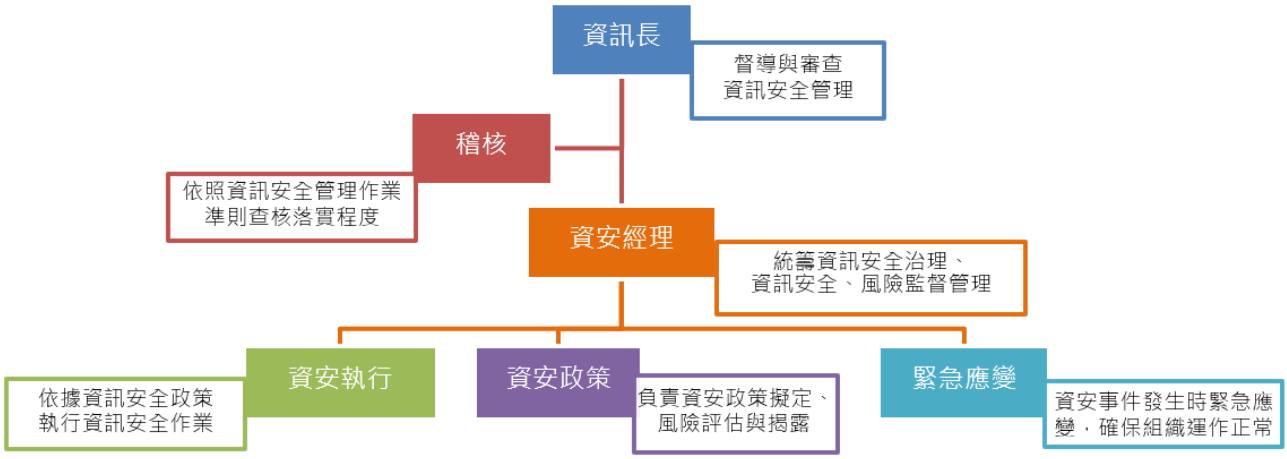
資通安全管理

(一) 敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

(1)企業資訊安全管理組織：

為加強資訊安全風險管理，本公司成立了資訊安全部門對資安風險進行專責管理與管制，其組織架構與各小組執掌如下：



(2)企業資訊安全管理策略與架構：

本公司為確保公司營運及客戶資訊之機密性、完整性及可用性，參考政府各項法規、ISO 標準、客戶稽查與業界實務，制定公司「資訊安全管理政策」，將相關規範與作業程序納入本公司內部管控制度，並依此為依據每年進行年度稽核，以降低公司面臨之內外部資安風險。

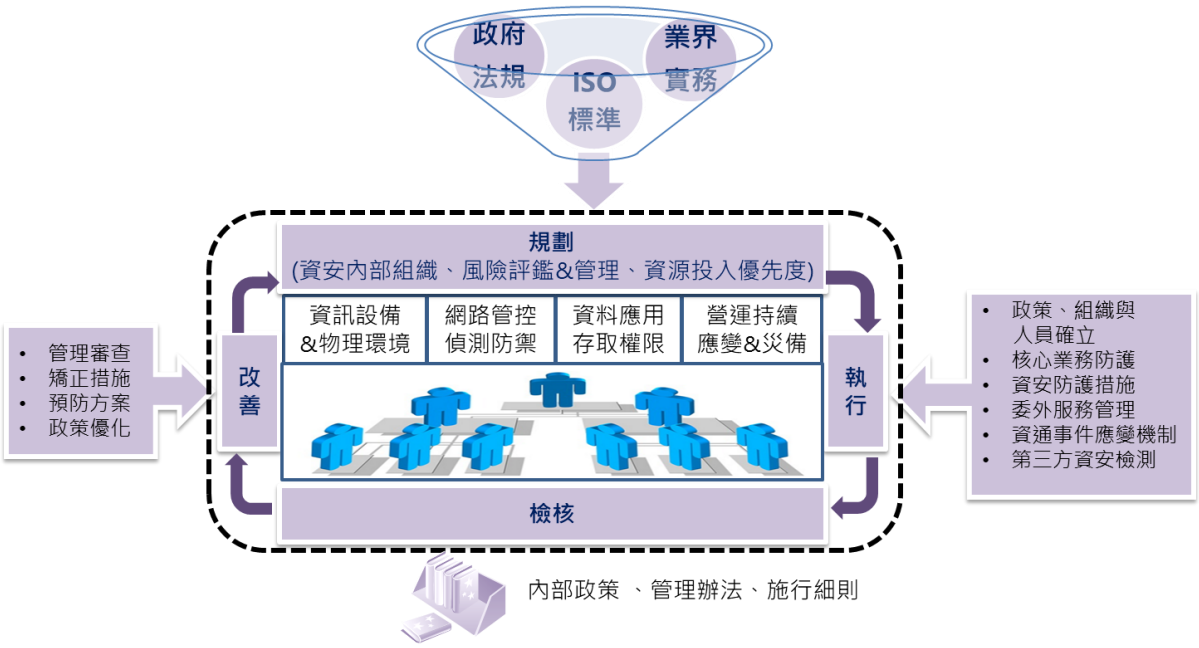
在資訊安全管理政策方面，依據規劃、執行、檢核與改善(Plan-Do-Check-Action)的管理循環機制，對資訊設備&物理環境、網路管控偵測防禦、資料應用存取權限、營運持續應變與災難備援等多方面設計公司安全架構，以求確實執行資安防護並落實資安風險監督與管理，達到公司內各系統能安全、穩定、高效提供服務。

1.「規劃階段」著重資安內部管理機制的建立，落實資安風險管理並制定出資安方案實施優先度計劃，從系統面、技術面、程序面降低企業內外部資安威脅，除提高公司資安管理強度外也達到客戶資安要求。

2.「執行階段」著重核心業務識別及防護，執行公司資安管理計劃，落實委外服務管理，定期進行企業營運持續計劃演練以確保遭受攻擊時能以最短時間、最小損失回復公司核心業務；定期委託第三方進行資安完整度檢測，以維護公司及客戶重要資訊資產的機密性、完整性及可用性。

3.「檢核階段」著重資安管理成效的審查，依據查核結果進行資安管理指標的持續優化。

4.「改善階段」以檢討及持續改善為本，著重資安政策的調整，依據資安管理審查及執行結果進行政策優化，確保資安管理政策能符合公司及客戶所需。



(3)具體管理方案：

1.「資訊設備使用管理」方面：建立資訊設備生命週期管理且落實執行，定期對資訊設備進行盤點以明確保管與使用責任。終端設備加強病毒的防範與資產管理管控，以確保其可用性。

2.「物理及實體環境」方面：對實體環境進出與設備可用度管理依相對應管理政策進行，以確保資訊系統能在安全、穩定的環境下持續提供服務。

3.「網路管控與偵測防禦」方面：從網路基礎設施、網通設備管理、傳輸等層面落實管控，以防杜來自網路層面的外部攻擊以降低資料外洩風險。集團對外網路皆有防火牆進行防禦，內部網路傳輸也加強網路管控與偵測防禦以降低駭客攻擊的風險。

4.「資料應用存取權限」方面：從系統開發、系統存取權限、系統備份與維護等方面進行管理，確保系統從評估到上線階段皆能在有效的管控機制下執行，並留下相關紀錄以供後續進行系統優化及維護；同時對委外廠商服務進行管理，在如期如質的要求下達到資料安全。

5.「營運持續與災難備援」方面：為提高公司資料與資訊系統可用性，於本年度強化集團資訊備份策略與作法，重新檢視各項備份標的、頻率與回復機制，關鍵系統並建立異地備援，以降低因系統問題或外部攻擊所造成公司營運的影響。建立業務持續運作管理機制，並定期測試演練，維持其可用性並降低公司營運之風險。

6.「人員管理」方面：依員工日常與專案之工作職掌授予其完成工作或業務所需之必要資訊存取權限，並定期審查以確認無權限衝突或過大之情事發生。人員晉用進行必要之考核與簽署相關作業規範，並參與資訊安全教育訓練，以讓員工充分瞭解資訊安全為應盡之義務；同時不定期進行資安宣導與教育訓練，讓資安意識落實於日常工作中。

(4)本公司資訊安全目標：

1. 符合法規法令之要求、主管機關命令以及客戶契約或專業職責等要求。
2. 客戶資料的保護及保存，以防止人為意圖不當與不法情形。
3. 確保提供服務的持續性與及時性。
4. 確保提供資料之正確與完整性。

(5) 112 年度資訊安全實施成果：

1. 集團防火牆成功阻擋約 120 萬次攻擊與威脅試探，平均 10 萬次/月。
2. 垃圾郵件防護成功攔截約 3.6 萬封病毒威脅郵件，平均 3 千封/月。
3. 終端設備防毒軟體，成功發現並阻擋近 7 千筆病毒及間諜程式攻擊。
4. 集團進行社交工程演練，有效提高員工資安意識。
5. 集團內部資安宣導 4/次；外部研討會參與 15/次。

(6)資安政策：

勤誠為加強資訊安全風險管理，成立了資訊安全部門，並指派 2 位專責人員對資安風險進行管理與管制。

且編列並執行多項資訊安全方案，以落實與優化公司內部資訊政策。