資通安全風險管理

瑞昱為保護企業員工、客戶、投資人與合作夥伴之資通訊安全，以支持企業營運持續與發展之願景，致力於發展資訊安全策略並持續精進，免於因人為疏失、蓄意或天然災害等導致資訊資產竊取、不當使用、洩漏或破壞等風險，瑞昱訂有「資訊安全風險管理架構」，透過持續精進風險管理，不斷地強化治理策略、人員訓練，並進行考核審查與配套措施，打造堅實、安全、與可信賴的企業數位環境，作為公司永續經營的堅固基石。

一、瑞昱資通安全風險管理架構

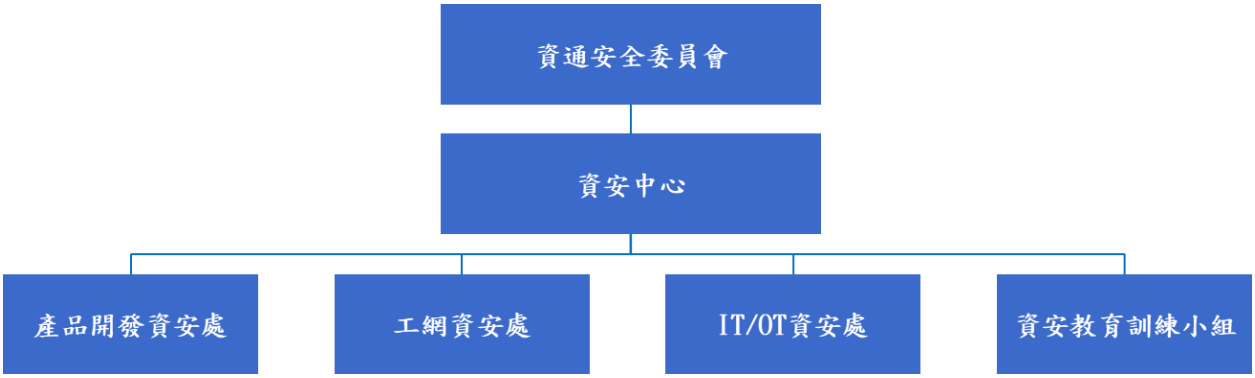
- **為落實與提升資訊安全治理策略，瑞昱成立資通安全委員會**

  負責檢視資安政策制定與執行成效，由總經理擔任主席，各單位一級主管擔任當然委員，每年至少舉行一次委員會議，並向董事會報告資安整體執行情形。另也成立資安中心處理資安政策與執行。

- **2022 年任命資安長與成立資安中心**

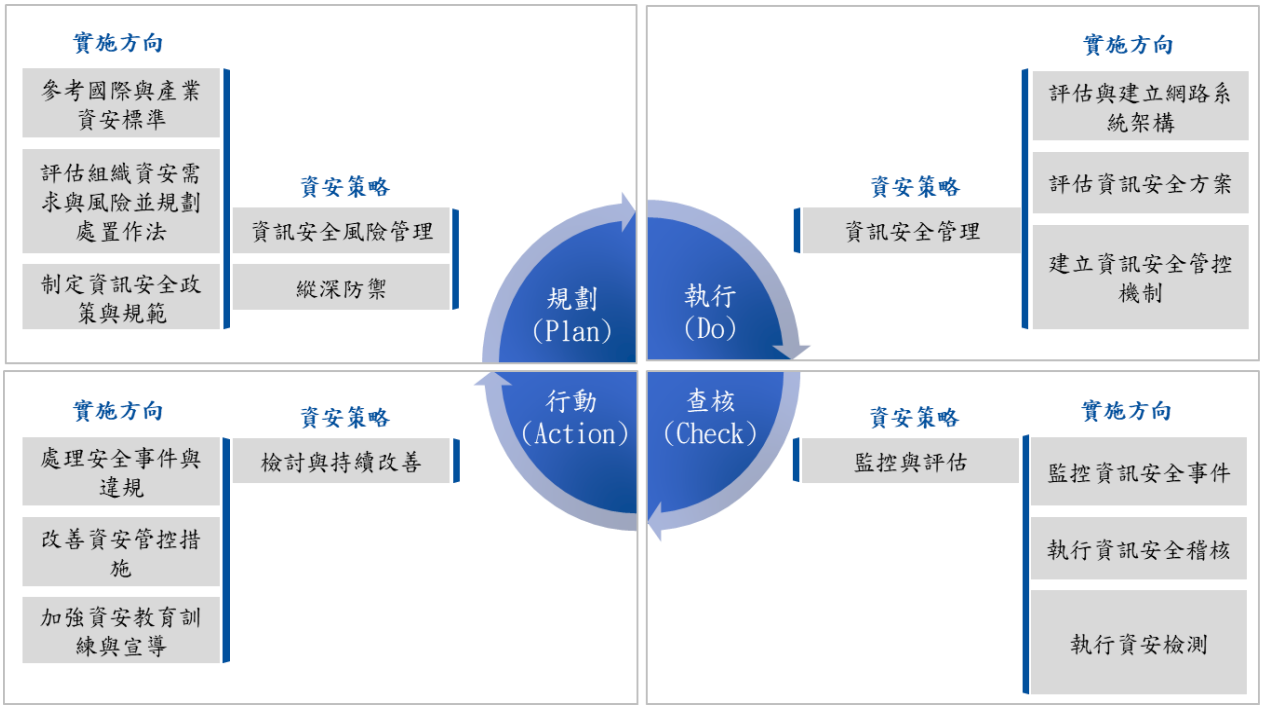
  為落實與提升資訊安全風險管理，瑞昱成立資安中心(CSC)並任命資訊安全長(CISO)領導，為企業資安專職專責單位，負責制定與推廣資訊安全政策、規劃與審查資訊安全措施有效性、跨部門資安任務協調、資安認證專案管理、重大資安事件應變、供應鏈資安稽核與資安內部稽核等工作，下轄產品開發資安處、工網資安處、IT/OT 資安處、資安教育小組，參考國際資安標準統籌資訊安全政策制定與執行資訊安全政策各項資訊安全保護措施，確保資訊安全管理達到機密性、完整性與可用性之目標。

資通安全委員會架構圖



二、持續強化瑞昱資安風險管理機制

瑞昱業務涉及 IC 研發、製造、銷售並提供 IC 產品之軟硬體應用及 IP 開發等，透過各式通訊、儀器設備與資訊系統等資訊科技，與產業鏈上下游及客戶密切合作進行產品研發與交付，瑞昱透過訂定與實施資訊安全管理機制以維護組織資訊安全。為積極管控組織資安風險，支持組織營運發展，評估重要性、風險影響性與對應改善效益，建構縱深防禦機制，並採用 PDCA（Plan-Do-Check-Action）方法，持續強化組織資安風險管理機制。



三、具體管理方案與成效

未發生重大資安事件造成營運、商譽受到影響與損失，亦無因違反資訊安全而導致員工、供應商與客戶向公司進行投訴的情形。

網路管理安全

防火牆管控
強化內外網路的存取安全，即時阻擋惡意流量。

惡意威脅防禦
主動辨識威脅並阻擋外部惡意、不當傳輸行為，減少惡意程式攻擊。

產品安全

風險改善
定期召開會議，對已知的問題因應及預防再發，並對於高發生機率的風險提出改善對策，提升產品開發環境的資安控管，及對智慧財產的遵循要求。

漏洞通報
依公司資安通報流程，啟動漏洞問題修正應變程序，並向上彙報，提升產品漏洞管理與處理效率。

客戶機密保護
採用合約遵循系統、合法授權程序、安全通訊傳輸、帳號權限控管、專用儲存區等機制，落實客戶機敏資訊保護。

電腦安全管理

帳號密碼管理
定期強制變更密碼，且密碼規則具備相當的複雜度，強化個人帳號密碼，降低個人電腦盜用風險。

防毒管控
防毒伺服器自動派送更新病毒定義檔到使用者端電腦，有效阻隔及防範電腦病毒。

端點偵測及回應
透過 EDR 即時監控端點電腦，對端點電腦異常威脅進行風險偵測，提高對於資安事件威脅的掌握，並快速識別資安事件及回應，以緩解風險。

檔案管理

最小授權原則
採用文件管理(DMS)、數位版權管理(DRM)確保最小授權原則避免資料外洩。

資訊系統管理

確保授權原則與可用性
採用合法授權程序、雙因素驗證、安全通訊傳輸、存取權限控管、重要資訊系統備份備援機制

人員資安意識與能力

強化人員警覺能力與資安意識
執行社交工程演練、資安教育訓練與學習成效評核、資安宣導，強化人員警覺能力與資安意識，並遵守資安規範。

持續提升資安人員專業
鼓勵參與專家研討會與資安認證考試，持續提升資安人員專業，貢獻於組織資訊安全工作。