強化
「隱私權保護聲明」

《國際商業雜誌》
資訊安全
卓越獎

《全球銀行及金融評論》
2022 臺灣最佳
公司治理獎

導入
ISO 22301:2019
營運持續管理系統及
BS 10012 PIMS
個人資訊管理系統

# 02
# 美好誠生活

| GRI 重大主題 - 關鍵主題對應 | |
|---|---|
| 205:反貪腐 | 405:員工多元化與平等機會 |
| 201:經濟績效 | 417:行銷與標示 |
| 203:間接經濟衝擊 | 418:客戶隱私 |

| 永續承諾 | 對應 SDGs | 行動方案 | 2027 年目標 |
|---|---|---|---|
| Reduce Inequality<br>消弭不平等 | 5 性別平等 | 促進性別平等<br>(董事、高階主管) | • 至少一席女性董事。<br>• 提升各階層主管女性占比。 |
| Mitigate and Adapt to Climate Change<br>減緩與調適氣候變遷 | 13 氣候行動 | 導入並持續深化氣候風險管理 | • 建立整合性氣候風險管理儀表板,持續進行指標與目標之管理及監控。<br>• 將氣候風險的考量納入其他風險管理機制中,包括信用風險之壓力測試、市場風險(如 Climate VaR)、流動性風險與作業風險等。<br>• 每年持續完成範疇三盤點、監控作業及對外揭露,並擴大範疇三投融資的盤查範疇及提升盤查資料的數據品質。 |

## 2022 年六大資本成果彙整

**IN PUT**

- 財務資本
  - 提升公司治理相關投入費用 719.05 萬元
  - 投入資安經費 ( 包括軟硬體及授權相關費用 ) 14,093.6 萬元

**OUT PUT**

- 智慧資本
  - 資安戰情平台部署率 100%

## 2022 年永續發展工作計畫成果彙整

| 策略 | 2022 年目標與執行成果 | 2022 年達成情形 | 2023 年目標 |
|---|---|---|---|
| 精進公司治理 | • 強化董事會職能，提供多元化董事進修規劃；評估將功能性委員會納入外部績效評估範圍<br>• 強化審計委員會職能，各期財務報表須經過其同意；增加內部稽核主管與獨立董事單獨溝通之頻率<br>• 將 ESG 績效與董事酬金、高階薪酬連結，檢視永續績效與內部管理機制有效性<br>• 強化重大性議題與公司績效之連結，建置可衡量之量化目標，將目標明確連結至高階主管薪酬<br>• 辦理第八屆公司治理評鑑之辨識落差題目與精進工作，並預備第九屆公司治理評鑑自評 | 已達成 | • 強化董事會職能<br>1. 提供多元化的董事進修規劃，且董事會成員接受年度氣候相關教育訓練時數達 3 小時 / 年<br>2. 落實董事成員多元化<br>3. 辦理董事會及功能性委員會之外部績效評估<br>• 持續強化審計委員會職能，期中財務報告須經審計委員會同意；內部稽核主管每年至少 2 次與獨立董事進行單獨溝通<br>• 評估增設其他功能性委員會<br>• ESG 相關績效納入金控總經理及高階經理人變動獎酬連結，並檢視永續績效與內部管理機制有效性<br>• 強化隱私權保護聲明，並強化揭露隱私權政策及程序於整合風險 / 合規管理架構中<br>• 辦理第九屆公司治理評鑑之辨識落差題目與精進工作，並預備第十屆公司治理評鑑自評 |
| 誠信經營 | • 至少每半年召開一次誠信經營委員會議，陳報防範不誠信行為方案遵循情形查核結果與本公司及子公司檢舉案件處理情形<br>• 辦理年度誠信經營委員會之績效評估<br>• 辦理金控及各子公司「誠信經營及檢舉制度」年度教育訓練<br>• 整合教育訓練與誠信政策聲明簽署機制，以有效追蹤誠信經營相關政策落實情形 | 已達成 | • 召開誠信經營委員會議，呈報誠信經營委員會 2022 年績效評估結果、防範不誠信行為方案遵循情形查核結果、本公司及子公司檢舉案件處理情形、防範不誠信行為方案之妥適性與有效性檢視情形<br>• 執行年度全體董監及同仁之教育訓練及誠信簽署機制，以有效追蹤誠信經營相關政策落實情形<br>• 加強資訊揭露覆核行為準則 / 道德準則有效性之辦理情形<br>• 持續關注誠信經營國際發展趨勢及法令異動，配合調整內部規範，俾利金控及各子公司遵循，符合國際潮流 |

## 2022 年永續發展工作計畫成果彙整

| 策略 | 2022 年目標與執行成果 | 2022 年達成情形 | 2023 年目標 |
|---|---|---|---|
| 提升資訊透明度 | • 增加官網溝通回饋管道與社群網路互動，並提升企業永續發展專區資訊完整性 | 已達成 | • 持續進行官網優化<br>1. 專區介紹頁（Landing Page）：規劃各專區新增介紹頁，以強化各專區的亮點呈現，便利使用者閱讀重要資訊<br>2. ESG 亮點專訪：企業永續發展專區新增 ESG 主題亮點專訪，受訪象為內部主管或與客戶，主題包括綠色融資、綠色商品、綠色債券、普惠金融等 |
| 優化風險管理機制 | • 持續檢視風險管理機制完備性，關注與管理資訊安全、網路安全、數據隱私管理等相關新興風險，建立治理機制<br>• 建立上游供應商氣候風險之情境分析及財務量化計算<br>• 鑑別短中長期氣候風險傳導路徑，並具體掌握重大性氣候風險對營運策略與財務規劃之影響，以評估營運策略的氣候韌性 | 已達成 | • 持續強化 TCFD 治理 / 策略 / 風險管理之氣候相關指標之揭露<br>• 持續強化營運及業務氣候變遷轉型風險短 / 中 / 長期之鑑別及分析潛在財務衝擊影響<br>1. 依營運及業務之生命週期不同，持續強化營運及業務氣候變遷轉型風險短 / 中 / 長期之鑑別<br>2. 評估自身營運轉型風險低碳轉型之短 / 中 / 長期潛在財務衝擊影響<br>3. 除現行「傳產製造 – 金屬及其製品製造業」外，擴大評估高碳排產業及環保署列管高碳排企業之轉型氣候風險情境分析及潛在財務衝擊影響<br>• 持續強化辨識新興風險之特定性，以清楚描述該風險對於營運及業務之影響<br>• 建立範疇三投融資組合碳盤查盤點、監控與揭露機制<br>1. 建立盤點及監控機制，並於每年定期執行及追蹤範疇三投融資組合碳排放量 / 目標設定情形<br>2. 每年於永續報告書或 TCFD 報告書對外揭露 |
| 強化資訊安全 | • 定期召開資安委員會／資安交流會議檢視資安相關規定與事件，強化資安事件應變與分析<br>• 優化管理面、技術面、人員面控制措施，有效管控資訊系統之資安風險<br>• 自動化情資整合治理，持續最佳化資安防禦<br>• 進行資安攻防演練<br>• 強化新興金融科技的資安防護機制，建構敏捷資安策略與架構<br>• 落實資安費用之樽節成本政策，並精進集團資訊資源綜效，推動共通性資安合作<br>• 拔擢資安優秀人才，進行資安精英培育，以逐步落實資安防護工作並提升自我防護能量 | 已達成 | • 定期召開資安委員會／資安交流會議，檢視資安相關規定與事件，優化資安事件應變與分析<br>• 電腦系統資訊安全評估計畫及檢測，改善並提升網路與資訊系統安全防護能力<br>• 降低網路詐欺行為之發生機率，持續導入釣魚網站及偽冒行動軟體偵測服務，針對非官方之可疑網站及偽冒行動軟體進行監控、檢測、追蹤及下架<br>• 持續優化自動化情資整合之資安偵測及防禦機制<br>• 辦理資安事件通報應變演練和資安攻防模擬演練，整合跨部門事件處理及危機應變能力，確保維持強健資安體質<br>• 因應金融數位轉型及創新應用，識別新興科技資安風險，提升資安防護量能<br>• 落實資安費用之樽節成本政策<br>• 拔擢資安優秀人才，進行資安精英培育 |

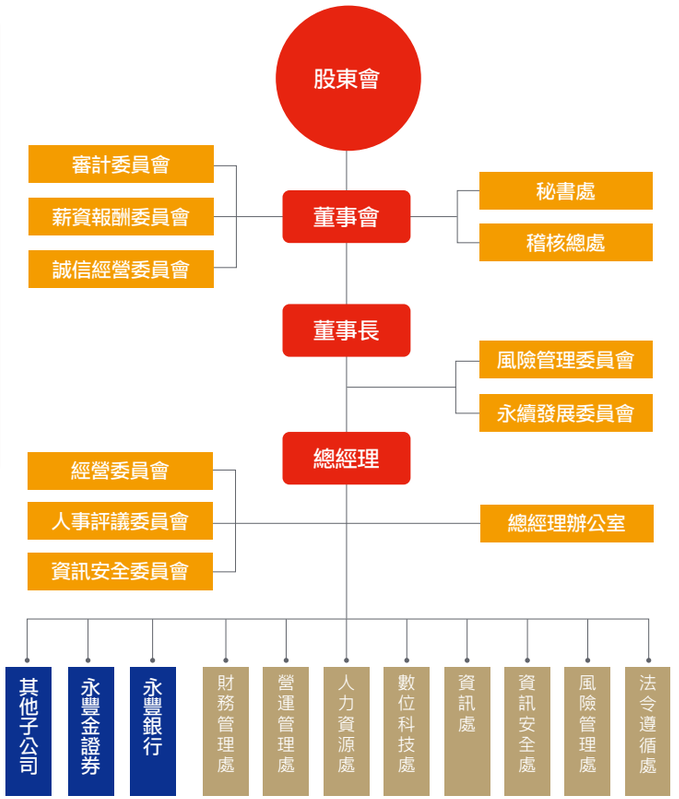
註：永豐金控最新永續工作規劃與目標設定，請參考永豐金控官網之「永續發展目標與願景」

# 2.1 公司治理

## 2.1.1 治理架構

為建立良好公司治理制度，永豐金控參酌「金融控股公司治理實務守則」及「上市上櫃公司治理實務守則」訂定「公司治理守則」，以下為主要施行方向：

| 永豐金控「公司治理守則」施行之主要方向 |
| --- |
| 遵循法令並健全內部管理 |
| 保障股東權益及金控與子公司及其他關係企業間之公司治理關係 |
| 強化董事會職能 |
| 發揮審計委員會功能 |
| 尊重員工及利害關係人之權益 |
| 資訊充分揭露增加透明度 |




永豐金控依「薪資報酬委員會組織規程」、「審計委員會組織規程」及「誠信經營委員會組織規程」分別設置「薪資報酬委員會」、「審計委員會」及「誠信經營委員會」等三大功能性委員會。

永豐金控功能性委員會一覽表

| 委員會名稱 | 委員會組成 | 職掌 | 組成規章與重要辦法 | 2022 年運作情形 |
| --- | --- | --- | --- | --- |
| 第三屆審計委員會 | 由永豐金控全體獨立董事組成，許建基獨立董事為召集人（註）。 | • 監督內部控制之有效實施<br>• 監督公司遵循相關法令及規則、存在或潛在風險之管控 | 審計委員會組織規程 | 共召開 12 次會議，出席率 100% |
| 第四屆薪資報酬委員會 | 由永豐金控全體獨立董事組成，薛琦獨立董事為召集人（註）。 | • 訂定董事及經理人績效評估與薪資報酬之政策、制度、標準與結構<br>• 定期評估董事及經理人之薪資報酬 | 薪資報酬委員會組織規程 | 共召開 10 次會議，出席率 100% |
| 第二屆誠信經營委員會 | 由永豐金控、永豐銀行、永豐金證券全體獨立董事組成，薛琦獨立董事為召集人（註）。 | • 負責誠信經營政策與防範方案之審議及監督經理部門執行成效，並定期向董事會報告遵循情形<br>• 將誠信與道德價值融入公司經營策略<br>• 審議誠信經營之相關防弊措施、監督制衡機制<br>• 建立檢舉制度並監督其執行之有效性 | 誠信經營委員會組織規程<br>誠信經營守則<br>誠信經營作業程序及行為指南 | 共召開 2 次會議，出席率 100% |

註：2023 年 5 月 24 日股東會進行董事改選，新一屆審計委員會召集人為馬文玲，薪資報酬委員會召集人為潘維大，誠信經營委員會召集人為潘維大。

## 2.1.2 股權結構

永豐金控依法揭露股東結構如下，其中政府機構持股比例未超過5%，可參考永豐金控年報第76頁。

股東結構　　2022 年 8 月 16 日；單位：股

| 數量 / 股東結構 | | 政府機構 | 金融機構 | 其他法人 | 個人 | 外國機構及外國人 | 合計 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 普通股 | 人數 | 6 | 33 | 775 | 323,576 | 1,388 | 325,778 |
| | 持有股數 | 99,723,703 | 796,549,486 | 3,909,528,352 | 3,400,374,020 | 3,177,589,087 | 11,383,764,648 |
| | 持股比例 | 0.88% | 7.00% | 34.34% | 29.87% | 27.91% | 100% |
| 甲種特別股 | 人數 | — | — | — | 1 | — | 1 |
| | 持有股數 | — | — | — | 10,000,000 | — | 10,000,000 |
| | 持股比例 | — | — | — | 100% | — | 100% |

### 2.1.2.1 家族成員持股占比

永豐金控大股東何壽川個人及其持有50%以上股份的公司持有本公司股份合計超過5%，大股東何壽川同一關係人2023年3月31日申報持股21.01%（同一人及同一關係人持股逾10%以上之大股東），詳細請參閱公開資訊觀測站「銀行（金融控股公司）大股東持股變動情形申報表查詢」。

# 2.1.3 董事會組成與運作

## 2.1.3.1 董事會組成

永豐金控第八屆董事會由7位董事組成，包含執行董事1席，非執行董事6席，其中符合臺灣法規定義之獨立董事共有3位(占比43%)，符合國際實務(即DJSI定義)之獨立董事為6位(占比86%)，除執行董事不適用非執行董事獨立性情形之外，董事長及其他非執行董事均符合國際定義之獨立性情形，詳細定義請詳董事組成背景表下方之註解。截至2023年5月24日董事平均任職期間為2.8年。永豐金控訂定「董事選舉辦法」，重視董事會組成之多元性，於「公司治理守則」明訂董事會組成應考量多元化，並就基本條件與價值(包含但不限於性別、年齡、國籍、種族及文化等)擬訂適當之多元化方針。另為落實董事會成員組成之性別平等，第八屆董事會包含3位女性成員，比率達40%以上，並由陳思寬女士續任董事長。

目前董事會成員有3位女性，4位男性，平均年齡55歲以上，其中博士3位，碩士4位，皆具備金融業或其他產業相關專業背景與經驗。綜觀7位董事各自擁有專業能力，董事會整體具備營運判斷、會計及財務分析、經營管理、危機處理、產業知識、國際市場觀、領導、決策、風險管理知識等各項能力。

永豐金控董事組成背景表

| 董事會成員姓名 | 基本條件 | | | | | | | 產業背景 | | | | | | 專業能力 | | | | | | | 金融產業相關學經歷 | 兼任情形 | 獨立性 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 國籍 | 性別 | 兼任經理人 | 年齡 | | | 任期期間 | 金融業 | | | | | 其他產業 | 金融 | 商務 | 法律 | 財務/會計 | 資安/資訊科技 | 氣候變遷/環保 | 風險管理 | | 兼任其他公司之職務少於四個(註一) | 非執行董事符合臺灣定義之獨立性情形(註二) | 非執行董事符合國際定義之獨立性情形(註三) |
| | | | | 55～60 | 61～65 | 66～70 | | 金控 | 銀行 | 證券 | 保險 | 投信 | | | | | | | | | | | | |
| 陳思寬 | 中華民國 | 女 | | ● | | | 2020/05/13～至今 | ● | ● | | | ● | ● | ● | ● | | ● | ● | | | ● | • 美國耶魯大學經濟學博士<br>• 中華經濟研究院院長，提供政府中長期經濟政策建議<br>• 星展(臺灣)商業銀行獨立董事<br>• 兆豐金控董事<br>• 兆豐銀行監察人<br>• 中央銀行理事<br>• 金融監督管理委員會金融監理沙盒申請案審查委員 | ● | | ● |
| 潘維大 | 中華民國 | 男 | | | | ● | 2020/05/13～至今 | ● | | | ● | | ● | ● | ● | ● | | | | | ● | • 東吳大學校長，法律學系專任教授(註四)<br>• 中國人壽保險股份有限公司獨立董事(註五) | ● | ● | ● |
| 蘇慧貞 | 中華民國/美國 | 女 | | | ● | | 2023/5/24～至今 | | | | | | ● | | | | | | ● | ● | ● | • 哈佛大學公衛學院環境衛生科學博士<br>• 國立成功大學校長<br>• 國立成功大學醫學院工業衛生學科暨環境醫學研究所特聘教授<br>• 中央研究院未來地球委員會中華民國委員會委員(註六) | ● | ● | ● |
| 馬文玲 | 中華民國 | 女 | | ● | | | 2023/5/24～至今 | | ● | | | ● | | ● | ● | | ● | | | | ● | • 野村投信總經理<br>• 安本標準投信總經理、業務行銷長<br>• 渣打銀行財富管理負責人<br>• 瑞士銀行投資商品暨服務部主管<br>• 匯豐銀行財富管理部主管、投資與保險主管<br>• 花旗銀行消費金融投資事業處經理 | ● | ● | ● |
| 朱士廷 | 中華民國 | 男 | ● | ● | | | 2017/12/05～至今 | ● | ● | ● | | | | ● | ● | | ● | | | | ● | • 國泰綜合證券董事長<br>• 凱基期貨董事長兼總經理<br>• 臺灣證券交易所副總經理兼發言人、董事<br>• 臺灣期貨交易所副總經理、董事 | ● | | 不適用(註七) |
| 葉奇鑫 | 中華民國 | 男 | | ● | | | 2018/05/01～至今 | ● | | | | | ● | ● | ● | ● | | ● | | | ● | • 律師(註八)<br>• 中華民國檢察官(註九)<br>• 東吳法律研究所兼任助理教授，教授個資法課程 | ● | | ● |
| 曹為實 | 中華民國 | 男 | | | ● | | 2020/05/13～至今 | ● | ● | ● | | | ● | ● | ● | | ● | | | | ● | • 巴克萊亞洲資本有限公司董事總經理 / 代理臺灣區總經理 / 大中華區環球金融及風險策略主管<br>• 摩根史丹利(Morgan Stanley Asia Limited)董事總經理<br>• 中華開發金控資深副總經理兼固定收益處部門主管 | ● | | ● |

註一：永豐金控「公司治理守則」第 28 條、38 條規定，本公司負責人兼任職務時，應確保本職與兼職之有效執行、不得有利益衝突或違反金融控股公司與其轉投資事業及子公司內部控制及監督制衡機制，及獨立董事不宜同時擔任超過四家上市上櫃公司之董事（含獨立董事）或監察人。

註二：非執行董事符合臺灣獨立性情形係參考臺灣金管會公布之《公開發行公司獨立董事設置及應遵循事項辦法》之獨立性董事定義，應於選任前二年及任職期間無下列情事之一：

(1) 非為公司或其關係企業之受僱人。

(2) 非公司或其關係企業之董事、監察人（但如為公司與其母公司、子公司或屬同一母公司之子公司依證券交易法或當地國法令設置之獨立董事相互兼任者，不在此限）。

(3) 非本人及其配偶、未成年子女或以他人名義持有公司已發行股份數額百分之一以上或持股前十名之自然人股東。

(4) 非 (1) 所列之經理人或 (2)、(3) 所列人員之配偶、二親等以內親屬或三親等以內直系血親親屬。

(5) 非直接持有公司已發行股份總數百分之五以上、持股前五名或依公司法第二十七條第一項或第二項指派代表人擔任公司董事或監察人之法人股東之董事、監察人 或受僱人（但如為公司與其母公司、子公司或屬同一母公司之子公司依證券交易法或當地國法令設置之獨立董事相互兼任者，不在此限）。

(6) 非與公司之董事席次或有表決權之股份超過半數係由同一人控制之他公司董事、監察人或受僱人（但如為公司或其母公司、子公司或屬同一母公司之子公司依證券 交易法或當地國法令設置之獨立董事相互兼任者，不在此限）。

(7) 非與公司之董事長、總經理或相當職務者互為同一人或配偶之他公司或機構之董事（理事）、監察人（監事）或受僱人（但如為公司與其母公司、子公司或屬同一母公司之子公司依證券交易法或當地國法令設置之獨立董事相互兼任者，不在此限）。

(8) 非與公司有財務或業務往來之特定公司或機構之董事（理事）、監察人（監事）、經理人或持股百分之五以上股東（但特定公司或機構如持有公司已發行股份總數百分 之二十以上，未超過百分之五十，且為公司與其母公司、子公司或屬同一母公司之子公司依證券交易法或當地國法令設置之獨立董事相互兼任者，不在此限）。

(9) 非為公司或關係企業提供審計或最近二年取得報酬累計金額未逾新臺幣五十萬元之商務、法務、財務、會計等相關服務之專業人士、獨資、合夥、公司或機構之 企業主、合夥人、董事（理事）、監察人（監事）、經理人及其配偶。但依證券交易法或企業併購法相關法令履行職權之薪資報酬委員會、公開收購審議委員會或併購 特別委員會成員，不在此限。

(10) 未與其他董事間具有配偶或二親等以內之親屬關係。

(11) 未有公司法第 27 條規定以政府、法人或其代表人當選。

註三：非執行董事符合國際獨立性情形係採用 S&P Global Corporate Sustainability Assessment (CSA) 獨董之定義，下列 9 項指標須至少符合 4 項，其中前 3 項需至少符合 2 項：

(1) 過去 1 年內，董事未任職本公司高階主管。

(2) 本年度董事及其家族成員未接受公司或任一子公司超過 60,000 美元，但受美國 SEC 4200 條款允許者得不在此限。

(3) 董事的家族成員未任職公司或任一子公司的高階主管。

(4) 董事非公司或經營團隊的諮詢顧問，且與公司諮詢顧問沒有利害關係。

(5) 董事與公司主要顧客或供應商沒有利害關係。

(6) 董事與其他企業或其經營階層間沒有服務契約關係。

(7) 董事與主要受公司捐獻之非營利組織沒有利害關係。

(8) 過去 1 年內，董事未任職於公司外部查核機構或擔任合夥人。

(9) 董事與董事會獨立性運作無任何利益衝突。

註四：潘維大著有公司法、票據法、商事法概論等書籍，針對企業間商業交易樣態、公司治理、策略規劃及政策法規具備充分知識與運作經驗。

註五：潘維大於任職中國人壽保險股份有限公司獨立董事期間參與重要政策審議及推動，核議「業務通路轉型專案」，全面為轉型推廣優化管理業務提升中國人壽整體市場競爭力，任內協助中國人壽連獲中華公司治理協會二次「特優認證」，績效顯著。

註六：蘇慧貞女士為美國哈佛大學環境衛生科學博士，研究專長包括永續發展、氣候變遷與環境科學。目前各國金融監理機關，均強調董事會對於金融業氣候治理的重要角色，「減緩與調適氣候變遷」亦為永豐金控三大承諾之一，董事會中包含具有氣候相關背景之董事，將有助於深化本公司董事會氣候職能。

註七：朱士廷為執行董事（公司經理人），故不適用非執行董事獨立性情形。

註八：葉奇鑫為臺灣少數具有理工和法律雙專業之律師，長期協助政府與企業因應金融科技與新興網路科技產生之法律問題，同時亦是金融科技（Fintech）領域的行業專家，專精於包含大數據、人工智慧、區塊鏈、物聯網（IoT）等新興科技法律議題。

註九：葉奇鑫於擔任檢察官期間草擬刑法第 36 章「妨害電腦使用罪章」，對於電子商務和資訊安全產業也著墨甚深，曾擔任電子商務公司和資安公司之高階經理人。

董事會多元性目標

| | |
|---|---|
| 獨立董事至少 3 席，不少於董事席次 1/3，且連續任期不超過 3 屆 — 已達成 | 至少一席女性董事 — 已達成 且女性董事比例達 40% 以上 |
| 兼任公司經理人之董事占董事席次比率不宜過高 — 已達成 | 董事會整體具備公司治理九大能力 — 已達成 |
| 董事會整體具金融、商務、法律、財務、資安、風管等 7 類產業專業背景 — 已達成 | 至少各 1 席具有銀行、證券專業之董事 — 已達成 |
| | 全體董監事簽署誠信經營政策之聲明 — 已達成 |

## 2.1.3.2 董事會運作

永豐金控董事會原則上每月召開1次，要求董事之最低出席率為80%。2022年董事會共開會13次，董事平均實際出席率達100%。各董事平均實際出席董事會情形，納入董事成員績效評估之衡量項目；董事對於有自身利害關係之議案均依法迴避不參與表決，董事出席情形及對利害關係議案迴避之執行情形請參閱2022年永豐金控年報第29-31頁。自2003年起，永豐金控為董事及監察人購買「董監事及經理人責任保險」，並每年檢討保單內容。

永豐金控經由公開資訊觀測站、公司網站及年報等管道，揭露董事進修及出席董事會情形，於年報及公司網站揭露董事會重大決議，且於年報揭露董事對利害關係議案迴避之執行情形，以提升董事會運作資訊透明度。關於永豐金控董事提名及遴選制度 🔗 ，以及董事會績效評估辦法 🔗 ，請詳見官方網站以及下載專區 🔗 。

永豐金控2022年度全體董事之進修均符合「上市上櫃公司董事、監察人進修推行要點」之規定，每位董事平均受訓時數8.71小時，高於法規規定6小時。進修課程包含公平待客之友善金融、如何落實對高齡消費者之保護、董事決策如何避免背信與非常規交易、洗錢防制國際趨勢與金融科技之運用、員工與董事薪酬議題探討、全球科技產業及供應鏈發展趨勢、從元宇宙熱潮看資訊安全的保護、策略與危機管理、公司治理3.0之ESG揭露要求、低碳投資展望與因應商業策略、企業併購實務、電動車與智慧車的技術發展與商機、量子科技的關鍵技術與商機等課程。董事進修情形請參閱2022年永豐金控年報第43頁。

### 2.1.3.3 董事會績效評估

永豐金控於2018年訂定「董事會績效評估辦法」，董事會及功能性委員會(包含審計委員會、薪資報酬委員會及誠信經營委員會)每年依該辦法所定之評估程序及評估指標執行績效評估，並應至少每3年委由外部專業獨立機構或外部專家學者團隊執行評估1次，於次一年度3月底前將績效評估結果提報董事會。2022年度本公司委任安永企業管理諮詢服務股份有限公司辦理董事會績效暨功能性委員會績效評估，個別董事成員則以內部自評方式辦理，目前已將公司治理及ESG表現納入董事酬勞給付考量，未來評估將ESG表現納入自評指標之一。

| 評估方式 | 評估期間 | 評估範圍 | 評估內容 | 評估結果 |
|---|---|---|---|---|
| 內部自評 | 2022 年 1 月 1 日至 2022 年 12 月 31 日 | 個別董事成員之績效評估。 | 1. 公司目標與任務之掌握<br>2. 董事職責認知<br>3. 對公司營運之參與程度<br>4. 內部關係經營與溝通<br>5. 董事之專業及持續進修<br>6. 內部控制 | 評分標準係依各衡量項目採比重加權方式計分，並將績效評估結果分為優、佳、良好、尚可、有待加強五級。<br>**「董事成員」自評結果均為「優」。** |
| 外部評估<br>( 委任安永企業管理諮詢服務股份有限公司執行評估 ) | | 董事會、審計委員會、薪資報酬委員會及誠信經營委員會之績效評估。 | 就董事會暨功能性委員會架構(Structure)、成員 (People)，以及流程 ( Process and Information) 等三大構面，以文件查閱、董事自評問卷及實地訪談方式評估。涵蓋八個項目：<br>1. 董事會暨功能性委員會架構與流程<br>2. 董事會暨功能性委員會組成成員<br>3. 法人與組織架構<br>4. 角色與權責<br>5. 行為與文化<br>6. 董事培訓與發展<br>7. 風險控制的監督<br>8. 申報 / 揭露與績效的監督 | 對於質化衡量指標進一步以三階段進行評估，包含：基礎、進階及標竿。經綜合評估，本公司在董事會暨功能性委員會架構 (Structure)、成員 (People) 及流程與資訊 (Process and Information) 方面的**綜合表現程度均為標竿。** |

## 2.1.4 高階薪酬政策

### 2.1.4.1 高階主管薪酬制度

永豐金控總經理及副總經理(高階主管)酬金係依個別專業資歷暨參考同業薪資水準，經金控薪資報酬委員會討論續提董事會核定。除每月固定的底薪、津貼外，並依據金控中長期策略檢視年度整體營運成果、個人績效及將未來風險等因素納入考量，依公司相關規定另行發給績效獎金及長期激勵獎酬。

為平衡短期與長期獎酬、組織經營與個人績效、現金與非現金等考量，永豐金控訂定「長期激勵獎酬計畫」，總經理及副總經理(高階主管)長期獎酬遞延比例約當績效獎金20%以上，設計變動薪酬之績效期間為3年，閉鎖期總計5年，遞延獎金給付形式採取虛擬股數及持股信託方式執行，透過永豐金控股票價值連結，使經理人之薪資報酬得與金控經營績效與長期發展方向密切相關。

此外為使經理人共享永續經營成果，永豐金控經理人於退休後享有優惠利率之「退休金優惠存款」及「優惠房貸」，期使持續支持公司業務發展。

#### 索回政策與說明

經理人如涉有觸犯法律、違反職業道德、失職或瀆職等行為，或因不當行為產生業務風險而造成公司利益或聲譽損失者，經董事會核准得調整發放比例，或索回獎勵發放。

### 2.1.4.2 高階主管永續績效目標

為實踐永續策略及推動進程，永豐金控已將永續發展納入2022~2024年金控四大策略之一，並將其列為總經理和高階主管的長期及短期績效目標內，以進一步與變動獎酬連結，相關目標說明如下：

#### 長期績效目標

金控總經理及副總經理(高階主管)長期激勵績效目標含未來3年金控及子公司財務績效表現、長期策略執行成效、TSR股東價值，同時需考量風險管理、公司治理及「永續指標」加權占比15%，將落實推動永續目標並取得國內外評鑑情形作為持股信託解鎖條件，連結經理人對長期績效的責任與擔當。

### 總經理短期績效目標

| 指標項目 | 權重占比 | 說明 |
|---|---|---|
| 財務指標 | 20% | 公司財務績效及相較同業表現水準，如 ROE、ROE同業排名、預算達成率、總資產、營收表現等。 |
| 策略指標 | 50% | 依據未來中長期策略展開之目標，如數位轉型、永續承諾達成情形、重大主題因應調適作為等。 |
| 永續及內控指標 | 30% | 致力實踐三大永續承諾，重視誠信經營、法令遵循及風險控管，實踐 ESG 各項重點工作(含關注氣候風險並推動淨零具體作為指標占比 10%)。 |
| 管理指標 | 額外考量項目 | 納入人力資源指標，人才發展及職業安全衛生推動作為。 |

### 高階主管短期永續績效指標

| 指標項目 | 權重占比 | 說明 |
|---|---|---|
| 重大主題因應調適 | 10% ~ 20% | 1. 重大主題之相關因應調適作為(如風險管理、公司治理、資訊安全管理)，除納入金控總經理績效目標，亦推展至金控各權責高階主管短期績效指標。<br>2. 金控各部門設置 KPI 永續指標占比至少 10%，按各部門職掌規劃永續經營指標，並納入高階主管短期(年度)績效目標且連動當年度績效獎金。 |
| 減緩氣候變遷與調適 | 8~10% | 為推動減緩氣候變遷與調適，將氣候相關 KPI 項目列入金控相關權責高階主管績效指標，分別為：<br>1. 提升內部氣候意識 (8%)<br>2. 淨零承諾，如溫室氣體盤查與認證 (10%)<br>3. 風險管理，如優化風險管理機制 - 導入並持續深化氣候風險管理 (10%) |
| 職業安全衛生推動 | 5% | 為推動職場安全，ISO45001 認證覆蓋率列入金控總經理績效目標，亦推展至金控權責高階主管短期績效指標，如：<br>ISO45001 認證覆蓋率、反歧視騷擾推動、照顧一個人保護一家人計畫員工健康管理計畫(請詳見 4.4.3 職場安全與健康) |

### 2.1.4.3 高階薪酬給付情形

2022年度永豐金控給付高階主管各項酬金總額占永豐金控稅後純益之0.44%，永豐金控合併報告內所有公司給付予金控總經理及副總經理級以上高階主管之各項酬金總額占財務報告內所有公司稅後純益之1.31%，其相關酬金資訊請參閱2022年永豐金控年報第27頁。永豐金控對高階主管持股尚無規範，截至2022年底永豐金控總經理無持股，高階主管(不含總經理)平均股權為其基本薪資之1.54倍。

### 2022年總經理與員工薪酬比例

| 總經理薪酬與員工平均薪酬比例 | 總經理薪酬與員工薪酬中位數比例 |
|---|---|
| 23.7 倍 ~ 39.5 倍 | 27.5 倍 ~ 45.9 倍 |

| 員工(不含總經理)薪酬平均金額 | 員工(不含總經理)薪酬中位數 |
|---|---|
| 1,265(新臺幣仟元) | 1,089(新臺幣仟元) |

| 總經理薪酬漲幅與員工薪酬漲幅中位數比例 |
|---|
| 25.45% |

註：上表係依循臺灣證券交易所「非擔任主管職務之全時員工薪資資訊申報作業說明」之相關規定辦理。

# 2.2 誠信經營與法令遵循

## 2.2.1 誠信經營文化

永豐金控於2018年設立「誠信經營委員會」，由金控、銀行及證券子公司之獨立董事共8位組成，每半年至少召開一次會議，負責誠信經營政策與防範方案之審議及監督經理部門執行成效，定期向法令遵循處、稽核總處等案件涉及相關單位了解不誠信行為風險及檢舉機制等執行情形，並於委員會會議後向董事會報告遵循情形及決議事項，相關執掌請詳見官網。2022年共召開2次誠信經營委員會會議，運作成果包括：

- 辦理誠信經營委員會2021年績效評估，彙整呈報各委員自評結果，做為誠信經營委員會檢討、改進之參考。
- 審議永豐金控及子公司防範不誠信行為方案遵循情形查核結果。
- 監督檢舉制度執行之有效性，如審議永豐金控及子公司檢舉案件處理定期報告。
- 監督誠信政策宣導及教育訓練情形。

### 2.2.1.1 誠信經營政策與管理

| 永豐金控誠信經營政策重點 | |
|---|---|
| 禁止提供或收受不合理禮物、款待或其他不正當利益 | 禁止侵害智慧財產權 |
| 禁止提供或承諾任何疏通費 | 禁止從事不公平競爭行為 |
| 禁止行賄及收賄 | 遵守保密協定及禁止內線交易 |
| 秉持政治中立立場，不提供政治獻金 | 遵循及宣示誠信經營相關規範 |
| 慈善捐贈或贊助依「捐贈管理辦法」辦理 | 建立商業關係前之誠信經營評估 |
| 利益迴避原則 | 避免與不誠信經營者交易 |
| 保密責任 | 防範產品或服務損害利害關係人 |

永豐金控針對不同利害關係人訂有全面性之誠信經營政策，作為金控及子公司所有同仁遵循之依據，明訂人員於執行業務時或從事商業行為的過程中，應以客觀方式處理公務，做好利益迴避。

永豐金控誠信經營規範一覽

| 名稱 | 對象 | 目的 |
|---|---|---|
| 「誠信經營守則」 | 本公司及各子公司之董事、監察人、經理人、受僱人、受任人或具有實質控制能力者 | 建立本公司誠信經營之企業文化及健全發展 |
| 「誠信經營作業程序及行為指南」 | | 落實誠信經營，並積極防範不誠信行為 |
| 「道德行為準則」 | 本公司及各子公司董事、監察人及經理人 | 導引本公司及各子公司董事、監察人及經理人之行為符合道德標準 |
| 「股權管理辦法」 | 本公司董事、經理人及持有本公司股份超過股份總額百分之十之股東 | 確保各項股權申報符合法令規定及避免內線交易等事宜 |
| 「員工基本工作規範」 | 本公司及子公司員工 | 使員工遵守各項金融法規、道德規範，並因應金融環境變化及維護職場紀律，確保營運安全 |
| 「供應商企業社會責任行為準則」 | 本公司及各子公司之供應商 | 為致力於落實社會責任、推動環境永續發展、維護基本人權，並期許合作之供應商能採用相同準則，一同善盡企業社會責任 |
| 「檢舉案件處理辦法」 | 本公司及各子公司之董事、監察人、經理人及全體員工 | 為促進健全經營建立檢舉制度，並於總機構指定具職權行使獨立性之單位負責檢舉案件之受理及調查 |

## 2.2.1.2 誠信經營落實情形

永豐金控及子公司每年定期對全體員工辦理誠信經營暨檢舉制度相關議題之教育宣導及誠信簽署，將誠信經營及檢舉制度相關政策規範納入新進同仁之職前教育訓練課程，並將遵循誠信經營政策聲明書列入到職簽署文件。2022年合計參與教育訓練及簽署之同仁(包含2022年新進同仁及派遣人員)，共計10,909人，參與率100%。

在供應商方面，永豐金控要求供應商遵循「供應商企業社會責任行為守則」，鼓勵供應商一同履行企業社會責任，並規範永豐金控及各子公司與他人建立商業關係前，應先評估代理商、供應商、客戶等對象之合法性、誠信經營政策，以及是否有涉及不誠信行為之紀錄，以確保其經營方式公平、透明。從事商業行為過程中，應向交易對象說明誠信經營相關規定，並明確拒絕直接或間接提供、承諾、要求或收受任何形式或名義之不正當利益。此外，永豐金控明定內外部之吹哨者舉報機制及檢舉管道，請詳官網以及下載專區。

反貪腐政策和程序溝通比率

| | | | 2022 | |
|---|---|---|---|---|
| | | | 已溝通人員數 | 百分比 |
| 董事會成員(註一) | | | 31 | 100% |
| 員工(註二) | 管理階層 | 臺灣地區 | 1,739 | 100% |
| | | 海外地區 | 90 | 100% |
| | 非管理階層 | 臺灣地區 | 8,728 | 100% |
| | | 海外地區 | 352 | 100% |
| 供應商(家數)(註三) | | | 420 | 95% |

註一：董事會成員包括永豐金控、永豐銀行、永豐金證券、永豐金租賃、永豐投信、永豐創投等六家公司。永豐金控法令遵循處每年提供金控「誠信經營守則」及「誠信經營作業程序與行為指南」等規章予金控及各子公司之董事及監察人參閱及遵循，另要求金控及各子公司董事及監察人每年出具遵循誠信經營政策之聲明。

註二：員工包括永豐金控、永豐銀行、永豐金證券、永豐金租賃、永豐投信、永豐創投等六家公司。永豐金控及子公司每年將誠信經營及檢舉制度相關政策規範納入在職同仁、派遣同仁及新進同仁之在職或職前教育訓練課程，2022 年合計參與反貪腐政策和程序溝通人數共計 10,909 人(排除溝通期間因產假、病假致未能返回工作崗位之員工)。

註三：本公司訂有「供應商企業社會責任行為準則」，已請 420 家往來供應商簽署「供應商企業社會責任承諾書」，且新進供應商 100% 簽署，並於 2022 年舉辦四場內外部相關內容教育訓練。

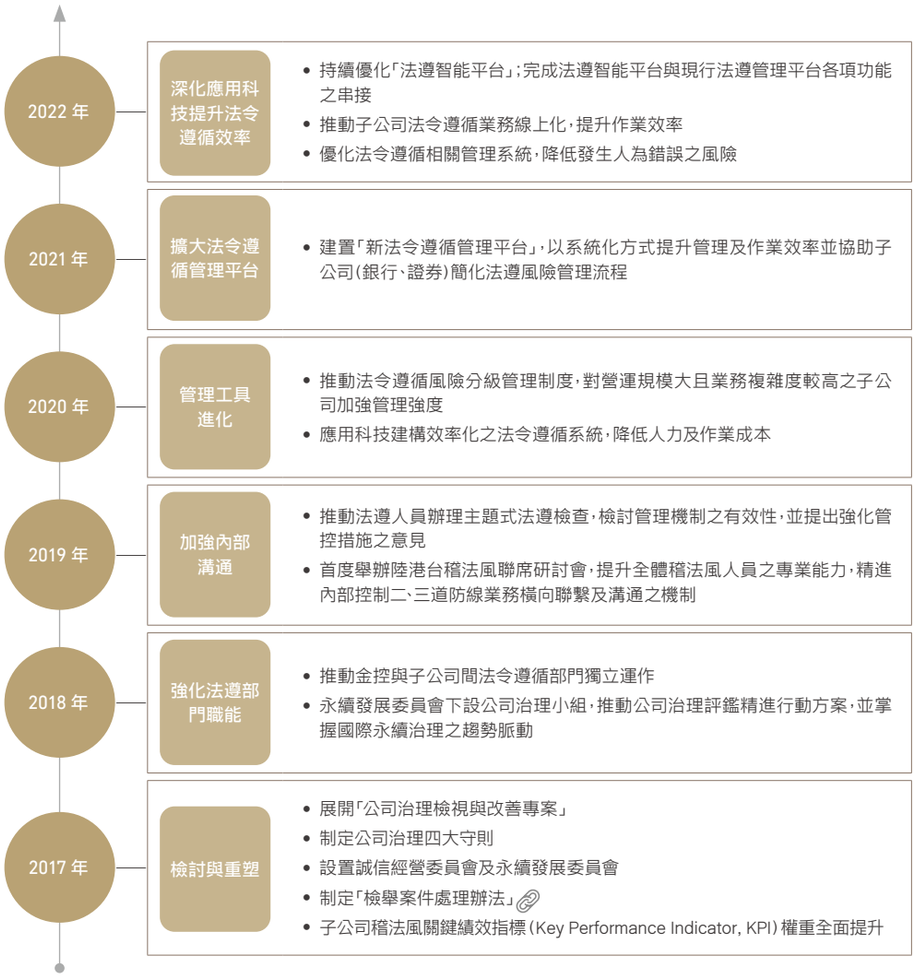
### 誠信經營落實盡職調查

永豐金控每半年配合法規檢視作業，審視行為準則規章的妥適性及有效性，於必要時修正相關規範；此外每半年辦理法遵自評，定期分析及評估較高不誠信行為風險之營業活動態樣，據此調整業務流程，強化內控管理機制。2022年永豐金控法令遵循處發動並督導各單位落實兩次法規檢視作業及兩次法遵自評，皆無發現異常或需修正相關內部作業規範之事項，各單位亦聲明無應改進事項。永豐金控針對較高不誠信行為風險之營業活動訂定防範方案，並定期檢討方案之妥適性與有效性，由誠信經營委員會負責審議，並報告董事會；經盤點及綜整永豐金控、銀行及證券子公司之內部規章，各公司已於相關內規中訂定確保誠信經營之防範方案，俾利同仁執行業務時遵循。不誠信行為亦納入稽核計畫中，定期透過內部稽核、外部檢查、裁罰案及主管機關函囑查核等事件進行規劃，以查核防範不誠信行為方案之遵循情形。2022年以銀行子公司行員涉挪用客戶款項及與客戶間有異常資金往來之案件所涉事項作為對不誠信行為之查核。

| 盡職調查程序 | 目的 | 執行成果 |
|---|---|---|
| 法遵自評 | 每半年分析及評估較高不誠信行為風險之營業活動態樣，以期防範於從事商業活動或執行業務過程中。 | 無發現異常或需修正相關內部作業規範，各單位並聲明無應改進事項。 |
| 規章檢核 | 每半年確認子公司誠信經營相關各項作業及管理規章均配合相關法規適時更新，確保各項營運活動符合法令規定。 | 永豐金控、銀行及證券子公司已於相關內規中訂定確保誠信經營之防範方案，俾利同仁執行業務時遵循。 |

## 2.2.1.3 法令遵循文化

永豐金控法令遵循文化推動進程




法令遵循處及相關權責單位定期舉辦溝通宣導及教育訓練，包括安排法遵部門定期講授重要法令修正內容及邀請外部具實務經驗的講師授課，2022年共舉辦108場教育訓練(包含實體及線上)，主題包括個人資料保護、消費者保護、防制洗錢及打擊資恐、沃爾克法則(Volcker Rule)、公平待客原則等，參訓人次達98,062人次，持續強化全體同仁遵法意識。

## 2.2.2 稅務政策

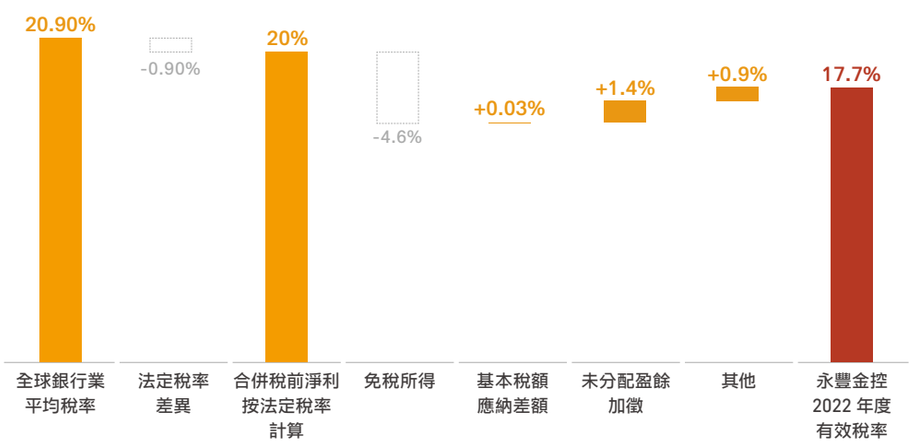
為落實企業永續經營及穩定成長目標，並因應稅務治理之國際趨勢，永豐金控已訂定「稅務治理政策」。永豐金控主要營運地區為臺灣，2022年度及2021年度之淨收益中，來自臺灣之比重分別為84.4%及86.4%，除了臺灣外，未有超過10%之淨收益來自其他單一國家。永豐金控遵循稅務法規，按規定期限報繳各項稅款，2022年及2021年於全球繳納所得稅稅款分別為新臺幣3,633,322仟元及1,649,494仟元，其中在臺灣繳納之所得稅款比重分別為81%及83%。有關各國淨收益占比與各項稅額數值請見附錄一、其他ESG數據資料。

近二年所得稅有效稅率及相關規定　　單位:新臺幣仟元

| 金控合併 | 2022 年度 | | | 2021 年度 | | 與銀行業平均有效稅率差異原因 |
|---|---|---|---|---|---|---|
| | 金額 | 有效稅率 | 銀行業平均稅率(註三) | 金額 | 有效稅率 | |
| 稅前淨利 | 19,404,715 | — | — | 18,649,230 | — | |
| 所得稅費用 | 3,443,715 | 17.7%(註一) | 20.90% | 2,438,225 | 13.1%(註一) | 因主要獲利地點臺灣之法定稅率為 20%，較全球銀行業平均低。各項稅額項目請見下圖「與銀行業平均有效稅率差異」與下表「所得稅費用與有效稅率項目」。 |
| 支付所得稅 | 3,633,322 | 18.7%(註二) | 21.28% | 1,649,494 | 8.8%(註二) | |

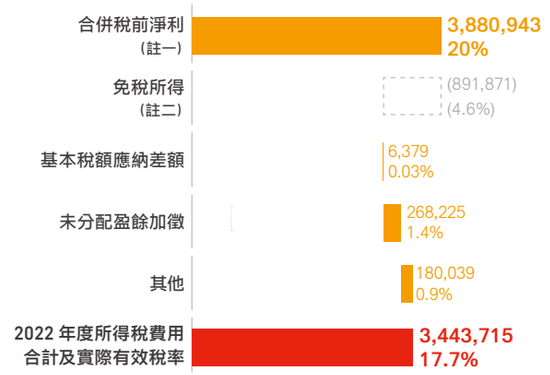
註一：所得稅費用除以稅前淨利，詳細項目請見下表 所得稅費用與有效稅率項目。
註二：支付所得稅除以稅前淨利。
註三：參考 DJSI 2023 Handbook，銀行業平均帳面有效稅率為 20.9 %，平均現金有效稅率為 21.28%。

2022 年度與銀行業平均有效稅率差異　　單位:新臺幣仟元

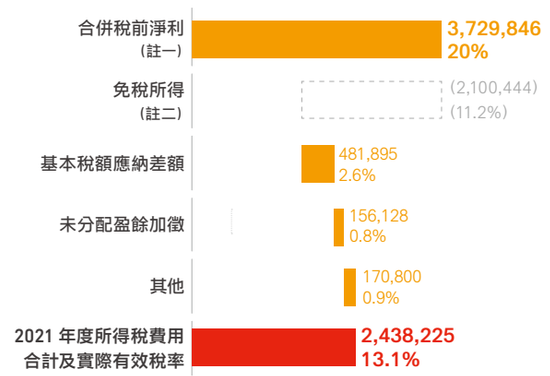


所得稅費用與有效稅率項目

2022 年度所得稅金額及稅率




2021 年度所得稅金額及稅率




註一：依「合併稅前淨利」按法定稅率 20% 計算。

註二：主要為「國際金融業務所得」及「證券交易所得」按法定稅率 20% 計算。

# 2.2.3 防制洗錢及打擊資恐

## 2.2.3.1 防制洗錢及打擊資恐政策

永豐金控已訂定「防制洗錢及打擊資恐政策」供金控及各子公司共同遵循；各子公司亦分別依循各該業別相關法令規定，以及所屬同業公會之自律規範及公約，並同時參照「防制洗錢及打擊資恐政策」之規範內容，自行訂定防制洗錢及打擊資恐之內部規範及作業程序。

永豐金控集團防制洗錢暨打擊資恐重要規範

- 防制洗錢及打擊資恐注意事項
- 客戶名稱審查作業
- 客戶身分確認及持續審查作業
- 重要政治性職務人士(PEPs)洗錢及資恐風險評估作業準則
- 可疑交易及帳戶監控作業
- 實質受益人及高階管理人辨識及驗證
- 特殊業務防制洗錢相關作業(包含：數位存款帳戶、虛擬通貨交易平台業者帳戶、第三方支付業者帳戶)
- 防制洗錢及打擊資恐風險作業細則
- 大額通貨交易資料申報作業

## 2.2.3.2 洗錢防制管理架構

為落實集團防制洗錢及打擊資恐(Anti-Money Laundering and Countering the Financing of Terrorism，AML/CFT)的工作及文化，永豐金控董事長下設「風險管理委員會」，由金控董事長擔任主席，負責監督及管理跨子公司洗錢防制及打擊資恐之風險，並管理相關資源之整合與分配，金控法令遵循處為AML/CFT專責單位，負責督導及協助子公司AML/CFT運作之規劃及執行。永豐金控訂定集團資訊分享政策及程序並建立資訊分享平台，以避免子公司橫向聯繫的疏漏，造成防制洗錢的缺口。在未違反個人資料保護及確保資訊機密性之前提下，要求各子公司應定期或不定期分享洗錢或資恐態樣及黑名單，並上傳至資訊分享平台供其他子公司參考辦理。

永豐銀行成立「防制洗錢委員會」，由總經理擔任會議主席，做為行內跨單位工作的管理及協調；同時設立防制洗錢中心，專責負責銀行有關防制洗錢與打擊資恐相關制度流程的制定及督導分行落實防制洗錢工作。其他子公司亦分別設有AML/CFT專責主管或人員，負責防制洗錢及打擊資恐之相關工作。

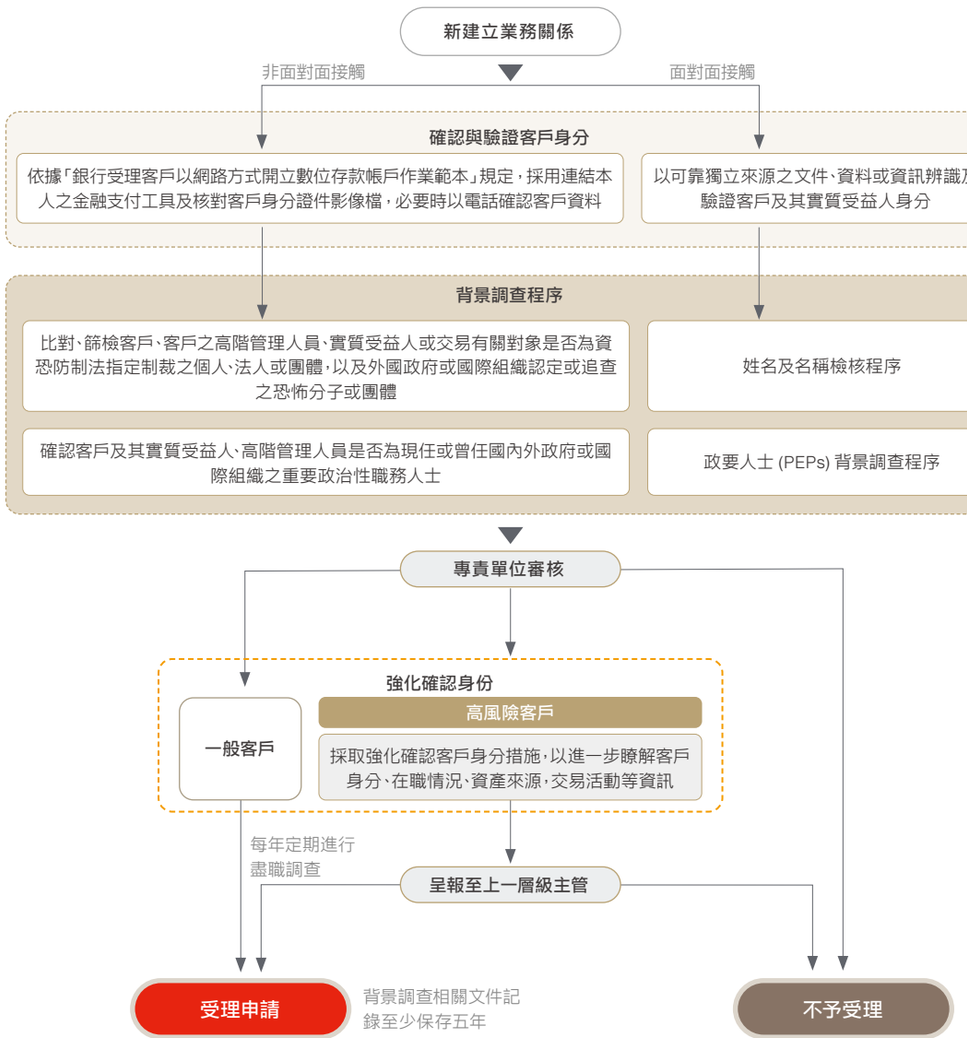
## 2.2.3.3 評估機制及結果

永豐金控要求旗下各子公司採行一致之方法論進行年度機構風險評估報告(IRA)。以銀行及證券為例，分別聘請外部顧問協助導入IRA方法論，針對四大風險因子設計評估問卷，使用評分機制，計算固有風險、控制措施，進而評估剩餘風險。永豐銀行依主管機關規定，應每年針對防制洗錢及打擊資恐內部控制制度之設計及執行，委請外部會計師出具確信報告；2023年3月會計師確信報告之結論為「有效，在所有重大方面係允當表達」，且報告內所列建議事項均已改善完成。

## 2.2.3.4 客戶盡職調查

為落實防制洗錢及打擊資恐工作，永豐銀行已建立詳盡客戶盡職調查(Customer Due Diligence, CDD)流程，涵蓋項目包含對線上或數位開戶之客戶的非面對面審核程序，以及對政要人士(PEPs)的背景調查、身分鑑別程序，詳情如下：

永豐銀行客戶盡職調查(Customer Due Diligence, CDD)流程




永豐銀行亦針對既有帳戶與交易進行洗錢與資恐防制監控。除以風險基礎方法建立帳戶及交易監控政策與程序外，永豐銀行更利用資訊系統，輔助辨識疑似洗錢或資恐交易。針對辨識出之警示交易，專責單位應就客戶個案情況判斷其合理性，如經檢視屬疑似洗錢或資恐交易者，不論交易金額多寡，於防制洗錢中心專責主管核定後立即向法務部調查局申報。上述所有相關文件紀錄應至少保存5年。

## 2.2.3.5 防制洗錢及打擊資恐教育訓練

為建立防制洗錢暨打擊資恐之法遵文化，永豐金控及子公司防制洗錢主管及人員以及相關業務單位主管，每年需修習至少12小時洗錢防制相關之內外部教育訓練。此外，亦針對所有員工定期舉辦防制洗錢教育訓練，參訓對象包括董事及高階管理人員、防制洗錢及打擊資恐專責主管及一般人員，訓練方式則以線上課程或實體課程方式舉行，訓練主題包含洗錢與資恐發展趨勢、防制洗錢實務研討、資恐案例分享等。

# 2.2.4 重大違反項目及改善措施

永豐金控及子公司管理階層與員工均致力於實踐誠信經營於日常行為與營運中，惟仍有不足之處須持續改善之項目，將持續精進。2022年重大違反項目計有永豐銀行勸誘客戶以融資方式購買理財商品、辦理房貸業務搭售房貸壽險商品及辦理保險代理人業務有不當銷售保險商品等情事、永豐投信及永豐金證券違反內部規章等共6件，裁罰金額共1,860萬元，案關人員依情節輕重受免職、記過、申誡、警告等處分，上述相關重大違反項目及改善措施詳情參閱年報第62-63頁；2022年無任何與利益衝突迴避、反壟斷與反競爭行為、洗錢與內線交易、環境、健康與安全及吹哨者機制相關情事。

2022 年重大及其他違反項目與改善措施

| 事件類別(註一) | 件數 | 事件說明 | 影響後果 | 改善狀況 |
|---|---|---|---|---|
| 貪腐或賄賂 | 1 | 永豐銀行前經理人及現職行員與客戶間有異常資金往來，且就授信案件與自身利益關係部分未適當迴避或保持明確分際，及未覈實申報利害關係人資訊。 | 依銀行局所列之缺失事項予以糾正，考量已改善完畢，無裁罰或非金錢制裁處分。 | • 強化員工帳戶往來情形之查核。<br>• 新增利益迴避之系統警示功能，並將利益迴避納入自行查核題項。<br>• 建立利害關係人資料完整性之定期清查作業。 |
| 違反作業流程或法令規範 | 5 | 1. 永豐投信債券基金月報記載內容與基金實際投資情形及公開說明書內容不一致。<br>2. 永豐金證券受理投資人檢舉案，查核發現業務人員與客戶有款項借貸；或與客戶涉有訴訟情事，惟公司未主動通報主管機關。<br>3. 永豐銀行辦理保險代理人業務與保險公司簽訂「電話行銷合作契約書」，未實際從事保險招攬，而向保險公司收取相當於佣金之報酬。<br>4. 永豐銀行有勸誘客戶以融資方式購買理財商品、辦理房貸業務搭售房貸壽險商品及辦理保險代理人業務有不當銷售保險商品等相關缺失。<br>5. 永豐銀行對高齡客戶申辦貸款有未確實執行認識客戶作業等缺失。 | 裁罰金額總計 1,860 萬元。 | • 增加基金商品之文宣審核流程，以加強確保內容與證券投資信託契約或公開說明書一致。<br>• 已將法遵處相關人員納入證券重大事項通報之副知對象，俾利於知悉後申報。<br>• 終止與保險公司間之電話行銷合作契約。並加強宣導涉有違規疑慮業務情事之相關重要法令。<br>• 建立全行統一之專業投資人資格認定政策及流程。加強購買金融商品之資金來源檢核及電訪作業機制。調整法遵風險警訊指標及發生較高警示時通報高階管理階層之作業，建置 1.5 道法令遵循防線。<br>• 修訂授信規範，對高齡客戶申辦貸款應審慎評估貸款用途與還款能力。 |
| 歧視或騷擾 | 4 | 2022 年經調查成立之職場反歧視相關申訴案件為 3 件，2022 年經調查成立之性騷擾相關申訴案件為 1 件。 | 屬內部申訴案件，非主管機關裁罰故無裁罰或非金錢制裁處分。 | 改善措施請詳見 4.4.3.3 職場平權與友善反歧視。 |
| 客戶隱私數據 | 3 | 2022 年永豐銀行發現 3 項缺失<br>1. 個人資料外洩事件處理程序。<br>2. 資料安全管理、人員管理及個資查詢覆核。<br>3. 外規完整內化、資料安全稽核機制。 | 屬內部發現缺失，皆已改善，故無裁罰或非金錢制裁處分。 | |
| 利益衝突 | 0 | 2022 年無相關違規事件。 | | |
| 洗錢或內線交易 | 0 | | | |

註一： 此處須揭露之重大違反項目不僅限於遭受主管機關裁罰之事件，亦包括違反永豐內部相關行為準則與反貪腐政策之事件，違反事件類別定義參考 RobecoSam 之 Dow Jones Sustainability Index (DJSI) 2023 年度商業道德應包含項目。

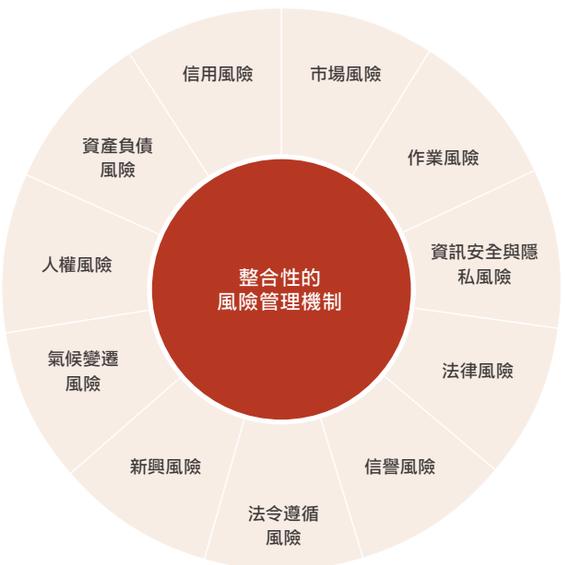
註二： 2022 年整體裁罰共 7 件，裁罰金額共 18,601,200 元；2021 年整體裁罰共 10 件，裁罰金額共 694 萬元。

# 2.3 風險管理

## 2.3.1 風險管理架構

永豐金控訂定之「風險管理政策」係於2009年經董事會通過，最近一次經董事會修正通過日期為2019年12月20日，除發展各子公司風險管理環境與文化外，亦完整訂定各類風險的整合性管理規範及限額、業務單位之業務權限及作業規範等風險管理程序，用以辨識、衡量、評估及管理各類型風險，永豐金控及各子公司之風險管理單位或人員定期向董事會報告風險管理執行情形暨改善建議，如遇重大暴險情事，應立即採取適當措施並向董事會報告；針對信用、市場、作業、資產負債、信譽、法律、法令遵循、策略風險及其他與營運相關之風險，包含新興風險及氣候變遷風險等，進行風險評估並建立風險回應措施，據以辨識金控層級之相關風險並研擬風險因應對策後，呈報適當之層級。

永豐金控風險管理機制




永豐金控風險管理程序


| 風險辨識 | 風險掃描 | 風險監控 | 稽核 | 風險報告 |
|---|---|---|---|---|
| 各業務單位採行風險自評、檢視稽核報告、關鍵風險指標等方式執行風險辨識。 | • 風險管理單位彙整辨識結果，並就事件發生影響程度、可能性等進行評估並衡量整體風險暴險程度。<br>• 風險管理單位每日搜尋負面新聞事件並發佈《Credit Warning》，由各子公司回報相關暴險與後續處理措施後，彙整提報金控風險管理委員會委員。<br>• 資訊安全等非財務風險會依相關規範執行災害復原、演練、偵測及防護措施。<br>• 新種業務承作，或新流程及系統生效前，辨識並評估其風險。<br>• 當內外部環境改變時，應立即重新進行作業風險辨識及後續相關工作。 | • 每日：針對市場風險，風險管理單位監控及呈報高階主管金控整體暨各子公司損益及市場風險值(VaR)之使用概況，嚴格執行部位之預警、超限或停損之風險管理處置措施。<br>• 每月 / 季：每月向董事會、每季向風險管理委員會報告各項風險類型與類別之風險胃納與風險程度、定期呈報風險管理委員會及董事會執行情形暨改善建議。如遇重大暴險情事，應立即採取適當措施並向董事會報告。<br>• 每年至少一次：依公司所訂定 / 調整之經營策略與預算目標，審查、辨識及評估各項風險類型(包括資本適足性、信用大額及集中度風險、市場風險值、及流動性風險等)與類別之風險胃納與風險程度，並經相應之核決層級審核通過後實施，並依上述頻率監控管理之。 | 稽核單位針對風險管理流程進行內部稽核，將風險類別項目區分為財務狀況、法令遵循、風險管理、內部管理、資訊管理及股權管理等六類。並依固有風險、控制措施有效性風險之風險評估結果，將查核規劃分為「指定專案查核項目」及「重點查核項目」。 | • 風險管理單位應定期向董事會報告風險管理執行情形、敏感性分析及壓力測試結果。<br>• 各子公司如有重大風險事件或有發生之虞，應立即呈報風險管理單位、總經理與董事長。 |

永豐金控風險以整合風險管理之角度，對影響公司價值之以下攸關風險類型(risk categories and risk type)之風險胃納(risk appetite)進行定期及不定期審查、辨識及評估，並以風險燈號揭示各項攸關風險之承受程度(risk tolerance levels)並予以排序，將評估結果定期呈報風險管理委員會及董事會。

| 風險類型 (Risk Categories) | | 風險類別 (Risk Type) | 風險胃納 (Risk Appetite) | 風險程度 (Risk Tolerance Level) | 風險監控 敏感性分析與壓力測試 |
|---|---|---|---|---|---|
| 1 | 資本適足率 | 資本適足率 | 高於法定比率某個水準 | 以 5 階段 ( 高、中高、中、中低及低 ) 風險燈號揭示風險之承受程度 | 依各種情勢演變，不定期模擬各種預測情境，於董事會呈報子公司信用風險及市場風險所可能遭遇之損失及對金控及各子公司資本適足率之影響。 |
| 2 | 信用風險 - 大額曝險 | 包括單一自然人、法人及關係人 / 關係企業授信、投資同一公司有價證券、及內部評等單一關係企業投融資等風險類別 | 占淨值一定比率 | | 風險管理單位不定期執行信用風險壓力情境模擬，將結果呈報董事會。 |
| 3 | 信用風險 - 集中度 | 對單一行業、高風險產業、國家、及內部高風險評等之投融資等風險類別 | 占淨值一定比率 | | |
| 4 | 市場風險 | 市場風險值限額 (VaR Limit) | 限額使用率 | | 市場風險管理單位每月執行壓力測試與敏感性分析，將結果呈報董事會。 |
| 5 | 流動性風險 | 包括債本比、融資使用率、流動性覆蓋比率及淨穩定資金比率等類別 | 高於法定比率某個水準 | | 永豐銀行至少每年執行流動性風險壓力測試，並將結果呈報資產負債管理委員會及董事會。 |

為辨識、評估及審視未來短中長期可能面臨之風險，永豐金不定期模擬各種預測情境，近年針對後疫情、中美貿易、科技及金融戰、俄烏戰事、台海危機等情勢辨識未來經濟前景所面臨之風險，永豐金控推估所面臨之5大風險及提出相關減緩措施如下：

| 風險事件 | | 針對該事件的管理與監控措施 | 敏感性分析與壓力測試 |
|---|---|---|---|
| 1 | 俄烏戰事能源大宗物資短缺 / 疫情擴散供應再度斷鏈 | • 監控高風險產業風險程度<br>• 評估受疫情或景氣影響列為預警、紓困、異常及逾催等關注客戶之營運狀況及後續因應 / 處理措施呈報金控主管會議 | 不定期推估未來風險因子變化模擬部位損失對資本適足影響，擬具市場信用及流動性因應對策 |
| 2 | 升息循環通膨預期企業經營困頓 / 市場波動加劇流動性枯竭 | • 每日預估及監控未來 1 個月市場風險值 (VaR)<br>• 評估受影響列為預警、紓困、異常及逾催等關注客戶之營運狀況及後續因應 / 處理措施呈報金控主管會議 | |
| 3 | 美元升值資金外逃新興國家債務危機 | • 新興國家政治紛擾及金融動盪者，施予限制性管制，承做該等國家業務應經所屬公司總經理同意<br>• 受影響列為預警、紓困、異常及逾催等關注客戶之營運狀況及後續因應 / 處理措施呈報金控主管會議<br>• 監控中國城農商行逾放、覆蓋率及所有子公司往來項目與曝險<br>• 積極依金控資訊安全管理政策及相關要點，強化資安管理、災害復原、演練、偵測及防護措施 | |
| 4 | 反全球化區域分裂地緣政治風險高升 | | |
| 5 | 中國結構政策問題引系統性風險疑慮 / 常態化軍事威嚇窮台政策資訊戰 | | |

| 基準日: 2022/12/30 | | 預測情境對資本適足率影響 | | | | | | 法定標準 |
|---|---|---|---|---|---|---|---|---|
| 公司 | 項目 | A. 輕微情境 | | B. 嚴重情境 | | C. 極端情境 | | |
| | | 2023/06 | 2023/12 | 2023/06 | 2023/12 | 2023/06 | 2023/12 | |
| 金控 | 資本適足率 (CAR) | 129.62% | 140.85% | 125.97% | 134.10% | 121.73% | 126.26% | 100% |

除上述風險類別與管理程序外，永豐金控及各子公司依其規模、業務性質或主管機關之規定建立自行查核制度、法令遵循制度與風險管理機制及內部稽核制度等內部控制三道防線，以維持有效適當之內部控制制度運作。此外，針對重大風險項目皆設有三道防線機制，並整合至公司整體風險/合規管理架構中，氣候變遷風險三道防線機制請詳2.3.5氣候變遷風險管理，隱私權請詳2.5.1隱私安全治理架構。

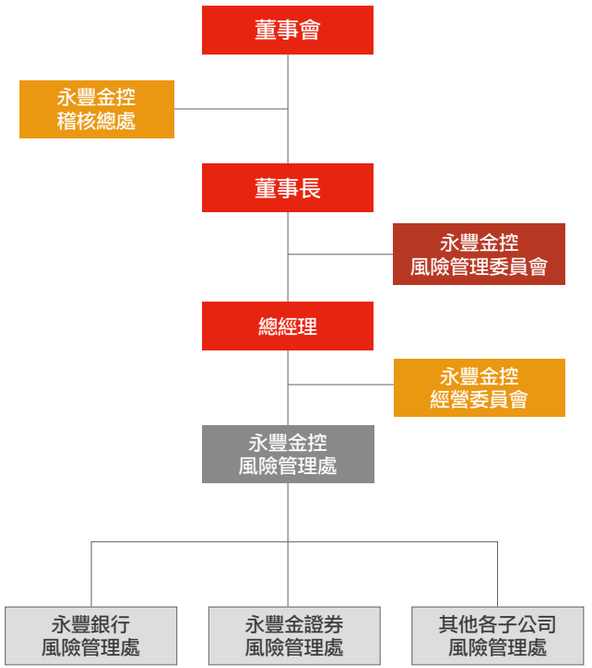
永豐金控內部控制三道防線

| 角色 | | | 權責範疇 |
|---|---|---|---|
| 1 | 第一道防線<br>營業與業務管理單位 | 自行查核 | • 就其功能及業務範圍所產生之日常營運進行辨識與管控<br>• 針對風險特性設計並執行有效之內部控制程序，以涵蓋所有相關之營運活動 |
| 2 | 第二道防線<br>風險管理、法令遵循單位與業務管理單位 | 法令遵循及風險管理機制 | • 依其業務職掌協助及監督第一道防線辨識及管控風險<br>• 就各主要風險類別負責訂定整體風險管理政策、監督整體風險承擔能力及承受風險現況向董事會或高階管理階層報告風險控管情形 |
| 3 | 第三道防線<br>稽核單位 | 內部稽核制度 | • 依據「金融控股公司及銀行業內部控制及稽核制度實施辦法」之規定建立總稽核制，並設置隸屬董事會之內部稽核單位，至少每半年向董事會及審計委員會報告稽核業務<br>• 以獨立超然之精神，執行稽核業務，協助董事會及高階管理階層查核與評估風險管理及內部控制是否有效運作，包含評估第一道及第二道防線進行風險監控之有效性<br>• 適時提供改進建議，以合理確保內部控制制度得以持續有效實施，並作為檢討修正內部控制制度之依據 |

2022 年稽核計畫重點面向

| | |
|---|---|
| • **財務狀況**<br>(財務及經營績效) | • **內部管理**<br>(轉投資管理、內部稽核運作、委外管理) |
| • **法令遵循**<br>(法遵制度、防制洗錢、打擊資恐及反武擴、公司治理) | • **資訊管理**<br>(資訊系統規劃、網路安全及資安維護、系統異常控管) |
| • **風險管理**<br>(利害關係人交易、集團暴險、共同行銷、個資保護、金融消費者保護、資金運用) | • **股權管理**<br>(大股東股權管理) |

永豐金控及子公司風險管理組織架構圖




永豐金控風險管理架構與職責

| | |
|---|---|
| 董事會 | 董事會為風險監督最高單位，除負責核定永豐金控風險管理政策、風險胃納或限額外，並授權管理階層負責日常風險管理工作。 |
| 風險管理委員會 | 由董事長擔任召集人，審議公司風險管理政策、組織、制度及整體限額，檢視整體暴險及風險狀況，監督各公司風險管理活動，整合協調重大風險事件之管理，審議其他有關風險管理議題。 |
| 稽核總處 | 隸屬董事會的稽核總處負責執行風險管理架構第三道防線的獨立稽查功能，由總稽核為最高主管，統籌各項稽核業務之規劃與執行。 |
| 風險管理處 | 風險管理處處長為風險管理單位最高主管，統籌本公司及各子公司整體風險管理政策與準則之擬定及風險管理制度之建置及規劃。各項政策、準則及制度經董事會通過後由風險管理處負責推動，並就各子公司執行成果及管理績效作定期評估。 |

## 2.3.2 風險文化經營

為有效提升風險管理之執行品質，金控風險管理處每年度針對各子公司之風險管理執行情形進行考核，項目包括「風險管理機制」、「風險管理意識宣導或教育訓練」及「風險事件通報」等，另外，每年各子公司會擬定「年度加強關注重點」項目，並且每季回報執行工作重點內容與達成率，考核結果將做為子公司年度管理成果之判斷因素。金控及各子公司風險管理人員之績效考核，則依據公司員工考核準則規定，就同仁年度之工作整體表現、目標達成情形及出勤狀況，個別評議其考核等級。

### 永豐金控風險文化塑造作為

| | |
|---|---|
| 員工績效納入風險管理績效 | • 依「子公司績效考核辦法」訂定考核指標，項目包括：「風險管理機制」、「風險管理意識宣導或教育訓練」及「風險事件之強化措施」等。 |
| 訂定主動通報機制 | • 鼓勵同仁在日常業務中發現潛在之風險事件，提出因應方案與處理對策，並主動通報單位主管。<br>• 根據「員工獎懲規則」之規定，員工如有具體建議或成效者得提報獎勵。 |
| 鼓勵內部參與及回饋 | • 資安風險方面，員工主動蒐集警調機關、TWNIC、F-ISAC、RSA 等網路資安攻擊情資，討論可行對策，持續改善風險管理機制。 |
| 產品開發流程納入風險評估 | • 規範各子公司應訂定新產品或新業務管理準則，並規範其相關風險評估、風險管理程序及控管機制、會計及作業處理程序，並經相關權責單位或董事會之核可。<br>• 透過架構審查會議評估資安管控措施，確保新系統之開發流程，符合安全軟體開發生命周期，以降低資安風險。 |
| 教育訓練與日常宣導 | • 定期舉辦稽法風聯席會議，討論法令遵循、風險管理及稽核相關議題，建構全公司風險管理文化。<br>• 金控及子公司主管及人員以及相關業務單位主管，每年需修習洗錢防制、法令遵循、誠信經營相關課程。 |

為有效提升風險管理之執行品質，且確保永豐金控及子公司全體同仁皆貫徹金控風險管理政策，金控風險管理處每年度針對各子公司之風險管理執行情形進行考核，且將內控指標與績效考核進行連結。有關永豐金控風險文化塑造情形請詳見官網。

永豐金控內控指標與績效考核連結比例

| 對象 | 比例 | 風險管理考核指標 |
|---|---|---|
| 高階管理人員 | 30% | 內控指標含稽核、法令遵循及風險管理等考核指標，比重各 10%，其中風險管理考核指標包括：<br>• 風險管理機制建立程度<br>• 風險管理教育訓練推動成果<br>• 風險事件之強化措施<br>• 風險管理政策與架構的妥適性<br>• 控管缺失、相關裁罰事件<br>• 各子公司對母公司的呈報作業的時效性與正確性<br>• 年度重點風險管理專案執行成效，包含金控風險資訊整合系統(IRIS)專案、新興風險鑑別專案、TCFD 專案 |
| 業務單位第一線主管 | 30% | |

除政策法規之依循外，教育訓練亦為提升企業內部風險管理效能之重要一環。2022年永豐金控董事會全體董事進修總時數達61小時；金控及各子公司風險管理人員及一般員工於2022年參與98場風險相關課程，內容涵蓋信用風險、市場風險、作業風險、洗錢防制法、資訊安全風險，總時數共12,134小時，提供全體員工汲取風險管理相關知識之管道，深植良好之風險管理文化。

2022 年風險相關教育訓練

| 對象 | 完訓人數(人) | 總時數(小時) | 訓練場次 | 主要訓練內容 / 課程 |
|---|---|---|---|---|
| 董事會成員 | 7 | 61 | 17 | 進修課程包含公平待客之友善金融、如何落實對高齡消費者之保護、董事決策如何避免背信與非常規交易、洗錢防制國際趨勢與金融科技之運用、員工與董事薪酬議題探討、全球科技產業及供應鏈發展趨勢、從元宇宙熱潮看資訊安全的保護、策略與危機管理、公司治理 3.0 之 ESG 揭露要求、低碳投資展望與因應商業策略、企業併購實務、電動車與智慧車的技術發展與商機、量子科技的關鍵技術與商機等。 |
| 風險管理人員 | 90 | 3,525 | 84 | 包含衍生性金融商品在職訓練、作業風險、資訊安全、洗錢防制、法令遵循等。 |
| 一般同仁 | 8,445 | 8,609 | 14 | 包含作業風險、授信風險控管實務及案例研討、高風險客戶財富與收入來源判斷、淨零排放趨勢探討等。 |
| 總計 | 8,542 | 12,195 | 115 | |

## 2.3.3 信用、市場、作業及流動性風險管理

永豐金控及各子公司皆對信用風險、市場風險、作業風險、流動性風險等四大面向分別建立完整之控管與評估機制，以有效辨識、衡量、監督及控管各類風險，同時定期彙總各子公司暴險狀況及控管並提報董事會。除嚴格遵循信用風險管理規範，永豐金控也意識到ESG趨勢對金融產業與授信業務可能產生之影響，因此積極回應國際標準，將ESG指標納入信用分析的衡量標準，以更全面的管理授信業務各種潛藏風險。

| 風險面向 | 信用風險 | 市場風險 | 作業風險 | 流動性風險 |
|---|---|---|---|---|
| 策略及流程 | 1. 建立信用風險管理政策，包括組織架構、管理準則、控管機制及風險報告制度。<br>2. 針對各風險面向訂定符合業務發展之限額管理機制，以管理及監控集中度風險。<br>3. 永豐金控於 2021 年起將氣候風險因素納入集中度風險限額控管標準，例如參考「全球氣候風險指數」訂定國家別風險分級指標。<br>4. 永豐銀行則早於 2019 年訂定「責任授信管理要點」，針對爭議性、敏感性產業 / 企業、高碳排產業 / 活動之環境保護 ( 含氣候變遷 )、社會責任、公司治理等 ESG 風險進行盡職調查暨審慎評估，並檢視是否已擬具減緩與補償措施相關行動方案，進行授信管控。 | 1. 以風險值限額控管整體市場風險。<br>2. 交易簿部位每日依市價評估，並執行停損機制。<br>3. 提升衍生性及結構型商品的評價能力與控管機制。<br>4. 在投資評估程序中，參考專業機構 (如國際金融公司、世界銀行、聯合國等相關組織) 之指導原則與標準，並運用 ESG 評分機制、ESG 相關之標竿指數成分股或其他 ESG 相關之外部資源或工具，將 ESG 考量因素納入風險評估中，強化投資前評估。 | 強化作業風險管理文化及內部控制環境，建立標準作業流程及適當控制程序，以有效減降作業風險發生。 | 1. 確保多元、穩定之資金來源，維持適當流動性，確保履行債務承諾及支付能力。<br>2. 控管指標包括流動比率、資產負債期差、資金來源及運用分析、信用額度及籌資工具分析等。 |
| 風險控管及衡量 | 金控風險管理處定期彙總各子公司資產品質分類、備抵呆帳及損失準備等資料、以及商品別、行業別、金額別、海外地區國家及前十大集團暴險狀況等資訊，並訂定同一人、同一關係人、同一關係企業、同一行業、海外地區國家別等集中度風險限額，將各項暴險狀況及限額控管情形提報董事會。 | 各子公司依商品類型分別訂定風險管理指標控管，並將 ESG 考量因素納入風險評估中，運用外部資源與工具強化投資前評估。金控風險管理處定期彙總各子公司市場風險暴險狀況及限額控管情形提報董事會。 | 各子公司對於本身所發生之作業風險事件，分析發生原因、損失情形及預防方法，並納入各項流程改善之參考。金控風險管理處則定期將作業風險事件及損失情形提報董事會。 | 各子公司訂定流動性風險指標控管。金控風險管理處則定期將子公司流動性風險狀況及限額控管情形提報董事會。 |

永豐銀行目前亦針對貸款組合進行情境分析，第二支柱要求之壓力測試情境設定係考量未來繼續經營上可能面臨之負面情境，並依程度不同區分為輕微與較嚴重之兩項壓力情境進行測試，參考國內外經濟成長率、失業率、利率水準與房價水準等經濟指標，推估對風險鏈結指標(包含營授比、十足擔保比率、當期貸放成數(CLTV)、負債比(DBR)等指標)之影響；未來將持續評估將氣候變遷、自然資源限制、人力資本風險與機會、網路安全風險等情境納入測試。相關資訊請參考3.1.3 責任授信。

# 2.3.4 新興風險管理

永豐金控訂有「新興風險管理要點」，依其建置新興風險辨識、衡量、監控、報告與減緩措施等管理機制。於2019年起，每年皆參考外部機構發佈之新興風險相關報告進行新興風險鑑別，並彙集子公司意見，辨識出金控層級新興風險及研擬風險減緩及管理措施，呈報管理階層以提早布局與因應。

新興風險鑑別流程

**Step 1**

**新興風險鑑別流程啟動**

由金控風險管理處每年參考外部機構發佈之研究報告及產業標竿企業之永續報告書，提供風險因子清單及新興風險評估表。

**Step 2**

**子公司進行新興風險辨識及衡量**

各子公司參考風險因子清單，依其發生可能性、衝擊影響程度、可能發生期間，透過質化或量化的方法進行評估，辨識營運及業務應關注之新興風險，呈送新興風險評估表予金控風險管理處。

**Step 3**

**鑑別金控層級之新興風險與減緩與管理措施**

彙整各子公司鑑別之新興風險，綜合考量發生可能性、衝擊影響程度、可能發生期間，辨識出金控層級應關注之新興風險，並研擬對應的減緩及管理措施。

**Step 4**

**對外揭露**

每年於永續報告書中揭露金控層級關注之長期可能發生的新興風險。

## 2.3.4.1 新興風險辨識結果

永豐金控彙集各子公司之新興風險，依「發生可能性」及「衝擊影響程度」辨識出金控層級關注之新興風險，其中長期以「營運導入新興科技(如生成式AI)之潛在風險」及「地緣政治衝突」等兩大風險對永豐金控影響較大，擬具相關減緩及管理措施。

| 風險因子 | 營運導入新興科技(如生成式 AI)之潛在風險 | 地緣政治衝突 |
|---|---|---|
| 可能發生期間 | 長期 | 長期 |
| 風險描述 | 生成式人工智慧(Generative AI)是通過讓機器學習模型研究大量數據，從而具備生成創造性內容的 AI 技術。近年逐漸有不同的生成式 AI 應用工具發表推出，如 ChatGPT。<br>由於產業特性，數位轉型創新一直是金融業數位的重要議題，生成式 AI 在金融業的應用場景主要聚焦於金融分析、客戶服務、行銷銷售等業務。營運流程中導入生成性 AI 可能造成以下風險：<br>• 使用生成式 AI 技術若需與外部單位合作串接，可能增加遭受駭客攻擊、個資或機敏資料外洩之風險。<br>• 生成式 AI 有可能因原始學習數據的不精確造成生成內容存在偏差，從而導致錯誤的營業決策並造成企業財務或聲譽風險。<br>• 因生成式 AI 等金融科技的快速創新，監理法規變動愈趨頻繁及嚴謹，導致金融機構違規罰款機率變高，內控及法遵的成本也隨之上升。 | 因地緣政治衝突所引發之政經風險指金融活動與業務所投資之國家或地區，可能發生政治、社會或經濟變動的風險，如個別國家的政經情勢、政府貨幣政策的改變或國與國之間的地緣政治衝突等。<br>經濟學人發布之 2023 全球大趨勢包含俄烏衝突、地緣政治衝突升溫、經濟衰退、中國經濟成長放緩等多項國際政經情勢：<br>• 俄烏衝突的演變攸關能源價格、通貨膨脹、利率、經濟成長、糧食短缺，也使地緣政治衝突升溫，中國可能會趁機對臺灣採取行動，印度與中國的緊張局勢可能會爆發。<br>• 為抑制通膨壓力，多國央行陸續升息及縮減其資產負債表規模，主要經濟體恐將陷入經濟衰退。<br>• 隨著中國人口減少、經濟逆風，中國經濟成長放緩。<br>• 這些政經事件將影響主要經濟體金融市場劇烈震盪，也壓縮企業獲利。 |
| 風險類別 | 科技風險 | 地緣政治風險 |
| 影響層面 | 自身營運風險；法令遵循風險；聲譽風險；作業風險 | 授信業務；投資；產品及商品銷售 / 客戶服務 |
| 對業務 / 營運的衝擊或影響 | 永豐金控秉持「場景經營」與「AI 與相關數位科技」兩大策略，積極投入人工智慧與新興技術研發。若未來永豐在客戶服務、金融分析等業務上導入生成式 AI 技術，潛在的衝擊如下：<br>• 在客務服務中導入生成式 AI 技術(智能客服)，讓客戶可透過與智能客服互動。若智能客服運作需與外部單位作合作串接，將導致客戶個資、公司機敏性資料成為外部駭客攻擊目標的機率提高，有可能造成資安或個資外洩事件，使永豐遭受主管機關裁罰並產生重大商譽風險或財務衝擊。<br>• 在金融分析導入生成式 AI 技術，能快速大量地進行資料蒐集及分析。若生成式 AI 的原始學習數據存在偏見或錯誤，可能會產出偏差的分析結果，導致錯誤的商業決策，對永豐營運或財務造成衝擊。<br>• 永豐在營運中導入生成式 AI 等新興科技，為符合愈趨嚴謹的金融科技監理法規，或主管機構對 AI 技術的指引政策，內控及法遵的成本也將隨之提高。 | 永豐金控主要子公司為永豐銀行、永豐金證券，營業比重分別占 77.74%、20.07%，若金控及各子公司投融資之國家或地區發生政治或經濟變動，將使金融資產價格下跌、授信業務客戶違約風險提高影響子公司獲利，衝擊金控整體營收。<br>• 永豐銀行：地緣政治衝突可能造成原物料供應鏈受阻、物價上升等負面總經情勢，導致投融資與製造成本高升，壓縮企業客戶獲利空間，使投融資業務客戶還款能力減弱、違約機率提高，最終導致銀行預期損失上升。此外，若中國發生地緣政治衝突，由於本行對中國曝險占淨值 49%，一旦中國經濟成長放緩，將衝擊銀行獲利。<br>• 永豐金證券：國際政經情勢衝若突升溫將使得股債市受到衝擊，本公司依壓力測試結果：<br>若臺股加權指數下跌或海內外金融市場場動盪可能造成經紀及融資客戶違約率上升及自營業務產生台外幣金融資產損失，若採用嚴重情境模擬，預估損失約新臺幣 14 億元。 |
| 減緩及管理措施 | • 導入新興資安防護科技，提升資訊安全防護機制及個資保護管理強度。定期進行社交工程資安演練及個資侵害事故之緊急應變計畫演練等。<br>• 若使用生成式 AI 技術時需與外部單位合作串接，將規劃傳輸個資去識別化之流程，並持續優化系統資料傳輸架構安全性、檢視輸出回應內容的正確性等，確保資訊安全及個人資料保護。<br>• 導入生成式 AI 技術於營運應用時，將設計檢視原始學習數據是否準確之流程，並審慎評估應用情境及系統架構。<br>• 持續關注應用新興金融科技之風險及相關監理法規之變動，並規劃於員工教育訓練中加以宣導，加強相關意識，減低永豐營運、法遵及聲譽等風險。 | • 密切關注國際政經情勢及金融市場變化，當發生重大變化時檢視市場現況並因應變化調整資產組合。<br>• 考量產業未來發展及國家政經發展情勢，訂定同一行業授信及投資限額、海外地區國家別限額，定期監控限額管理情形。<br>• 強化貸後監控與管理機制，主動關注受景氣影響之高風險客戶營運狀況，必要時增提擔保或到期收回等方式降低風險。<br>• 每日監控金控整體暨各子公司損益及市場風險值 (VaR) 之使用概況，嚴格執行部位之預警、超限或停損之風險管理處置措施。<br>• 依經濟情勢演變，模擬各種預測情境進行壓力測試，並依壓力測試結果，擬定相關因應措施。 |

### 2.3.4.2 營運韌性

因應新冠肺炎疫情(Covid-19)於2020年初所引發的全球大流行疫情，永豐金控自2020年即妥善擬定「營運不中斷計畫」，透過分組辦公、異地備援、居家上班等備援機制，確保提供客戶穩定且優質的服務。2021年進一步訂定「模擬疫情情境之因應管控機制」及「疫情通報與控管流程」，攜手全體同仁做好疫情防護，保障同仁及客戶的健康安全。2022年配合政府「正常生活、積極防疫、穩健開放」的步調，永豐金控在兼顧防疫安控與業務推動下，逐步放寬防疫管制，讓業務活動回到常軌，同時加速數位轉型發展。

新冠肺炎疫情對永豐金控的影響評估與風險管理

| | |
|---|---|
| 對營運的影響 | 因應 2022 年國內疫情反覆，永豐金控除了適時啟動居家上班及異地備援外，同時也訂定金控職場接觸者應變措施，以降低疫情的衝擊。永豐銀行推出「iBranch 金豐便平台」全流程數位化分行服務，打造疫情期間的新臨櫃旅程。此外，所有分支機構營運未受影響服務不中斷。 |
| 對財務的影響 | 本公司及各子公司於 2020 年 2 月中旬疫情擴大之際即已針對信用、市場、流動性等風險採取相關因應措施、並隨疫情演變適時調整。<br>**信用風險**：針對 2022 疫情發展狀況整體經濟環境對本集團授信資產品質之影響，金控各子公司持續關注列為預警、紓困、異常及逾催案件及各子公司逾期放款及提存等資產品質概況，風管處並定期整合資產品質資訊於金控主管會議報告。<br>就中國結構性政策風險及台海情勢之影響方面，金控及各子公司已針對中國四個風險面向，研擬之因應對策與強化措施，並呈金控會議報告。<br>**市場風險**：因應新冠肺炎疫情的不確定性及全球經濟局勢變化，市場波動率劇烈，易影響財務數字平穩性，執行投資時密切注意市場變化，並適時避險。分散海外投資之幣別、國家別及產業別、平衡固定利率及浮動利率債券部位比重、並視市場狀況動態管理存續期間。<br>**流動性風險**：金控風險管理處每日監控銀行子公司資金進出狀況，與到期日缺口等流動性指標，維持充足之營運資金，同時定期檢視各子公司營運資金概況及資金緊急應變措施之有效性，以確保各子公司營運正常。 |
| 對供應鏈的影響 | 永豐金控在地採購占比達 97%，且各項採購項目皆備有可替代的供應商，以確保供應不中斷；本公司並未發生供應鏈供貨不足之情形，日常營運所需未受影響。 |

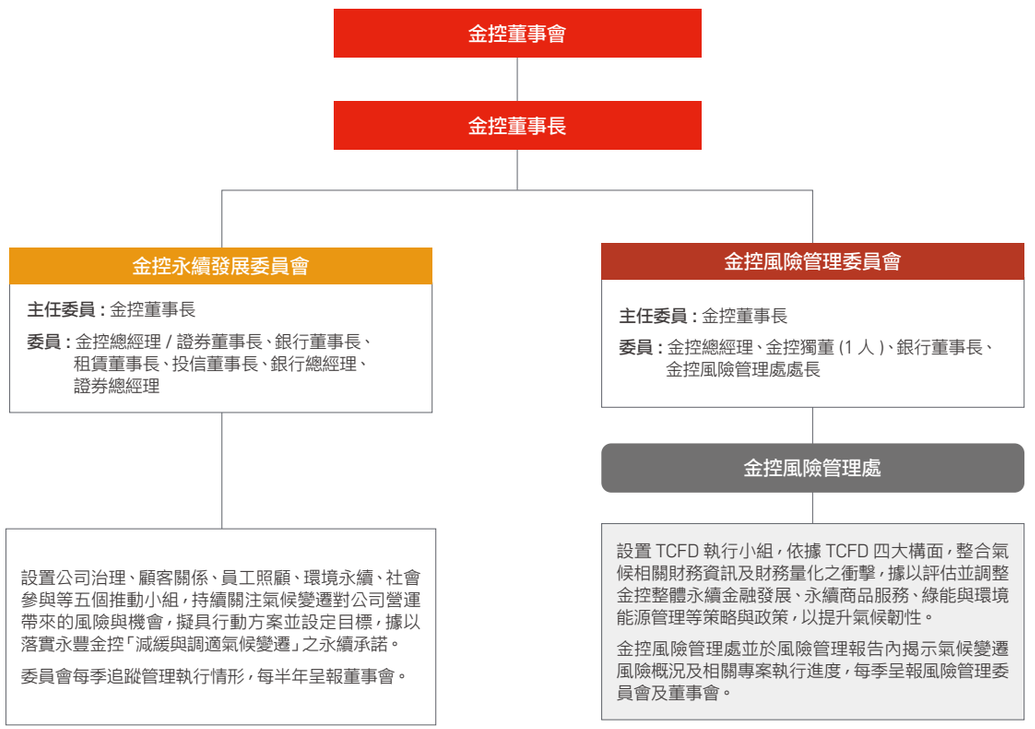
## 2.3.5 氣候變遷風險管理

永豐金控持續透過評估氣候變遷風險，制定相對的因應措施，鑑別氣候風險帶來的潛在危機與可能機會，同時依循氣候相關財務揭露建議書(Recommendations of the Task Force on Climate-related Financial Disclosures；TCFD)四大構面：治理(Governance)、策略(Strategy)、風險管理(Risk Management)、指標與目標(Metrics and Targets)揭露氣候相關資訊。永豐金控於2021年正式成為TCFD支持者(TCFD Supporter)，期望持續擴大金融業之影響力，為綠色金融產業的發展持續注入動能，並於2022年進一步發布「TCFD報告書」，增進氣候變遷相關資訊揭露的透明度與完整性，以回應國內外政策規範、評比機構等利害關係人對於氣候變遷風險與機會的關注。以下僅就TCFD建議揭露的四大構面進行重點摘要說明，詳細內容請參見「TCFD報告書 🔗」。

### 2.3.5.1 氣候治理

永豐金控董事會為氣候變遷相關議題最高治理單位，對氣候相關議題負最終監督與管理責任，董事長下則設有「永續發展委員會」及「風險管理委員會」，督導管理永續經營及氣候變遷相關重要議題。

永豐金控氣候治理架構



永續發展委員會由董事長擔任主任委員，金控總經理及主要子公司董事長、總經理擔任委員，管理氣候變遷風險與機會相關行動方案及目標之執行情形，以落實永豐金控「減緩與調適氣候變遷」之永續承諾；執行情形每半年呈報董事會。風險管理委員會亦由董事長擔任主任委員，金控獨立董事(1人)、總經理及銀行董事長等擔任委員，管理氣候變遷相關之風險，以強化氣候韌性。永豐金控將「氣候變遷風險」納入「風險管理政策」，並建立「氣候相關風險與機會管理要點」，以健全氣候風險與機會的管理機制。2021年起，永豐金控風險管理處每季於風險管理報告內揭示氣候變遷風險(包含實體風險、轉型風險各項指標)概況，並呈報風險管理委員會及董事會。風險管理委員會下設置「TCFD執行小組」，以風險管理處為統籌單位，擬訂氣候風險管理準則、建立氣候風險管理機制，每季討論進度、檢視KPI執行狀況，並呈報風險管理委員會與董事會。TCFD執行小組依循TCFD四大構面：治理、策略、風險管理、指標與目標揭露並管理氣候資訊。

為實踐永續策略及推動進程，永豐金控已將永續發展納入2022~2024年金控四大策略之一，並將其列為總經理和高階主管的長期及短期績效目標內，以進一步與變動獎酬連結，相關目標說明請參閱2.1.4高階薪酬政策說明。

## 2.3.5.2 氣候策略

為建立整合性的風險管理架構，永豐金控將「氣候變遷風險」納入「風險管理政策」，並制定「氣候相關風險與機會管理要點」，以評估集團自身業務之氣候相關風險與機會，衡量相關風險與機會對財務、業務規劃及策略之影響，並且擬定因應氣候變遷所採取之減緩及調適行動。針對氣候風險與機會之鑑別，永豐金控採取之管理流程可分為：彙整氣候風險及機會清單、辨識子公司層級之風險/機會、鑑別金控層級之風險/機會並提出減緩或調適措施、以及對外揭露及溝通等四步驟。

2022年度永豐金控共鑑別出3項重大氣候變遷相關風險，詳見下表：

| 風險類別 | 轉型風險 - 政策和法規 | 轉型風險 - 政策和法規 | 實體風險 - 立即性 |
|---|---|---|---|
| 風險事件 | 碳價與碳稅 / 排放、減碳目標與報告義務之政策或節能耗電政策或法規趨嚴，可能導致授信及投資對象營運獲利減少、影響公司債權或收益。 | 政府推行的低碳政策，使得大量高碳排產業 ( 如：化石燃料產業 ) 之設備將受人為加速折舊而在使用周期中提前沖銷，價值下跌而形成「擱淺資產」(Stranded Asset)。 | 颱風、強降雨等極端氣候引起的異常事件，造成營運處所或設備損害、營運中斷或人員傷亡。 |
| 潛在財務衝擊 | 債權損失增加 投資收益減少 | 債權損失增加 投資收益減少 | 營運成本增加 |
| 可能發生期間 ( 註 ) | 中期 | 長期 | 中期 |
| 減緩與調適措施 | 1. 「顧客關係」小組負責規劃永續金融商品的發展藍圖、推動責任投資、持續深化並落實責任授信。<br>2. 呼應國際趨勢與國家宣示 2050 淨零目標，永豐金控董事會在 2022 年 3 月 15 日正式通過我們企業的淨零目標，承諾在 2030 年以前達到自身營運淨零排放，在 2050 年以前達成全資產組合的淨零排放，並且成立跨子公司、跨部門的淨零專案小組 (Project Management Office; PMO) 擬定短中長期工作目標。<br>3. 金控訂定「責任投資管理要點」作為推動與執行責任投資之指導方針。<br>4. 金控風險管理處統籌「TCFD 情境模擬財務衝擊量化分析」及成立 TCFD 執行小組，依財務量化之衝擊，評估並調整金控整體永續金融發展、永續商品服務、綠能與環境能源管理等現行策略與政策，提升氣候韌性。 | 1. 呼應國際趨勢與國家宣示 2050 淨零目標，永豐金控董事會在 2022 年 3 月 15 日正式通過企業的淨零目標，承諾在 2030 年以前達到自身營運淨零排放，在 2050 年以前達成全資產組合的淨零排放，並且成立跨子公司、跨部門的淨零專案小組 (Project Management Office; PMO) 擬定短中長期工作目標。<br>2. 金控風險管理處統籌「TCFD 情境模擬財務衝擊量化分析」及成立 TCFD 執行小組，依財務量化之衝擊，評估並調整金控整體永續金融發展、永續商品服務、綠能與環境能源管理等現行策略與政策，提升氣候韌性。 | 1. 本公司訂定「天然災害緊急應變作業要點」劃分權責及建立緊急通報程序，把握關鍵時機迅速採取積極有效應變行動，以防止損害擴大、消弭災害危機，儘快恢復正常營運。<br>2. 達停班標準即依主管機關規定停止上班、以保障員工生命財產安全；颱風警報發佈前均通知各單位檢查門戶、疏通排水、備妥防災設備，建立緊急事件通報名冊，做好事前防範及事後處理措施，以儘速恢復正常營運。<br>3. 行舍地點優先考量排水系統建置完整之都會區，並以屋齡短、設備建材新穎、耐震係數高且非低窪地區之建築物為主，使發生災害時之影響減至最低。<br>4. 投保天然災害險，以因應極端氣候產生之風險。<br>5. 各單位平時擬妥任務編組，及緊急聯絡電話以備緊急狀況之需。 |

註：短期 -2023 年底以內可能會發生、中期 -2024~2025 年 ( 含 ) 可能會發生、長期 -2025 年 ( 不含 ) 後可能會發生。

2022年度永豐金控亦鑑別出3項重大氣候變遷相關機會，詳見下表：

| 機會類別 | 機會事件 | 潛在機會影響 | 可能發生期間 ( 註 ) |
|---|---|---|---|
| 產品與服務 | 配合政府政策與法規，對再生能源或綠色產業擴大投、融資及創新發展永續金融商品及服務，擴大商機。 | 收入增加 | 中期 |
| 市場 | 增加發行、投資綠色債券或參與綠能相關產業承銷案件，有利於進入新市場、爭取循環經濟新商機。 | 收入增加 | 短期 |
| 產品與服務 | 推廣都市更新或改造綠建築專案，取得投融資商機。 | 收入增加 | 中期 |

註：短期 -2023 年底以內可能會發生、中期 -2024~2025 年 ( 含 ) 可能會發生、長期 -2025 年 ( 不含 ) 後可能會發生。

此外，永豐金控分別針對整體價值鏈不同部位的氣候變遷風險建立情境分析模型，並執行財務衝擊的量化計算，採用之方法學與情境簡述如下：

| 風險類別 | 風險因子 | 採用情境 | 分析標的 | 分析結果(註三) |
|---|---|---|---|---|
| 實體風險 | 強降雨淹水 | • RCP 8.5 | 供應商營運所在地、自身營運所在地、自有不動產、授信擔保品及投融資客戶工廠所在地 | 於本情境下，合計各分析標的之預期損失，對金控資本適足率之潛在影響程度落在低度。 |
| | 乾旱 | • RCP 2.6<br>• RCP 8.5 | 供應商營運所在地、自身營運所在地及投融資客戶工廠所在地 | 於各時間點之所有情境下，合計各分析標的之預期損失，對金控資本適足率之潛在影響程度皆落在低度。 |
| | 海平面上升 | • RCP 2.6<br>• RCP 4.5<br>• RCP 8.5 | 供應商營運所在地、自身營運所在地、自有不動產、授信擔保品及投融資客戶工廠所在地 | 於各時間點之所有情境下，合計各分析標的之預期損失，對金控資本適足率之潛在影響程度皆落在低度。 |
| 轉型風險 | 碳成本繳納 | • 國際組織綠色金融體系網絡(NGFS)：<br>1. Below 2 度 C(註一)。<br>2. Net Zero 2050/ 1.5 度 C(註二)。<br>• 國際能源總署(IEA)：<br>1. 永續發展情境 (SDS)，約當 Below 2 度 C(註一)。<br>2. 2050 年淨零排放情境 (NZE)，約當 Net Zero 2050/ 1.5 度 C(註二)。 | 供應商 | 評估供應商預期碳成本轉嫁金額，於各情境在各時間點，對金控資本適足率下降之潛在影響程度皆為低度。 |
| | | | 屬「高碳排產業」與「環保署列管高碳排企業」之投融資部位 | 評估屬分析標的之投融資部位，合計信用風險與市場風險之整體增額預期損失，於各情境在各時間點，對金控資本適足率下降之潛在影響程度皆為低度。 |
| | 經濟部「一定契約容量以上之電力用戶應設置再生能源發電設備管理辦法」 | 國家自主貢獻 (NDC) | 屬「用電大戶」之投融資部位 | 評估屬分析標的之投融資部位，合計信用風險與市場風險之整體增額預期損失，於各情境在各時間點，對金控資本適足率下降之潛在影響程度皆為低度。 |
| | 2030 年自身營運淨零排放目標 | 2030 年以前達到自身營運淨零排放。 | 自身營運 | 評估永豐金控為達成淨零排放目標增加之減碳成本，於各時間點，對金控資本適足率下降之潛在影響程度皆為低度。 |

註一：相當於 SBT 目標途徑：每年線性減排 2.5%。

註二：相當於 SBT 目標途徑：每年線性減排 4.2%。

註三：影響程度低度代表預期損失推估對金控資本適足率下降影響小於 1%，約為 17 億新臺幣以下。

## 2.3.5.3 氣候風險管理

永豐金控將「氣候變遷風險」納入「風險管理政策」，並建立「氣候相關風險與機會管理要點」，以健全氣候風險與機會的管理機制。同時，各子公司已逐步將氣候風險整合至各項業務中，在投融資業務中分別訂定「責任投資管理要點」與「責任授信管理要點」進行管控。同時，另訂有「天然災害緊急應變作業要點」及「供應商企業社會責任行為準則」等規範，以審慎管理所面對之信用、市場及作業風險。

永豐金控透過內部控制三道防線架構，劃分各防線之氣候風險管理職責與管理機制，說明如下：

**第一道防線：於辦理相關業務時，應評估氣候風險，將氣候相關風險納入業務考量**

辦理各項業務與營運活動時，將氣候風險納入業務考量，辨識氣候風險與其他風險之關聯性，如信用風險、市場風險、作業風險及流動性風險等，控管日常營運之業務，採取適當辨識、評估與管理程序，以確保風險在初期就能被適當控管。依據所辨識或評估之氣候風險高低或風險次序，對於氣候風險高之業務或交易採行差異化風險管理措施。

**第二道防線：有效監控第一道防線對於氣候風險管理之執行，並應確保相關作業均遵守法令規範**

- 訂定整體政策及建立管理制度，協助各相關單位落實氣候變遷風險管理及監督第一道防線管理風險執行情形。
- 追蹤新增修法令予相關單位檢視，以確認各項作業及管理規章均配合主管機關所公布之氣候風險相關法規進行適時更新。
- 執行實體風險與轉型風險之情境分析以評估氣候風險對其業務之影響及韌性，並每季於風險管理報告中揭示，呈報風險管理委員會及董事會。

**第三道防線：應評估第一道及第二道防線進行氣候風險監控之有效性，並適時提出改進建議**

應評估第一道及第二道防線進行氣候風險監控之有效性，並適時提出改進建議。

## 2.3.5.4 氣候指標與目標

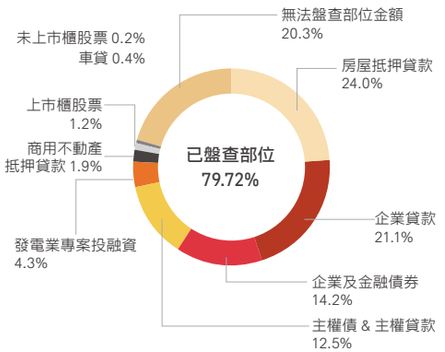
面對氣候相關風險與機會帶來的挑戰，永豐金控承諾將於2030年達成自身營運淨零排放，2050年達成全資產組合淨零排放。永豐金控自2018年起每年進行組織型溫室氣體盤查(請詳5.1.2.1溫室氣體管理)，更透過設定SBT、逐步提高綠電使用比率、擴大替代能源融資、綠債發行等計畫推動目標，並將逐步透過投融資業務策略調整(例如：撤資高碳排產業融資、支持清潔能源與新創技術、協助客戶減碳與低碳轉型節能等方案)擴大涵蓋層面，進一步發掘氣候相關機會，以推動整體價值鏈之低碳轉型。相關規劃皆已具體納入永豐金控永續發展短中長期重點工作中(請詳專章3-布局淨零排放、以及1.1.3三大永續承諾及永續發展目標-減緩與調適氣候變遷)。

永豐金控共訂有氣候治理、氣候機會、綠色採購、綠色營運、資本配置、內部碳定價、氣候風險管理、氣候議合、溫室氣體排放、能源使用等面向之氣候指標，並設短中長期目標，詳細內容請參本公司2022年「TCFD報告書」；未來將每季透過永續發展委員會檢視及追蹤各項指標及目標之達成情況，並滾動式修正，持續強化本公司氣候韌性並掌握業務機會。

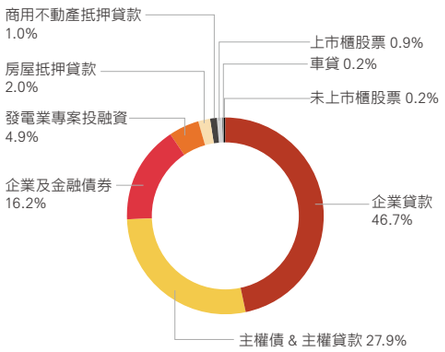
## 2.3.5.5 範疇三投融資碳盤查

永豐金控依循「碳會計金融合作夥伴關係(PCAF)」所發布之《金融業全球溫室氣體盤查和報告準則》(Financed Emissions: The Global GHG Accounting and Reporting Standard)之方法學針對2022年12月30日之投融資部位進行碳盤查，盤查範疇涵蓋房屋抵押貸款、企業貸款、企業及金融債券、主權債與主權貸款、發電業專案投融資、商用不動產抵押貸款、上市櫃股票、車貸以及未上市櫃股票等資產類別，整體覆蓋率為79.72%(已盤查部位金額占整體投融資部位金額)。永豐金控之投融資部位之碳排放(Financed Emissions)為544萬公噸二氧化碳當量($tCO_2e$)，整體碳足跡(Carbon Footprint)為3.4公噸二氧化碳當量($tCO_2e$/每新臺幣佰萬元投融資金額)。關於各資產類別與投融資各產業別碳盤查結果請詳見2022年「TCFD報告書」。

範疇三投融資碳盤查覆蓋率




財務碳排放占比 ( 公噸 $tCO_2e$)




財務碳排放盤查結果 - 各資產類別

基準日:2022 年 12 月 30 日

| 資產類別 | 投融資金額 (新臺幣佰萬元) | 財務碳排放 (公噸 $tCO_2e$) | 碳足跡 (公噸 $tCO_2e$/ 每新臺幣佰萬元投融資金額) | 資料品質分數 (1: 最佳 5: 最差) |
|---|---|---|---|---|
| 企業貸款 | 422,102 | 2,540,853 | 6.0 | 3.6 |
| 主權債 & 主權貸款 | 250,131 | 1,519,507 | 6.1 | 2.0 |
| 企業及金融債券 | 285,201 | 882,963 | 3.1 | 2.3 |
| 發電業專案投融資 | 86,212 | 265,119 | 3.1 | 3.0 |
| 房屋抵押貸款 | 480,402 | 109,187 | 0.2 | 4.0 |
| 商用不動產抵押貸款 | 37,586 | 55,590 | 1.5 | 4.0 |
| 上市櫃股票 | 23,056 | 47,864 | 2.1 | 1.1 |
| 車貸 | 6,964 | 8,468 | 1.2 | 3.4 |
| 未上市櫃股票 | 4,610 | 8,559 | 1.9 | 3.0 |
| 總計 | 1,596,263 | 5,438,111 | 3.4 | 3.2 |

## 2.3.6 人權風險鑑別與管理

永豐金控於訂有「人權政策」，將政策適用範疇擴大至合作夥伴、上游供應商、下游客戶，並增加客戶審查政策，避免供應商與客戶對其員工進行強迫勞動、雇用童工、人口販運、與違反工作權之情事。另外2022年增訂「待遇平等」並將「歧視」議題修訂為「歧視與多元包容」，以因應國際人權趨勢發展，發揮企業影響力。

| 員工 | 客戶 | 供應商 |
|---|---|---|
| 永豐金控自 2018 年啟動人權盡職調查機制，結合「性騷擾防治措施、申訴及懲戒要點」，設立專用溝通管道(如專線電話、信箱等)，致力於建立多元、平等、包容的職場友善環境。 | 永豐金控重視客戶的聲音，制定「公平待客原則政策及策略」，以公平待客十大原則為基礎，建立以公平待客為核心的商品思維，與客戶共同創造社會價值。 | 永豐金控制定「供應商企業社會責任行為準則」，並與重要供應商簽署「供應商企業社會責任承諾書」，期許供應商採用一致原則，落實人權保障。 |

### 2.3.6.1 人權風險盡職調查流程


永豐金控自2019年起定期進行重大人權議題鑑別，檢視自身營運及價值鏈(含供應商、客戶)相關活動，蒐集主要利害關係人對人權風險的意見。2022年度透過問卷，進一步鑑別價值鏈中包含不同性別員工、供應商以及客戶產業屬性相關之人權議題，請利害關係人就「嚴重程度」與「發生頻率」兩面向以1~10等級評估相關人權風險，共計調查回收221份有效問卷，鑑別出永豐金控價值鏈上、中、下游的重大人權議題並評估潛在風險族群，提出對應之人權風險減緩措施。

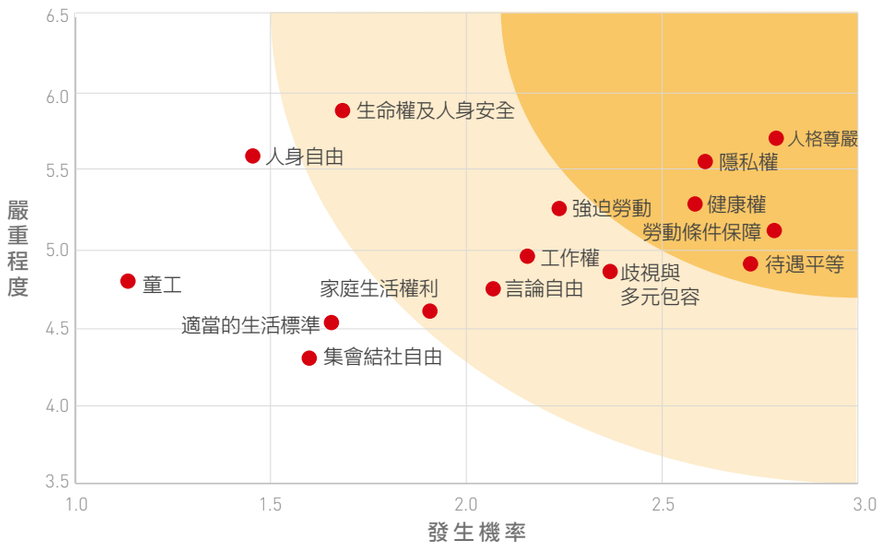
人權風險鑑別的範疇及對象

| 鑑別對象 | 人權風險清單 | | | 鑑別涵蓋群體 |
|---|---|---|---|---|
| 供應商 | 強迫勞動 | 工作權 | 健康權 | • 員工<br>• 女性<br>• 兒童<br>• 原住民<br>• 移工<br>• 第三方聘僱勞工<br>• 當地社區 |
| 客戶 | 童工 | 人身自由 | 生命權及人身安全 | |
| 員工（自身營運） | 集會結社自由 | 適當的生活標準 | 待遇平等 | |
| | 勞動條件保障 | 家庭生活權利 | 言論自由 | |
| | 歧視與多元包容 | 隱私權 | 人格尊嚴 | |

## 2.3.6.2 人權風險鑑別結果

透過利害關係人問卷調查，永豐金控於2022年初步鑑別出具重大衝擊人權議題分別為「人格尊嚴」、「隱私權」、「勞動條件保障」、「待遇平等」和「健康權」，檢視臺灣各產業環境違反人權相關法規案件統計（以勞動條件保障、工作權、歧視與多元包容、強迫勞動與人格尊嚴為常見案例），並交叉比對永豐金控自身營運期間曾發生勞動條件保障與強迫勞動之人權事件與相關申訴，顯示與初步鑑別的重大人權議題為相同類型。價值鏈上中下游所關注的重大人權則如下表所示，其中「女性」族群之鑑別結果與整體鑑別結果則無重大差異。此外，永豐金控於人權事件發生時依法實施補救措施或相關作業，相關申訴案亦循申訴處理機制辦理，詳情請參閱4.4.3.3職場平權與友善反歧視。

永豐金控重大人權風險議題矩陣




永豐金控 2022 年價值鏈風險鑑別結果

## 2.3.6.3 價值鏈風險識別結果及減緩措施

永豐金控依盡職調查分析結果檢視減緩措施推動之合適性，並整合協調人權風險適用範疇、追蹤風險發生之情形，如遇有發生相關重大人權事件，後續依相關措施規範或運作準則研擬補救措施。永豐金控人權政策及減緩與補救措施均適用於金控及各子公司共214個營運據點，員工端設有人事評議委員會，如發生違反人權事件之情事，將列入委員會討論事項，檢視相關規範適法性、並研擬相關措施，降低未來發生率。供應商透過定期供應商大會及供應商企業社會責任承諾書簽署率，要求供應商不得發生違反人權事件之情事；業務面於投資/授信評估時檢視是否符合人權要素，如遇有相關情事將列入未來合作評估項目之一。

### 員工及客戶重大人權議題與減緩措施一覽表（供應商風險辨識及減緩措施說明請詳5.2.1永續供應鏈管理）

| 主要影響之利害關係人 | 重大人權風險議題 | 議題風險說明 | 風險辨識比例（註） | 減緩措施涵蓋比例 | 減緩措施說明 |
|---|---|---|---|---|---|
| 員工 | 人格尊嚴 | 永豐金控發生損害人格尊嚴情事，例如職場霸凌、騷擾等。 | 20.0 % | 100.0 % | • 訂定「永豐金控防治申訴及調查處理要點」，定期舉辦「職場不法侵害與職場性騷擾防治」教育訓練課程，提升主管及員工性別平權之觀念，如遇有性侵害或性騷擾之情形時，採取立即且有效之糾正及補救措施。<br>• 訂定「職工獎懲辦法」，職場暴力或霸凌設有積極處理機制。<br>• 設置性騷擾申訴專責單位、申訴專線與專用電子信箱，提供員工即時的幫助(如 EAP 服務、護理諮詢)。 |
| | 隱私權 | 永豐金控未妥善管理商業訊息、客戶和員工的個人資訊，以致發生資料被盜取、外洩或濫用等情事，同時相關資訊無法依其意見刪除或調整，例如未經過客戶許可洩漏客戶資料予第三者。 | 21.6 % | | • 訂定「員工服務準則」，凡屬公司核心資訊及擁有之智慧財產權，員工皆有保守秘密、妥善保管運用及適當維護之義務。<br>• 實施「資訊安全宣導教育訓練」課程，提升員工資訊安全知識。<br>• 隱私權相關減緩措施請詳「2.5 隱私安全」。 |
| | 勞動條件保障 | 永豐金控所提供的勞動條件無法妥善保障員工基礎經濟條件、生活、健康與安全，例如敘薪過低無法支持生活、輪班休息時間過近、連續上班時數過高、工作環境危害過高等。 | 0.01 % | | • 「員工出勤管理準則」及「員工薪資暨各項津貼等發給準則」，載明薪資管理相關管理方針，依員工實際加班狀況給予加班費及補休假。<br>• 提供員工每日上下班及出勤管理提醒通知，並定期統計員工加班情形。 |
| | 待遇平等 | 永豐金控提供之薪酬與人力資源運用政策受國籍、種族、性別、性向、年齡、宗教、政治傾向、身心障礙等因素而發生不公平之情形，或以與工作表現無關之指標作為薪資給付的標準。例如擔任相同工作職務者，卻因性傾向而領取較低薪資等。 | 0.3 % | | • 於人權政策中增訂「維護待遇公平」條文，並提供適當的申訴機制，減緩與回應危害員工權益之情事。<br>• 年度考核設有申覆機制，永豐銀行員工如對結果有異議，得提出績效考核申覆，由人資單位彙整提報審查。 |

註：風險辨識比例 = 鑑別出具風險之員工人數 / 當年度正職員工總人數。

| 主要影響之利害關係人 | 重大人權風險議題 | 議題風險說明 | 風險辨識比例（註） | 減緩措施涵蓋比例 | 減緩措施說明 |
|---|---|---|---|---|---|
| 客戶 | 健康權 | 永豐金控客戶的工作場所中發生對人體健康的危害，使人員需透過治療才得以完全或部分恢復健康，例如工傷、職業病、意外受傷等。 | 5.3% | 100.0 % | 制定「責任授信管理要點」，將 ESG 要素納入徵審系統之『徵信風險訊息揭露檢核項目』，並進行 ESG 風險評估檢核與要素審查，深入了解客戶的情況，協助改善並評估擬具減緩及補償措施。(請詳 3.1.2 責任投資、3.1.3 責任授信) |
| | 生命權及人身安全 | 永豐金控客戶的員工於工作場所內或於執行業務的過程中，發生人身安全或其生命受到立即威脅的情形。例如公司未提供安全防護設施導致工人從高處墜落死亡或觸電身亡等。 | 5.3% | | |
| | 勞動條件保障 | 永豐金控客戶所提供的勞動條件無法妥善保障員工基礎經濟條件、生活、健康與安全，例如敘薪過低無法支持生活、輪班休息時間過近、連續上班時數過高、工作環境危害過高等。 | 5.3% | | |
| | 強迫勞動 | 永豐金控客戶發生以任何懲罰之威脅，迫使非自願提供的工作或服務，手段例如欺騙、孤立 、恐嚇及威脅、扣留身分文件、扣發薪資、抵債勞務、苛刻的工作及生活條件、超時加班與少報工時等。 | 5.3% | | |

註：風險辨識比例以鑑別問卷調查回應推估，節錄調查結果呈現高風險之產業占整體調查對象之比例。

### 違反人權事件與改善措施

2022年永豐金控發生4件人權風險相關之事件，針對相關事件說明及改善措施請詳見「2.2.4重大違反項目及改善措施」及「4.4.3.3職場平權與友善反歧視」。永豐金控皆已啟動員工教育訓練，並透過各種管道與員工溝通並規劃未來改善方案。詳細內容請參閱2022年永豐金控年報第133頁。

### 人權議題教育訓練成果

| 課程 | 人數(人) | 時數(小時) |
|---|---|---|
| 資訊安全認知宣導 | 9,129 | 23,762 |
| 職場不法侵害預防與性騷擾防治 | 5,841 | 4,848 |
| (專案)性別平等與職場不法侵害實務 | 27 | 108 |

# 2.4 資訊與網路安全

## 2.4.1 資訊與網路安全治理架構

永豐金控具備完整之資訊與網路安全治理架構，董事會為監督集團資訊安全相關策略最高權責單位，並由具資訊安全相關背景之葉奇鑫董事負責監督集團之資安相關策略，於總經理下設置「資訊安全委員會」，作為管理資訊安全之最高單位，另有「資訊安全處」及「資訊處」，綜整金控及子公司相關之資安相關的政策、技術，與資源之整合。為因應《金融控股公司及銀行業內部控制及稽核制度實施辦法》，永豐金控及永豐銀行於2022年由董事會通過增設資訊安全長，由副總經理層級擔任；永豐金證券亦於2021年12月由董事會通過設立資訊安全長。

**永豐銀行及永豐金證券均將年度資訊安全整體執行情形納入內部控制制度聲明書，並由該公司董事長、總經理、總稽核、資訊安全長、總機構法令遵循主管聯名出具內部控制制度聲明書。**

永豐金控之資訊與網路安全治理架構與權責分工

| | |
|---|---|
| 董事會 | 監督集團之資安相關策略。 |
| 總經理 | 其下設置資訊安全委員會。 |
| 資訊安全委員會 | 審議資訊安全政策及辦法、檢視資訊安全管理制度、提升資訊安全意識及研議相關教育訓練計劃、以及評估及議定資訊安全之相關基礎設施。 |
| 資訊安全長 | 為因應《金融控股公司及銀行業內部控制及稽核制度實施辦法》，於 2022 年 1 月由董事會通過增設資訊安全長，由李相臣副總經理擔任。 |
| 資訊安全處 | 隸屬於金控，下設資安治理組以及資安技術組，負責資安發展策略及政策及資安技術之選用及資源整合。 |
| 資訊處 | 隸屬於金控，下設資訊管理組及系統管理組，負責整體金控之軟硬體投資與資訊架構規劃。 |
| 資訊安全專責單位 | 子公司銀行、證券子公司依循金控「資訊安全政策」成立資訊安全專責單位，並持續更新 ISO 27001 資訊安全管理系統證照，並定期將資安以善盡對客戶或投資人的個人資料保密職責。 |

負責監督資訊與網路相關策略之董事與高階主管

| | | 姓名與職稱 | 專業資安背景 |
|---|---|---|---|
| 治理階層 | 董事會 | 葉奇鑫董事 | 曾任 eBay 臺灣交易安全長、中華龍網(資訊安全) 總經理、臺灣板橋地方法院檢察署檢察官(智慧財產權及電腦犯罪專組)。 |
| 管理階層 | 資訊安全長、資訊安全委員會召集人兼資訊安全處處長 | 李相臣副總經理 | 曾任富邦金控資安長與資訊長、內政部警政署刑事警察局科技犯罪防制中心主任、警政署資訊室主任。 |

# 2.4.2 資訊與網路安全管理

## 2.4.2.1 資安管理落實

永豐金控訂定「資訊安全政策」，確保金控及各子公司資訊處理符合資訊安全相關規定，且每年均檢視資訊安全政策及資訊安全事件應變流程是否符合營運環境及主管機關之規範要求、對資訊安全重大議題進行評估；永豐金控、永豐銀行及永豐金證券定期以電子郵件方式公告內部資訊安全政策予所有員工，並定期進行教育訓練，以提升員工對資訊安全之認知。永豐金控也於「供應商企業社會責任行為準則」中訂定商業道德資訊隱私之規範，要求供應商應合理保護業務往來的業務資訊及個人資料，以確保公司及個人隱私不被洩漏而受到損害。

為加強永豐金控內部的資訊安全防護能力，集團內部依不同頻率進行資安風險及其脆弱度的評估，了解系統及內部控制中潛在的資安相關威脅。永豐金控及子公司於2022年並無發生因意外事件對資訊系統或設備造成損害的罰鍰及財務損失。

永豐金控已建立跨公司之「電腦資安事變應變小組」，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。另藉由外部專業資安顧問，以其業界豐富之資安事件應變經驗，即時提供內部應變團隊適切且專業的建議與緊急應變支援。此外，永豐金控亦持續精進進階持續性威脅(APT)防護系統、防禦DDoS攻擊、電子郵件內容過濾、惡意軟體偵測、網站及APP弱點掃描及安全檢測等項目；同時針對高風險系統(如ATM、SWIFT系統)進行架構隔離及系統防護強化。永豐銀行及永豐金證券資訊相關單位所提供之系統管理、資料庫管理、網路管理、資訊安全管理和相關基礎設施維運活動皆取得ISO27001之認證。永豐銀行配合主管機關推動「金融資安行動方案」，於2022年完成「資訊安全治理成熟度評估」，導入國際標準「ISO 22301:2019營運持續管理系統」，已於2023年取得外部驗證證書，另「BS 10012 PIMS個人資訊管理系統」預計2023年7月取得外部驗證證書。詳細的資安風險政策及相關評估、通報流程，請見永豐金控官網。

### 永豐金控2022年資安管理系統精進作為

| | |
|---|---|
| 永豐金控 | • 定期召開資訊安全交流會議，著重資安相關規定與事件，優化資安事件應變與分析。<br>• 制定「電腦資安事件應變小組設置細則」，降低事件損害，達到金控整體資源整合及相互支援之運作。 |
| 永豐銀行 | • 制定「資訊暨資安營運持續準則」和「資訊暨資安營運持續細則」，加強營運持續管理之運轉機制，降低資訊作業風險及保障客戶權益，共同確保資訊系統及服務之可用性。<br>• 修訂「資訊安全細則」，修正系統開發與維護管理作業須知、自動化設備管理作業須知、電子金融業務安全控管作業須知、防毒軟體管理作業須知、流程自動化機器人運行須知等，確認資訊安全與網路安全管理制度之落實。 |
| 永豐金證券 | • 修訂「資訊安全政策」，完善教育訓練及宣導之作業事宜。<br>• 修訂「資訊作業管理要點」，進行資訊系統分級管理。<br>• 修訂「行動應用程式 (APP) 管理要點」，增訂程式原始碼之安全規範。<br>• 修訂「物聯網設備安全管理要點」，明確各相關權責單位與職掌。 |

### 永豐金控資安管理落實作為

| 項目 | 頻率 | 主要內容 |
|---|---|---|
| 檢核資安檢核報表檢核 | 每日 | 透過檢核資安報表發掘潛在資安事件，降低威脅與影響。 |
| 召開資安戰情中心月會 | 每月 | 檢視端點主機、特權帳號、使用者行為以及威脅獵捕等監控點措施，並進行分析與討論。 |
| | | 檢視資安戰情中心月會決議事項，以及資安監控點等措施執行狀況進行研議。 |
| 審查弱掃報告 | 每季 | 審查網頁及主機弱點掃描報告及追蹤弱點修補執行進度，並持續追蹤弱點修補，強化資安能量。 |
| 審查滲透測試報告 | 每半年 | 針對網頁及 SWIFT 執行滲透測試，並追蹤修補弱點執行進度，強化資安能量。 |

## 2.4.2.2 資安風險議題趨勢

鑒於全球不斷發生資安威脅與攻擊，除持續評估公司內部可能遭遇之資訊安全風險，永豐金控也高度關注並監控金融新興科技衍生之資安議題，每月召開資訊安全交流會議，檢視金控資訊安全防護機制及計畫，也召開資訊安全戰情中心月會，分析是否遭受已公開的重大資訊安全威脅事件攻擊。

截至目前，永豐金控所觀察到之新興資安風險和趨勢多與近年來風行的行動支付、網路銀行相關的網路威脅有關，包括利用社交工程技巧將惡意程式碼注入以控制重要資產設備竊取資料之網路社交工程攻擊、利用應用程式漏洞竊取使用者身分資料和登入憑證之行動裝置應用服務威脅、以及網路銀行帳號的攻擊與密碼盜竊等。

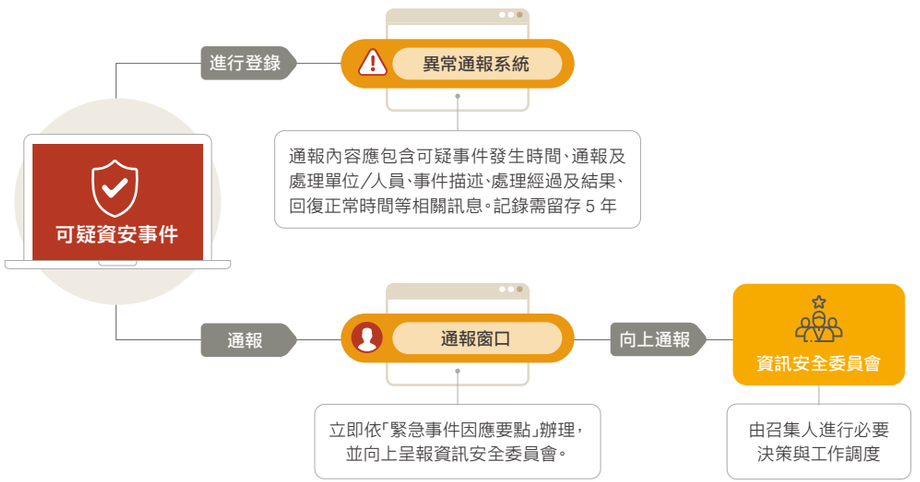
### 資安相關趨勢

| 資安趨勢類別 | 可能發生頻率 | 可能造成的資安威脅 |
|---|---|---|
| 網路社交工程攻擊 | 每年至少 5 次相關事件 | 利用社交工程技巧將惡意程式碼注入，造成駭客有機會控制重要資訊資產設備。 |
| 勒索軟體攻擊 | 每年至少 5 次相關事件 | 近年勒索軟體事件頻出，駭客透過系統漏洞或釣魚郵件進行部署並將企業組織中高價值電腦檔案進行加密，並要求交付贖金以獲得金鑰進行解密，若否駭客會將機密資料公布上網。 |
| 分散式阻斷服務攻擊 | 每年至少 3 次相關事件 | 駭客利用多台被控制的電腦，製造大量網路流量，其目的為消耗對方之系統資源，使其系統癱瘓，最後無法提供服務，造成營運中斷。 |
| 供應鏈攻擊 | 每年至少 3 次相關事件 | 近期駭客利用第三方服務軟體找尋攻擊路徑(如漏洞或版本更新)間接入侵目標組織內部系統，一旦入侵成功便得以橫向移動至其他單位，造成其他單位之損失，擴大組織受到的威脅。 |

### 2.4.2.3 資安管理流程及系統

根據永豐金控「資訊安全政策」，各單位如發生資訊安全事件，應立即依「緊急事件因應要點」辦理。資訊安全處應評估影響範圍、擬定應評估影響範圍、擬定因應計畫，並通報資訊安全委員會召集人進行必要決策與工作調度。此外，永豐金控及其子公司每年執行營運持續計畫(BCP)與緊急事件應變程序之測試，以完善營運持續管理計畫。另永豐銀行已取得ISO 22301:2019營運持續管理系統之外部驗證。

資安事件通報處理流程圖




## 2.4.3 專業培訓及教育訓練

為強化內部之資訊安全思維，永豐金控每年針對全體同仁實施資安線上教育訓練，課程內容包括資安基本概念、資訊安全相關趨勢說明、社交工程手法介紹、內部規範宣導、資訊安全意識培養等，並已將資訊安全之遵循程度納入員工績效評估項目。

2022 年永豐金控員工資安教育訓練執行情形

| 子公司 | 對象 | 教育訓練成果 |
|---|---|---|
| 永豐銀行 | 資安專責人員 | 依規範完成 15 小時以上資訊安全專業課程訓練或職能訓練，並取得 22 張專業證照及 51 張上課證明。 |
| | 一般人員 | 總機構、國內外營業單位、資訊單位、財務保管單位及其他管理單位之人員，依規範完成 3 小時以上資訊安全宣導教育訓練，課後並進行社交工程演練，社交工程演練通過比例 97.54%，對於未通過社交工程演練同仁，則加強相關教育訓練並以考試通過驗證。 |
| 永豐金證券 | 資安專責人員 | 依證券商內部控制制度標準規範完成 15 小時以上之資訊安全專業課程訓練或職能訓練並通過評量，並取得 9 張專業證照及 9 張上課證明。 |
| | 一般人員 | 依證券商內部控制制度標準規範，對其他使用資訊系統之從業人員完成 3 小時以上資訊安全宣導教育訓練，社交工程演練通過比例 99.05%，對於未通過社交工程演練同仁，則加強相關教育訓練並以考試通過驗證。 |

永豐金控 2022 年資安專案及執行成果

- **資安成熟度評估**：資安規範係奠基於可共通遵循之防護基準，為持續精進資安管理，與符合金融管理委員會推動對金融機構之期望，參照 F-ISAC 標準執行資安治理成熟度評估專案，藉由比較資通安全的風險與成熟度等級，找出資通安全弱點，持續調和風險與強化內控之程序。
- **營運持續管理 (BCM)**：配合主管機關推動「金融資安行動方案」工作，執行六項評估活動及教育訓練，包括營運持續管理系統差異分析、制定營運衝擊分析報告、制定營運持續計畫與提供營運持續演練情境、執行自行查核並覆核改善建議，及陪同外部驗證單位查核與提供查核結果改善建議。
- **成大永豐產學合作案 - 金融資安攻防模擬平台**：透過建置實境演練的模式下培養更多資安人才，同時提升企業資安防護量能。
- **資安設備日誌收容分析**：為確保永豐銀行資訊安全偵測可收容及保存資安設備事件日誌，透過客製儀表板分析及統計攻擊事件，深入剖析即時資安威脅，降低資安風險。
- **紅隊演練專案**：為強化資安演練廣度與深度，提升資安人員處理資安事件應變能力，永豐銀行及永豐金證券透過紅隊演練模擬駭客真實從外部侵入，以利掃描、滲透及評估檢驗內部資安防護能力。

# 2.5 隱私安全

## 2.5.1 隱私安全治理架構

永豐金控設置個人資料保護管理執行小組，作為隱私安全保護之最高單位，由副總經理層級之主管擔任召集人，督導及負責隱私安全保護推動及治理、風險監督及管理、提升隱私安全意識及研議相關教育訓練計劃等事項，而永豐金控子公司包含銀行、證券、證券(歐洲)、投信等均設置資料保護長(DPO)，並由專責單位負責客戶資料保護相關工作。永豐金控個人資料保護管理執行小組每6個月至少召開一次會議，討論永豐金控及子公司的隱私安全保護實務與個人資料保護管理措施，且永豐銀行及永豐金證券每年針對資訊安全風險管理系統(含客戶個資與隱私安全保護)進行外部查核與認證。

永豐金控個人資料以整合性企業風險管理框架與三道防線進行風險管理，從風險辨識、衡量、回應、監控與報告，實施全面性風險管理，建立相關風險指標、風險監控點與預警機制，並依風險屬性訂定限額控管，採行質化及量化併行方式定期評量各項風險，積極監控與管理，並定期向個人資料保護管理執行小組、審計委員會及董事會呈報個資管理情形。永豐金控三道防線相關作法請詳見2.3.1風險管理架構。

| | 權責單位 | 權責 |
|---|---|---|
| 第一道防線 | 風險承攬單位 ( 業務單位 ) | 確保業務行為符合法令及內部各項規定 |
| 第二道防線 | 風險管理單位 ( 如風險管理處、法令遵循處、資訊安全處等等 ) | 獨立風險管理及監控 |
| 第三道防線 | 稽核單位 | 建立稽核準則及獨立執行稽核查核 |

## 2.5.2 隱私安全管理

為防範營運對客戶、員工隱私權的危害，永豐金控及子公司每年辦理一次個資保護自行評估以鑑別潛在的隱私風險，將個資法令所列之重要控管事項納入自評項目，包括維護個人資料之正確性、個資盤點、風險評鑑、認知宣導及教育訓練、資料安全管理、個資外洩演練、保密義務及個資查詢覆核、外規完整內化、查核缺失改善、個人資料紀錄保存、委外作業等控管事項，2022年永豐銀行發現3項缺失(包括個人資料外洩事件處理程序；資料安全管理、人員管理及個資查詢覆核；外規完整內化、資料安全稽核機制)均已改善。此外永豐金控及子公司於2022年辦理9場隱私安全相關之教育訓練，參與人次共計8,607人。

| 個資保護措施 | 說明 |
|---|---|
| 個資盤點 | 每年辦理一次盤點查核，以確認所保有之個人資料現況，界定其納入本辦法之範圍。 |
| 風險評鑑 | 界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之風險，並根據風險評估之結果，檢討或調整本公司涉及個人資料之管理機制。 |
| 外洩演練 | 如有提供電子商務服務，其系統所採行「防止外部網路入侵對策」及「非法或異常使用行為之監控與因應機制」等資訊安全措施，應每年辦理一次演練及檢討改善。 |
| 個資自我評估 | 為持續改善個人資料安全維護，各單位應每年提出一次自我評估報告，針對評估報告中有違反法令之虞者，規劃、執行改善及預防措施，授權總經理核定，並定期提報董事會備查。 |

### 2.5.2.1 隱私政策

為保障客戶個人資料安全與隱私，永豐金控於2022年修訂「隱私權保護聲明」，適用範圍涵蓋永豐金控整體營運，並規範供應商共同遵守，承諾將隱私權視為永豐金控風險之一，落實風險管理與評估，強化客戶資料隱私的權益與保障；並訂有「客戶資料保密措施」，公告客戶個人資訊之蒐集、範圍與使用方式，資料安全及保存方法等；且訂定「個人資料保護政策暨檔案安全維護辦法」，落實個資使用之各項規範。永豐金控所訂定之「供應商企業社會責任行為準則」中亦規範第三方供應商應合理保護業務往來的業務資訊及個人資料，以確保公司及個人隱私不被洩漏而受到損害。永豐銀行於2022年4月受SGS推薦取得BS 10012:2017 個人資訊管理系統認證，預計於2023年6月取得該證書。

「隱私權保護聲明」摘要

| | |
|---|---|
| 適用範疇 | 隱私權聲明適用於永豐金控整體營運範疇，包含本集團暨所屬各子公司、並呼籲供應商與商業夥伴共同遵守。本公司亦規範供應商應遵守本公司隱私權保護聲明，以確保本集團公司及個人隱私不被洩漏而受到損害。 |
| 負責人員與部門 | 本集團組織上應設置個人資料保護管理執行小組，執行小組召集人由總經理指定高階主管一人擔任 |
| 風險管理機制 | 本集團將隱私權納入集團之風險管理流程中，並將相關機制列入內部控制及稽核項目 |
| 處分機制 | 違反隱私權保護規定之職員將依據相關規定處分，若客戶之個人資料外洩，本集團將立即依本公司「緊急事件因應要點」辦理，並通知相關當事人。 |
| 查核機制 | 本集團將依據金融控股公司及銀行業內部控制及稽核制度實施辦法，委託會計師依主管機關規定辦理個人資料保護與防制洗錢及打擊資恐機制專案查核。 |

永豐金控所有與客戶個資蒐集之相關行為皆依據「金融控股公司法」、「金融控股公司子公司間共同行銷管理辦法」、「個人資料保護法」及其他相關法令規定辦理，並於官網公告之「客戶個資保密措施」中善盡告知客戶個資蒐集相關事項之義務。告知項目如下：

永豐金控告知客戶個資相關事項

| | |
|---|---|
| 個資蒐集方式 | 個資利用目的 |
| 個資儲存及保管方法 | 個資揭露對象<br>(含第三方揭露政策) |
| 個資安全及保護方法 | 個資變更修改方式 |
| 利用範圍(包含基本資料、帳務資料、信用資料、投資資料、保險資料) | 共同行銷選擇退出方式告知<br>(Opt-out) |

2022 年個人資訊作為次要目的使用(註)的戶數與比例

| | |
|---|---|
| 個人資訊作為次要目的使用(註)的戶數 | 3,161,725 個 |
| 個人資訊作為次要目的使用(註)的比例 | 62.31% |

註：於原先收集資料目的以外的個人資料使用。例如：使用於商品行銷推廣。

個人資料作為次要目的使用的步驟

**選擇加入(Opt-In)**
- 客戶得選擇是否同意提供姓名或地址以外之其他資料作為行銷建檔、揭露、轉介或交互運用之欄位。
- 經客戶以簽名或其他得以辨識客戶同一性及其意思表示之方式確認，僅在有客戶同意下才會蒐集使用其資料。

>>

**資料變更或修改**
- 可至往來子公司之營業據點申請變更。
- 除法令另有規定外，亦可透過永豐金控之各子公司客服中心申請變更。

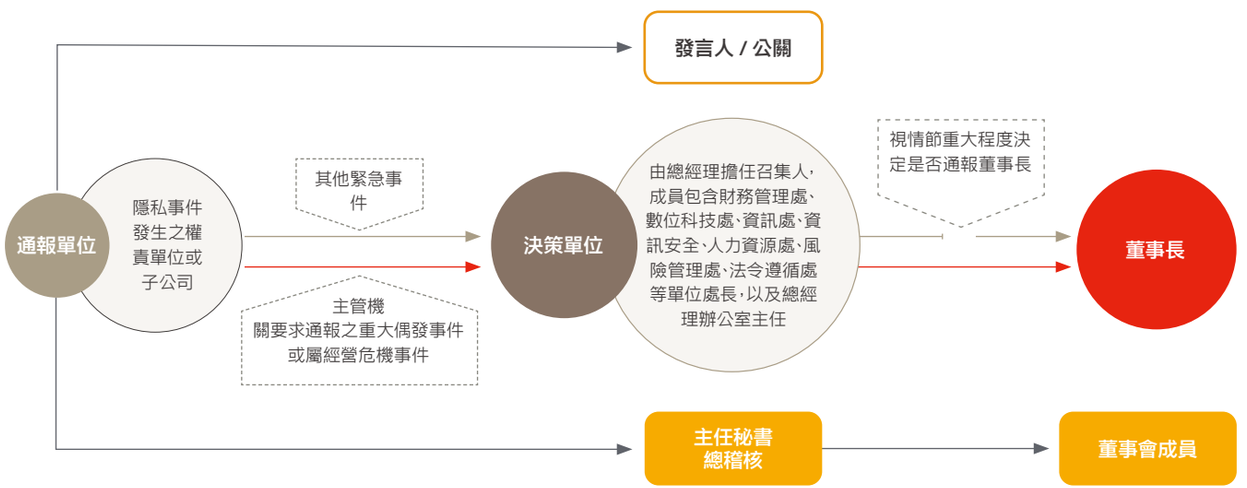
>>

**選擇退出(Opt-out)**
- 客戶得以書面、電子郵件或致電客服中心等方式通知永豐金控之子公司，要求停止共同行銷交互運用客戶資料。
- 永豐金控之子公司將依據客戶通知意旨，儘速於合理工作日內停止客戶資料交互運用於共同行銷活動。

## 2.5.2.2 隱私事件通報流程

根據永豐金控「個人資料保護政策暨檔案安全維護辦法」，若出現疑似客戶隱私外洩、客戶個人資訊遭駭客攻擊或其他隱私相關事件，相關之部門主管應立即依永豐金控「緊急事件因應要點」辦理，通報個人資料保護管理執行小組之召集人及執行秘書，並於2天內完成回報應變措施與處理方式(包括載明控制當事人損害之方式、查明事件後通知當事人之方式、查明事件後通知當事人之內容等)。永豐金控及其子公司之「員工獎懲規則」亦規範如同仁洩露客戶資料穩私，造成其權益受損益者，由單位主管將懲處名單提交人力資源部門，按分層負責管理辦法核決權限表呈請權責主管核定。

永豐金控隱私安全事件通報機制




## 2.5.3 隱私外洩情事

永豐金控及子公司於2022年未有遭到外部及其他監管機關投訴之情事，未有經證實與侵犯客戶隱私權或遺失客戶資料之事件發生，也未有涉及個人可識別資訊(PII)外洩之情形。永豐金控將持續強化各相關保護機制，以落實客戶隱私保護之責任。

個資申訴管道

| | 客服專線 | 線上客服 / 客服信箱 |
|---|---|---|
| 永豐金控 | (02) 8761-2285 | privacy@sinopac.com |
| 永豐銀行 | 0203-08989<br>(02) 2505-9999 | https://bank.sinopac.com/GCSDsp/DspOnLineService.aspx |
| 永豐金證券 | 0800-038-123<br>(02) 6630-8899 | https://www.sinotrade.com.tw/CSCenter/CSCenter_13_6 |
| 永豐投信 | (02) 2312-5066 | http://sitc.sinopac.com/newweb/contact/page.do |
| 永豐金租賃 | (02) 8161-2395 | service.spl@sinopac.com |
| 永豐創投 | (02) 2393-3315 #333 | - |