

6.4 資訊安全

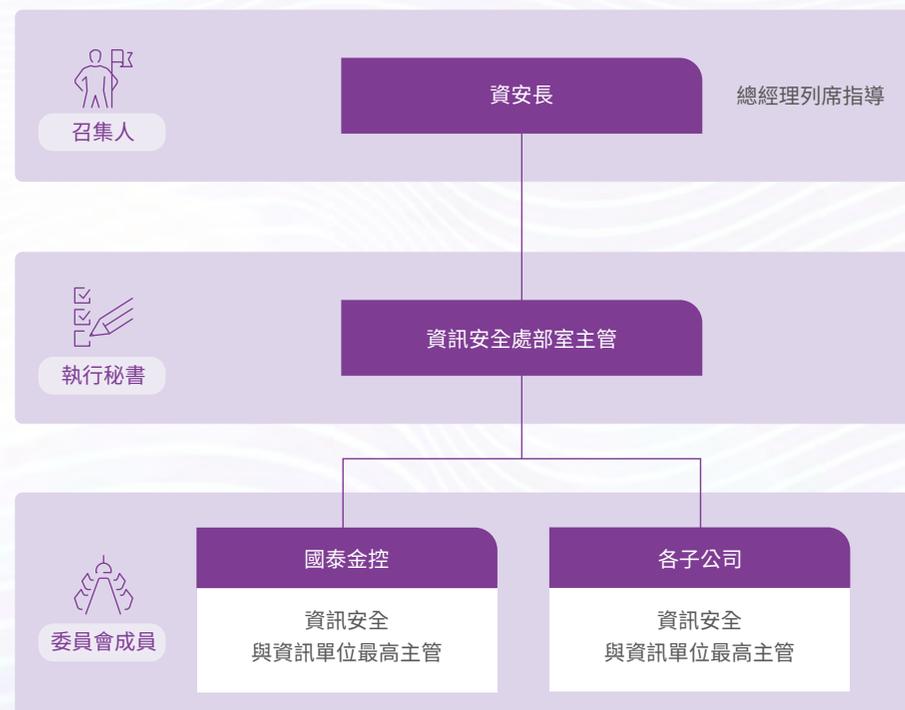
SASB：FN-CB-230a.1、FN-CB-230a.2

6.4.1 資安治理

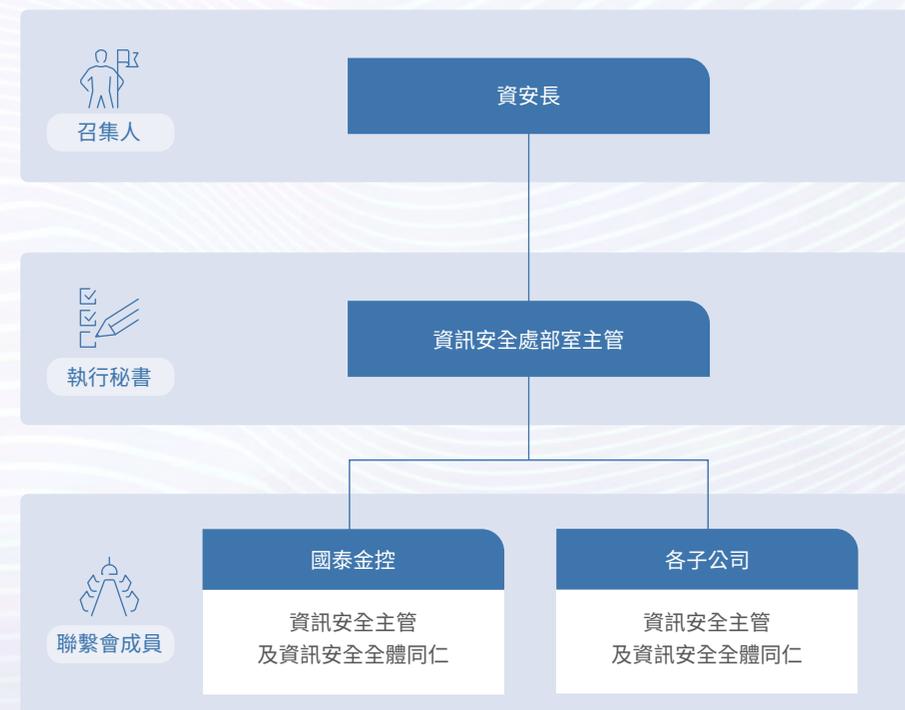
國泰金控與主要子公司皆依法規要求設立資安長或成立資安專責單位，負責規劃、監控及執行資訊安全管理作業，並每年於董事會提報前一年度資安執行情形。而國泰金控設有跨公司之金控資訊安全委員會，由資安長擔任召集人，並邀請總經理列席指導，掌理集團資訊安全政策之擬議及管理制度之推展，定期於每半年召開一次會議，並於當年度董事會提報前一年度資訊安全整體執行情形報告。

其中董事會成員苗豐強先生曾任聯華神通集團董事長，長期專注於 IT 研發製造、軟體開發、系統整合、資訊安全等領域，其經驗助於國泰對資訊安全與發展之管理。另為有效進行橫向溝通聯繫，並達成金控及子公司整體資訊安全管理的一致性，設有跨公司之金控資訊安全聯繫會，定期於每月召開一次會議，全力投入資安控管及提升品質。

• 資訊安全委員會



• 資訊安全聯繫會



目錄

- 董事長的話
- 國泰永續影響力故事
- 關於國泰金控
- 永續評比與獎項肯定
- 01 永續策略與治理
- 02 氣候
- 03 健康
- 04 培力
- 05 永續金融
- 06 永續治理**
- 07 附錄

|| 強化資安韌性 (Resilience)

目錄

董事長的話

國泰永續影響力故事

關於國泰金控

永續評比與獎項肯定

01 永續策略與治理

02 氣候

03 健康

04 培力

05 永續金融

06 永續治理

07 附錄

措施	對應行動說明																														
訂定資訊安全政策	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 為即時掌握資安風險並能提早進行因應，國泰金控於 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	<ul style="list-style-type: none"> 已整合金控集團資源建立跨公司之「資安緊急應變小組」參與應變協助，並透過事件通報以及緊急應變程序，即時掌控本公司及子公司之資安事件狀況 資安事件營運持續計畫的作業規劃，以每年所擬定的情境腳本辦理資安事件應變演練，讓同仁熟悉應變流程且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，藉由外部專業資安顧問及應變團隊合作，以其豐富之資安事件應變經驗，提供適切且專業的建議與緊急應變支援 																														
資安管理系統內部稽核	<ul style="list-style-type: none"> 國泰金控之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），並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 																														
導入 ISO 27001 資訊安全管理系統	<ul style="list-style-type: none"> 至 2024 年底止，全集團資訊系統導入 ISO 27001 之涵蓋率達 98.8%，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 國泰金控於 2023 年通過 ISO 27001:2022 驗證，2024 年擴大驗證青埔機房，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，並持續維持證照有效性，各公司證照有效期限及驗證版本如下： <table border="1"> <thead> <tr> <th>公司</th> <th>金控</th> <th>銀行</th> <th>人壽</th> <th>產險</th> </tr> </thead> <tbody> <tr> <td>版本</td> <td>2022</td> <td>2022</td> <td>2022</td> <td>2022</td> </tr> <tr> <td>證照有效期限</td> <td>2023/10/04 ~2026/10/03</td> <td>2023/11/26 ~2025/10/31</td> <td>2025/02/27 ~2028/02/26</td> <td>2023/01/16 ~2025/10/31</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>公司</th> <th>證券</th> <th>期貨</th> <th>投信</th> <th>投顧</th> </tr> </thead> <tbody> <tr> <td>版本</td> <td>2022</td> <td>2022</td> <td>2022</td> <td>2013</td> </tr> <tr> <td>證照有效期限</td> <td>2025/04/11 ~2028/04/10</td> <td>2025/04/01 ~2028/03/31</td> <td>2025/03/27 ~2028/03/26</td> <td>2022/07/19 ~2025/0/18</td> </tr> </tbody> </table>	公司	金控	銀行	人壽	產險	版本	2022	2022	2022	2022	證照有效期限	2023/10/04 ~2026/10/03	2023/11/26 ~2025/10/31	2025/02/27 ~2028/02/26	2023/01/16 ~2025/10/31	公司	證券	期貨	投信	投顧	版本	2022	2022	2022	2013	證照有效期限	2025/04/11 ~2028/04/10	2025/04/01 ~2028/03/31	2025/03/27 ~2028/03/26	2022/07/19 ~2025/0/18
公司	金控	銀行	人壽	產險																											
版本	2022	2022	2022	2022																											
證照有效期限	2023/10/04 ~2026/10/03	2023/11/26 ~2025/10/31	2025/02/27 ~2028/02/26	2023/01/16 ~2025/10/31																											
公司	證券	期貨	投信	投顧																											
版本	2022	2022	2022	2013																											
證照有效期限	2025/04/11 ~2028/04/10	2025/04/01 ~2028/03/31	2025/03/27 ~2028/03/26	2022/07/19 ~2025/0/18																											
強化集團雲端治理安全	<ul style="list-style-type: none"> 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

面對數位轉型的浪潮下，培養同仁的資安意識與文化，確實落實資安控管。關於國泰金控歷年資訊安全教育訓練執行成效請見附錄表 30。



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，並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 2024 年並未發生重大資安事件，而資訊外洩案件請詳見 6.5.4 個資保護。

措施	對應行動說明
白帽駭客入侵演練	<ul style="list-style-type: none"> • 國泰人壽、國泰世華銀行、國泰產險、國泰證券及國泰投信每年皆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駭客攻擊的漏洞與情境，包含連線狀態管理、存取權限測試、權限提升與跳脫等，並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	<ul style="list-style-type: none"> • 每年國泰金控暨各子公司委請外部專業廠商執行電腦系統資訊安全評估，包含資訊架構檢視、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，據此追蹤系統安全狀況並實行改善措施，並要求針對其中所發現重大風險項目完成 100% 改善
建立威脅情資分享與分析機制	<ul style="list-style-type: none"> • 已設置有「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 • 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」，及與刑事警察局簽署「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及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	<ul style="list-style-type: none"> • 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，以避免客戶受害並降低可能風險

目錄

- 董事長的話
- 國泰永續影響力故事
- 關於國泰金控
- 永續評比與獎項肯定
- 01 永續策略與治理
- 02 氣候
- 03 健康
- 04 培力
- 05 永續金融
- 06 永續治理**
- 07 附錄

