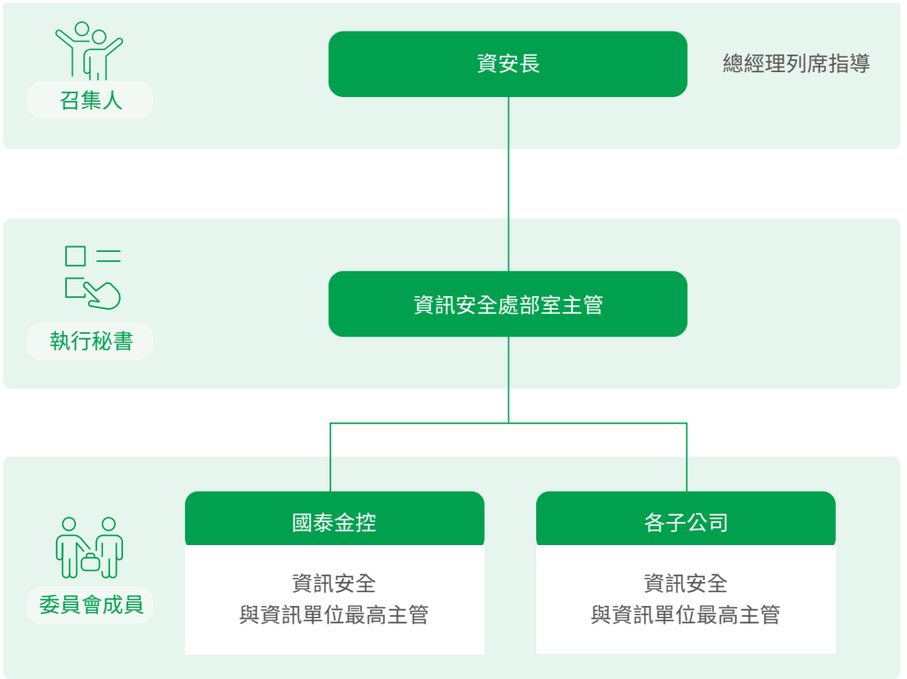
6.4 資訊安全

SASB：FN-CB-230a.1、FN-CB-230a.2

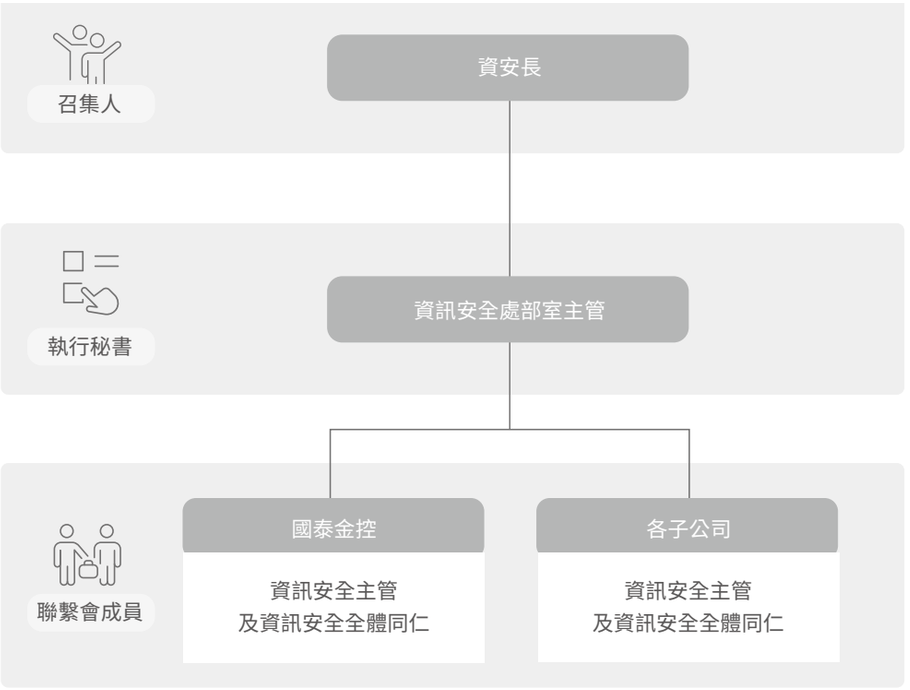
6.4.1 資安及科技治理

國泰金控與主要子公司皆設立資安長或成立資安專責單位，負責規劃、監控及執行資訊安全管理作業，並每年於董事會提報執行情形。國泰金控設有跨公司之資訊安全委員會，由資安長擔任召集人，並邀請總經理列席指導，掌理資訊安全政策擬議及管理制度推展，每半年召開一次會議，並於當年度董事會提報資訊安全整體執行情形報告。另為有效進行橫向溝通及達成集團資訊安全管理一致性，設有跨公司之資訊安全聯繫會，每月召開會議，致力於資安控管及提升品質。本公司自 2025 年 8 月 16 日起，將資訊安全納入風險管理委員會執掌，成立「風險管理暨資訊安全委員會」。由董事會指派至少三名董事組成，其中半數以上為獨立董事，監督本公司風險管理與資訊安全運作機制。

資訊安全委員會



資訊安全聯繫會



公司營運中樞雲：AI 引領未來金融治理

執行內容

- **AI 治理與技術框架：**國泰金控以「AI 即服務」（AI as a service, AIaaS）為策略，實踐 AI Ready、AI Native、AI Empower 三大主軸，更領先業界發展「國泰生成式 AI 技術框架 GAIA」，其中四大核心—「國泰專屬金融領域知識庫」、「企業級 AI 模型中心」、「自主研發複合層級護欄技術」及「賦能集團 AI 公民化」，全面推動集團 AI 治理。
- **集團大規模上雲，進入雲端優先階段：**國泰金控持續推動雲端轉型，已完成超過百套系統上雲，並正式邁入「雲端優先（Cloud First）」階段，以提升彈性、加速導入新技術並強化營運韌性。為大幅提升上雲效率，亦推出「Smart Archie 雲端自動化解決方案」，結合生成式 AI 與 Multi-Agent 技術，讓多個 AI Agent 分工協作，打造雲端架構師團隊，實現雲端架構設計自動化。
- **開源創新、接軌國際，加速技術現代化：**國泰積極參與國際開源生態系，為台灣首家加入「雲原生運算基金會（CNCF）」之金融機構，同時著手建立「開源計劃辦公室」及「開源審查委員會」，建立標準化開源軟體治理流程，確保技術選型之安全性與合規性，加速集團數位轉型步伐。

強化資安韌性（Resilience）

強化資安韌性（Resilience）

措施	行動說明
訂定資訊安全政策	• 國泰金控暨各子公司皆訂定「資訊安全政策」，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
建立 7X24 資安監控中心（Security Operation Center, SOC）服務機制	• 於 2020 年建立 7X24 資安監控中心服務機制 • 多維度關聯分析資通安全設備、網路設備、作業系統等日誌 • 即時預警及判斷資安事件、異常連線等行為，並建立處理追蹤機制，落實資安風險管控措施
資安事件應變及營運持續計畫	• 整合集團資源建立跨公司之「資安緊急應變小組」，透過事件通報及緊急應變程序，即時掌控資安事件狀況 • 資安事件營運持續計畫之作業規劃，以每年擬定情境腳本辦理應變演練，以利在資安事件發生時快速應變 • 資安營運持續計畫與應變演練的支援資源包括人力、系統、設備、場地與廠商 • 藉由外部資安顧問及應變團隊合作，以其豐富之資安事件經驗，提供專業建議與緊急應變支援
提升零信任成熟度	• 依金管會零信任指引框架為基礎，強化整體資通安全與營運韌性，並督導各子公司落實資安治理
資安管理系統內部稽核	• 資訊安全管理系統驗證範圍為資訊相關部門，每年辦理一次資訊安全管理系統之內部稽核作業，以確保組織的資安政策、程序與實務符合標準（如 ISO／IEC 27001） • 依稽核結果持續追蹤與改善，以持續確保資訊安全管控措施之落實

強化資安韌性（Resilience）

措施	行動說明
導入 ISO 27001 資訊安全管理系統	• 國泰金控於 2024 年通過 ISO 27001：2022 驗證，2025 年擴大驗證雲端策略發展部、國泰碳管理系統，及持續優化資訊安全管理機制 • 國泰金控旗下重要子公司皆已通過 ISO 27001 國際標準驗證，並取得由英國標準協會（BSI）頒發之證書，藉此完善資安治理架構與資安管理體系，並強化資安事件的預警、通報與應變流程，提供客戶安全無虞的金融服務，各公司證照有效期限及驗證版本如下：

公司	金控	銀行	人壽	產險
版本	2022	2022	2022	2022
有效期限	2023／10／04~2026／10／03	2023／11／26~2026／11／25	2025／02／27 ~ 2028／02／26	2026／01／16~2029／01／15

公司	證券	期貨	投信	投顧
版本	2022	2022	2022	2022
有效期限	2025／04／11 ~ 2028／04／10	2025／04／01 ~ 2028／03／31	2025／03／28 ~ 2028／03／27	2025／07／19~2028／07／18

強化集團雲端治理安全	• 協助數位轉型專案納入金控雲端安控管理要求

6.4.2 資安管理機制與教育訓練

面對數位轉型浪潮，培養同仁的資安意識與文化，落實資安控管。關於國泰金控歷年資訊安全教育訓練執行成效請見附錄 7.3 表 29。

資訊安全教育訓練

採安全設計（Security by Design）策略	✓站在業務角度，於服務或商業模式設計初期納入資訊安全為考量因子 ✓專案初期，資安人員即以業務立場進行安全設計，使企劃人員理解資安相關議題 ✓推動將資安規範及系統架構檢視納入雲端專案變更審查（Change Advisory Board, CAB）流程
資訊安全教育訓練	✓每年全體員工「資訊安全教育訓練」達 3 小時，各公司 2025 年完訓率皆達 100% ✓資訊安全專責單位人員每年至少接受 15 小時以上專業資訊安全訓練
社交工程演練	✓透過社交工程演練持續提高同仁警覺性，防範惡意程式經由社交方式入侵 ✓加強資安宣導避免點擊社交工程郵件，並設置「可疑信件（社交工程）通報頻道」以提升資安意識

6.4.3 資安機制驗證與侵害管理

國泰金控暨子公司於發現網路攻擊及惡意程式入侵等重大資安事件時，將啟動「資安事件通報暨緊急應變機制」，由各公司資安事件緊急應變小組進行應變處置，並依循「國泰金控暨子公司重大資訊安全事件通報暨緊急應變管理要點」辦理，統一由國泰金控彙整各公司重大資安事件呈報資安委員會。國泰金控 2025 年並未發生重大資安事件。

資安措施		對應行動說明
白帽駭客入侵演練	參與公司	✓國泰人壽、國泰世華銀行、國泰產險、國泰證券及國泰投信
	模擬情境	✓連線狀態管理、存取權限測試、權限提升與跳脫等
	進行方式	✓每年委請專業顧問執行白帽駭客入侵演練，以各式駭客手法模擬可能遭遇攻擊的情境 ✓針對演練結果中所發現的漏洞與風險項目進行改善
電腦系統資訊安全評估	參與公司	✓國泰金控暨各子公司
	評估項目	✓資訊架構檢視、網路活動檢測、弱點掃描與滲透測試、安全設定檢視、合規檢視等
	進行方式	✓每年委請外部專業廠商執行電腦系統資訊安全評估，據此追蹤系統安全狀況並實行改善措施 ✓針對所發現重大風險項目完成 100% 改善
威脅情資分享與分析機制	設置「集團資訊與威脅情資共享機制」	✓針對重大資安情資進行通報分享，以進行改善及防禦措施
	資安聯防	✓與法務部調查局簽署「國家資通安全聯防與情資分享合作備忘錄」 ✓與刑事警察局簽署「金融阻駭反詐暨資安聯防專案合作意向書」 ✓增強國泰金融集團資安聯防之防禦縱深，構築公私資安協作框架建立共同聯防機制
外部偽冒事件偵測暨關閉	7x24 資安監控機制	✓已建立 7x24 偵測並關閉存在於企業外部的偽冒詐騙標的（網站、APP、社群平台）機制，避免客戶受害並降低可能風險