5.4 資訊安全

5.4.1 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，做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。本行設立資訊安全部作為資安專責單位，負責制定全行資訊安全政策，規劃資訊安全架構藍圖，協同重大資訊安全事件應變處理、資訊安全防禦機制與緊急應變計畫檢視；監督資訊安全整體執行情形、資訊安全宣導與教育訓練；檢視資訊安全法令遵循情形。本行於 2022 年設立資安長一職，綜理資訊安全政策推動及資源調度相關事務。資安專責單位每年定期向董事會進行年度資訊安全整體執行情形報告；每半年定期向總經理及相關單位督導主管召開資訊安全委員會。

資訊安全政策之核決層級為董事會，每年定期檢視以確保資訊資產的機密性、完整性、可用性及適法性。為確保資安政策之遵循與推動、督導與協調資安管理工作，本行成立跨單位之「資訊安全委員會」，由總經理擔任主任委員，邀集資訊相關、法務、法令遵循、風管、資訊安全、數位驅動等單位之督導主管為委員共同組成，並由資訊安全長擔任執行秘書，每半年至少召開一次會議。

配合產業脈動與新興科技與雲端應用，依循相關法規及自律規範，維持國際資安認證書有效性，包含由第三方獨立機構每半年驗證之 ISO 27001:2022，以及每年驗證之 PCI DSS 支付卡產業資料安全標準。導入「美國聯邦金融機構監督委員會網路安全評估工具 (FFIEC CAT)」及「行政院國家資訊安全會報技術服務中心政府機關資安治理成熟度評估機制」進行資安成熟度評估，依評估結果定期檢討及改善，每年也透過獨立的專業顧問執行資訊安全評估作業、白帽道德駭客資安檢測及實施必要之強化措施，以持續強化本行資訊安全防護。此外，有鑑於金融服務委外及跨業合作之型態發展，本行亦透過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。

5.4.2 資安行動方案與成果

- **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，並委請獨立的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之要求，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。

- **執行金融資安行動方案：**

本行已完成金管會發布之「金融資安行動方案 1.0」中，由金融機構執行之項目，包含設置資安長、遴聘資訊安全諮詢小組、導入國際資安管理與營運持續管理標準並取得驗證、配合金控建立之電腦資安事件緊急應變規劃作業、辦理資安治理成熟度評估、建置資安監控服務中心機制、鼓勵資安人員取得國際證照，以及於異地備援演練納入實際業務運作驗證等。針對 2022 年 12 月 27 日所發布之「金融資安行動方案 2.0」，本行亦完成其他辦理項目，如完成駭客入侵與攻擊模擬演練 (BAS)、零信任架構導入及因應重大資安事件及天然災害之資料之保全專案，持續強化本行資安防護能力，致力於提供安全、便利、營運不中斷的金融服務，並完備本行之資訊安全管理。

- **資安防護與強化措施：**

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，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，以及資安事件應變等機制，期能針對各式新種的資安威脅，在前中後三階段都有妥適的準備與因應。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，以維護本行及客戶之權益及減少資安事件發生之損失。本年度共投入資安經費共 20,530 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 109,867 萬元共計約 18.6%。本行亦鼓勵員工考取資安證照，截至本年度為止本行共累計取得 164 張資安認證，涵蓋管理類及技術類證照，如：ISC2 CISSP/CC、ISACA CISM/CISA/CRISC、ISO 27001/27017/27018/27701/42001、EC-Council CEH/ECSA/CHFI/ECIH/CTIA、CompTIA Security+ 及 iPAS: 中級資安工程師等相關證照。

5.4.3 交易系統及內部運作防禦行動

國泰世華的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 7x24 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，以確保交易的安全性和防護措施的有效性。

5.5 法令遵循

本行設立法令遵循部，建立與執行法令異動傳遞、教育訓練、海內外法遵業務聯繫以及董事即時通報等機制，確保所有業務符合法令規範。本行總機構法令遵循主管定期向總經理彙報本行法令遵循制度執行情況與檢討內容，並至少每半年向董事會及審計委員會呈報法令遵循業務執行情形和公平待客原則執行情形報告，如發現有重大違反法令或遭金融主管機關調降評等時，應即時通報董事，並就法令遵循事項，提報董事會及審計委員會，有效督導並推動全行法令遵循業務的落實。為符合主管機關監理及金融檢查意見要求，將持續研議各項法令遵循業務之優化措施及因應規劃，並就行內各項新商品、新服務或向主管機關申請開辦之新種業務，出具符合主管機關法令及本行內部規範之意見。藉由現行之業務聯繫會議、教育訓練、督導管理與改善檢討管道，本年度將持續督導國內各單位及國外分子行辦理法令遵循事務之執行成效，並就主管機關、金控及本行稽核室檢查意見，確實進行檢討與改善，以達全行遵法合規之目標。本行引入金融科技以優化作業流程，建置法令遵循系統來集中管理各項法令遵循業務執行，並利用人工智慧 (AI) 技術開發內外規關聯性分析工具。