6.4 資訊安全

6.4.1 資訊安全管理政策

為了提升金融服務品質和穩定性，並有效管理資訊安全風險，國泰世華訂有資訊安全政策，遵循母公司國泰金控的資訊安全藍圖，作為資訊安全防護實施的指導方針，持續強化資安防護能力，達成安全、便利、營運不中斷的金融服務。

本行設有資訊安全專責單位，並由副總經理以上兼任資訊安全長，統籌政策推動與資源調度。資安專責單位負責：檢視資訊安全法令遵循情形、規劃資訊安全政策與架構藍圖、協調重大資安事件應變、定期檢視防禦機制與緊急應變計畫、監督各單位執行成效、並推動宣導與教育訓練。透過以上作為識別資訊安全風險並採取因應措施。

除資訊安全專責單位，為確保資安政策之遵循與推動、督導與協調資安管理工作，本行設有跨單位資訊安全委員會，由總經理擔任主任委員、資安長擔任執行秘書，委員會成員涵蓋資訊、法務、法遵、風管、資安、數位驅動等督導主管；每半年至少召開一次會議，並每年向董事會報告整體資安執行情形。於合規與成果方面，為配合產業脈動與新興科技及雲端應用，本行依循相關法規及自律規範，持續維持第三方驗證之國際認證，包含 ISO 27001:2022 與 PCI DSS 支付卡產業資料安全標準。並於本年度通過 ISO/IEC 27017 雲端服務資安管理認證，為國內首家在公有雲取得該認證之金融機構。

資訊安全組織架構圖

6.4.2 資安行動方案與成果

本行定期辦理電腦系統資訊安全評估、各項應變演練、滲透測試、雲端服務安全組態檢測、入侵與攻擊模擬演練、白帽駭客紅隊演練以及各項提供客戶服務程式檢測之強化措施外，也規劃資安情資蒐集與處理、資安監控中心、偽冒站台偵測下架以及資安事件應變等機制，針對各式新型態資安威脅，在前中後三階段都有妥適因應措施。有鑑於金融服務委外及跨業合作型態發展，本行亦持續強化第三方資訊供應商管理機制，以預防供應鏈可能造成之資訊安全風險。

此外，本行每年持續投保資安保險，針對各式新型態資安威脅得立即施以妥適因應措施，以維護本行及客戶權益及減少資安事件發生損失。本年度共投入資安經費共 50,456 萬元，包含軟硬體授權、人員訓練等費用，占本行資訊預算費用 137,231 萬元共計約 37%。本行亦鼓勵員工考取資安證照，截至本年度為止共累計取得 344 張資安認證，涵蓋管理類及技術類證照。

◆ 交易系統及內部運作防禦行動

本行安全防護設置包括異常網路流量的監控和防護、網路防火牆、網頁應用防火牆、入侵偵測防禦系統，以及端點防護機制（防毒和 EDR）。並設置資訊安全監控管理平台，用於彙整各類不同資安防護設備之安全事件日誌，並集中管理、儲存、搜尋和轉送至資訊安全監控中心 (Security Operation Center, SOC)。此監控中心提供 7×24 小時的服務，負責分析和監控系統中任何可能違反資訊安全的機密性、完整性、可用性的訊息內容，一旦發現異常事件將立即通報、處理並追蹤，以確保交易安全性和防護措施有效性。

◆ 執行金融資安行動方案

本行已完成金管會於 2020 年 8 月 6 日發布之「金融資安行動方案 1.0」及另於 2022 年 12 月 27 日「金融資安行動方案 2.0」中增訂之各項屬金融機構應辦理項目。此外，本行依據「金融業導入零信任架構參考指引」訂定導入計畫，持續評估及擴大至各高風險場域，也透過資安成熟度評估工具持續強化本行金融業資安防護能力，達成安全、便利、營運不中斷的金融服務。

◆ 偕同第三方專業顧問評估國內外相關資安落實度

本行為提升整體資訊安全並配合金融業資訊安全法規要求，包含海外分支機構每年定期辦理電腦系統資訊安全評估作業，並委請獨立專業顧問公司評估本行整年度資訊安全整體執行情形，就評估結果連同內控聲明書於次年度第一季前呈報董事會。此外，為深入了解海外分支機構的資訊安全執行情況，透過安排資安人員偕同第三方顧問進行實地檢視，確保海外各項作業符合資安法規且落實各項資安管控要求，期將資訊安全深植於企業文化，落實並提升資訊安全防護能量。

6.4.3 資訊安全教育訓練

本行每年定期辦理資安教育訓練，訓練對象區分為一般員工、資安專責人員與董事會成員三類，聚焦持續強化資安意識、專業技能與經營階層之資安督導職能。

項目	一般人員資安教育訓練	資安專責人員教育訓練	董事會成員教育訓練
訓練總人數	12,226	32	15
完訓率	100%	100%	100%
訓練總時數（小時）	36,678	2,263	15