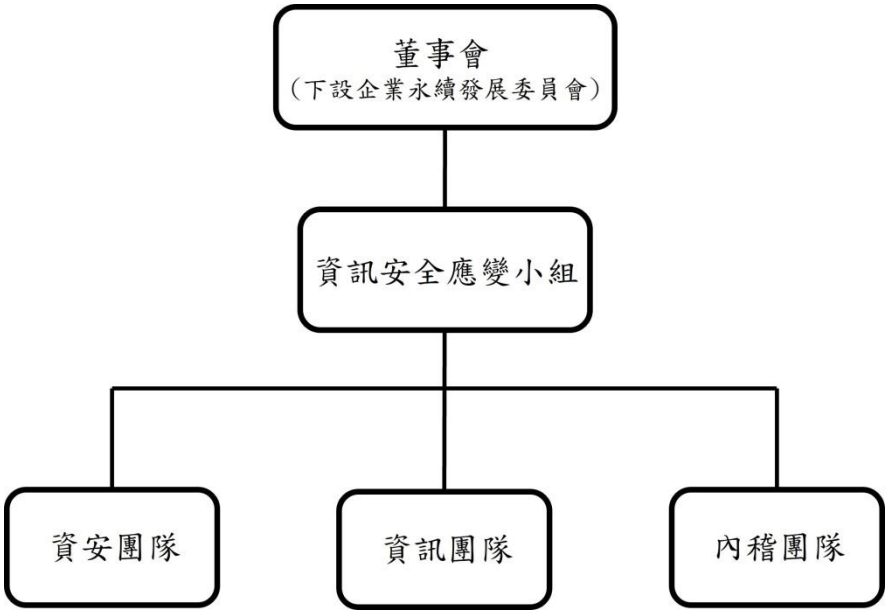
六、資通安全管理

(一)資通安全風險管理架構

透過建立資通安全風險管理架構，降低內外部資通環境所帶來未知的資安威脅及風險。本公司於民國 112 年設立「資通安全應變小組」負責統籌資通安全作業規劃、執行及維護資通安全管理系統；同時推動資通安全政策之執行，遵循標準作業程序以落實風險管理並定期進行內部資通安全查核，以確保本公司資通安全管理運作之有效性。

本公司財務長擔任資通安全長暨資通安全應變小組主席，公司內各單位（包含資訊、法務、稽核、研發、生產等）主管均為應變小組成員；同時資訊部為首要權責單位設置資通安全主管乙名、專責人員乙名及專業資訊人員數名，專責公司資通安全相關事務，落實各作業符合標準程序並追蹤實施情形。

本公司資通安全應變小組透過每年管理審查會議，不斷重新審核資安績效指標達標率及本公司採取對應的控制措施與方策，確保資通安全管理體系持續運作的適用性、適切性及有效性。應變小組每年向董事會彙報資安管理成效及資安策略方向，並不定期召開資通安全工作檢討修正會議。



(二)資通安全政策

本公司致力於企業永續經營的目標,確保本公司各資通系統維持有效地運作，資通安全政策效力涵蓋本公司及海外子公司，是以「一、建立符合法規與客戶需求之資通安全管理規範；二、提升全體同仁意識，資通安全人人有責的共識；三、保護本公司資通訊的機密性、完整性與可用性以符合內外部關注方之期望；四、提供安全的研發、生產、辦公環境，確保公司永續營運的量能」為指導準則。

各項資通安全管理規定遵守政府相關法規（如：資通安全管理法、上市上櫃公司資通安全管控指引、公開發行公司建立內部控制制度處理準則、個人資料保護法等）之規範以支援各業務正常運作，以期資安威脅導致營運損失的影響降到最低。本公司全體員工以此資通安全政策作為管理及遵循之依據。

本公司致力保護資通資產之機密性、完整性與可用性，並保障資訊資料隱私之安全，共同努力以達成下列資通安全管理目標：

(1) 重視各資通資產目標之風險等級加以鑑別與分級，以確保資通資產的機密性、完整性、可用性。

(2) 維護本公司及海外子公司作業環境資通安全之一致性，兼顧資通安全規範與資訊交換及分享。

(3) 各項資通安全管理規定，須符合政府資通安全相關法令、規定與政策要求。

(4) 所有資通作業相關措施，須確保符合本公司資通安全要求，防止敏感性與機密性資料外洩或遺失。

(5) 適當保護資通資產(含各公務所用軟體、硬體、網路通訊設施及資料庫等)，採行合宜之備援回復設施及作業，防止未經授權或因作業疏忽對資通資產所造成之損害，並定期演練上述備援回復作業。

(6) 本公司執行之各業務專案，對應適當資通安全管理措施，以確保相關資通受到適當保護。

(7) 落實資通安全內部稽核制度，使查核管理實務以達有效地執行及矯正預防。

(8) 建立營運持續運作計畫，確保本公司營運服務持續運作。

(9) 定期實施資通安全教育訓練，加強意識與強化其對相關責任之認知。

(三)具體管理方案

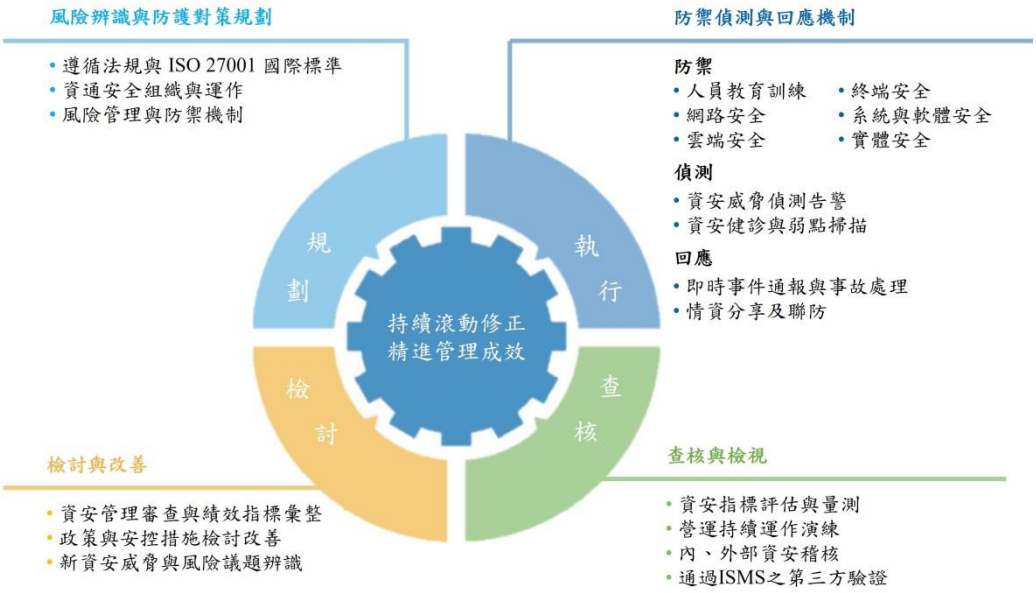
本公司積極強化整體資通系統之安全性，自資通安全規範開始，乃至於資通環境基礎之設計、系統維護及升級汰換、專業人員訓練、員工資安意識提升宣導，均納入資通安全整體考量範圍，每年進行自我檢視相關制度是否符合環境變遷，並依需求適時調整。

「規劃階段」著重資安風險管理，本公司已於 112 年導入 ISO/IEC27001:2013 資訊安全管理系統（InformationSecurityManagementSystem,ISMS)並通過驗證審查，維持證書有效期至 114 年 10 月 31 日。

「執行階段」建構多層資安防護機制，執行相關資安檢測作業，持續導入資安防禦創新技術，將資安控管機制整合系統化，以符合資安管理作業流程並加以監控。

「查核階段」積極稽核資安管理成效，依據查核結果提出矯正及預防對策，將其衡量並量化分析，提升資安目標落實度及可視性。

「檢討階段」則以檢討修正、落實監督及管理審查確保資安管理持續精進並有效執行。



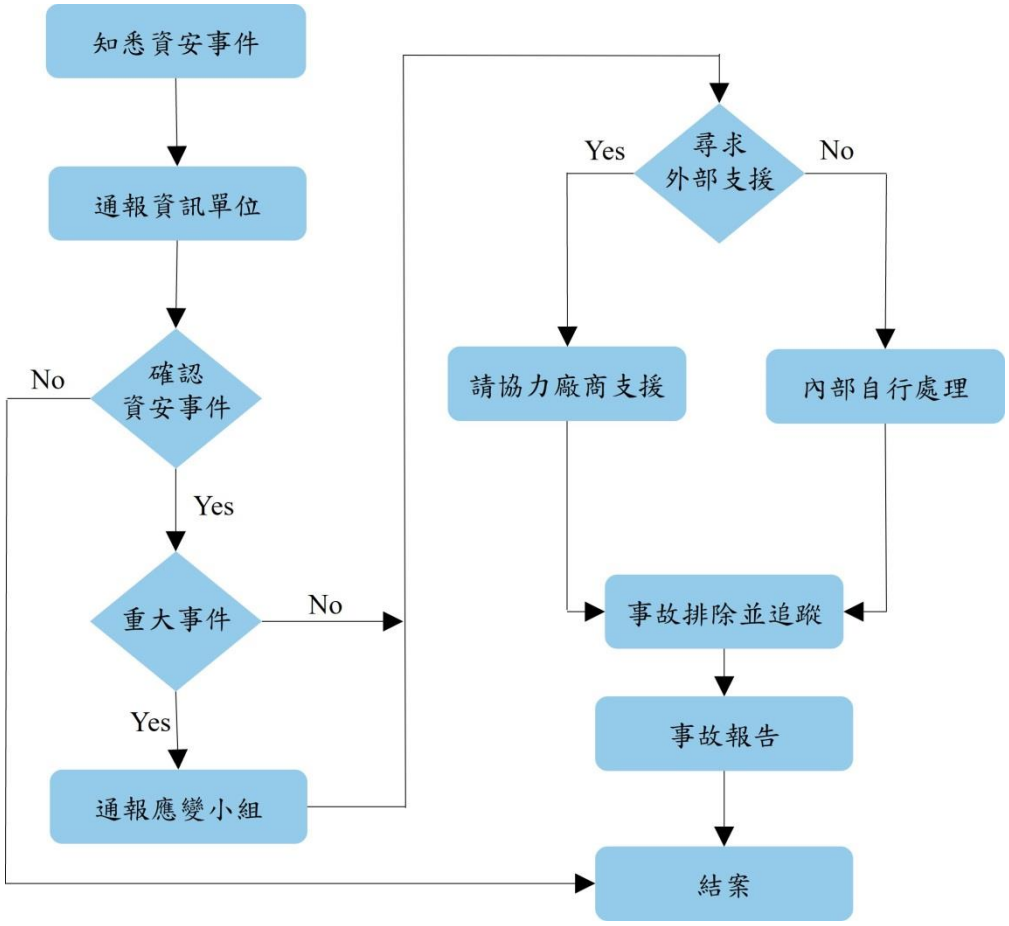
從系統面、技術面、程序面降低企業資安威脅，以符合資通安全要求；建構高規格的機敏資訊保護措施，持續強化本公司資通安全管理，具體施行措施包含如下：

類別	說明	管控措施
權限管理	人員及群組帳號及認證方式管理、權限管理、系統管理權限控管。	(1) 帳號管理作業，均依作業程序申請及經各權責主管核准後進行使用及變更，離職或職務變更後立即撤銷其使用權限，以防止未經授權之存取。 (2) 定期審視系統相關帳號權限。 (3) 系統帳號生命週期及帳戶權限管理。 (4) 核心資通系統採行多因子認證及限定登入點方式管制。
存取管理	資料流控管及稽核，實體設備存取管理、稽核紀錄及事件調查作業。	(1) 重要資通系統之資料流之進出、修改及行為歷程等活動，加以保存其存取稽核紀錄。 (2) 資通系統主控台之實體安全防護。 (3) 資通系統之稽核紀錄分析與自動異常告警作業。 (4) 依重要性及風險程度進行資通安全等級分區處理。 (5) 資通安全所適用範圍之相關機敏資訊文件避免非經授權的存取。
威脅及風險管理	對於內部員工、外部人員、系統潛在弱點所可能帶來的資訊風險進行評級，並施以降低風險之處置。	(1) 全體員工電腦預置作業標準化。 (2) 外部廠商存取本公司資通系統之作業規範。 (3) 新技術導入之風險評估作業流程。 (4) 採縱深防禦架構及郵件內容過濾機制等，降低外部網路攻擊及釣魚信件的入

		侵機率。 (5) 自動分析回應資安威脅系統（FortiSIEM）與應用程式白名單（ApplicationWhitelisting）機制。 (6) 加強端點安全，使用者電腦定期更新並安裝防毒軟體。 (7) 定期進行人員資通安全宣導及教育訓練，提高人員的資通安全意識。
系統完整性及可用性管理	維護資料與系統之可用性與完整性，發生災害或受破壞時，可回復正常作業。	(1) 主機已完成虛擬化作業，並以叢集方式設計，以提升系統之可用性。 (2) 導入大型儲存裝置，並搭配定期自動化本地及異地備份作業，並依計畫進行還原測試，確保系統之完整性與可用性。 (3) 基礎設施多重備援機制，多套不斷電系統搭配自動發電機，內外網路線路及設備多重備援，降低資通服務中斷的機率。
營運持續運作管理	營運持續計畫及災難復原演練規劃，確保資通系統之可用性。	(1) 分析資通作業衝擊性並訂定營運持續管理計畫實作演練。 (2) 同時建立資通安全事件應變計畫，依事件嚴重度等級進行影響和損失評估，採取對應的事件通報及災難復原行動。

本公司遵循金融監督管理委員會、臺灣證券交易所及櫃檯買賣中心之相關法規要求，當發生資安事件時，需對外發佈重大訊息，資安團隊提交事件報告予資訊安全長與總經理室確認無誤，即可由財務處股務單位對外發出；資通安全事件過後，訂定資通安全事件的矯正及預防措施，並立即採取後續的改善行動。

資通安全事件處理流程尤為首重：當發現資通安全事件發生時，資安窗口統一將事件紀錄於ITS系統，留存事件相關跡證與紀錄並於第一時間發出內部公告，於最大可容忍中斷時間進行恢復，同時保存相關軌跡之跡證以供追蹤調查與數位鑑識作業。如仍無法恢復，將由資訊安全長召開「資通安全應變小組會議」對事件進行評估，適度調配各職責任務工作並會同外部資安專家研析處理方案。



(四)投入資通安全管理之資源

經歷全球後疫情時代，企業組織仍然不斷遭受攻擊者以不同的入侵手法攻擊，本公司資安防護策略也予以調整，因應整體資通安全發展趨勢，完成資通安全管理目標並持續投入資源：

(1) 專責人力：設立「資通安全應變小組」同時配置專職人員，負責公司資通安全規劃、技術導入與執行稽核，以維護及持續強化資通安全管理。

(2) 因應 112 年導入 ISMS 專案，進行相關工作會議已舉辦逾 22 場，參與人員包含外部顧問、本公司資訊及資安相關人員。

(3) 本公司已成為台灣電腦網路危機處理暨協調中心(TWCERT/CC)會員，該中心可提供資安事件諮詢及協調協處服務，使公司有效接收及傳遞資安情資。

(4) 本公司除每月固定於 EIP 入口網公告資安意識之宣導外，並於公共區域播放資安宣導影片及張貼資安宣導海報，另資訊部門如遇有特殊資安情資，其風險程度有可能影響本公司資通安全時，即時以通訊軟體及內部郵件方式告知相關同仁。

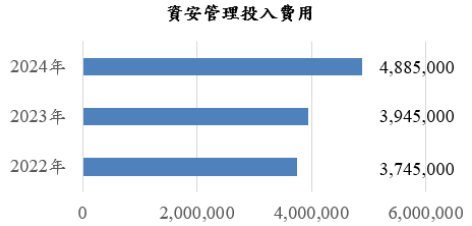
(5) 降低資通系統遭受攻擊的風險，保持主機系統安全性更新外，亦定期針對重要主機進行弱點掃描、資安健診等相關檢測作業，依檢測結果對其各風險等級之弱點進行識別與修復，減少攻擊者利用漏洞入侵系統的風險。

(6) 資通安全治理辦理情形已於 112 年 11 月 7 日本公司第三屆第一次企業永續發展委員會及第八屆第三次董事會議向董事會報告在案。

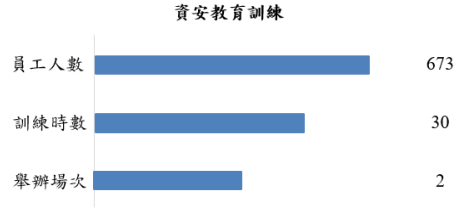
(7) 定期執行電子郵件社交工程演練，強化全體員工的資安意識與警覺性外，重視全球性攻擊的「商業電子郵件（BEC）詐騙」手法持續攀升且防不勝防的趨勢，加強以模擬攻擊者可能偽造的相關訊息為演練目標，提升社交工程防護能量。

(8) 持續投入資通安全管理相關費用及新年度預算，完善管理制度與強化技術應用之各項措施。

(9) 112 年 10 月舉辦 112 年資通安全教育訓練，全體員工均已參與受訓並完成考核(673 位)。同時新進員工全數通過資通安全教育訓練課程。



	2022年	2023年	2024年
金額(元)	3,745,000	3,945,000	4,885,000



員工人數(人)	訓練時數(分)	舉辦場次(次)
673	30	2

(五) 最近年度及截止至年報刊印日止，因重大資通安全事件所遭受之損失，可能影響及因應措施：本公司 112 年未發生任何衝擊公司營運的重大資通安全事件。