## 資通安全風險管理架構：

本公司成立資通安全風險管理架構，以確保企業在數位化過程的資訊安全與風險管理。由資訊安全管理委員會和資訊安全管理小組共同構成：

**一、資訊安全管理委員會**

包括主委、執行秘書和委員，負責制定資訊安全政策，決策重大資訊安全議題，並督導執行狀況，確保企業的資訊安全政策符合最新法規及數位科技。

**二、資訊安全管理小組**

由管理組、作業組、緊急處理組及查核組組成，負責推動、管理和持續改善資訊安全管理制度，並定期向總經理與董事會報告執行情況，涵蓋從風險評估到事件應變的全流程管理。

## 資通安全政策：

公司訂有「資訊安全政策」，以確保資訊機密性、完整性及可用性。該政策透過多方面的措施與聲明，確保本公司資訊系統的安全性。具體包括：

- 保護資訊系統及相關數據，防範毀損、失竊、洩漏、竄改等風險。
- 強調與業務相關廠商及員工了解並遵守資訊安全聲明。
- 定期進行資訊安全稽核，確保內部程序符合外部規範。
- 建立專屬應變計畫，針對不同等級的安全事件制定相應的解決方案。

## 具體管理方案：

公司依據「上市上櫃公司資通安全管控指引」，採用 PDCA 循環運作模式，並參考國內外先進企業的最佳實踐，建立並持續改進資訊安全管理制度，全面強化企業數位化轉型中的安全防禦能力。具體措施如下：

**一、規劃與建立(Plan)**

1. 分析需求與風險：
   - 資產風險評估，識別潛在威脅與弱點。
   - 制定風險管理策略。
2. 制定管理規範與政策：

- 建立「資訊安全政策」。
- 制定資訊安全規範與工作流程。

3. 配置資源與組織架構：
   - 指派專責單位負責相關工作。
   - 提供必要資源與預算，確保政策執行可行性。

**二、實施與運作**

1. 資訊安全作業程序實施：
   - 部署技術防禦措施，如防火牆、入侵檢測系統 (IDS)、端點安全軟體等。
   - 執行存取權限管理，限制未授權人員進入關鍵系統或資料。
2. 教育與訓練：
   - 定期對全體員工進行資訊安全意識訓練。
   - 提供專業技能培訓給資訊安全人員。
3. 事件應變管理：
   - 制定並演練持續營運計畫。
   - 確保能快速回應、回報並減輕損害。

**三、監督與查核**

1. 內部稽核：
   - 定期檢查政策與程序執行情況，確認是否符合既定標準。
2. 外部檢測與評估：
   - 聘請第三方進行滲透測試與漏洞評估。
3. 績效評估：
   - 定期檢討關鍵績效指標，如事件數量、回應時間及資訊安全事件。

**四、維護與改善**

1. 持續改進：
   - 根據稽核結果和實際運作中發現的問題並改善。
   - 定期修訂「資訊安全政策」與相關文件。
2. 應對新興威脅：
   - 持續追蹤新型資安威脅與技術趨勢，及時更新防護策略。
   - 強化威脅情報分享機制，參與業界資安聯盟。
3. 技術升級：
   - 評估現有技術是否符合需求，必要時進行設備與系統升級。

## 資源投入與量化：

**一、資安監控與告警系統**

- 每年提列百萬元以上預算，用於導入監控系統及第三方資安服務。

**二、事件應變與演練**

每年安排至少 2 次大型資安事件應變演練，包含：

- 社交工程攻擊模擬演練，員工對社交工程攻擊的辨識成功率達 100%。
- 備份還原演練，確保數據可在緊急狀況下可在 8 小時內恢復。

**三、教育與訓練**

- 每年定期舉辦場資安訓練與宣導活動，2024 年 6 月 27 日宣導活動的員工參與率達 88.5%，內容涵蓋基礎資安知識、應變操作及針對不同職能的專業課程。

**四、資訊安全聯防與認證第三方合作**

- 積極參與國內外資安聯防組織，如 TWCERT/CC 等，每年發佈超過 12 篇資訊安全宣導文章與案例分享。
- 每年至少一次聘請外部資訊安全顧問進行滲透測試與各項系統漏洞評估。