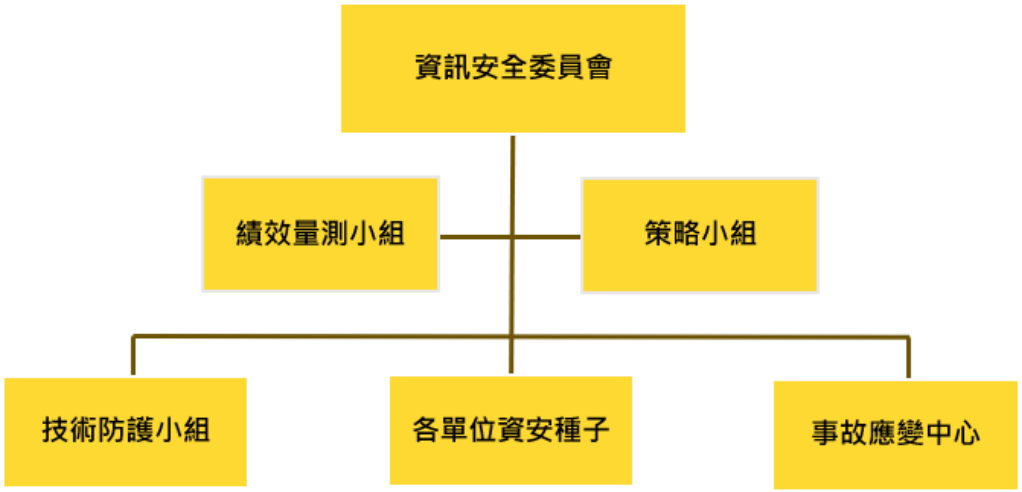
資通安全風險管理架構

力旺公司為持續強化資訊安全治理，於民國 102 年 4 月成立「資訊安全委員會」，負責制定資訊安全管理政策與規範。民國 111 年導入 ISO 27001 國際標準之資訊安全管理架構，並且擴編資訊安全推動組織，由總經理擔任「資訊安全委員會」召集人，各單位副總及一級主管擔任資訊安全委員，共同推動與督導資訊安全工作之計劃與執行成效。

資訊安全委員會每季定期開會，審查資訊安全政策執行情形並裁示、議決各項資訊安全議題 ，並且每年向董事長報告年度資訊安全推動工作之計畫與成效。稽核室亦每年對資訊安全管理作業進行查核並向董事會報告查核結果。

資訊安全推動組織架構



資通安全政策

本公司採取 ISO 27001 資訊安全管理系統 (Information Security Management System，ISMS) 之架構，作為公司建立資訊安全管理制度之基礎。依據 PDCA（Plan-Do-Check-Action）流程，以循序漸進、持續改善之原則，確保公司資訊業務運作之有效性與持續性，維護資訊資產之機密性、完整性、可用性，及各項資安作為之法規遵循性。

具體策略方案

本公司從政策推動面、管理制度面、防護能力面、意識教育面四個面向，提出具體之資訊安全策略方案:

(1) 推動資訊安全政策：力旺公司「資訊安全委員會」由總經理及各單位副總及一級主管組成，督導安全策略的規劃與執行，確保資訊安全政策之有效推動與落實。

(2) 提升資安治理成熟度：導入 ISO 27001 資訊安全管理系統，建置符合國際標準之資訊安全管理架構，本公司於 112 年 4 月取得 ISO 27001 資訊安全認證，目前證書之有效期為 112 年 4 月 5 日至 115 年 4 月 4 日。

(3) 強化技術防護能力：力旺公司參考美國國家標準暨技術研究院(NIST) 所提出網路安全框架(CSF - Cyber Security Framework) 的五大核心功能：識別(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)、復原(Recover)，同時整合 ISO 27001 管理系統的要求，全面檢視並進行資訊安全防護技術的強化。

(4) 加強人員資安意識：每年舉辦全員之“資安政策及資安意識”教育訓練課程，並且隨時掌握政府及業界最新資安與預警訊息，於重大軟體更新或資安威脅事件時，通知同仁應注意及配合事項。

投入資通安全管理之資源

本公司積極投入企業資訊安全工作，配置相關之人力資源及設備進行資訊安全制度之規劃、監控及執行，完成的措施及執行成果如下：

(1) 完成 ISO27001 資訊安全管理系統之轉版專案（ISO 27001:2022），依據 ISO27001 新版內容檢視及強化現有之資訊安全系統，並成功於 114 年 4 月正式通過 ISO27001:2022 的轉版認證。

(2) 每月定期召開資訊安全策略規劃暨執行會議，每季定期召開資安委員會議，113 年度共召開 12 次資訊安全策略規劃暨執行會議，4 次資安委員會議。

(3) 強化同仁資安防護意識，新進員工及全體員工每年進行資訊安全教育訓練及資訊安全政策宣導，以及定期舉辦社交工程釣魚郵件演練。

(4) 強化資通系統及相關設備之存取控制，進行帳號及權限盤點作業、採用最小存取權限原則、建置特權帳號管理體系、加強密碼管理機制、針對系統管理作業實行紀錄與稽核，以杜絕未授權的系統操作等。

(5) 強化公司區域網路及相關設備之防護與監控，完成網路分區架構設計，以實體防火牆設備區隔出各資訊服務區塊，將公司內重要性、風險等級不同的設備進行網路區隔，限制區域間存取權限，降低惡意程式的跨區橫向移動的風險，強化活動稽核以落實持續診斷與防範。

(6) 強化軟體及應用系統安全，制定應用系統開發維護之資安防護及控制措施，落實系統 patch 更新，即時修補高風險漏洞，定期執行弱點掃描，於系統上線前執行源碼掃描安全檢測等。

資通安全風險與因應措施

力旺電子已建立網路與電腦相關資安防護措施，並透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性。面對瞬息萬變的資訊安全威脅時，這些網路攻擊會嘗試入侵公司對外網站及郵件伺服器，進而破壞或企圖竊取公司的機密資訊，在遭受嚴重網路攻擊的情況下，可能會失去公司重要的資料，對外的聯繫也可能因此停擺。惡意的駭客亦能試圖將電腦病毒、破壞性

軟體或勒索軟體導入本公司的網路系統，以干擾公司的營運、對本公司進行敲詐或勒索。為了預防及降低此類攻擊所造成的傷害，本公司已強化網路防火牆與網路控管以防止電腦病毒跨區域擴散，依電腦類型建置端點防毒措施，並導入偵測與處理惡意軟體的解決方案。

針對特定軟體、韌體中已被公開揭露的漏洞，在企業尚未安裝修補更新或對漏洞進行防禦前，駭客或犯罪集團可能開發零時差漏洞攻擊手法或惡意程式，以取得電腦系統控制權或窺探機密資訊。為了預防及降低此類攻擊所造成的傷害，本公司已導入零時差防護軟體，在漏洞被修補前提供適當防護，防止漏洞被駭客利用。此外，公司為有效防範分散式阻斷服務（DDoS）攻擊，公司已建置對應的防護機制，避免因遭受攻擊而導致服務中斷。