

資通安全與隱私風險管理架構

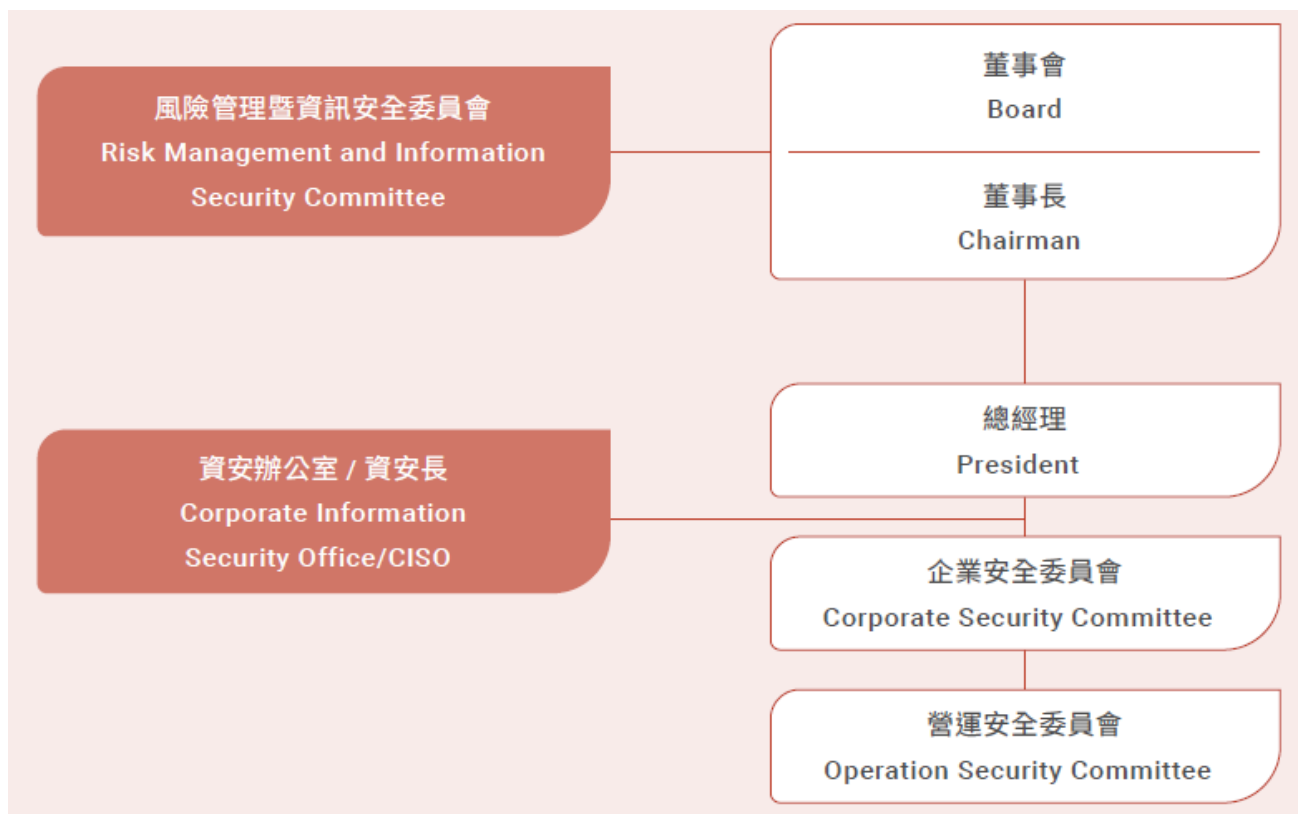
資通安全與隱私風險管理組織

為展現對資訊安全與客戶隱私的重視與承諾，遠傳設有資通安全組織。更於民國(以下同)113年5月3日董事會通過將「風險管理委員會」更名為「風險管理暨資訊安全委員會」，定期審查資訊安全與隱私保護策略、重點計畫及管理成效。此外，管理組織亦包含總經理、企業安全委員會、營運安全委員會之所有事業群代表共30人以上。並設置資安專責單位-資安辦公室及資安長。資安長由總經理指派，直接向總經理報告。藉由各級委員會於所屬事業群內推動及宣導資通安全與個資安全相關事務，及協調跨事業群資安維護之權責與分工，以確保全公司整體資訊安全之落實管理與維運。

資通安全政策

遠傳考量法規要求、個資保護、風險管理以及危機管理等構面，制定資通安全政策(參閱官網/公司治理,[連結](#))，且定期依內外部需求檢討修訂相關政策規範，內容包含營運資訊安全、技術安全、實體安全以及人員安全之管理。每年亦進行資安風險評鑑，辨識網路攻擊等重大風險議題，並結合年度計劃，採行避免、降低、轉移等因應對策，以加強管控相關風險。

資通安全組織及權責



組織	職責
風險管理暨資訊安全委員會	審查資訊安全與隱私保護策略、重點計畫及管理成效，並定期向董事會報告風險管理運作情形。
企業安全委員會	建立安全政策與治理架構、核可安全計畫與資源預算、管理公司整體安全風險。
營運安全委員會	建立安全目標，管理安全相關政策規範之規劃、訂定、執行與審查，並依風險項目規劃資源與因應計畫，確保符合管理規範與落實管理。
資安辦公室 / 資安長	資安長由總經理指派，負責推動及監督公司的資通安全與個資安全相關事務。 資安辦公室協助制定安全政策規範、負責政策推動與宣導、綜理各委員會運作。

具體管理方案與投入資源

114年企業安全委員會共召開4次會議，營運安全委員會共召開6次會議，主要討論重點包含資安政策檢視與修訂、全球主要風險威脅與趨勢分析，相關法規如資通安全管理法修訂，高風險議題鑑別，因應對策與強化方案等。針對高風險議題，亦定期於風險管理暨資訊安全委員會中向董事層級報告，再提報至董事會。

為持續提昇整體安全及資安防護，114年各相關單位已規劃並完成多項計畫，包含網路攻擊防護強化、實體安全強化、營運持續計畫演練等，並持續優化資安監控及縱深防護機制，透過大數據技術分析，整合內部及外部聯防組織等資安情資，強化高風險告警機制，以達到 7*24 即時的偵測、應變與處理。另一方面，遠傳亦持續評估資安保險之必要性，以做資源最佳化配置。

此外，遠傳為塑造資安意識文化，於內部網站成立專區進行全員宣導，以期內化全體員工之資安風險意識。114年度辦理「個資隱私保護及去識別化處理」及「社交工程攻擊防禦術」二場全員教育訓練，完成度皆達100%。(以上訓練皆包含正職員工與約聘人員)。另外，為提供客戶安全的服務使用環境，及持續強化與養成同仁資安技術能量，遠傳亦針對資安專責人員及資訊人員辦理專業及職能訓練，以期能於系統開發生命週期各階段皆納入資安管控措施，強化整體安全性及韌性。

為確保資訊安全管理與個人資料保護機制的適切性與有效性，遠傳持續關注國際趨勢與標準要求，每年定期透過外部第三方機構進行國際標準驗證，積極檢視與持續精進。

114 年遠傳資訊安全與個資保護管理認證	
ISO 27001 資訊安全認證	連續 21 年於資安領域通過驗證，範圍包括行動服務與固網服務啟用異動、出帳繳款、客戶服務等流程，維運支援系統之開發維護，及網際網路資料中心維運管理等。 (本認證最新有效期自 114 年 4 月 29 日起至 116 年 4 月 30 日)
ISO 20000 服務管理認證	連續 17 年於服務管理領域通過驗證
BS 10012 個資管理認證	連續 13 年於個資保護管理領域通過驗證，範圍包括全省門市服務申請、蒐集客戶資料、出帳與資料處理作業等
ISO 29100 隱私保護框架認證	114 年通過隱私保護管理領域驗證，範圍包括行動通信客戶資料去識別化處理及行銷分析作業等。
CSA STAR 雲端安全認證	連續 12 年通過 CSA STAR 條件較嚴苛的 Level 2 認證，取得 CSA STAR 認證的最高榮譽
ISO 27017 雲端服務資安認證	連續 7 年通過雲端服務資訊安全領域驗證
ISO 27018 雲端個資保護認證	連續 7 年通過雲端個人資料保護管理之驗證