資通安全風險管理架構

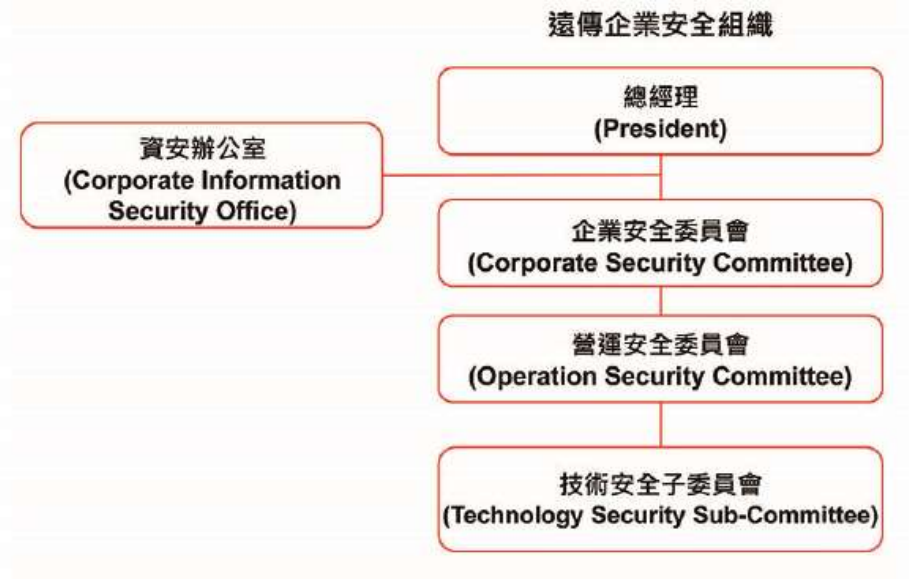
資通安全風險管理架構

為展現對資訊安全與客戶隱私的重視與承諾，遠傳以「珍惜所託、保護客資；深得信賴、永續服務」的資安與個資保護願景，成立企業安全組織，成員包含總經理及所有事業群代表共30人以上，並設置資安專責單位-資安辦公室及資通安全長，資安長由總經理指派，直接向總經理報告，負責推動及監督公司資通安全與個資安全相關事務，協調跨事業群資安維護之權責與分工。

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「建構安全可靠之整體網路、確保營運持續與強韌性、遵循主管機關與法令要求、保障用戶隱私資料安全」之資通安全政策，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，辨識網路攻擊等高風險議題，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。

企業安全組織架構及權責



企業安全組織各級委員會由各事業群代表組成，依其職責於所屬事業群內推行管理，以確保全公司整體資訊安全之落實管理與維運。

組織	職責
企業安全委員會	建立企業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。本委員會並設有資安長，負責推動及監督公司的資通安全與個資安全相關事務。
營運安全委員會	建立企業安全目標，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	協助制定安全政策規範、負責政策推動與宣導、綜理各安全委員會運作。
技術安全子委員會	檢視及評估資訊技術領域之資安風險，建立適當之管控措施以確保資訊資產防護與完善之資訊安全環境。

具體管理方案與投入資源

111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，111年各相關單位已規劃並完成多項計劃，包含網路攻擊防護強化、實體安全強化、營運持續計劃演練等，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。111年度已辦理「個人資料保護法解析」(共5,369人參與)及「資訊安全防護基礎篇」(共5,300人參與)等資安教育訓練。(以上課程參與人數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。

111 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 18 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
ISO 20000 服務管理認證	連續 14 年於服務管理領域通過驗證
BS 10012 個資管理認證	連續 10 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
CSA STAR 雲端安全認證	連續 9 年通過 CSR 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 4 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 4 年通過雲端個人資料保護管理之驗證