

# 風險管理政策、組織架構與運作情形

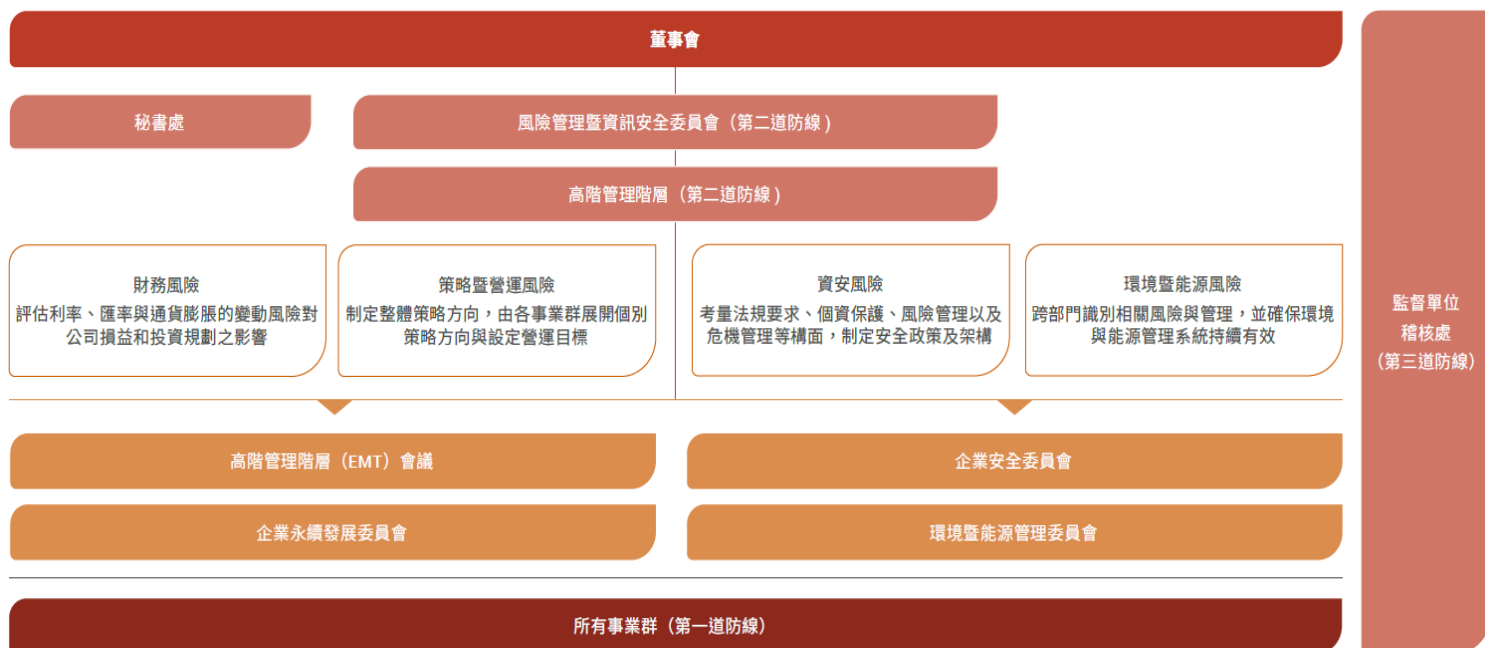
## 風險管理政策與範疇

為落實企業風險管理，遠傳參考國際標準「ISO 31000 風險管理系統原則及指導綱要」，並依循 P-D-C-A 模式制定「風險管理政策」，經 107 年 11 月 5 日董事會核准通過，作為所有事業群之指導原則。政策內容涵蓋管理目標、組織架構與權責、風險管理程序等機制，以有效辨識、衡量、監督與控制各項風險，並將風險控制在可接受的範圍內。遠傳並於 112 年 2 月 15 日董事會依台灣證交所公告「上市上櫃公司風險管理實務守則」持續檢視與優化風險管理機制的運作。「風險管理委員會」自 107 年設立，為董事層級之功能性委員會，成員由董事會決議委任，且半數以上為獨立董事。為強調對資訊安全之管理，於 113 年 5 月 3 日董事會核定通過調整為「風險管理暨資訊安全委員會」，以持續展現遠傳對資訊安全與客戶隱私保護的關注與重視。

遠傳以「財務風險」、「策略暨營運風險」、「資訊安全風險」、「環境暨能源風險」落實風險管理範疇，並建立多層次風險管理架構，包含所有事業群、高階管理階層、風險管理暨資訊安全委員會、董事會與稽核處，以兼具風險管控、監督、及風險回應的彈性，於快速變遷的經營環境掌控風險，達成企業策略目標。

## 組織架構與職責

所有事業群為遠傳風險管理的第一道防線，負責所屬單位日常風險之辨識評估、管理與報告，並採取必要之因應對策。高階管理階層及風險管理暨資訊安全委員會為第二道防線，負責審查、訂定風險管理政策，擬訂風險胃納或容忍度，及監督審查重大風險管理情形。稽核處為第三道防線，負責獨立審查風險管理機制運作的遵循性及有效性。



組織	職責
董事會 最高決策單位	核定風險管理政策與架構。 確保營運策略方向與風險管理政策一致。 監督整體風險管理機制之有效運作。
稽核處 監督單位 (第三道防線)	執行稽核。 提報稽核結果予董事會。
風險管理暨資訊安全委員會 (第二道防線)	審查風險管理政策與架構、風險胃納或容忍度。 審查重大風險議題之管理報告。 審查資訊安全與隱私保護策略、重點計畫及管理成效。 定期向董事會報告風險管理運作情形。
高階管理階層 (第二道防線)	擬訂風險管理政策與架構、訂定風險胃納、容忍度及目標。 執行董事會及委員會決策。 統籌資源有效配置、監督管理公司整體風險。 核定風險控管的優先順序與風險等級。 建立風險管理文化。
秘書處 風險管理推動與執行單位	協助委員會議事運作。 協助政策規範之擬定、推動與宣導訓練。 定期檢視公司風險類別、統籌風險評鑑結果及提報核可。 協助監督各部門風險管理活動之執行及跨部門協調溝通。 定期彙整提報公司風險管理執行情形。
所有事業群 (第一道防線)	負責所屬單位日常風險之辨識評估、管理與報告，並採取必要之因應對策。 監控各項風險狀況，確保控制程序有效執行，即時傳遞呈報風險資訊，以符合相關法規及公司政策。 負責相關規範之推動與宣導。

董事會為風險管理最高決策單位，負責核定公司風險管理政策與架構並督導機制之有效運作。風險管理暨資訊安全委員會審查風險胃納、風險容忍度及重大風險議題管理報告，並每年至少一次向董事會報告風險管理運作情形。

## 風險管理程序

遠傳風險管理程序主要參考國際標準「ISO 31000 風險管理系統原則及指導綱要」及P-D-C-A 架構訂定，包含風險辨識、分析、處理、監督與審查。



此外，遠傳針對不同風險類別訂定風險胃納，並定期檢視，提報高階管理階層及風險管理暨資訊安全委員會，經核可後，供所有事業群作為風險評估及因應處理之依循。

▶ 遠傳四大類別風險胃納說明如下：

#### 1. 財務風險

遠傳對財務曝險或損失持審慎的態度。我們期望在謹慎的財務政策、充足的業務投資和多方利害關係者的利益之間取得適當的平衡，在實現策略目標的過程中追求最佳報酬。

#### 2. 策略暨營運風險

遠傳願意接受創新技術解決方案的合理風險，以滿足快速變化的商業環境中的客戶需求。同時，遠傳承諾遵守相關法律及提供客戶高品質的服務。我們實施嚴格的政策，竭盡所能地降低營運持續的風險，以維持市場競爭力和優良的高譽。

#### 3. 資安與隱私風險

遠傳對未經授權存取系統和機敏資訊採取零容忍態度。我們實施強力的管理面與技術面管控措施以降低風險，確保資通訊基礎設施與客戶資料的安全。

#### 4. 環境暨能源風險

遠傳努力將環境危害和能源供應不足的風險降至最低。我們應用創新技術，落實環境永續發展，以完整備援規劃及多元再生能源提升設施韌性，致力降低業務營運的風險。

## 2023 風險管理運作情形及董事會報告

所有事業群每年定期依重大性原則，考量經濟、環境及社會面等公司治理議題，對客戶、投資人及其他利害關係人可能產生的重大影響進行辨識風險，並依營運衝擊與可能性進行風險評估。每年至少執行兩次以上風險辨識及評估作業，包含由資安辦公室(秘書處) 啟動之評鑑作業，及符合各項國際標準要求之定期風險評鑑。各單位應依風險胃納、風險評鑑結果及其優先次序，擬定風險管理計畫及採取必要因應對策。

此外，各部門於日常營運中須不斷觀察或衡量曝險狀況，並定期（如：每週或每月）提交監測報告。若發現重大曝險狀況並威脅到財務、業務狀況或法律合規性，應立即採取適當措施並向相關主管和緊急應變小組報告。權責單位應根據監測審核結果和發生的風險事件進行檢討及改善，以持續確保風險治理的有效性。對於重大風險議題，除定期於高階管理階層報告風險狀況、強化管控計畫外，亦提報至風險管理委員會進行審查。2023 年風險管理委員會已分別於 2 月 14 日及 8 月 8 日共召開 2 次會議，並於 11 月 3 日董事會報告風險管理監督之情形。

2023 年秘書處已召開 3 次會議，統籌所有事業群執行風險辨識及評鑑結果、呈報高階主管階層核定，並擇定高風險議題至高階管理會議、風險管理委員會進行審查，內容包含主要威脅分析、風險因應對策及執行情形，議題包含如下：

風險議題	衝擊分析	因應策略
網路攻擊風險	因應後疫情的遠距辦公趨勢、地緣政治衝突及全球網路攻擊增長 98%，威脅可能性增加。2023 網路攻擊情況持續嚴峻，遠傳監控與分析發現，遠端存取趨勢、5G 與客戶端應用的普及(ex.APP 等)，將造成網路流量增加及 DDoS 攻擊、服務中斷風險。	遠傳持續嚴密監控新型攻擊型態並進行全員社交工程宣導與訓練，2023 持續強化偵測、優化縱深防禦 Defense-In-Depth (DID) 機制、及定期舉辦跨單位聯防演練。以期能更快速因應、即時通報、控制與復原作業，提升企業服務韌性。
系統障礙風險	依威脅情資中心 FortiGuard Labs《2023 下半年全球資安威脅報告》分析，新漏洞被利用速度較上半年增加 43%。老舊系統可能因效能不足與存在無法修補弱點情形，導致服務風險及系統障礙可能性提高，為提供客戶更迅速、優質與安全的系統服務體驗，遠傳持續檢視與優化流程與汰換系統。	遠傳秉持零錯誤的精神為企業宗旨，定期檢視障礙事件並針對根因進行檢討，採取下列措施： <ul style="list-style-type: none"> <li>強化系統服務監測</li> <li>提升系統服務穩定</li> <li>持續服務復原演練</li> </ul> 透過優化監控、演練強化跨團隊間的通報、應變、控制與復原，以降低對公司的營運衝擊。
氣候變遷風險	隨著氣候變遷議題的加劇，全球對於減碳管理的要求和強度逐步提升，可能對遠傳的營運型態和成本造成重大衝擊。國家再生能源政策導致電價上漲或電力供應不穩定，可能造成遠傳營運成本增加以及能源結構改變。此外，碳費實施和政策變化也將直接衝擊公司的成本效益。	遠傳依循 SBT 設定科學減量目標，中期 2030 年以相較於基準年 2021 年減碳 42% 為目標，積極以落實節能、增設綠能因應。有關財務衝擊和因應。

## 新興風險

遠傳因應國內外情勢，持續關注辨識環境面、社會面、治理面的新興風險，評估對營運的衝擊、並擬定策略處理措施以降低對企業的衝擊。年度辨識新興風險與因應措施如下：

關鍵新興風險	風險領域	潛在衝擊	分析調適減緩措施
地緣政治風險	地緣政治面	<p>依據牛津經濟研究院 2023 年 8 月 2 日發布的《全球風險季度調查結果》，針對 100 多家國際企業調查顯示，國際企業界對全球經濟主要威脅的看法發生顯著轉變，包括台海、南北韓等地緣政治緊張局勢，被認為是未來五年的首要風險，一旦地緣政治緊張局勢的加劇，可能會引發第三大風險的「去全球化風險」。遠傳為關鍵基礎設施提供者，包含基站、行動通信網路、機房等重要設施，面對不穩定的地緣衝突問題，評估可能衝擊與影響如下：基礎設施攻擊和網路安全威脅：地緣政治緊張局勢可能危及行動通訊網路正常運作；例如近年來，透過科技觸發的國家層級網路攻擊可能性持續存在，對關鍵基礎設施威脅更顯著增加，此情境將可能導致電信通訊服務中斷，造成企業或個人通訊聯繫中斷的風險。</p> <p>供應鏈中斷：行動通訊所需之網通設備，面對全球地緣政治緊張局勢，若某些地區的供應鏈中斷，將可能導致公司提供的通訊基礎設施關鍵元件或設備供應鏈無法得到及時供應，造成通信服務的中斷或降級的風險。</p>	<p>備援、備份和復原計畫：制定有效的備援備份機制和復原計畫、建立異地備援方案、增加設備元件備用存量、加強定期演練，以確保關鍵業務的營運持續與在緊急情況下快速應變、恢復服務正常運作。</p> <p>多元化供應鏈：建立多元化的供應鏈來源，減少對特定地區或供應商的依賴性。</p>
能源短缺	環境面	<p>能源短缺對於遠傳營運風險主要電力供給與水資源兩方面（電力及水資源費用佔遠傳營業費用約 10% 左右），可能衝擊包含：</p> <p>供電不穩定或缺水：可能造成通信服務中斷或品質下降情況，產生客戶相關賠償等問題。</p> <p>營運成本增加：由於政府能源轉型需求，高成本再生能源佔比持續增加，以及國際石化燃料價格持續上漲、再生能源因天候或災害造成供應不穩定，或政府能源轉型失敗造成能源短缺等因素影響，未來需支付更高的電費（推估後續三到五年可能上漲幅度達 20%~30%），或因能源短缺需增加備援之營運成本。</p> <p>影響服務品質和滿意度：基站和設備運作不正常，將造成通話品質不佳、網絡速度減慢或不穩定等，影響客戶的使用體驗和滿意度，導致企業形象受損。</p>	<p>遠傳定期評估能源使用狀況，制定綜合的長期能源策略、設定能源管理目標，採取多面向因應管控因應對策，包含：</p> <p>減碳目標設定：遠傳已通過 SBT 科學減量目標，目標為 2030 年將範疇 1+2、3 溫室氣體排放量控制在較 2021 年降低 42%。</p> <p>技術創新與數位轉型：優化能源管理控制系統、導入高效能轉換電力設備、汰換老舊設備等提升能源使用效率，降低能源成本和溫室氣體排放。</p> <p>備援電力系統及儲水設備的容量和擴充：定期進行備援容量評估、建立緊急支援供應商與週期性汰換老舊緊急備援設備，確保未來能源使用需求。</p> <p>導入儲能系統：加強對能源儲存技術的應用，有效利用間歇性能源，在能源短缺時提供臨時的能源支援，提供穩定的能源供應。</p> <p>布局多元化能源：建立多樣化的能源供應結構，減少對單一能源短缺的風險。</p>

## 敏感度分析和壓力測試

遠傳針對財務風險及非財務類風險，包含營運風險、資訊安全風險、環境暨能源等不同類型的風險進行敏感性分析或壓力測試。權責單位負責識別和分析潛在的威脅和弱點，每年並針對不同風險定期進行敏感度分析或壓力測試，實施控制措施，並持續監控和改進，以確保風險管理的有效性。

### 財務類風險

遠傳財務單位每年定期進行財務風險識別，針對評估結果對公司 EPS 的影響，進而進行避險及財務風險管理策略之調整，以確保公司之曝險尚在可控範圍內。

### 非財務類風險

在環境暨能源風險方面，遠傳依氣候相關財務披露工作組 (TCFD) 的建議，全面盤點分析氣候變遷可能影響、潛在的能源風險等。遠傳每半年都會針對主發電機房進行防災演習，包括模擬颶風洪水和和其他自然災害。並模擬颶風等可能造成停電缺電情形，對主要機房緊急發電機進行負載壓力測試 (無載測試每月兩次 / 有載測試每半年一次)，並與外部供油廠商簽訂合約與演練。

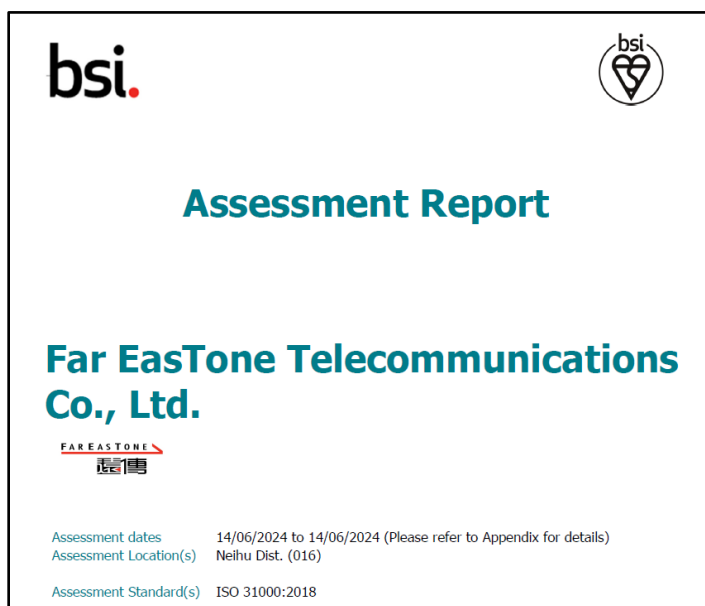
在資訊安全及隱私風險方面，遠傳每年定期進行風險鑑別、分析評估，並制訂營運持續計畫(BCP, Business Continuity Plan)，由各權責單位模擬天災、網路攻擊等情境，每年規畫多次網路服務、核心資通系統等營運持續演練測試，並持續檢討改善，以確保關鍵服務營運持續不中斷。

## 監督與管理

遠傳關注內、外部風險並持續檢視精進風險管理運作機制。除於各風險層面導入國際驗證，包含ISO 27001 資訊安全管理、BS 10012 個資隱私管理、ISO 20000 系統服務管理、ISO 50001 能源管理、ISO 14001 環境管理、ISO 14064-1 溫室氣體盤查等，每年定期由權責單位啟動各領域風險辨識、分析評估、風險處理及矯正預防。此外，更透過外部第三方國際驗證機構進行ISO 31000 風險管理查核，對遠傳整體的風險管理運作進行全面完整性及有效性檢視、提供建議，以持續精進與優化。

內部亦由稽核處擔任監督單位，定期於稽核計畫中檢視企業內風險運作情形，並將結果提報董事會。2023 年稽核處已針對遠傳企業風險管理機制進行稽核。透過所有事業群、高階管理階層、風險管理委員會及董事會、稽核處等多重防線的機制設計與運作，兼具風險管控、監督、及風險回應的彈性，確保及時掌控風險、迅速因應並實質管理，達成企業策略目標。

[ISO 31000:2018 第三方查核報告]



## 風險文化與意識宣導

遠傳所有董事每年皆透過外部訓練課程與座談，持續關注與了解整體最新風險、可能機會與挑戰，詳官網/董事進修情形。

此外，風險管理有賴於全體員工共同把關，為塑造風險意識文化，遠傳定期透過教育訓練課程、宣導訊息、內部網站等途徑對全體員工傳達風險管理目標、政策、風險管理程序及處理原則，以持續強化風險意識。2023年已辦理「防範內線交易」、「誠信經營與從業規範」、「職業安全訓練:職場健康與安全」、「防範社交工程攻擊」及「生成式AI的安全使用宣導」等全員訓練課程，期以內化及提昇全體同仁對風險的辨識、通報及管理意識。

於各單位的作業中，遠傳亦要求須建立必要的風險控管機制。例如對產品與服務系統的開發，秉持Security by Design 的概念，於系統開發生命週期各階段中納入資安管控措施，並要求於上線前須依標準進行必要的安全測試，以強化提供客戶整體服務的安全性及韌性，確保服務品質。

而在人員的激勵上，遠傳所有員工每年依人員職務及年度目標訂定對應績效KPI，在工作上的風險管理和敏捷因應亦是評估指標之一，結合公司績效考核制度，對於有優良表現的員工予以表彰及獎勵，如核發績效獎金、特殊獎勵金，以鼓勵及塑造全體同仁的管理責任與風險意識。包括但不限如下：

- 門市與客服風險管理獎勵：針對客戶服務品質、營運準確性、顧客滿意度與關懷社會責任等指標提供獎勵。
- 資安與緊急應變管理獎勵：因應風險情境的緊急應變，以降低對客戶及公司的影響提供獎勵。
- 業務及營運創新風險管理獎勵：針對業務創新與營運作業的風險控管等評估並提供獎勵。