三商家購股份有限公司
Simple Mart Retail Co., Ltd.

風險小組管理政策及執行情形

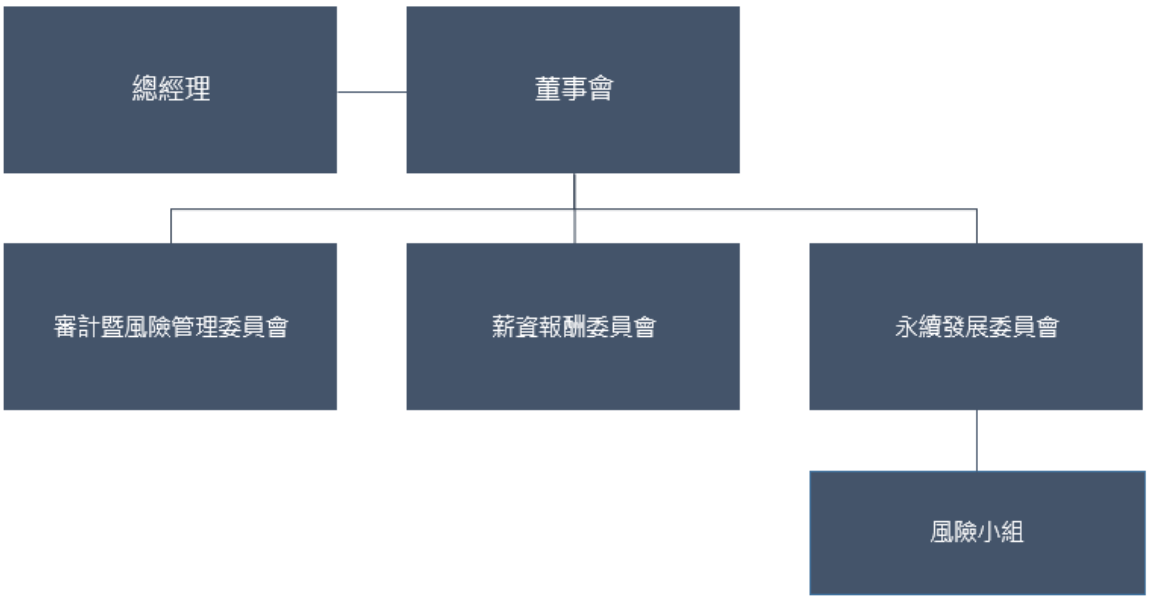
為強化公司治理並建立健全的風險管理作業流程，本公司於 2024 年 5 月 3 日將「審計委員會」更名為「審計暨風險管理委員會」，由審計暨風險管理委員對公司風險管理進行督導。

審計暨風險管理委員會成員皆由本公司獨立董事組成，成員及其專業能力如下：

功能性委員會	召集人	成員	專業能力						
			會計及財務分析能力	法律	經營管理	危機處理	國際市場觀	領導能力	決策能力
審計暨風險管理委員會	蔡孟霖	蔡孟霖	✓		✓	✓	✓	✓	✓
		林再林			✓	✓	✓	✓	✓
		黃銘傑		✓	✓	✓	✓	✓	✓

另本公司於 2024 年 8 月 2 日成立永續發展委員會，旗下設置風險小組，主要負責公司風險及資安管理，由余念蒙行政長擔任小組召集人，小組遵循本公司於 2021 年 4 月 28 日訂立之風險管理政策與程序(經董事會通過)，定期辨識與評估潛在危機，依本公司組織環境、階段性策略目標擬定評量計畫，期待有效降低及改善風險項目，將因業務活動所產生的各項風險控制在可接受的範圍。風險小組召集人並分別於 2024 年 8 月 2 日列席審計暨風險管理委員會報告、2024 年 12 月 27 日列席董事會報告風險管理執行情形。

組織架構：



依本公司「審計委員會組織規程」，審計委員會之運作包含監督公司存在或潛在風險之控管，本公司已於 2024 年 5 月 3 日董事會通過將「審計委員會」更名為「審計暨風險管理委員會」，並要求風險小組至少半年一次至審計暨風險管理委員會或董事會報告風險評估及後續執行情形，由審計暨風險管理委員會督導風險管理。

管理範疇：

本公司因應企業經營所可能面臨的各項風險以及有可能帶給利害關係人的衝擊，訂立風險管理政策與程序，掌握科學證據原則、事先預防原則、資訊透明原則，建構風險管理體系。本公司辨識出八大風險類別可能之風險情境、發生機率、影響程度、風險值與風險等級，規劃合適之權責單位、因應對策、控制措施。透過量化風險與風險認知，對風險不確定性進行評估，進一步辨識本公司可接受之風險，協助做出精準決策。

八大風險與權責單位

風險類型	風險事件(事件、原因、可能的後果)	風險等級	因應對策/控制措施	權責單位
公共安全風險	事件：人為或意外 原因:由人為因素所造成公司資產損失或影響日常營運之風險，如火災、停電、屋況問題、設備故障、搶/竊案或其他不可預期之事件。 後果:可能造成人員傷亡、營業中斷或財物損失	高度風險	1. 加強相關設備配置(如: 乾粉滅火器、緊急照明燈、乾冰等) 2. 加強人員教育訓練(定期訓練及不定期災害演練、設定相關安全規範及應變措施) 3. 相關保險投保作業(如: 商業火險、公共意外責任險、現金險、營造綜合險、竊盜險等) 4. 落實日常檢查作業(火源管理、分店禁菸政策、建物及設備保養維護) 5. 落實重大事件的通報機制，建立後勤人力支援	營運處
資訊安全風險	事件:資訊設備、系統故障及資安事件 原因:因關鍵營運系統中斷而影響日常業務運作之風險，如硬體設備/軟體系統故障、資訊人員離職或委外服務廠商因故終止服務、新導入系統建置不良而與業務功能需求有重大差異等因素。 後果：物流中心/門市運營中斷、庫存不準而影響訂貨(缺貨或呆滯風險)、客戶投訴、影響財務結算及付款	高度風險	1. 建置備援機制，並重要設備、系統與廠商簽訂保固或維運合約 2. 重要系統資料庫定期備份及建立災害復原計畫 3. 程式版本更新時須由核決權限部門主管核准，以評估更新風險範圍與測試程序是否足夠，並進行程式版本管理機制 4. 重大異常事件發生後須建立事件報告與修復手冊 5. 依據資訊職能與技術別建立代理人/工作輪替機制，並避免綁定於單一維運供應商且無替代供應商可支援之情事。 6. 三商家購於 2023 年成立「資訊安全管理專屬單位」，並配置資安專責主管 1 名及 1 名資安專責人員與 2 名資安承辦人員，合計 4 名，主係確保資通安全管理制度之運作，並訂定資訊安全管理政策，以強化本公司資訊安全管理，確保資料、系統、設備及網路安全，保障公司與全體員工之權益，並全面提升資安意識。為確保相關資訊系統的運作風險得以有效控制，「資訊安全管理專屬單位」每年至少召開一次檢討資安作業，必要時得召開臨時會議，並每年彙總後分別向審計委員會及董事會報告。	資訊處
個人資料風險	事件:員工及顧客個人資料外洩 原因:透過外部侵入、公司內部竊取等手段取得相關資訊，	中度風險	1. 定期進行網路資訊、電腦系統之安全維護、控管及檢查機制 2. 確保紙本資料、電腦、自動化機器或其他存放媒介物報廢汰換或轉作其他用途時之資	資訊處

風險類型	風險事件(事件、原因、可能的後果)	風險等級	因應對策/控制措施	權責單位
	或經由紙本及電子資料傳輸、保存、銷毀疏失產生資料外洩，並可能有固有資訊遭竄改、損毀、滅失之風險。 後果:公司聲譽受損、供應商及消費者資料外流或冒用、影響日常營運、法律問題及處分		料清理 3. 簽訂保密切結書，並加強員工教育宣導(安排個人資料保護法基礎教育宣導及數位學習教育訓練每年至少至少2小時) 4. 本公司所屬人員需以專屬帳號密碼登入，方能使用電腦設備及資訊系統進行蒐集、處理、利用個人資料 5. 機房設置門禁、監視錄影及防火設備，並備份重要個人資料 6. 電磁資料視實際需要以加密方式傳輸 7. 三商家購保護消費者個人資料與隱私權，遵循「個人資料保護法」，建立本公司個人資料保護管理作業程序，並落實各項安全維護措施，以確保本公司各項業務所蒐集、處理及利用之個人資料(以下稱個資)能有效進行管理與保護，於2023年成立「個人資料管理專責單位」負責推動個人資料保護管理事宜。	
環境風險	事件：自然災害 原因:地震、洪水、颱風等可能導致人員傷亡、營業中斷與財物損之失天然災害。 後果：物流中心/門市業務中斷、財產和庫存損壞	中度風險	1. 相關保險投保作業(如公共意外責任險) 2. 落實日常檢查作業(店內外建築物之設施定期維修和保養) 3. 落實重大事件的通報機制，建立後勤人力支援 4. 不定期辦理災害演練	行政總處
食品安全風險	事件：重大食品安全問題 原因:供應商未能提供符合標準的商品，或從製造、儲藏至配送過程中，因不良管控使品質發生變化，導致產生食品污染物、食品添加物、食品微生物等風險。 物流及門市未即時檢視商品之有效期限，恐違反食品安全衛生管理法以販售過期食品，致損害公司企業形象。 後果：公司聲譽受損、客戶/銷售損失、法律問題及處分。	中度風險	1. 年度供應商評鑑 2023 年美廉社合作的代工生產(簡稱OEM)供應商有72家，共評鑑72家(評鑑率100%)。其中評比A級優良廠商37家(占比51.4%)；B級合格供應商17家(占比23.6%)；C級供應商15家(占比20.8%)D級供應商3家(占比4.2%)；E級供應商0家(占比0%)。 2. 加強供應商新品提報之控管及審核 3. 針對高風險商品採週期輪替性檢驗計畫 4. 進口商品由報關行、報驗行及公司品保進行成份及產地審核 5. 自有品牌商品須由供應商提供商品技術規格書，並由公司品保審核商品成份、定期至工廠進行實地評鑑。 6. 減少引進短效期商品，確認保存期限及條	供應鏈處

風險類型	風險事件(事件、原因、可能的後果)	風險等級	因應對策/控制措施	權責單位
			件是否適合門市販售 7. 物流及門市依 SOP 檢視商品效限，並由安管稽查室定期實地查核 8. 相關保險投保作業(如產品責任險)	
公關風險	事件：媒體/社交網絡中的負面報導 原因：由於商品、員工或顧客服務品質不佳或其他因素，在傳統或網路媒體、社交平台上出現負面報導或謠言，使公司權益受侵害、聲譽受損或財產損失。 後果：公司聲譽受損、客戶/銷售損失、政府調查/起訴	低度風險	1. 密切關注媒體報導，並對信息來源進行查證及分析 2. 即時對不實報導及負面新聞進行媒體說明或平衡發稿 3. 透過法務部門撰擬聲明函件 4. 評估影響範圍，涉及財務損失等重大事件則向警察局或相關政府行政機關備案 5. 透過內部教育訓練以提升各項服務品質並有效降低客訴發生機率 6. 設置智慧財產權利義務及相關業務管理單位	行銷處
財務風險	事件：財務及投資風險 原因：包含公司之金融資產或負債因市場風險因子波動使得價值發生變化，及因轉投資標的過於集中、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，或長期投資被投資公司之營運風險，所造成種種損失。 後果：損失增加、資產減損、公司聲譽受損、額外支出	低度風險	1. 定期監控市場匯率、利率變動狀況並進行評估 2. 若有大額且長期性資金需求時權衡當時利率市場狀況，評估是否以現金增資等其他方式籌措所需資金 3. 設定投資風險屬性並定期評估各類投資風險 4. 每月檢視資金貸與他人及為他人背書保證之情形	財務管理處
勞動安全風險	事件：員工及協作商之職業安全 原因：因職場暴力、職業災害、未落實勞動安全檢查或教育訓練等因素，造成勞工或協作商身體及心理健康危機。 後果：員工流失、裁罰或賠償、法律責任、公司聲譽受損	低度風險	1. 定期對員工進行健康與職業安全培訓、災變演練，內部職安衛教育訓練總時數達 16,166 小時。 2. 提供定期員工體檢(每年一次) 3. 建立申訴管道及專案受理組織 4. 設置法規要求之合格職業安全衛生相關人力 5. 根據流程/組織的變化設定及定期審查相關預防計畫 6. 關注勞工職業安全衛生相關法令規定 7. 成立運動性社團或舉辦活動	人力資源處

運作情形：

本公司積極推動落實風險管理機制，主要運作情形如下：

- 為落實穩健公司治理，本公司於 2021 年 4 月 28 日訂立風險管理政策與程序，並定期辨識與評估潛在危機。依公司組織環境、階段性策略目標擬定評量計畫，期待有效降低及改善風險項目，促使企業永續經營。
- 本公司風險小組成員每週高階主管會議中報告是否辨識新風險或原風險等級是否有異常變化，暨各項風險評估結果及執行情形，並每年至少一次向董事會報告其運作情形。2024 年分別於 8 月 2 日列席審計暨風險管理委員會報告，2024 年 12 月 27 日列席董事會報告風險管理執行情形，包含風險項目之評估、固有風險項目、風險因應措施及實際執行之情形等。
- 因應社會人口結構變化、消費型態轉變與氣候變遷等重大議題，本公司將積極關注相關法規，除定期檢視新興議題，也同時掌握同業的動態情報。
- 本公司除針對新進人員進行宣導告知本公司重要風險及防範等相關應變措施外，另安排個人資料安全及法令遵循相關等課程以加強同仁風險安全意識。
- 本公司於 2024 年 8 月 2 日於審計暨風險管理委員會報告針對本公司八大風險透過質化(透過文字描述)與量化(具體可計算之數值指標)標準，以衡量公司可承受之風險限額(風險胃納)，以風險等級及公司對於該風險之重視程度綜合評量各項風險胃納，並對胃納程度較低之風險進行高強度的因應措施。

✧ 審計暨風險管理委員針對風險提出相關建議：

委員建議	公司回覆及執行情形
台灣有地震也有淹水，後續在找開店點時應把類似建築物結構、當地地勢及交通問題納	後續開店會再評估並留意相關風險，並將可辨識的內容加強保險。

入考慮，若只是商品破損沒有關係，但若壓到員工或顧客就會影響到人身安全。	
正常的安全風險可以加大保額，但之前千面人的案件要留意如何處理，關於此類狀況建議應該要有相關 SOP 公關危機處理小組。	目前門市皆裝設攝影鏡頭，若有事先收到相關訊息，會優先將該門市預防性關閉，後續再將證據提供，也會再做相關研擬，並訂定 SOP。

- 本公司於 2024 年 8 月 2 日審計暨風險管理委員會及 12 月 27 日董事會針對資安風險進行報告，包含：

1. KPMG 資訊稽核項目改善：透過外部稽核意見提升資訊內控品質。
2. 資安健診(每兩年)：年度例行健診，確保資訊設備與網路無明顯漏洞。
3. 網站與 APP 資安檢測(每年)：年度例行檢測 (強化 B2C 系統安全性)。
4. 系統災害復原演練(分年計畫實施)：預防重大災害或駭客攻擊時能重新恢復系統服務。
5. 物流中心無線網路設備更新(專案)：提升網路穩定性與使用效能，汰換既有 Wifi 老舊設備，強化網路安全、物流中心擴建之網路布建。
6. 資安架構與發展藍圖：編制資安發展藍圖完善風險評估架構與補強計畫。

✧ 審計暨風險管理委員針對資訊安全提出相關建議：

委員建議	公司回覆及執行情形
資安問題跟個資問題是越來越嚴肅的問題，建議應持續強化人員素質，包含上外部課程，以利取得資訊。也建議資訊和外部廠商有更多接觸，包含和廠商討論更多防範的措施。	已編列資安預算，包含資安健檢等相關檢測，後續會繼續評估加強。

- 本公司另於 2024 年 12 月 27 日董事會，人力資源處針對 ISO45001 建置進行報告，有助於提供組織、勞工與其他人員一個安全與健康的工作場所，以防範失能、

工作傷病、疾病甚至是死亡，並且透過反覆的流程，達到持續改善職業安全衛生績效，預計 2025 年初取得認證。

審計暨風險管理委員已針對報告內容進行督導及提供建議，並要求相關權責部門主管定期於審計暨風險管理委員會及董事會報告。