

2020 風險管理政策運作情形報告

一、利率、匯率變動、通貨膨脹情形對公司損益之影響及未來因應措施：

本集團各公司財務體質健全、自有資金充足，資金規劃以保守穩健為原則，首重安全與流動性，資金成本提高之風險有限。

單位：新台幣仟元

	2018 年度		2019 年度		2020 年前三季	
	金額	占營業收入比例 (%)	金額	占營業收入比例 (%)	金額	占營業收入比例 (%)
利息收入	9,333	0.19%	10,657	0.22%	4,985	0.14%
利息費用	10,097	0.20%	11,263	0.24%	7,146	0.21%
兌換利益 (損失)淨額	33,452	0.67%	(15,504)	(0.33%)	(17,109)	(0.50%)

由於所占各項比率均不高，故利率、匯率、通貨膨脹情形對集團營收及獲利之影響程度不大。本集團營運所需資金以自有資金為主，借款為輔，109年第三季銀行借款金額計\$370,165 仟元，占資產總額\$4,312,013 仟元之8.58%，故利率之變動對本集團獲利之影響程度有限。惟本集團基於穩健仍對擬定下列具體措施：

1. 每日蒐集利率變動資訊，以適時採取適當之因應措施。
2. 若利率走低，則適時調整舉借利率較低借款以償還利率較高之借款，如利率走高，可能侵蝕本集團整體獲利時，將評估以現金增資或發行可轉換公司債方式來取得所需之資金，以降低對銀行借款之依存度，分散利率變動之風險。

本集團產品之主要銷售地區為歐洲、美洲及亞洲等海外市場，而產品主要之零組件大部分係購自台灣廠商，僅部分原物料如 IC、電源供應器及特殊用途之面板等係向國外採購，故外購比率並不高。而外銷交易主要係以美元及歐元計價，在扣除購料之少許美元或歐元需求後，呈現美元或歐元之淨外幣部位，因此匯率變動對本集團之獲利有一定程度之影響。而本集團針對持有外幣部位可能產生之匯兌風險採取如下之因應措施：

1. 由財務單位依據國際間政經情勢發展、與金融機構保持聯繫並蒐集即時匯率資訊，以充分掌握匯率變動趨勢。
2. 採自然避險方式，藉由應收、應付外幣項目沖抵，預估匯率未來走勢維持適當外匯部位以因應未來外幣付款需求外，適時結售外幣淨部位，以降低匯率變動對公司之影響。
3. 以避險而非投資交易為原則，與往來金融機構簽訂遠期外匯合約，以規避匯率變動風險。

由於近年來全球經濟景氣成長仍處於遲緩階段，通貨膨脹之情形對本集團尚無明顯影響。

二、從事高風險、高槓桿投資、資金貸與他人、背書保證及衍生性商品交易之政策、獲利或虧損之主要原因及未來因應措施：

本集團並未從事高風險、高槓桿投資、衍生性商品交易、資金貸與他人及為他人背書保證之情事。未來如從事衍生性商品交易則以避險而非投資交易為原則，以規避匯率變動風險。

三、國內外重要政策及法律變動對公司財務業務之影響及因應措施：

除下列所述者外，經評估最近年度國內外重要政策及法律變動對本集團財務業務並無重大影響，未來亦將隨時掌握相關訊息，評估重要政策及法律變動對於本集團之影響，採行必要之因應措施。

國際財務報導準則第16號「租賃」(IFRS 16)

- A. 國際財務報導準則第16號「租賃」取代國際會計準則第17號「租賃」及其相關解釋及解釋公告。此準則規定承租人應認列使用權資產及租賃負債（除租賃期間短於12個月或低價值標的資產之租賃外）；出租人會計處理仍相同，按營業租賃及融資租賃兩種類型處理，僅增加相關揭露。
- B. 本集團自108年起將屬於承租人之租賃合約按IFRS 16處理，採修正式追溯，不重編前期財務報表。

四、科技改變及產業變化對公司財務業務之影響及因應措施：

工業電腦廠商一致看好新一波產業成長動能在人工智慧與物聯網相關應用，掌握技術利基、應用市場利基及垂直應用產業的經營策略利基。本公司將藉全球經銷網與深耕專案，彙集顧客需求與市場動向資訊，以快速提供能滿足客戶產品規格。於財務運作上，更針對產業之特性，加強現金流量管理，分散經營風險。

五、企業形象改變對企業危機管理之影響及因應措施：

自創立以來，即積極強化公司內部之經營管理，並持續提升產品品質管理之能力，為健全公司治理及加強董事會相關職能，本公司已依證券交易法第十四條之二規定設置三位獨立董事，於100年8月成立薪資報酬委員會，協助董事會執行薪酬管理機能，104年6月設置審計委員會，且於105年10月成立提名委員會。近年開始參與「企業社會公益及企業志工推動協助方案」，協助企業發揮企業社會責任，將公益行動結合企業核心價值與企業營運做創新整合，推動企業志工服務善良文化，讓企業志工成為建構良好公民環境的重要資源，共同為關懷社會及改變世界盡一份心力。近來本公司之企業形象並無發生重大改變，市場上亦無任何不利公司企業形象之相關報導。

六、進行併購之預期效益、可能風險及因應措施：

本公司於108年以現金56,068仟元購入AXIOTEK ITALIA S.R.L.(簡稱AXIT)100%股權，AXIT原為本集團義大利經銷合作夥伴，併購後有利本集團拓展義大利鄰近區域工業電腦及相關電子產品銷售業績，增加營收貢獻。

七、擴充廠房之預期效益、可能風險及因應措施：無。

八、進貨或銷貨集中所面臨之風險及因應措施：

1. 進貨集中所面臨之風險及因應措施

本集團產品之主要原料可分為半導體IC類、印刷電路板類、液晶面板、電源供應器與IPC產品（包括單板電腦及工業電腦機箱），由於原料種類繁多，加上主要原料國內之電子零組件供應廠商眾多，產品替代性高，且未曾發生斷貨情事，故尚無進貨集中風險之虞。

2. 銷貨集中所面臨之風險及因應措施

本集團並未發生對單一銷貨客戶之銷貨比重達15%以上之情事。故無因銷貨集中所面臨風險之疑慮。

九、董事、監察人或持股超過百分之十之大股東，股權之大量移轉或更換對公司之影響、風險及因應措施：無。

十、經營權之改變對公司之影響、風險及因應措施：無。

十一、訴訟或非訟事件：

本集團並無其他已判決確定或尚在繫屬中之重大訴訟、非訟或行政爭訟事件，其結果可能對股東權益或證券價格有重大影響者。

十二、其他重要風險及因應措施：

本公司已成立風險管理組織，整體風險管理政策主要是建立不同的風險預警網路及報告系統，並藉由有序的風險控制及監控，因應各種突發狀況之發生，期能有效落實管理以將風險衝擊降至最低。

1. 風險管理組織：

組織名稱	權 責
董事會及高階決策組織	1. 公司風險管理及政策訂定 2. 督導重大風險因應方向及確保風險管理機制
執行長室	1. 佈達決策組織訂定之風險管理決策 2. 重要風險之預警及彙總重大風險因應對策與處理結果
稽核室	1. 負責風險事項之監控及追蹤
總公司及各子公司	1. 部門職掌之日常風險管理活動 2. 公司管理風險決策之執行 3. 公司重大列管風險事件，主動回報具體對策及執行成效

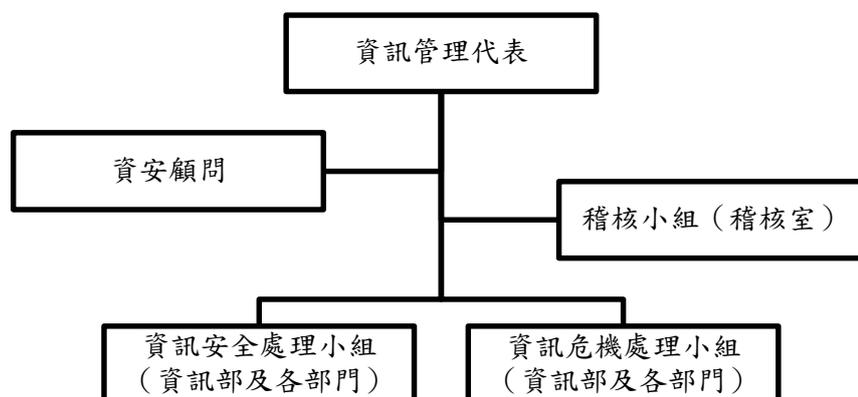
2. 重要風險項目及管理架構：

重要風險項目	風險管理 權責單位	風險審議機制	決策與監督
市場風險、新客戶開發、競爭者行動	業務暨行銷處	經營決策會議	董事會 為各項風險 因應及處理 之最高決策 機構
產能風險、訂單不足及供料延遲、原料價格變動	執行長室 業務暨行銷處 資材部		
資訊風險	資訊部		
政策及法令遵循	執行長室 財務處		稽核室 負責風險事 項之監控及 追蹤
投資、匯率及財務風險 衍生性商品交易及資金運用管理	財務處		
訴訟及非訟事項	法務室		
財務報表表達、資訊揭露、 資金貸與他人及背書保證之管理	財務處		
董事及大股東股權異動		董事會	
董事會及股東會議事管理	公司治理主管		

3. 資訊安全風險管理：

(1) 資訊安全組織架構：

- A. 本公司資訊安全之權責單位為資訊部，設置資訊主管一名及專業資訊人員數名，負責訂定資訊安全政策、規劃及執行資訊安全政策推動與落實，並定期向董事會報告公司資安治理概況。
- B. 本公司稽核室為資訊安全監理之督導單位，設置稽核主管一名及專職稽核人員一名，負責督導資安執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低資安風險。



(2) 資訊安全風險：

在資訊安全風險方面可分為資訊紀錄暨電腦系統及設備進行評估分析。資訊記錄包含資料庫、資料檔、系統規劃與設計文件、使用與操作手冊、業務流程、合約、教育訓練教材、制度文件、內部控

制管理辦法、其他相關典章制度等，而電腦系統包含：電腦作業系統、應用系統、開發工具、套裝軟體、公用程式等項目。本公司有關單位依據過去公司內部之資安事件及全球資安案例評估資安風險，其主要風險為資訊不當使用及流出，以及操作人員對於電腦系統不熟悉，誤使用有病毒之設備。為因應管理資訊風險，本公司資訊管理作業訂有相關內控制度及作業辦法，在財務及非財務之資訊管理透過權限設定及核決權限的設計進行管控外，平時對員工進行宣導，應避免透過公司網路收發或下載與業務無關之郵件或軟體，以避免佔用公司之網路資源，及增加電腦病毒感染機會，防止因人員疏忽所造成資訊安全的危害，在資訊系統及設備方面，公司並設置防火牆及防毒軟體並定期掃毒，病毒碼及修補程式應即時更新，以防止駭客或電腦病毒之侵害

(3) 資訊安全政策

- A. 依P.D.C.A循環流程管理持續改善，維護公司重要資訊系統的機密性、完整性與可用性，促使本公司資訊安全管理制度能貫徹執行、有效運作、監督管理。
 - a. Plan 預知管理：防止入侵攻擊，防止意外（備份），制訂資訊安全政策。
 - b. Do 應變管理：損失控制，災難復原（還原），改變內部作業程序。
 - c. Check 改善追蹤：檢視真相，防止二次災害
 - d. 資訊風險評估機制。
 - e. Action 推動執行：資訊安全政策執行，同仁資訊安全教育訓練
- B. 降低資訊安全管理與營運風險及電腦病毒危害中斷服務的頻率，加強企業同仁對資訊安全的認知，降低資安事件，強化組織對內外之風險管理，提昇客戶對本公司品質滿意度並達到企業持續營運的目標。

針對風險管理，分為三個面向對應及預防風險事件的發生。預防資安事件(事前)：防止入侵、防毒、防意外(備份)及防外洩。處理資安事件(事中)：防止災害擴大，停止損失，最短時間復原(還原)。調查資安事件(事後)：調閱，查核，檢討，持續改善(P.D.C.A.)，風險控制，防止再度發生。