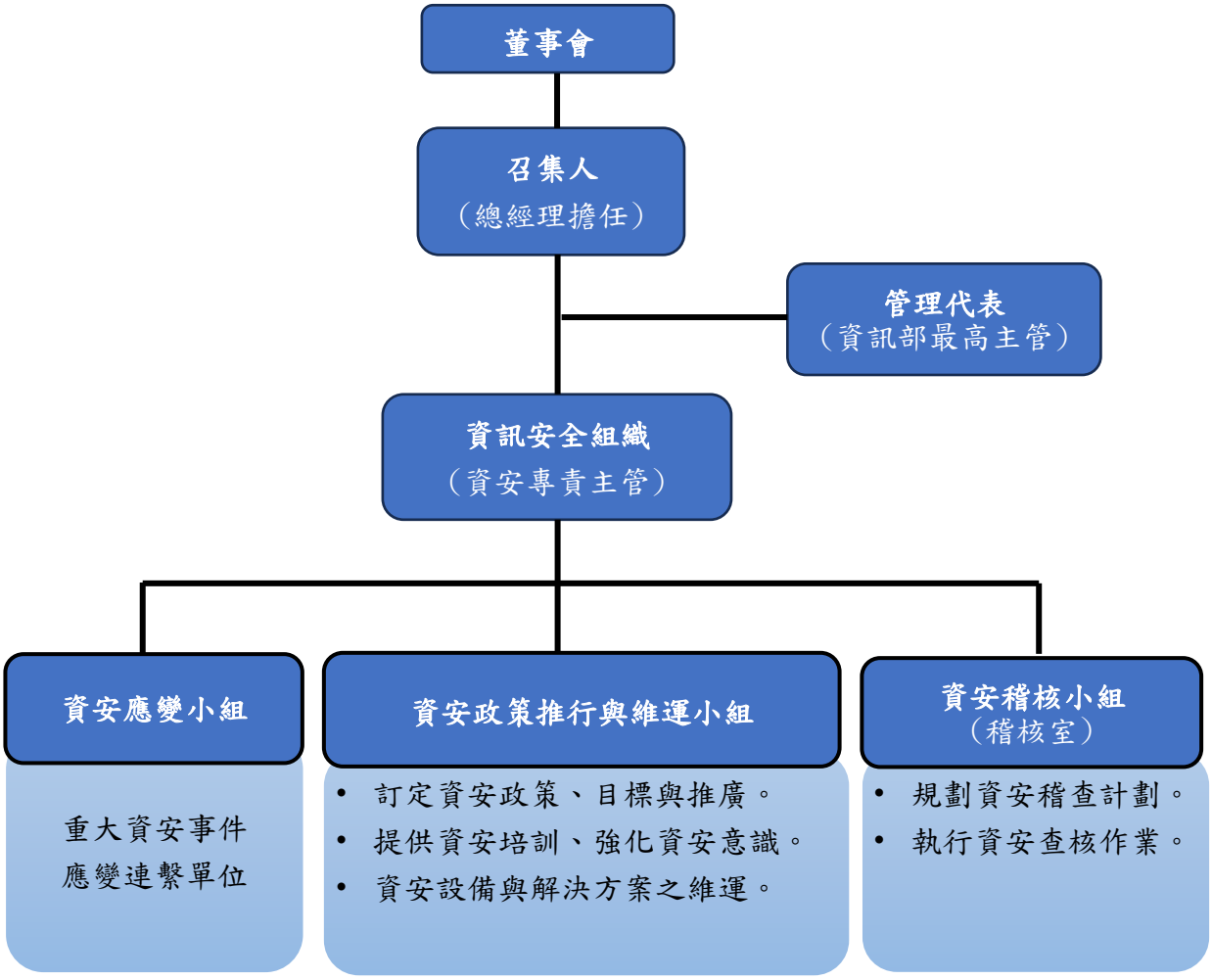
資訊安全管理架構

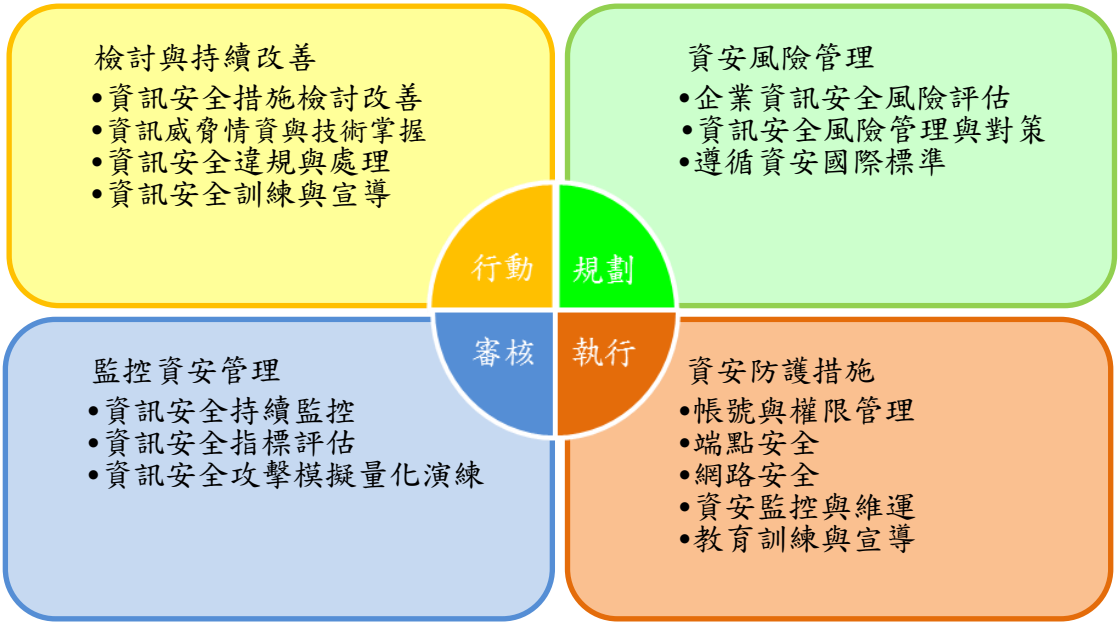
環隆科技於民國 111 年設立「資訊安全組織」，下轄資訊部，負責資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由總經理擔任召集人負責本系統管理審查資通安全相關會議，管理代表擔任副召集人召開與主持本系統管理，資安專責主管負責資安管理的範疇、政策；資安推行小組主要確保資安任務及作業正常運行，包含應變小組、政策推行與維運小組及資安稽核小組，同時每年進行資安風險評估、識別並降低潛在威脅。



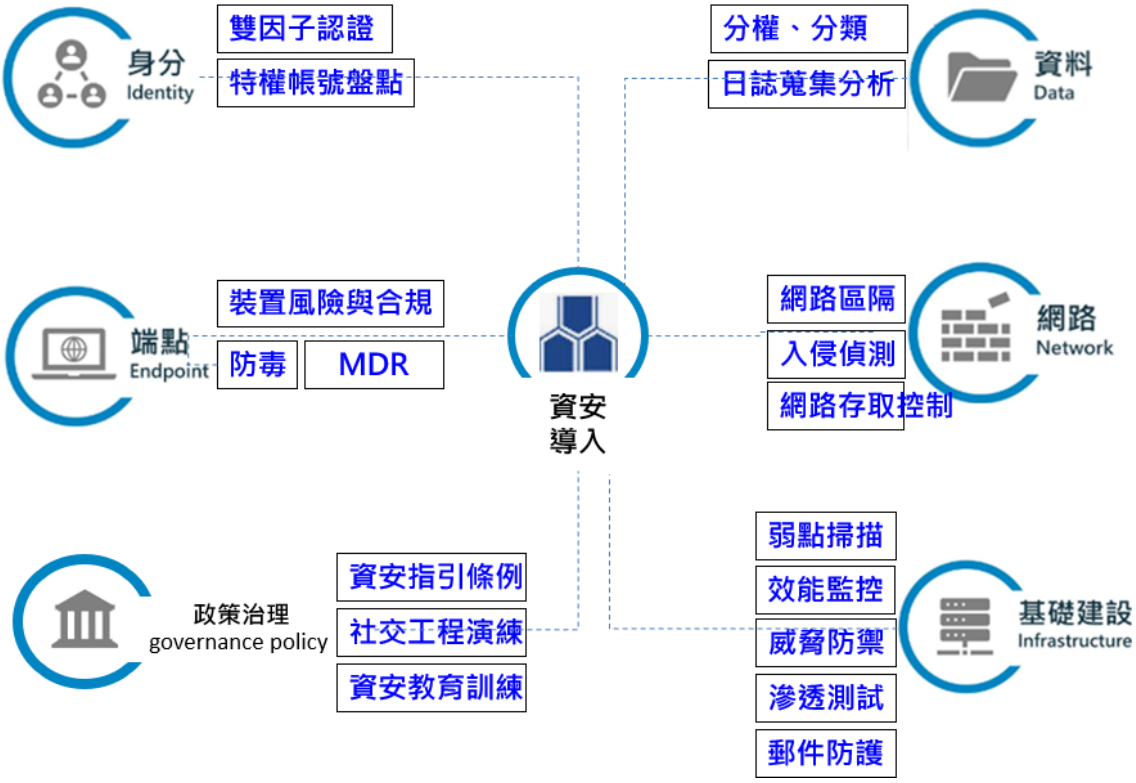
1. 企業資訊安全管理策略與架構

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，以金管會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

4.1 資安會議定期開會討論資安議題，114 年度開會次數超過 24 次。
4.2 截止 114 年底本公司未有因重大資安事件所遭受之損失之情事。
4.3 進行全員資安教育訓練與社交工程釣魚測試，以提升資安意識。

- 114 年共計 43 名新進員工參與資安教育訓練，完成率 100%。
- 114 年度全廠資安教育訓練上課人數共計 45 名。
- 資安月提升安全意識訓練，受訓人數 46 名。

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。