。只要通貨膨脹率沒有達到聯準會的預期，加息步伐就不會停止，美元也易漲難跌。 3.美聯儲貨幣政策 寬鬆的貨幣政策會讓美元貶值，相反，緊縮的貨幣政策會讓美元升

項次	風險辨識	因應對策
		值。聯準會正通過加息和縮表兩種調節手段去減少貨幣總量的流通，如果緊縮程度高於市場預期，將會推動美元升值。 4.其他央行貨幣政策 在美國實施緊縮的貨幣政策時，其他國家央行也在加息和縮表。如果其他國家的貨幣政策緊縮程度大於美國，那麼美元會相對貶值。 5.地緣政治的不確定性 當地緣政治的不確定性上升（如俄烏衝突及以巴戰爭）時，通常會更傾向於持有安全貨幣去避險。避險貨幣主要有國際貨幣美元，歐元，日元，瑞士法郎和黃金，其中美元作為世界交易量最大的貨幣，歷年來都是資本避險的第一選擇。 本公司截至112年11月底集團合併兌換利益淨額分別為23,398仟元，占合併營業收入淨額比率1.18%，兌換損益所占比率不高，且因本公司進、銷貨主要均以美金及人民幣報價居多，部分進銷貨可產生相抵效果，故整體匯兌因素對本公司影響並不重大。本公司為降低匯率變動對損益之影響，所採取之因應措施如下: 1. 隨時蒐集匯率變動之相關訊息，並參閱銀行及投資機構提供之金融財經資訊，與銀行間保持密切聯繫，充份掌握匯率市場走勢，且適時採取兌換外幣款項之措施，調整外匯部位，以降低匯兌風險。 2. 利用自然避險，將外銷收入之外幣資產與向大陸子公司採購產生之外幣負債互抵，在資金調度上，利用美元貨款承作定存，獲取美元與台幣利差。 3. 銷貨報價考慮匯率因素，以保障公司之合理利潤。 4. 集團財務人員每二週更新一次各關係企業最近三個月之資金規劃預估表，以隨時掌握資金狀況，減少資金閒置，平日帳上可使用之資金皆依最近三個月之資金規劃預估表作資金管控。並於每月結帳後，即可視當時整體經濟環境、觀察市場匯率變化，視時機將帳款與銀行預先融資運用，以降低匯率波動之風險。
3	通貨膨脹風險	全球主要經濟體國家多會將通膨率控制在大約平均 2%，以便使物價溫和上漲，有利經濟成長; 反觀今日，受到近年美中貿易大戰、COVID-19 疫情、俄烏戰爭以及以阿衝突等因素，致使產業供應鏈產生瓶頸，也讓全球的糧食、原油、天然氣等原物料價格上漲。通貨膨脹危機逐漸加深，導致整體經濟面臨原物料上漲的壓力。美國聯準會自 2022 年 3 月以來的持續升息，甚至是縮表政策，遏止通貨膨脹，但卻也引發市場產生停滯性通膨的疑慮。而歐洲央行也早於 2022 年 3 月加速量化寬鬆措施退場，讓「資產收購計畫」接替「疫情緊急資產收購計畫」。因此，全球經濟體皆已正式面臨通貨膨脹所導致之全球經濟下修的風

項次	風險辨識	因應對策
		險。 面對通貨膨脹風險，本公司也採取以下因應對策： 1. 本公司除隨時注意原物料市場行情變化，適時購入生產所需原料，並加強存貨控管，以降低因原物料價格變動對本公司損益造成的影響。 2. 審慎檢視資金運用效益及獲利率。先重新評估各項營運活動的成本，再分析當下所面對的經濟環境下，能掌握的利潤率，從而檢視及找出提高利潤率的解決方案，同時繼續確保高品質的產品與服務。 3. 重視營運效率，營運效率愈高，獲利率可能也跟著提升，使用可檢核的工作流程、工具與科技，以檢視與改善營運效率、但在追求改善營運效率的同時，尤其在通貨膨脹當下，雇主與員工站在相同陣線，溝通非常重要。
4	存貨風險	電腦及零件供需產業界正面臨全球高通膨、升息、俄烏紛爭、以巴衝突等不確定性，加上疫情期間的提前消費，導致電腦相關產業需求銳減。因此，「去化庫存」已變成整體產業需面對的風險，預計自 2023 年第三季起有機會逐步調整完畢。 面對存貨呆滯風險，本公司採取之因應策略如下： 1. 呆滯預防的控制措施 對呆滯存貨的產生需要追根溯源，做到提前預防和發現呆滯。在採購、銷售等整個供應鏈環節上全面預防呆滯存貨的產生，需要公司全體部門參與、有效整合供應鏈、快速應變並及時處理經營管理中遇到的問題。 2. 業務部門因應對策： (1) 業務人員要和客戶充分溝通，瞭解客戶需求，對客戶的訂貨進展情況進行分析、及時做好相關的溝通、督促和指導，以確保客戶能按照預期需求進行訂貨，防止客戶取消或變更訂單，提高訂單履約率和預測準確率。當市場需求預期變化，銷售訂單取消或變更時，業務部門應在變更發生後及時通知原廠供應商，及時針對尚未進貨之產品依據合約規範取消其訂單，以防止呆滯料的產生。對已發生的呆滯料，業務部門應提出相應的處理意見。 (2) 提高銷售預測的準確性，重點是通過客戶的歷史銷售資料、經營能力、庫存情況及市場變化等情況，對相應產品的市場需求做出合理預測。 (3) 由於客戶計畫變更產生的備貨呆滯，在一定條件下由客戶自行承擔。

項次	風險辨識	因應對策
		(4) 業務支援暨倉儲部門嚴格執行先進先出的原則，定期盤點，確保庫存資料的準確。 3. 呆滯存貨處理的改善對策: 對於已造成的呆滯，業務及生管部門應每月整理、更新呆滯存貨，責任部門要想辦法處理，將損失降為最低。若是外部原因導致的呆滯存貨，其損失可以轉嫁，應將呆滯存貨控制的重點放在解決內部因素導致的呆滯存貨。除了需要對庫存呆滯存貨處理流程重新進行梳理、確定呆滯責任歸屬以及將呆滯存貨處理與部門績效掛鉤。
5	資安風險	本公司遵循資訊安全管理制度，各項資訊作業不僅全力符合資訊安全標準流程與資訊安全法令法規，完備資訊安全治理制度，同時提升資安防禦能力，以降低資訊科技應用以及環境變遷所帶來未知的資安威脅風險。 一、本公司資訊安全政策 1. 資訊安全風險管理目的：強化資訊安全管理、確保資訊的機密性、完整性與可用性、資訊設備(包括電腦硬體、軟體、週邊)與網路系統之可靠性以及同仁對資訊安全之認知，並確保上述資源免受任何因素之干擾、破壞、入侵、或任何不利之行為與企圖。 2. 資訊安全風險管理組織:「資訊安全推動小組」統籌資訊安全管理等事項之協調、規劃、稽核及推動，成立跨單位之資訊安全推動組織。若組織有重大變更時（如組織調整、業務重大異動等）重新評估本政策之適用性。本政策將依照評估結果、相關法令、技術及業務等最新發展現況予以適當修訂，以確保符合實際需求。 3. 資訊安全推動小組：組織成員包括各單位最高主管，由總經理擔任本組織的召集人，如因職務調動應即刻指派遞補人員並辦理交接。  4. 資訊安全執行職責劃分：由資訊部最高主管指派資訊部人員擔任資訊安全應變小組，負責資訊安全須知、計畫及技術規範之研議、建置及評估等事項以及執行各項資訊安全作業，包含資訊安全預防及事件處理。並由稽核室負責資訊機密維護及安全稽核等事項。

項次	風險辨識	因應對策
		5. 資訊安全防護及控制措施：參考依據美國國家標準技術協會(NIST)的網路安全框架（Cybersecurity Framework，CSF），採取「辨識」、「防禦」、「偵測」、「應變」、「復原」、「訓練」等步驟來為企業資安做把關。 二、資訊安全實施計劃： 1.人員管理及資訊安全教育訓練： (1) 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。 (2) 針對管理、業務及資訊等不同工作類別之需求，進行資訊安全宣導，建立員工資訊安全認知，提升資訊安全水準。 2.電腦系統安全管理： (1) 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守。 (2) 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。 (3) 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。 3.網路安全管理： (1) 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。 (2) 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取，防火牆之設定及工作日誌檔需定期檢核，並經適當主管核閱。 (3) 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。 (4) 定期更新偵測病毒軟體之版本，定時自動偵測病毒，並訓練所有人員使用偵測病毒軟體，防止外之病毒。 (5) 訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。 (6) 關閉不必要之網路服務。任何網路服務皆需提出申請，經權責主管核准後，由資訊部人員開通之。 4.系統存取控制： (1) 訂定系統存取政策及授權規定，並以書面、電子或其他方式告

<table>
<tr><th>項次</th><th>風險辨識</th><th>因應對策</th></tr>
<tr><td></td><td></td><td>知員工及使用者之相關權限及責任。
(2) 離(休)職人員，應立即取消各項資訊資源之所有權限，並列入離(休)職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
(3) 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過三個月為原則。
(4) 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。
(5) 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。
5.系統發展及維護安全管理:
(1) 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
(2) 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。
(3) 委託廠商建置及維護重要之軟硬體設施，應在本公司相關人員監督及陪同下始得為之。
6.資訊資產安全管理:
(1) 建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。
(2) 依據公司機密保護、電腦處理個人資料保護及公司資訊公開等相關法規，建立資訊安全相對應的保護措施。
7.實體及環境安全管理:
就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。
8.業務永續運作計畫之規劃與管理:
(1) 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
(2) 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。
三、2023 年已實施之資訊安全重大管理方案:
<table>
<tr><th>項目</th><th>方案內容</th></tr>
</table>
</td></tr>
</table>

項次	風險辨識	因應對策		
			防火牆防護控管	防火牆設定連線規則，預設只開放基本上網、郵件收發等連線。 如有特殊連線需求需經請權限經部門主管與資訊部最高主管核准始能開放。 隨時監控防火牆網路連線狀況。
			資訊機房安全控管	機房進出有門鎖，進出需要有鑰匙，非經允許不得進入。 機房有 UPS 不斷電系統，不正常停電時電源不會中斷，待大樓發電機啟動仍可正常使用，資訊人員有時間可以做後續處置。 機房檢查紀錄表紀錄機房溫溼度、伺服器、網路設備狀況。
			防毒軟體控管	公司有安裝企業端點防毒軟體伺服器集中監控管理。 使用者的電腦都要安裝企業端點防毒軟體並定時更新防毒軟體病毒碼，降低中毒風險。
			郵件安全控管	郵件伺服器有主動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及惡意連結內容的郵件。 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。 郵件伺服器會保留所有郵件進出的備份資料。
			資料備份機制控管	資訊系統程式與資料庫皆設定每日完整備份，然後再備份一份到 NAS 備份主機。 公司內各部門檔案存放在檔案伺服器，並由資訊部統一備份到 NAS 備份主機保存。 每周將備份資料放到行動硬碟交管理部人員做異地備援存放。 重要相關文件由文件管理系統控管版本與權限，並在不同廠做主機與資料異地備援。