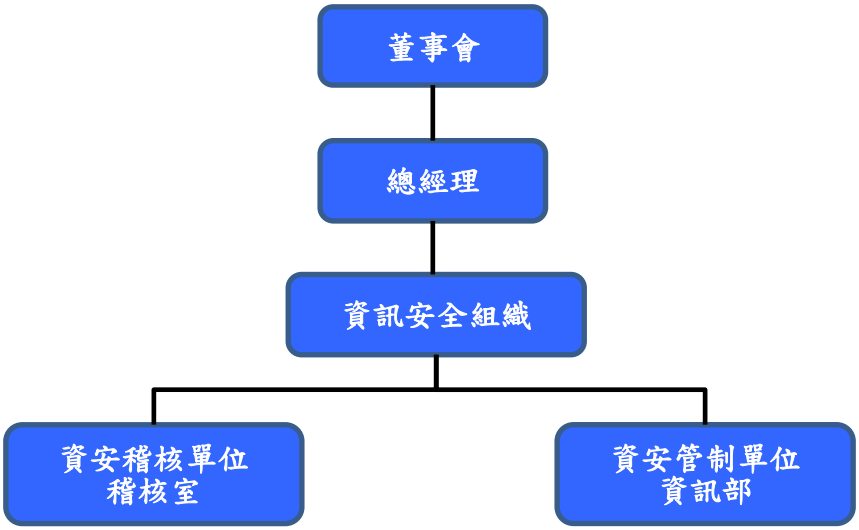
資訊安全管理架構

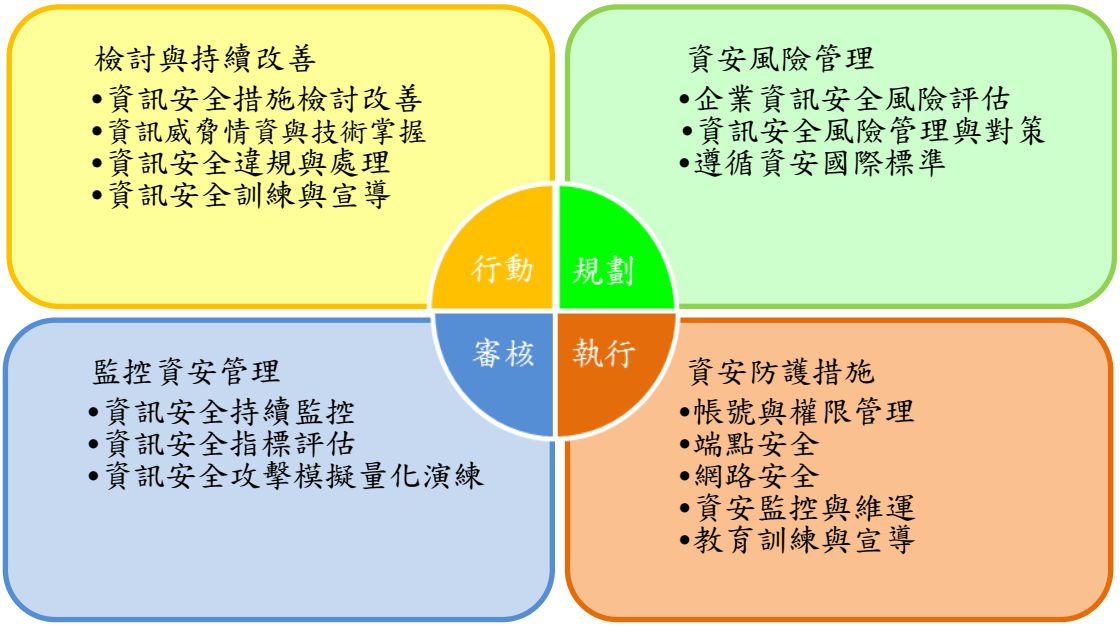
環隆科技於民國 111 年設立「資訊安全組織」，下轄資訊部，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由資訊安全組織最高主管每年向董事會彙報資安管理成效、資安相關議題及方向。每半年召開會議，檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。



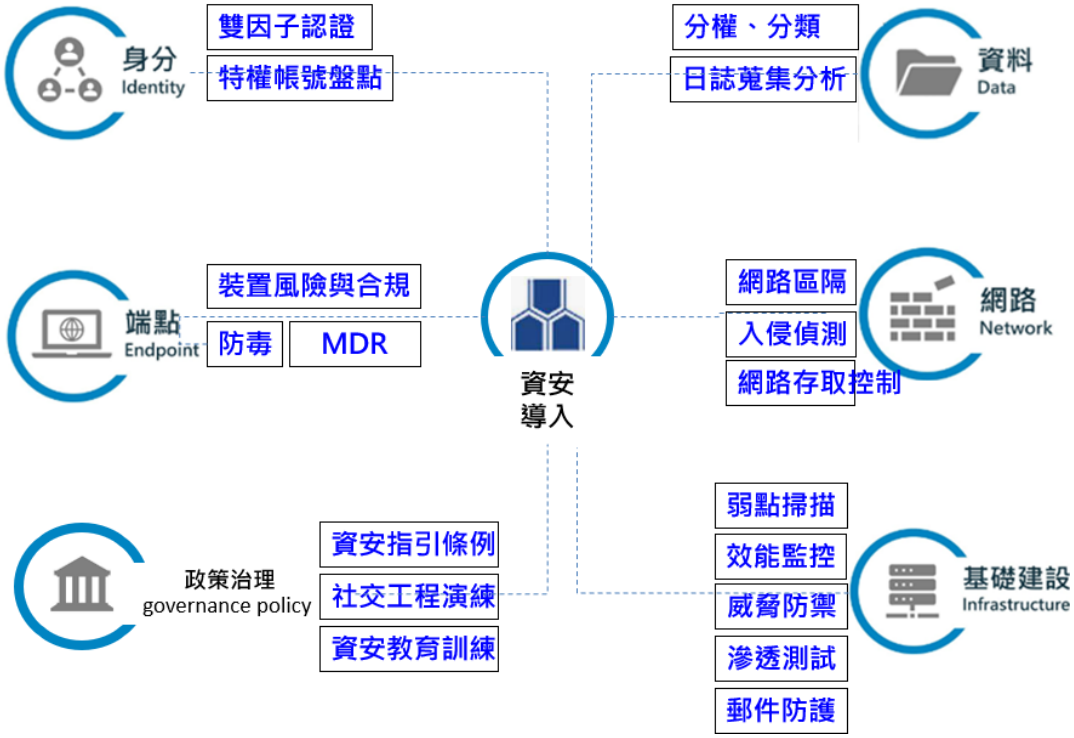
1. 企業資訊安全管理策略與架構

本公司資訊安全之權責單位為資訊部，該部設置資訊主管乙名，與專業資訊人員數名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實。每年稽核室會定期查核，若查核發現缺失，立即要求受查單位提出改善措施，且定期追蹤改善結果以降低內部資安風險，並每年定期向董事會報告資通安全管理及執行成果。

2. 企業資訊安全風險管理與持續改善架構



3. 資通安全具體管理方案



3.1 身分安全：

- 導入雙因子認證強化外部對內存取之帳號驗證安全。
- 並定期盤點特權帳號。

3.2 端點安全：

- 核心主機、電腦建置 MDR 服務，以 7*24 持續監控，防堵惡意攻擊行為。
- 依電腦類別佈署端點防毒、資產盤點與安裝權限等管制措施。

3.3 資料安全：

- 依單位制定權限存取內容、各系統依權限開放存取對應功能。
- 透過集中式管理平台保存軌跡紀錄。

3.4 網路安全：

- 導入網路存取控制(NAC)，阻斷外來設備連網。
- 強化網路防火牆控管，防止病毒跨區擴散。

3.5 基礎建設(監控、維運)：

- 建置系統、網路監控平台、異常告警服務。
- 定期執行弱點掃描，安全漏洞修補與滲透測試。
- 導入郵件防護過濾，提高郵件安全。

3.6 治理政策：

- 設立資安稽核組，以資安指引訂定與檢討資安政策與目標，並定期向董事會報告。
- 定期舉辦資安教育訓練與郵件社交工程演練，提供員工資安意識。

4. 投入資通安全管理資源

政策 **7 規範**

新增修訂 7 個資安規範
民國 112 年 7
民國 111 年 2
民國 110 年以前 4

資安委外服務

- 核心系統建置 MDR 7*24 監控服務，防堵惡意攻擊行為。
- 對外系統滲透測試與漏洞修補。

訓練/宣導

112 年度所有新進員工皆完成資訊安全教育訓練課程，共 **176** 名新進人員。

6 次電子郵件社交工程演練

執行 6 次電子郵件社交工程釣魚郵件演練，演練人數超過 **700** 人

資安防護 112 年資通安全防護總投資超過 **360** 萬

- 111 年成立資安專責小組，並定期開會討論資安架構，開會次數超過 **35** 次。
- 強化防火牆區域管理：導入 Server 區、產線區規則存取管理，並啟用 IPS 入侵防護。
- 啟用 VPN 雙因素認證：強化外部對內存取之帳號驗證安全。
- 網路存取、電腦管理：導入 Pixis、Forescout 合規平台，強化端點存取安全。
- 核心系統雲端備份建置。

5. 資通安全風險與因應措施

依據內部資訊安全事故管理流程，評估資安相關風險等級並採取應對風險管理方案及定期檢討，環科建置多層次防禦網，由外而內包含防火牆、入侵偵測、防毒系統、弱點掃描及修補程式管理等，並定期委外資安廠商進行滲透測試，以確保持續提升資安防禦能力。