中國航運股份有限公司
風險管控運作說明

風險管控政策

本公司訂定「風險管控政策」提 109 年 12 月 8 日董事會通過，本公司風險管控組織採跨部門組成形式，基於當前資本結構與企業模式並顧及公司企業策略與收益目標下，定期評定公司的風險取向。並依據風險管控程序分析特定風險所獲得的結果，來制定公司應對風險時的策略，每年一次向董事會報告運作情形。為有效控制風險，依緊急應變計畫設置任務性緊急應變行動小組，由總經理召集並擔任總指揮。

本公司於 111 年 5 月 12 日成立審計委員會後，由其監督公司存在或潛在風險之管控；並由專責單位依據重大性原則進行分析，與內外部利害關係人溝通，透過檢視相關資料，據以評估具重大性之環境、社會、公司治理等 ESG 議題。

風險管理範疇

本公司風險管控事項包括「決策風險」、「法律風險」、「投資性風險」、「匯率利率及流動性風險」、「市場風險」、「船舶運務風險」、「資訊安全風險」及「氣候變遷風險」等。

基於當前資本結構與企業模式並顧及公司企業策略與收益目標下，會定期評定公司的風險取向。依據風險管控程序分析特定風險所獲得的結果，來制定公司應對風險時的策略。

執行情形

本公司已於日常營運活動中將企業風險管理融合於公司治理的核心流程中，並視風險事項需求分別召開每週/每月/每季檢討會。

提報 114 年 11 月 11 日之董事會報告風險管控組織執行之業務，包括：

一、 職業安全衛生方面：

1. 本公司發布之永續報告書榮獲勞動部職業安全衛生署舉辦「企業永續報告公開職業健康與安全績效主動評比」績優企業，展現本公司對於職業健康與安全(Occupational Health and Safety, OHS)的推動成效良好。
2. 每季召開職安衛委員會議，提出建議及推行安全衛生相關事項。
3. 每月安排衛教資訊宣導及臨場醫護服務，增加員工照護資訊及健康守護觀念；員工體檢後，臨場醫護就檢查檢果之分析評估及改善建議。
4. 不定期依當時狀況，以郵件方式提醒同仁注意舉凡勞動部電子報訊息、辦公室施工工程、流行傳染病疫情、颱風及天氣變化等所產生之風險，並確實宣傳對應之防範措施。

5. 定期檢驗大型設備：電梯、低壓電、發電機、空調主機等；定期檢測辦公環境二氧化碳濃度。
6. 本公司及各子公司、聯絡處（含陸運、倉儲及船隊）依營業特性、所處建物性質及規模進行消防與防災之教育訓練。包括安排總部大樓所屬之自衛消防編組成員至台北市防災科學教育館體驗災害模擬並實際操作各項消防設備等訓練，增進日常防災知識，保障員工及公司財產安全。
7. 本公司總部及子公司之部分工作場所已完成 AED（自動體外心臟電擊器）之設置，總部並通過 AED 安心場所認證，每年持續安排員工接受『CPR+AED 訓練課程』。
8. 安排新進同仁接受職業安全衛生相關之教育訓練。
9. 為維護同仁身心健康，推行相關計畫並據以執行。

二、 法遵風險管理：114 年度已進行 5 次法務講習，分別針對合約風險控制、租屋相關法律知識、反詐騙宣導、誠信經營及性別平等與防治職場性騷擾等主題進行說明。另針對集團保險出險狀況分析提供改善建議、考量新增財產或責任等風險，據以調整保險額度及範圍。

三、 人事執行與員工關懷：本公司重視員工身心健康與工作幸福感，114 年度共辦理 4 場心理健康講座，主題涵蓋「壓力調適與心理韌性」、「主管敏感度與關懷技巧」、「職場壓力管理」及「心理韌性關鍵要素」等，協助員工及主管強化自我覺察與壓力因應能力，提升整體職場心理健康素質。

為進一步完善心理健康支持機制，公司正式導入「員工協助方案」（Employee Assistance Program, EAP），透過專業第三方資源提供保密且即時的協助，協助員工面對工作與生活挑戰，促進身心健康平衡，並共同營造具支持性與永續性的工作環境。

同時，為推動績效與人才發展並重制度，公司導入 SAP SuccessFactors 模組，建立「績效與發展雙軌機制」，以量化數據呈現考核結果，串接獎酬與發展流程，達成員工成就感提升與公司永續目標並進的雙贏成果。

四、 各部門皆定期進行內部風險控管，如財務部、資訊部、海運部、合併子公司（陸運、倉儲及汽車）皆至少每周一次定期性會議針對營運風險進行評估管理。

五、 資訊安全風險管理：由資訊部門負責，每季召開資訊管理會議，本年度投入維護資訊安全設備及軟體之金額約計 305 萬元，其管理執行情形如下

1. 檢視防火牆配置 - 除固定之防火牆更新作業外，已強化擴充防火牆功能，包括增加入侵防護、防毒、防殭屍病毒、網址過濾及報表功能，可在閘道端將有問題之連線予以阻斷，且可透過產出之報表了解網路狀態，加強監控及分析，現階段已建置好高可用度(high availability)的機制，可避免單一設備故障造成網路中斷。

另外，VPN 連線將原本傳統單一密碼驗證方式改為動態密碼驗證，增加連線安全性。

2. 檢視網路活動 - 除原有之未經授權軟體禁止安裝等軟體控管外，亦控管相關對外通訊程式，避免內部文件透過其他方式外流。安排年度社交工程演練並加強宣導，以強化員工的資安意識。與各點間之傳輸亦透過 VPN 加密方式傳輸避免資料外洩。
3. 網路、伺服器安全監控 - 增加系統管理權限帳號鎖定，避免受外力及入侵被竄改，提高系統安全性，並增加監控機制，當系統資料被修改時會即時發送郵件通知管理人員。建立主機弱點掃描機制，針對現有主機進行弱點掃描及漏洞修補，以確保主機安全性。
4. 主機容錯機制建置及異地備援 - 除已設置即時備援機制、每年 11 月執行災害演練測試，以確保即時備援機制正常。目前正進行營業持續計劃(Business Continuity Planning)，現階段已完成主機異地備援機制及網路備援，確保在發生災害時系統能夠持續穩定運作及確保資料完整性。而文件保存方面亦規劃透過系統自動將重要資料定期複製及備份。
5. 強化用戶端資訊安全 – 建置 WSUS(Windows Server Update Services)服務，針對使用者電腦定期集中更新管理，確保電腦持續進行安全性更新。套用群組原則加強密碼複雜度管控，增加安全性。本年度已陸續將使用者作業系統升級至新版本，同時也安排導入文件加密管理及資料遺失保護措施，強化文件管理。
6. 資安健診 – 安排資通院(國家資通安全研究院)評鑑優良之第三方單位及 KPMG 進行資訊安全環境檢視及資通安全防護控制檢視，包括網路架構、網路活動、使用者端及伺服器主機、目錄伺服器及防火牆安全設定、資料庫等，同時也持續進行網路架構改善，以提升安全性。