資通安全管理

資通安全風險管理架構、資通安全政策

本公司持續以保險服務第一品牌為目標邁進，透過制定「資訊安全政策」，設立「資訊安全管理會議」，由總經理擔任會議召集人，資訊安全長擔任執行秘書，並由直屬總經理管轄之「資訊安全部」負責綜理資訊安全治理、資安系統防護及資安事件應變等業務，定期於資訊安全管理會議中呈報推動狀況、新興議題及因應方案，於董事會呈報資安策略藍圖執行成效、關鍵風險監控指標及重大資安議題。

具體管理方案及投入資通安全管理之資源等

資訊安全防護上，首重事前預防及應變準備，從資安治理、資安防禦、監控與回應、情報與聯防及個資保護 5 項策略，全方位建構資安與個資防護措施，並領先同業全公司取得ISO 27001資訊安全管理認證、ISO 27701隱私資訊管理認證及BS 10012個人資料保護認證，榮獲「保險卓越獎資訊安全推展卓越獎」、「台灣企業永續獎資訊安全領袖獎」、「工商時報數位金融獎數位資訊安全優質獎」、「旺旺中時服務評鑑大賞資訊安全獎」、「F-ISAC會員情資分享表現特優機構」等獎項。

資安治理	已訂定資訊安全策略與藍圖，以及可具體執行之資安策略模組與工作項目，透過建立董事資安諮詢機制，將資安納入決策考量，持續評估並提升資安治理成熟度，積極實踐發展永續金融之決心。
資安防禦	已參考美國國家標準技術研究院網路安全框架2.0(NIST CSF 2.0)從治理、識別、防護、偵測、回應、復原等架構，設計、規劃縱深防禦技術機制。為更即時掌握風險及應變，已擬定零信任架構導入計畫，並運用延伸式偵測與回應、第三方自動化評估等技術，透過自動化攻防演練、紅藍隊演練，模擬真實駭客手法，驗證資安防護的有效性。
監控與回應	已打造7天24小時資安事件監控體系，藉由整合的資訊安全管理平台，分析調查各項資安事件，採用金融資安監控中心資安監控組態基準、弱點與情資管理平台，自動化追蹤與管理弱點及蒐集情資，增進資安事件與監控情資關聯分析之即時性及有效性，並投保資安保險，轉嫁資安事故風險。
情報與聯防	已加入金融資安聯防監控中心(F-SOC)與金融資安資訊分享與分析中心(F-ISAC)，串接F-SOC提供情資分享，提升資安人員專業能力，於資安事件發生時，及時分析及回傳資安情報資料，強化跨機構協調聯繫及應變能量。
個資保護	已持續推動資安與個資管理整合，領先同業將ISO 27001資訊安全管理標準、ISO 27701隱私資訊管理標準驗證範圍擴展至全公司，確保客戶隱私安全。

風險影響及因應措施(註一)

審視全球資安新聞、國際資安研究報告、F-ISAC威脅情資、主管機關重大裁罰、資安及個資侵害事故等恐造成財務損失之風險，將上述風險列入關鍵風險指標，透過各項資安具體方案進行防護，以有效控管風險。

重大資通安全事件及損失(註二)

114年度未發生重大資通安全事件及造成損失之資安事件。

註一：說明資通安全風險對公司財務業務之影響及因應措施
註二：說明最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實及原因