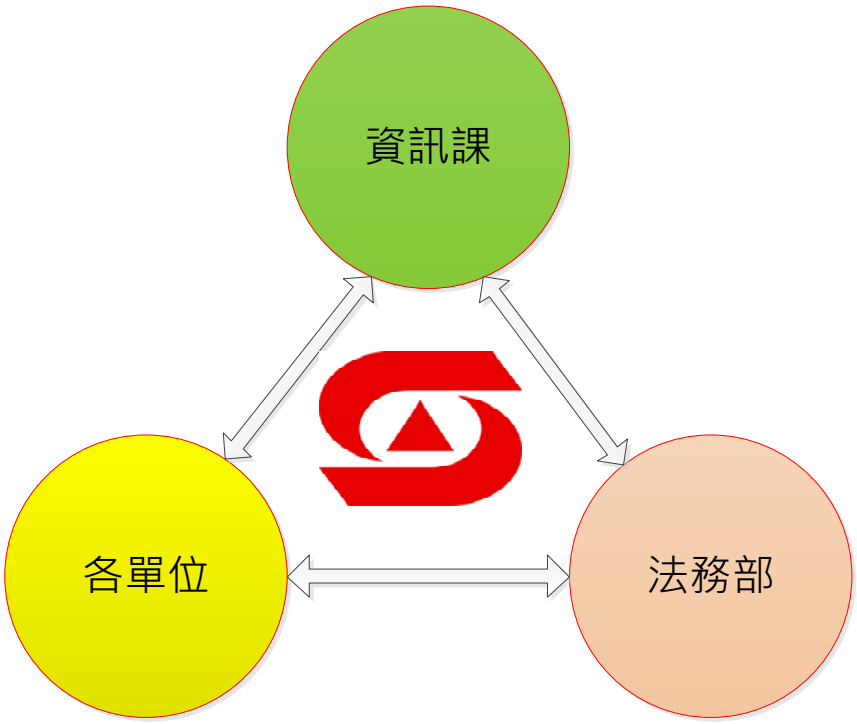
# 資訊安全管理架構說明

## 資訊安全風險管理架構

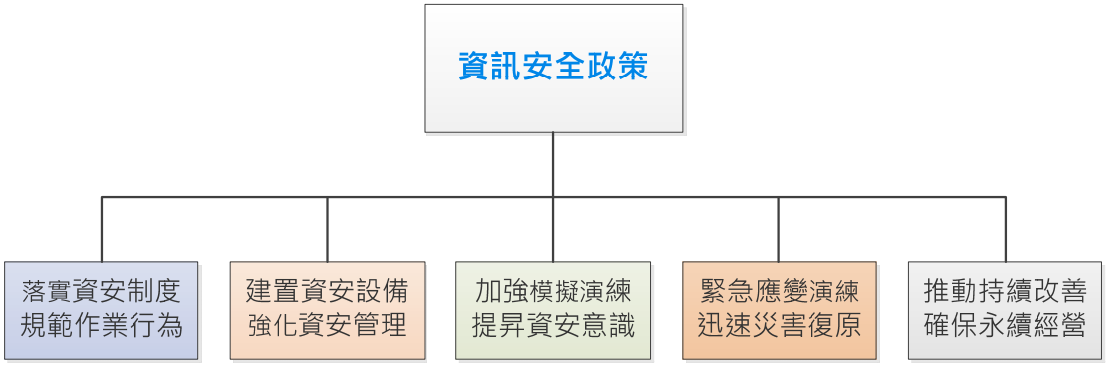
本公司資訊安全之權責單位為總管理處資訊課，負責規劃、執行及推動資訊安全管理工作，推展員工對於資訊安全意識。

本公司資訊安全之稽核單位為法務部，負責安全監控管理之查核，若查核發現缺失，立即要求其單位提出相關改善計畫並呈報，且定期追蹤改善成效，以降低內部資安風險。

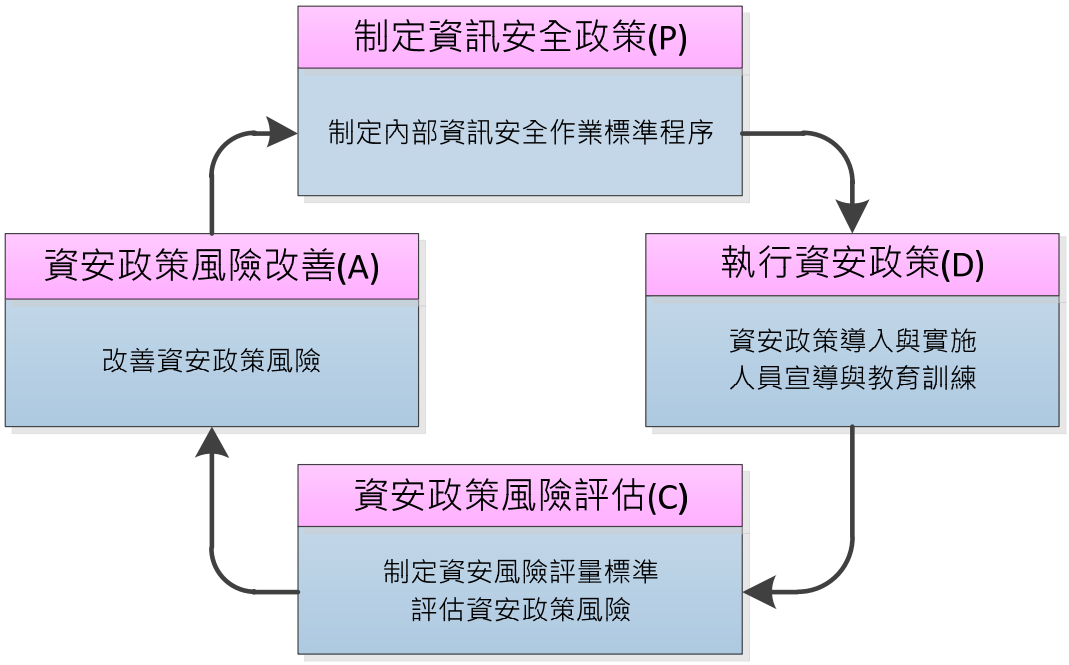



## 資訊安全政策

為確保公司資訊之機密性、完整性與可用性，避免遭受各種威脅，降低對企業之傷害，提昇企業投資報酬率及商機，並達到永續經營目的, 而制定資訊安全政策



針對資訊安全之工作按制定政策、執行、查核與行動來進行活動，以確保資訊安全可靠度之目標達成




**資訊安全管理措施，如下：**

| 資訊安全管理措施 | | |
|---|---|---|
| **管理措施** | **說明** | **作業方式** |
| **權限管理** | 人員帳號、權限管理之管理 | 人員帳號權限管理與審核 |
| | | 人員帳號權限定期盤點 |
| **存取管控** | 人員存取內外部資料之控管 | 內/外部存取管控措施 |
| | | 人員帳號存取設定 |
| **外部威脅** | 內部潛在弱點、中毒管道之防護措施 | 主機/電腦弱點檢測及更新措施 |
| | | 防火牆政策管理 |
| | | 病毒防護與惡意程式檢測 |
| | | 情境模擬演練 |
| **系統可用性** | 系統可用狀態與服務中斷時之處置措施 | 即時監控系統/網路狀態 |
| | | 服務中斷之應變標準程序 |
| | | 資訊備份機制 |
| | | 定期災害復原演練 |