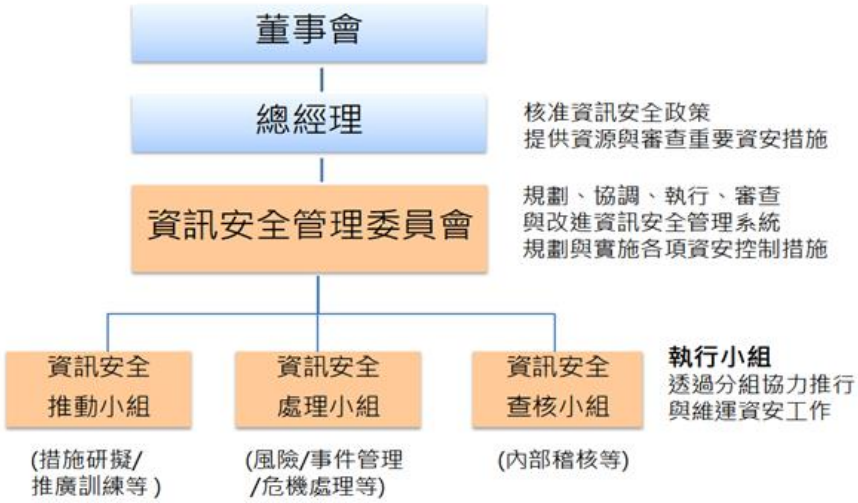
一、資通安全管理策略與架構

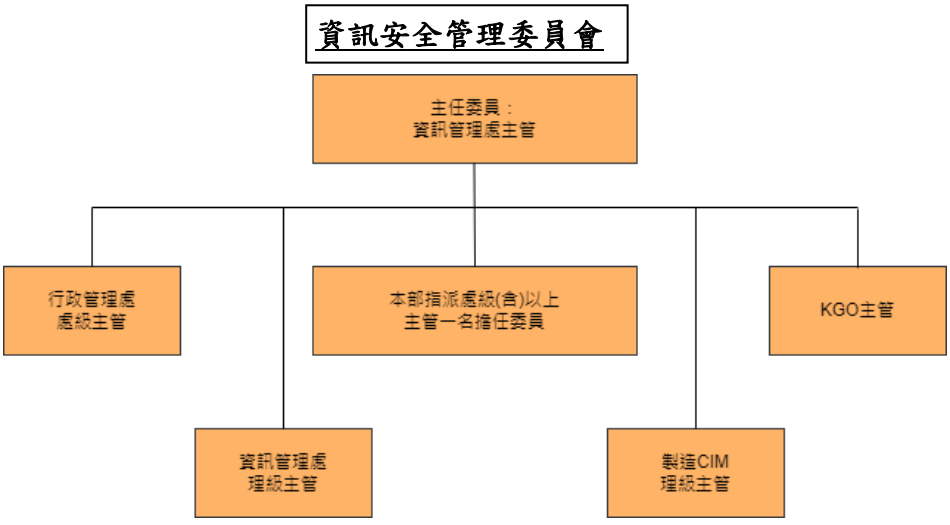
敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。(法規依據: 年報準則第 18 條第 6 款第 1 目)

(一) 資通安全管理架構

凌巨公司在民國一百一十年成立「資訊安全管理委員會」統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，建立管理框架以啟動與控制資訊安全的實施。此委員會直接對總經理報告，並由主任委員每年定期向董事會彙報資安管理成效、資安相關議題與未來資安規劃方向。



「資訊安全管理委員會」由資訊管理處主管擔任主任委員，KGO 主管擔任委員會成員，及經營管理本部、經營企劃本部、經營戰略本部、製造本部等各本部長推派人員擔任委員會成員，並設置內部稽核主管為觀察員，每月召開會議，檢視及決議資訊安全政策措施、研議資訊安全相關之新增重大議題、定期審核資安防禦成效。另於資訊管理處轄下成立「資訊安全部」，專責公司資訊安全規劃與具體管理措施執行查核，落實資安管理的有效性。



（二） 資通安全政策

凌巨公司的資訊安全政策涵蓋本公司及海外子公司，並遵循以下準則:

1. 建立符合法規與客戶需求之資訊安全管理規範。
2. 透過全員認知，達成資訊安全人人有責的共識。
3. 提供安全的資訊處理、傳送及儲存環境，以保障客戶、公司與全體員工之權益。
4. 強化資訊安全管理，確保各項資訊資產之機密性、完整性、可用性及網路安全，取得客戶信任，俾使凌巨集團業務之永續營運。

為有效落實資安管理，透過資訊防護系統及管理策略，從系統面、技術面、程序面降低企業資安威脅，依照「規劃－執行－查核－行動」(PDCA, Plan-Do-Check-Act）循環以持續改善。

- 規劃階段：著重資安風險管理，建立凌巨集團資訊安全管理規範，定期修訂資訊安全管理方案、程序及措施，使資訊系統能在標準的管理規範下運作，降低因人為所造成的安全漏洞或異常。
- 執行階段：建構多層式資安防禦，將資安控管機制整合內化於軟硬體日常維運，系統化監控資訊安全，確保重要資訊資產的機密性、完整性、可用性及網路安全。
- 查核階段：積極監控資安管理成效，依據查核結果進行資安指標衡量，並透過外部弱掃測試，以確保持續提升資安管理及防禦能力。
- 行動階段：檢討與持續改善，發現問題立即處理，並適時地將對策反映至管理規則修訂上。持續進行全員資安教育訓練及資安宣導，以提升資安意識。

於 2024 年 PDCA 資訊安全事件改善單 1~11 月共 38 件改善完成度 100%，1~6 月在循環檢視上半年完成度 100%。

（三） 具體管理方案

- 以多層式資安防禦架構提升資安能力：
  a）網路安全: 導入次世代防禦系統 IPS,APT,WAF。因應攻擊手法數據化，強化防火牆網路控管策略。
  b）郵件安全: 集團郵件防禦系統升級，採用最新 APT，DLP，防毒及防偽冒系統。
  c）裝置安全: 裝置周邊控管，阻擋利用裝置橫向感染發生。
  d）導入 EDR、 MDR 等防禦系統，針對使用端電腦、伺服器，自動關聯攻擊鏈，阻斷橫向攻擊鏈發生。

- 精進資安管理程序:
  a）應用程式安全：持續強化應用程式安全控管機制，並整合於開發流程中。

b) 強化權限管理：定期盤點集團所有文件存取權限及各系統平台管理者權限。
c) 強化人員帳號管理，導入多重認證機制。

- 檢討與持續改善:
  a) 每月召開資訊安全委員會會議，確認資安管理成效，檢討研議資安相關議題或事件，2024 年已進行 11 次(每月)資訊安全委員會，並於內部行資安委會資訊公告。
  b) 加強員工對郵件社交工程攻擊的警覺性，執行釣魚郵件防禦偵測，2024 年已執行 3 次全員社交工程演練，並完成員工資安訓練到課並完成考試達成率 100%。

- 風險控制: 定期進行系統脆弱度測試及分析，並加以補強與修護，2024 年弱點掃瞄執行 3 次(每季)，進行漏洞修正完成率 100%。

（四） 投入資通安全管理之資源

對應資訊安全管理事項及投入資源如下:

- 資安防禦系統及設備：
  (a) 於 2024 年 EDR 改善更新軟體套件，且 Window 全面升級至 Win10，若遇特殊需求無法升級至 Win10，一律阻擋對外上網。另外，Chrome 瀏覽器一律升級至最新版本。
  (b) 伺服器防禦: 於 2024 年因應虛擬化系統弱點公告，發佈資訊安全更新，升級至 7.0 U3s 版本。
  (c) 郵件防護系統升級: 於 2024 年因應弱點更新公告，郵件系統進行更新 20 次，已升至 mp8 第 49 版，新郵件防護系統更新 11 次，已升級至 6.1.07.001 版
  (d) 防火牆設備升級：於 2024 年底升級防火牆設備，國際間不斷有許多新型的網路攻擊手法，為了提升安全性，新防火牆設備採用 AI 防毒引擎(包含行為識別的條件 EX:檔案運行)，傳統一般只有特徵碼比對，新設備其包含自動化阻斷異常與識別多元性的攻擊手法。
- 專責人力: 設有專職之「資訊安全部」，設有資安主管兩名名及資安人員一名，負責公司資安架構設計、資安維運與監控、資安事件回應與調查、社交工程演練、災害復原演練、協助資安委員會資安政策展開工作等。
- 教育訓練:
  (a)所有新進員工到職一周內完成新人資訊安全訓練，完成度:100%。
  (b) 全體集團員工每年須進行至少一次資安訓練課程，完成度:100%。
  (c) 每季一次社交工程演練，及社交工程後調訓，完成度:100%。
- 資安公告:
  a) 每月定期公告資安委員會會議要項，讓所有員工了解公司資安防禦狀況及成效，傳達資安的重要性。
  b) 因應內外部資安事件，每月不定期進行資安宣導公告，以提升同仁資安警覺性。

- 客戶滿意: 無重大資安事件，無違反客戶資料遺失之投訴案件。
- 資訊安全政策更改：今年因應資安政策修改版本，凌巨集團資訊安全管理規範更改 2 次，GP 資訊管理辦法更改 3 次

二、重大資通安全事件

凌巨科技於民國 113 年度未有重大資安事件之發生，也未有因資安事件造成公司的損失影響。

三、資通安全風險與因應措施

在資訊科技快速變化時代，網路攻擊事件層出不窮，資安風險已成為各企業營運重要考量因素。凌巨科技股份有限公司為求公司永續發展及營運，在 2021 年成立「資訊安全管理委員會」，組織成員皆為公司各機能之高階主管，推動資訊安全相關策略訂定與執行，並定期舉辦會議，討論資訊安全管理制度實施情形，以及相關預防與矯正措施，並於會議後將資安執行成效及風險概況公告全體員工，建立「資訊安全，人人有責」之意識。

凌巨公司特別重視資安與網路風險之防範，故建構了一套多層式的資安防禦網，由外對內包含防火牆、入侵偵測、阻斷內部橫向式擴散 EDR 防禦系統、伺服器安全 7X24 小時資安專家 MDR 防禦系統、弱點掃瞄及修補程式管理。郵件防護部份，導入新式防禦系統，包含 APT 防禦、變臉防禦、郵件行為防禦、郵件防毒、及過濾垃圾信系統。在提升公司全員資安意識上，每季進行實測社交工程演練，針對資安意識較弱員工進行再教育訓練; 定期進行全體員工資訊安全訓練等。以上各種措施，都是為了確保持續提升凌巨公司的資安防禦能力。

凌巨公司已建立全面的網路與電腦相關資安防護措施，依照現有的管理制度及控制措施，病毒、木馬及蠕蟲等傳統的惡意程式及傳統的駭客外部攻擊不易對本公司資訊系統造成損害，但不能保證本公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響，故凌巨資安團隊時刻抱持謹慎嚴謹的態度，透過持續監控所有資安防禦系統結果紀錄，檢視和評估資安風險係數，針對風險較高或出現疑慮狀況，資安人員會立即採取措施，快速應變，以確保當網路攻擊發生時損失降至最小範圍。