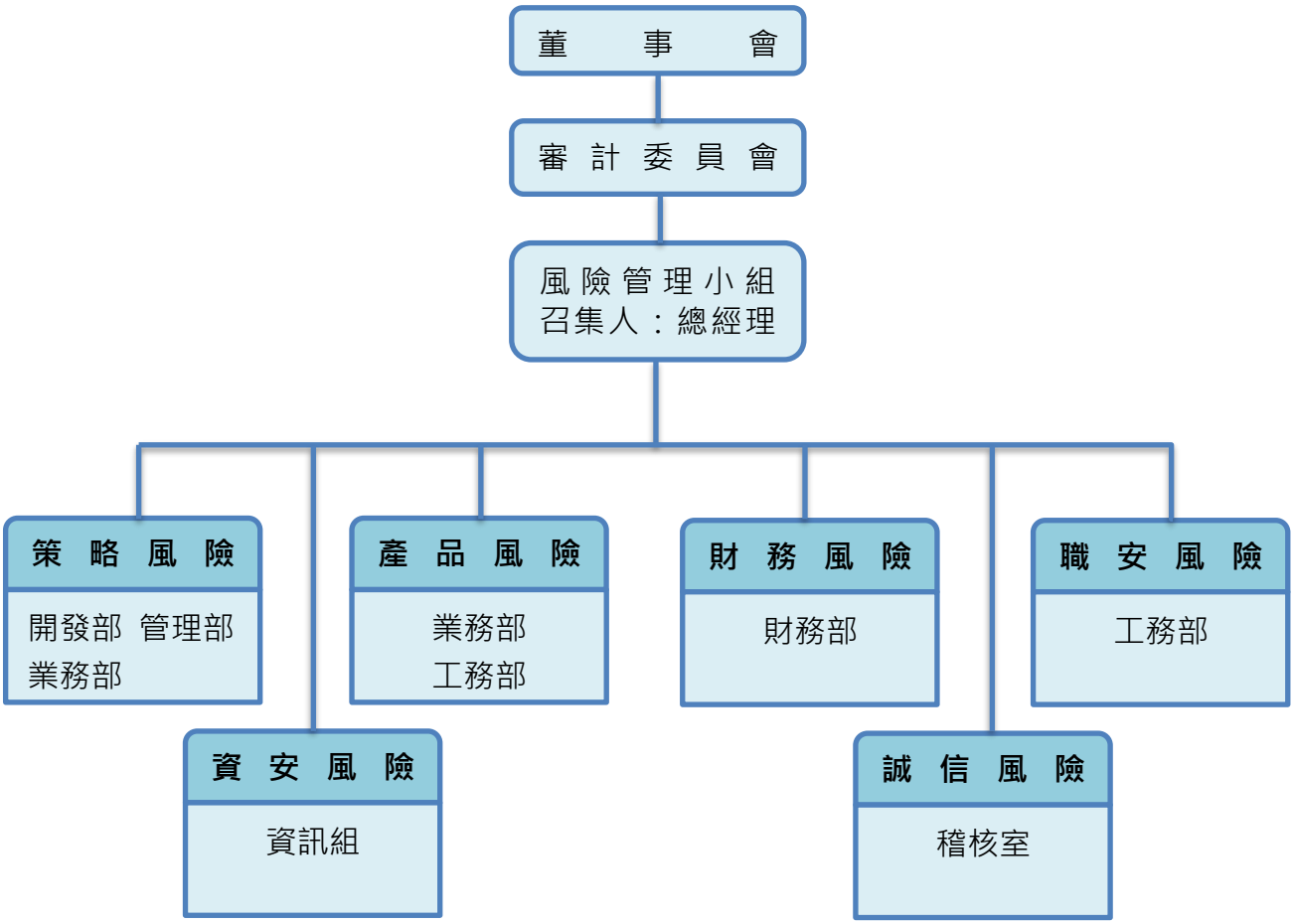
風險管理架構及運作情形

由於建設業需投入大量資本，包括土地、營造、銷售、財務和管理等方面，加上建築期間較其他產業長，回收進展較慢，而且存在著不容忽視的景氣循環風險。因此，公司定期召集各部門主管鑑別經營潛在的風險，透過單位間的橫向資訊交流，歸納並分析各項風險之優勢與劣勢；此外，亦長期關注產業趨勢及市場變動，掌握風險變化，以有效減少各種風險對企業的衝擊，進而提升經營績效。

風險管理小組架構



1.董事會：董事會為公司風險管理之最高單位，負責核准、審閱和監督公司風險管理政策。

2.風險管理小組：由審計委員會督導風險之管理，並且由總經理擔任召集人，負責統籌風險管理工作，成立跨部門之風險管理小組，定期聽取各單位主管之報告，綜理本公司整體之風險管理事項、檢視各單位風險控制管理報告，定期追蹤執行與改善進度，並每年一次向董事會報告。各單位主管負有單位內作業最初風險管理之責任，推動並落實整體風險管理為目標，確保風險管理及控制之機制與程序能有效執行。

風險管理小組工作職責

- **擬定各項風險管理制度、架構及機制**
- **審查風險管理報告、策略及改善計劃**
- **檢視各單位風險管理報告，追蹤執行與改善進度**
- **溝通佈達風險管理事項及檢視評估風險管理措施之有效性**
- **每年一次向審計委員會及董事會提出風險管理運作情**

運作情形

本公司自 112 年起積極推動及落實風險管理機制，由總經理負責統籌風險管理工作，並每年一次向董事會報告，主要運作情形如下：

日　　期	會　議	主　要　運　作　情　形
112 年 11 月 10 日	董事會	訂定「風險管理政策與程序」
113 年 03 月 14 日	董事會	擬訂「風險評估及因應措施」並向董事會報告
113 年 11 月 11 日	董事會	針對 ESG 三大議題，鑑別出營運、財務、環境等風險，據以擬訂相關風險管理策略
114 年 11 月 11 日	董事會	針對 ESG 三大議題，鑑別出營運、財務、環境等風險，據以擬訂相關風險管理策略

資訊安全政策

為揭示本公司對資訊安全之重視，建立資訊安全管理機制以確實掌握資訊設備及網路安全，保障公司作業電腦化規劃及資料處理之機密性、可用性及完整性，當資安風險或緊急事件發生時，本公司具備應變處置原則及能力，以確保業務迅速恢復正常運作，特制定 **資訊安全政策** 。

管理架構

本公司資訊安全之權責單位為資訊安全室，負責訂定公司資訊安全政策，規劃資訊安全措施，並執行相關資訊安全作業，下設資訊安全主管及資訊安全人員 1 名。

本公司稽核室為資訊安全風險查核單位，依據內部控制管理程序及電腦化資訊循環作業辦法，每年定期執行資訊安全檢查，若有發現缺失或資安事件，旋即要求受查單位提出相關改善計畫並呈報董事會，定期追蹤改善成效，使資訊通安全檢查制度持續穩健落實，並不定期執行資安會議，以降低資安風險。

管理機制與投入資源

- 制度規範：訂定「電子計算機管制辦法」，規範本公司資訊運作環境及人員資訊安全行為，並依資訊安全法規與營運環境變遷，擬定及修訂資通安全防護機制與方案。
- 軟硬體維護：推展各項應用系統，協助與電腦相關之自動化作業，促進各部門對電腦軟、硬體之充分有效使用，並建置各式資安防護措施，以提升整體資訊環境之安全性。
- 人員訓練：透過內部教育訓練提升資訊人員的專業職能，於企業內部宣導資安相關注意事項，以提升全體員工對資訊安全之危機意識與應變能力。

管理方案

相關資訊安全具體執行措施如下：

項目	具體措施
電腦系統 安全管理	• 設置防火牆以阻擋外部網路攻擊 • 電腦皆安裝防毒軟體，定期更新病毒碼及排程掃描，降低病毒感染機會 • 伺服器每日備份，定期異地存放
網路 安全管理	• 設置防火牆，控管網際網路的存取，屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用 • 採用多層式防毒與垃圾郵件過濾系統，管控郵件安全 • 用戶端連線採行加密連線，提供安全連線機制
實體及安全 環境管理	• 本公司伺服器與網路設備均設置於專用機房，機房門禁採用人員全程陪同進出，且保留進出紀錄存查。 • 機房配有消防設施，減少災難損害 • 每季定期進行災難復原演練，並呈核報告
資訊/系統 存取控制	• 資料存儲依帳號權限嚴格管控 • 建立遠端連線與安全認證(遠端連線視需求開放使用)
個資管理	• 供應商合約加註保密條款，規範個資及機密資料保管之責 • 紙本合約於保存年限後，由管理部統一銷毀

投入資通安全管理之資源

113 年		114 年	
項　　目	投入金額(元)	項　　目	投入金額(元)
集團資安健檢	375,000	集團資安健檢	378,000
電腦設備汰換	100,000	電腦設備汰換	100,000
防毒軟體	37,500	防毒軟體	37,500
伺服器+防火牆 硬體保固合約	50,000	伺服器+防火牆 硬體保固合約	10,000
備份設備更新	20,000	伺服器主機更換	182,000
機房網路設備及 UPS 電池更換	25,000		

並於每季對全體同仁辦理資訊安全管理課程訓練及宣導，向員工宣導資訊安全之責任，提升其危機意識與資訊安全觀念，防止因遭受攻擊而產生資料外洩之風險。

日期或期間	教育訓練或宣導內容	對象	方式
113/03/08、113/06/07 113/09/11、113/12/02 114/02/10、114/04/14 114/06/16、114/09/10 114/11/20	ERP 密碼原則宣導	全體同仁	公告簽名

113/01/10、113/02/15 113/05/16、113/08/14 113/11/20、113/12/19 114/01/10、114/03/12 114/06/11、114/07/01 114/08/13、114/09/10 114/10/15、114/12/11	資安宣導	全體同仁	公告簽名
114/01/15、114/06/26 114/09/17、114/11/19	資訊安全教育訓練	全體同仁	專題講座

運作情形

本公司自 112 年起成立資訊安全室，配置資訊安全主管及人員各一位，負責資訊安全事宜，並每年一次向董事會報告，主要運作情形如下：

日　　期	會　議	主　要　運　作　情　形
113 年 11 月 11 日	董事會	1. 委外廠商進行資安稽核及健檢，協助改善集團資安漏洞及降低集團資安風險 2. 113 年度未發生重大資安事件 3. 明年度資訊安全強化重點: (1)委託廠商進行稽核及健檢(2)社交工程郵件演練(3)持續內部所有同仁的資安宣導與教育訓練
114 年 11 月 11 日	董事會	1. 114 年委外廠商進行資安稽核及健檢，協助改善集團資安漏洞及降低集團資安風險 2. 114 年度未發生重大資安事件 3. 115 年度資訊安全強化重點: (1)委託廠商進行稽核及健檢(2)社交工程郵件演練(3)持續內部所有同仁的資安宣導與教育訓練