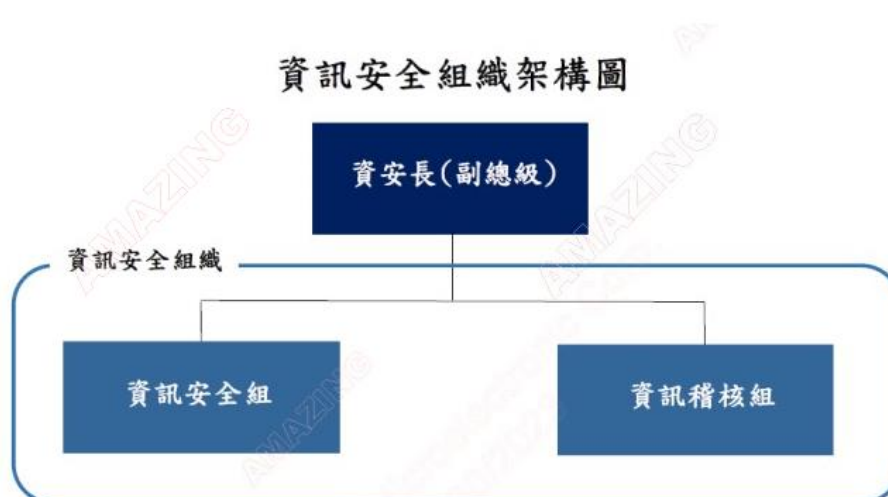


資訊安全風險管理

晶焱科技股份有限公司 參照 資通安全管理法、個人資料保護法 與 國際資訊安全管理規範 ISO27001，設 資訊安全組織 直屬總經理，資安召集人等同於資安長(副總級) 由 資訊單位最高主管 擔任，管理規劃資通安全與個資保護，以維護資料、系統、設備及網路環境之機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)下，達成下列管理目標：

1. 維持營運持續，確保資訊系統維持一定水準之系統可用性。
2. 保護本公司運營資訊，避免未遭授權之存取、破壞，確保資料之完整度。
3. 規劃營運持續應變措施，迅速完成災害復原。

組織架構



資訊安全管理政策

建立制度化、文件化及系統化之管理機制，持續監督及審查管理績效，以

落實資通安全管理及營運持續之理念，並達到下列：

- 建立及落實資通安全管理政策
- 全面導入資訊安全管理系統(ISMS)
- 培訓資訊單位於資通安全領域之專業能力
- 強化整體資通安全環境及資通安全應變能力
- 達成資通安全管理政策量測指標

執行下列風險控制管理及具體管理方案：

- 資訊安全政策訂定
- 資訊安全組織與權責
- 資訊資產分類與管制
- 資訊安全風險分析與評估
- 人員安全管理與教育訓練
- 實體與環境安全
- 通訊與作業安全
- 存取控制安全
- 系統開發與維護安全
- 資訊供應商之委外服務管理

- 資安事件管理
- 營運持續運作管理與演練
- 資訊安全對策之查核與持續改善

具體執行管理方案

1. 建立系統化 資訊安全管理系統，對資通安全以 PDCA 方法即時因應處理
2. 以國際資安教範(如 NIST 之資安事件應變指南)，進行階段式應變措施 建置
 - A. 事前安全防護
 - i. 機房基礎建設備援與溫濕度監測、資安宣導與終端防毒軟體建置等等
 - B. 偵測與分析
 - i. 網路流量異常監測與內部防毒偵測分析等等
 - C. 隔離、清除與復原
 - i. 異常監測之控管處理與備份管理等等
 - D. 事後處理
 - i. 確認風險來源，必要時修改管理控制項，進行補強措施或風險規避

投入資通安全管理之資源與里程碑

1. 於 Aug 30, 2021 加入 TWCERT/CSIRT 資安聯盟，分享資安情資，區域聯防
2. 於 Feb 23, 2022 取得 ISO27001 國際資安認證，建立資通安全風險與異常管理作業程序，善盡上下游供應商營運持續之本份

3. 於 2021 已導入暨建置 國際資安大廠之“ 資安預警與即時情資應對系統” ，

強化資安防禦能量；並定期進行內部資安風險追蹤，持續改善