

# 新門科技股份有限公司

## 風險管理政策與程序

### 第一條 目的

為強化公司治理，建立健全之風險管理機制，將各項可能產生之風險控制在可承受範圍之內，建制風險管理系統，並作為各類風險管理及執行依據，以提升風險管理之作業效能，特訂定本政策與程序。

### 第二條 權責

- 一、 ESG 發展委員會：為公司風險管理之最高單位，以遵循法令，推動並落實公司整體風險管理為目標，明確了解營運所面臨之風險，確保風險管理之有效性，並負風險管理最終責任。
- 二、 風險管理小組：由最高管理階層及各單位代表組成。
  - (一) 召集會議與各單位討論內外部議題、利害相關者關注議題、重大環境面、不可接受風險蒐集，進行各項議題的風險衡量。
  - (二) 執行稽核並產出風險管理報告呈報與揭露。
- 三、 各單位主管：辨別所屬單位重大風險項目，並提出風險回應對策。
- 四、 股務室：依主管機關規定揭露相關資訊，並於公司網站、永續報告書及年報揭露與風險管理有關資訊。

### 第三條 定義

- 一、 風險鑑別：包含權責單位、內外部議題、利害相關者、關注議題、問題描述。
- 二、 風險分析：包含可能影響、衝擊度、發生率(可能性)、風險數、風險等級。

### 第四條 作業內容

- 一、 企業風險管理組織與作為：企業風險管理區分為三個組織層級，進行分工運作。組織架構(參照附件一風險管理小組組織圖)。

風險管理組織	說明
第一層風險管理組織	各單位主管或業務承辦人為其承辦業務之風險責任人，須依相關業務之內部控制及內部規範執行業務，為最初的風險發覺、評估及控制的直接單位。
第二層風險管理組織	為各營運/後勤單位主管或經指派之部門風險管理人員負責相關業務之風險管理，並依據實際業務之運作，審視作業程序或指導書，並應注意主管機關公告之最新法規增(修)訂及業務相關函令，必要時得增(修)訂相關內部規範。
第三層風險查核組織	風險管理小組須審視本公司及重要子公司危害、營運、財務、策略及合規等主要風險管理相關機制之完整性，並應確實依照本政策及相關風險管理辦法監控各單位之相關風險。

- (一) 各單位應對所管理業務之風險進行監控，當風險程度超過管理目標時，應對高階主管報告與提出因應措施，進行改善。
- (二) 風險管理小組應定期對 ESG 發展委員會報告年度稽核計畫及執行成果。
- (三) 企業營運風險管理：由各層級單位，依各單位之管理權責與工作要求，於工作計畫與日常實施之各項體制流程中，皆需要具備風險觀念已完成 PDCA(Plan-Do-Check-Action)循環作業。

(四) 風險管理小組應依計畫指派評估小組召集人，並經由執行團隊溝通後，指派成員成立風險管理小組。

第五條 風險管理流程：風險評估包括風險辨識、風險分析、風險評量、風險處理、風險報告  
(參照附件二風險管理流程)。

一、 風險評估：風險管理小組於每年第四季將「風險與機會管理表」提供予各單位填寫。

二、 風險管理小組應依據各單位填寫後之「風險與機會管理表」召集會議，充分討論並參考主觀觀察與客觀營運數據，以識別各風險項目之可能性與衝擊度，並取得共識。「風險與機會管理表」填寫方式(參照附件三風險鑑別/風險分析說明)。

(一) 風險辨識：依據企業營運之策略改變、業務範疇、營運管理、地域變化、供應鏈、法令衝擊，客戶、產業變化，租稅政策、氣候改變…等可能狀態，分析企業內、外部面臨的營運情境，並依此整體(或個別)情境進行風險辨識作業。

風險構面	說明
1. 市場風險	國內外政治、經濟、監管要求、科技及產業變化等風險。
2. 營運風險	營運模式改變、組織架構調整、產品淘汰、產品及服務之設計及品質管理、重大合約風險管理、智慧財產權保護、企業形象之塑造及維護等風險。
3. 策略風險	銷售及採購對象之過度集中、單一地區銷售及採購之過度集中、相關產業投入之過度集中、相關併購等風險。
4. 財務風險	資產評估、信用及償付能力、流動性風險、會計政策之適用及變更等風險。
5. 投資風險	轉投資標的過度集中、高風險高槓桿操作、衍生性金融商品交易、金融理財等短期投資市價之波動、長期投資被投資公司之營運規範管理等風險。
6. 法律風險	未能遵循主管機關相關法規，或所簽訂契約本身不具法律效力、越權行為、規範不周、條款疏漏等其他因素，造成財務或商譽損失之風險。
7. 資安風險	一般及數位資訊安全及保密、無從確保資訊內容及處理方法、無從及時存取資訊及使用相關資產等風險。
8. 環境風險	溫室氣體排放管理、氣候變遷、碳權管理、能源管理、符合國際及當地環保法令或環評要求等風險。
9. 工作安全風險	職業安全衛生及健康、化學品管理、安全防護暨緊急應變、其他人為管理操作不當或失誤等風險。
10. 人力資源風險	員工或供應商之人權議題，包含但不限於勞資關係、童工、強迫勞動、人才發展管理，包括但不限於招募及留任人才、人才發展之風險。
11. 永續風險	a.經濟構面：經濟績效、採購實務、反貪腐、資訊安全等議題。 b.環境構面：能源、排放、廢棄物、水與放流水、環境法規等議題。 c.社會構面：勞資/雇關係、職業安全衛生、訓練與教育、人權、顧客健康與安全、客戶隱私、供應鏈 RBA 管理、社會經濟法規等議題。
12. 氣候變遷風險	為氣候變遷相關財務影響評估氣候變遷之風險來源，可參考 TCFD 等資訊進行風險項目之展開與風險衡量之作業，包含氣候變遷之轉型風險及實體風險： a.轉型風險：政策和法規風險、技術風險、市場風險、名譽風險。 b.實體風險：立即性風險、長期性風險。
13. 其他風險	非屬上述風險，但該風險將遭致重大損失等風險。

(二) 風險分析：鑑別與評估各項風險程度。

1. 提出風險項目(問題描述)：依各項風險構面，風險管理小組再展開為各項風險項目

分析，並給予更清楚之明確定義，以鑑別出企業營運可能面對的風險項目。

2. 風險管理小組對風險構面與風險項目之討論必須加以對應檢視，確認是否完整與可對應相關的企業營運環境分析實務狀態。
3. 風險管理小組進行之分析評估準則包含：可能性、衝擊度評價準則(各次評估可依組織情境進行修正)。

(1) 可能性評價準則：依本公司的管理經驗與指標紀錄，區分為 1~4 等級，以評估風險於組織內發生的機率。可經由風險監控之數據或參考相關類似產業的狀態，可能性評價參考表如下表：

可能性量表：參考指標			
如風險曾經發生過	情境	發生可能性程度	分數級距
如風險不曾發生過	平均每季可能發生二次以上， 平均每週人為阻止發生三次以上	非常大	4
	平均每季可能發生一次以上， 平均每週人為阻止發生二次以上	大	3
	平均每年都可能發生一次以上， 平均每週人為阻止發生一次以下	小	2
	平均每年發生不到一次， 平均每月人為阻止發生一次以下	非常小	1
如風險不曾發生過	(0~1 年內)非常有可能發生，預計該事件發生在大多數情況下，組織或是同業有經常發生的歷史紀錄。	非常大	4
	(1~3 年內)有較強的可能性此事件將會發生，因為過去在組織或是同業有頻繁發生的歷史紀錄。	大	3
	(3~6 年內)該事件可能有時會發生，因為過去在組織或是同業有發生過的歷史紀錄。	小	2
	(6 年以上)無預期的，但有一個微的可能性可能會發生。	非常小	1

(2) 衝擊度評價準則：

依本公司營業特性與狀態，區分為 1~4 等級，以評估風險事項於組織內發生時產生之衝擊程度。對組織衝擊可能是多個面向的影響，評估時應採取較高之衝擊程度為評估結果。衝擊度評價參考表如下表：

項目	衝擊度量表：參考指標			
設施/財務損失	損失重大 嚴重影響公司生存	造成公司重大虧損	盈利侵蝕	設施或財務 輕微損失
客戶流失	流失主要客戶	流失部份客戶	流失少數客戶	無流失
生命安全損害	大規模或嚴重人命傷亡 (如：2 人以上死亡或全殘)	中等之人命傷亡 (如：1 人死亡或全殘)	輕微受傷	無損傷
信譽傷害	嚴重	初期嚴重， 短期可恢復	中等， 信譽可恢復	輕微
法令違反	關廠/倒閉	巨額罰款、長期訴訟、 停工	短期訴訟	輕微
財務衝擊(NTD)	500~1,000 萬元	100~500 萬元	50~100 萬元	0~50 萬元
衝擊度	非常大	大	小	非常小
分數級距	4	3	2	1

(三) 風險評量：風險低、中、高之判定標準(詳請參考附件四、風險等級評分矩陣)。

高度風險項目應與經營團隊、高階主管確認策略方案，並填入「風險與機會管理表」之風險處理項目：

1. 行動方案(說明)
2. 負責單位
3. 預計完成時間或達成目標

風險管理小組針對高風險項目或必要報告項目，與所屬單位溝通協調，擬定行動方案(說明)，進行持續監控與改善。並納入稽核計畫定期查核。

(四) 風險處理：分為接受、規避、控制、移轉。

1. 接受：風險在容忍範圍內，予以容忍不作處理(低風險)。
2. 規避：風險在容忍範圍外，處理成本高於利益(禁止衍生性金融商品投資，禁止機密資料連網)。
3. 控制：降低發生率(權利分立、防火牆、加強內控)；降低衝擊度(氣囊、備援機房、緊急應變計畫)。
4. 移轉：轉由他人承受(購買保險、業務委外)。

(五) 風險報告：依據「風險與機會管理表」撰寫風險管理報告。風險管理執行落實之評估：

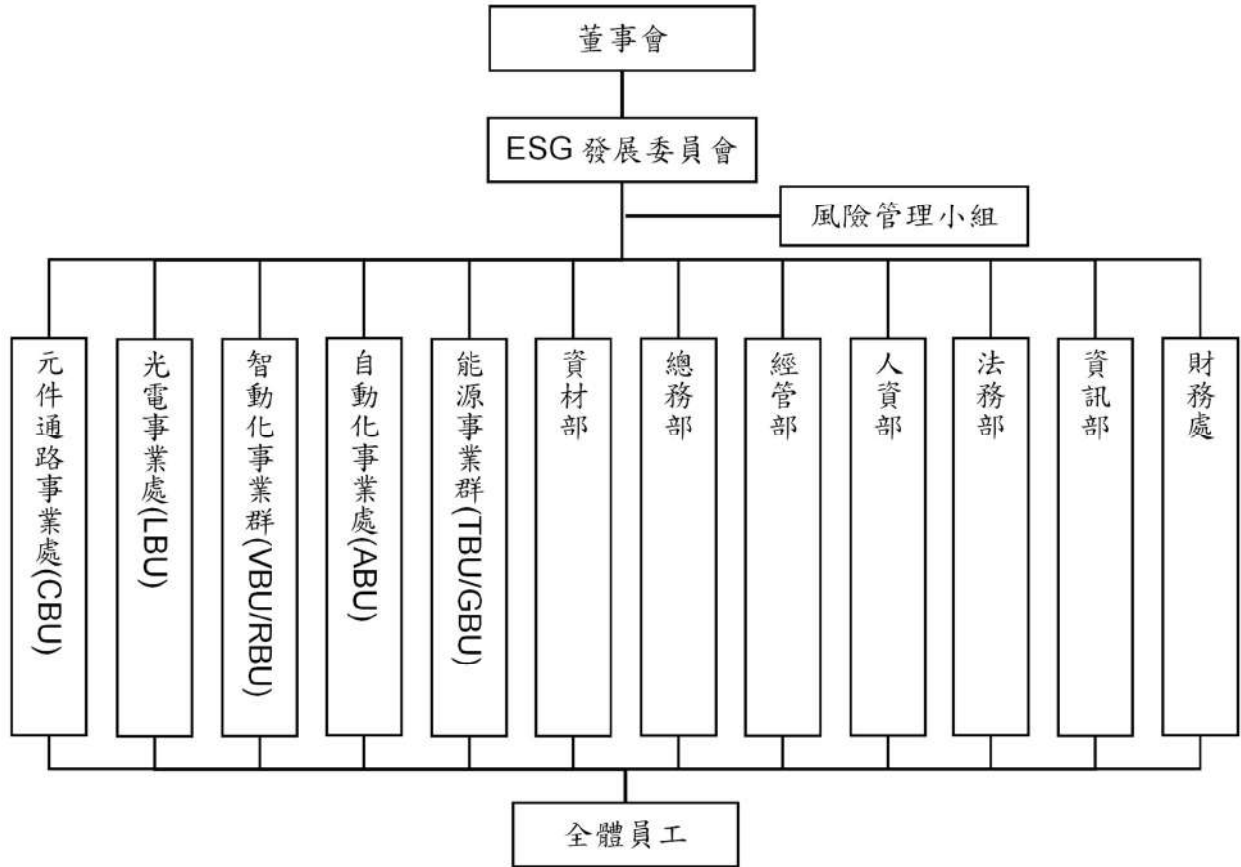
1. 由風險管理小組於次年度風險評估前，進行當年度風險管理是否有效落實執行之評估、確保制度落實與遵循。
2. 風險管理小組於每年年底前完成報告，每年至少一次向 ESG 發展委員會進行報告。
3. 風險管理小組確認風險管理情形後，由召集人每年至少一次向董事會進行報告。
4. 股務室依主管機關規定揭露相關資訊，並於公司網站、永續報告書及年報揭露與風險管理有關資訊。
  - (1) 風險管理政策與程序。
  - (2) 風險治理與管理組織架構。
  - (3) 風險管理運作與執行情形(包含向董事會及 ESG 發展委員會報告之頻率與日期)。

## 第六條 訂定與修訂

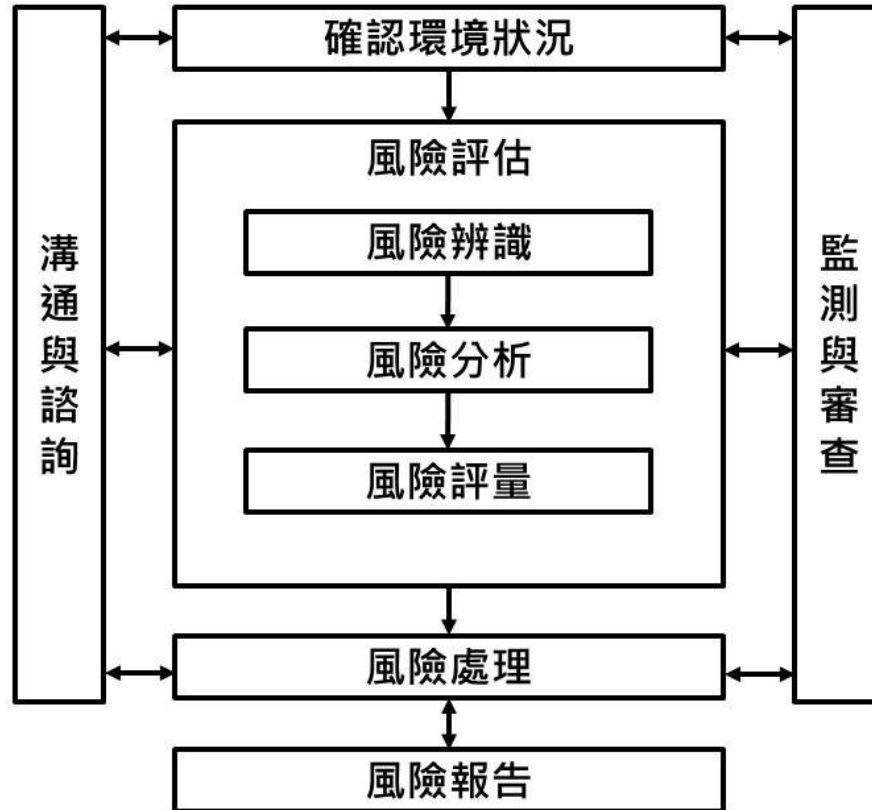
風險管理政策與程序之檢討及修正。

- 一、風險管理小組應隨時注意國際與國內風險管理制度之發展情形，定期檢視本公司企業風險管理政策與程序，並據以提出檢討改善建議，提交 ESG 發展委員會及董事會討論。
- 二、本風險管理政策與程序經董事會決議通過後施行，修正時亦同。
- 三、本風險管理政策與程序訂於民國 112 年 8 月 8 日。

附件一、風險管理小組組織圖



## 風險管理流程



附件三、風險鑑別/風險分析說明

風險/機會鑑別				風險/機會分析						
權責單位	議題(環境)		關注議題	(現狀)問題描述	可能影響	現行機制	風險評估			風險/機會
	內部/外部	利害相關者					衝擊(嚴重)度	發生率	風險數	

1. 權責單位：依據所負責的職能單位提出。
2. 內部/外部：議題發生源自於內部可控制處為內部議題，議題發生於內部不可控制處為外部議題。
3. 利害相關者：鑑別此議題之關注單位(外部、內部)。
4. 關注議題：以 4-6 字簡述關注議題方便查閱或類型管理。
5. (現況)問題描述：盡可能運用 5W 以獲得詳細的事件內容。  
 What-發生什麼事情  
 How-如何發生  
 Why-為何發生  
 Where-在哪裡發生  
 When-何時發生
6. 可能影響：以數據描述風險發生的結果以利下一步分析。影響營運績效、安全、法遵、時間、費用等。
7. 衝擊度：區分為非常大【4】、大【3】、小【2】、非常小【1】依照風險評估準則分析後填入等級分數。
8. 可能性：區分為非常大【4】、大【3】、小【2】、非常小【1】依照風險評估準則分析後填入等級分數。
9. 風險數：為衝擊度分數可能性分數。
10. 風險等級：依風險矩陣判定為高度、中度、低度。

風險處理				風險與機會評估	監督	備註
處理類別	行動方案(說明)	負責單位	預計完成時間或達成目標	風險/機會是否執行	效果說明	

11. 處理類別：分為接受、規避、控制、移轉，以上四項。
12. 行動方案(說明)：進一步行動方案說明。
13. 負責單位：行動方案負責人員或單位。
14. 預計完成時間或達成目標：行動方案目標的描述、完成時間或數據化的目標。
15. 風險/機會是否執行：經評估後的風險或是機會行動方案，是否會執行。
16. 效果說明：依據評估時間的規劃審查行動方案的有效性並記錄。
17. 備註：如遇特殊狀況，須填寫說明。

## 風險等級評分矩陣

衝擊度 可能性	1	2	3	4
4	中度風險 (4)	高度風險 (8)	高度風險 (12)	高度風險 (16)
3	低度風險 (3)	中度風險 (6)	高度風險 (9)	高度風險 (12)
2	低度風險 (2)	中度風險 (4)	中度風險 (6)	高度風險 (8)
1	低度風險 (1)	低度風險 (2)	低度風險 (3)	中度風險 (4)