2020

龍巖資訊安全風險管理架構

資訊處-網路系統部

資訊安全風險管理架構

資訊安全
組織架構

資安政策擬定
與執行推動

資訊安全
風險評估

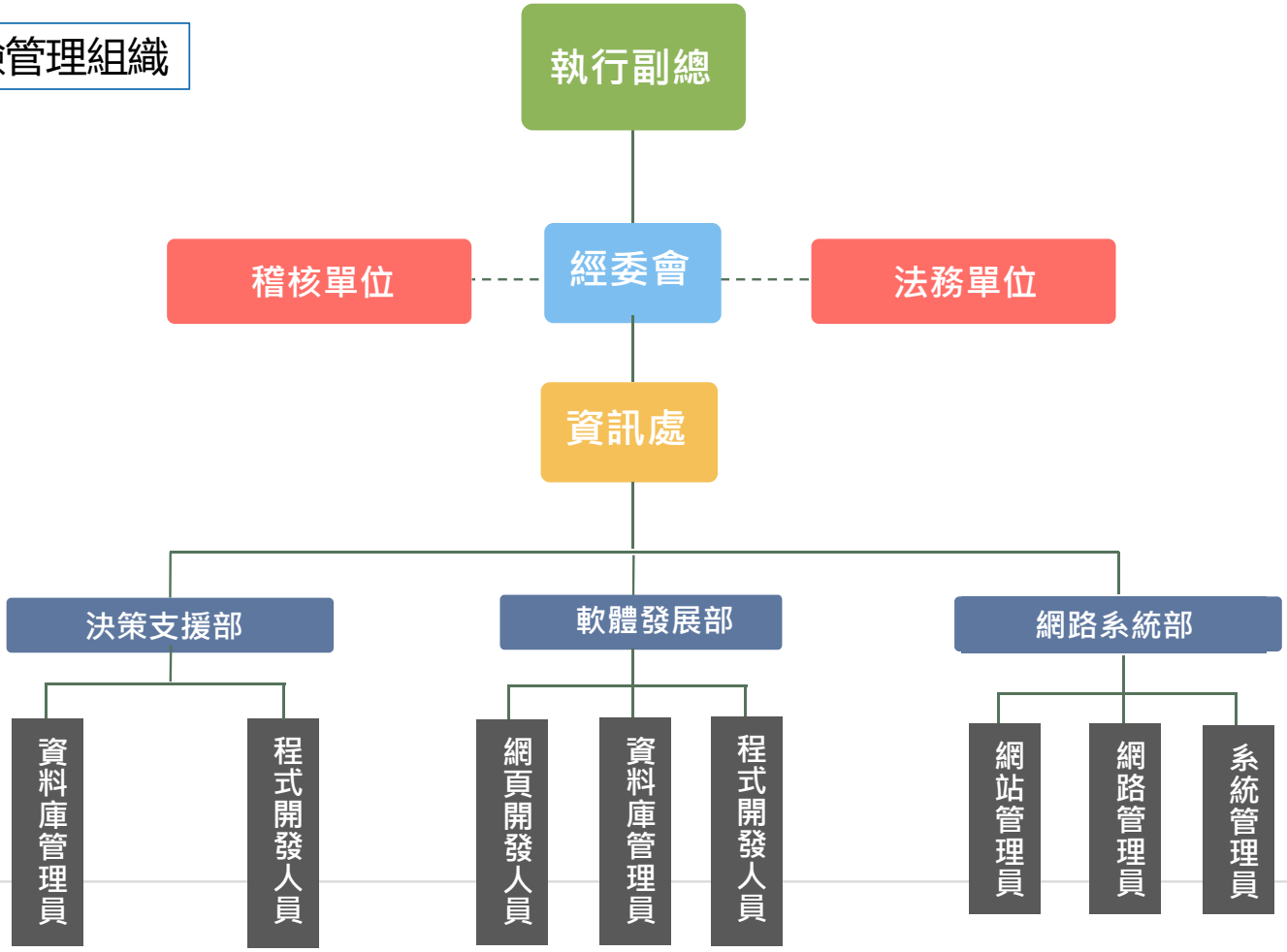
資訊安全
持續改善

資訊安全風險管理架構

- 本公司資訊安全之權責單位為資訊處，負責規劃、執行及推動資訊安全管理項目，推展資訊安全意識，並依。
- 本公司稽核室為資訊安全之查核單位，若查核發現缺失，可要求受查單位提出相關改善計畫並定期追蹤改善成效，以降低資安風險。
- 組織運作模式-資訊單位：規劃執行與改善、稽核單位：查核追蹤、各單位：資安作業配合與問題通報。
- 資訊安全管理模式採 PDCA（Plan-Do-Check-Act）循環式管理，確保資訊安全作業推動、風險控管與持續改善。

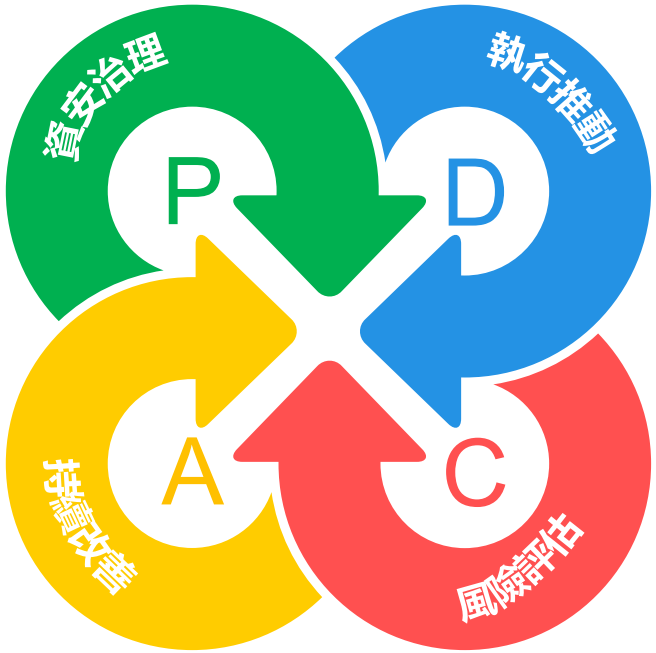
資訊安全風險管理架構

資訊安全風險管理組織



資訊安全風險管理架構

資訊安全管理模式

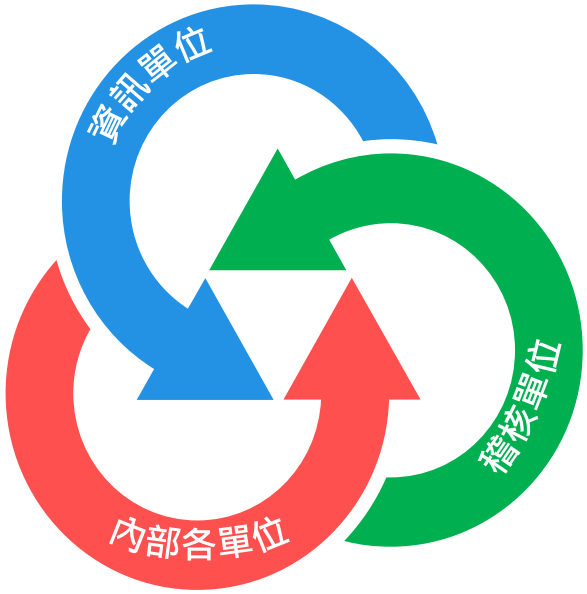


資安治理 (Plan)
- 擬定公司資安政策
- 制訂資訊安全作業

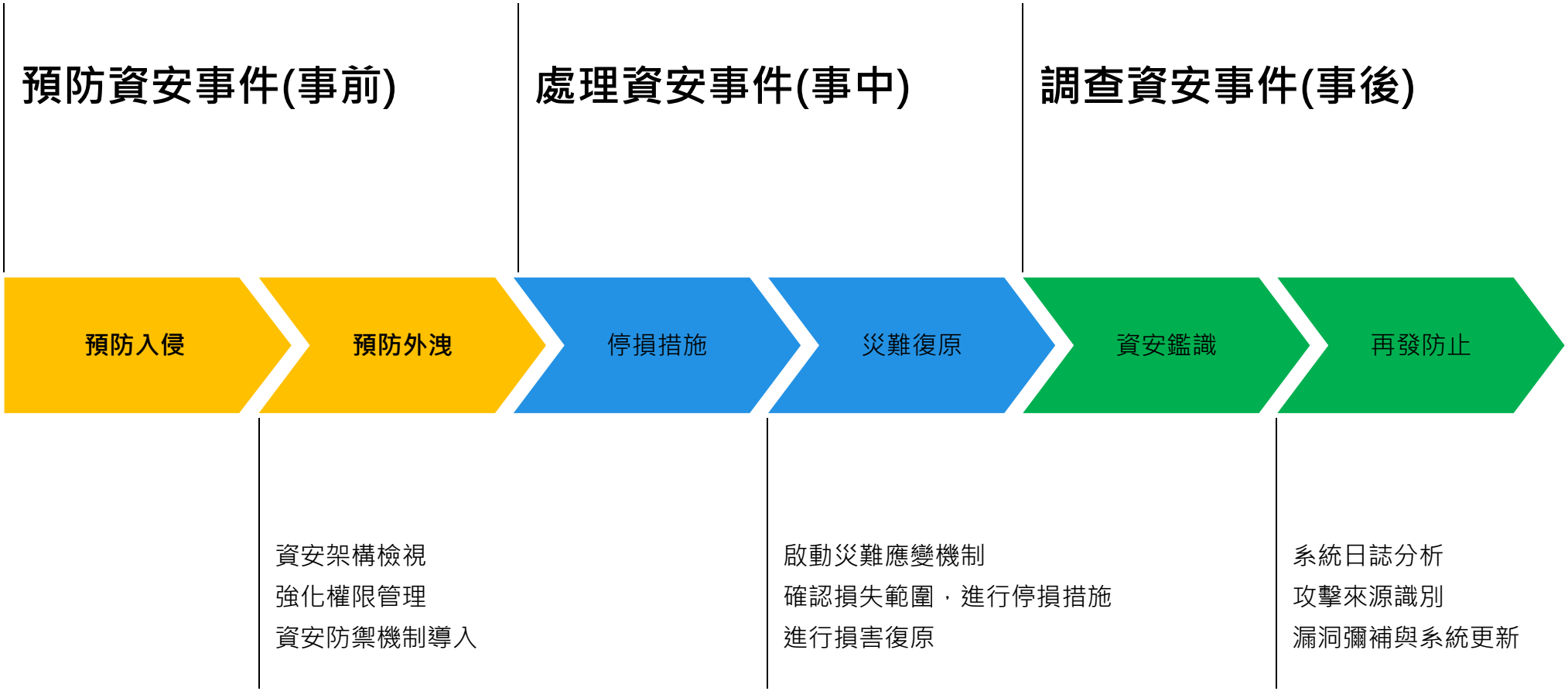
執行推動 (Do)
- 資安政策宣導與教育訓練
- 資安措施施行與導入

風險評估 (Check)
- 內部資安風險再評估
- 定期稽核

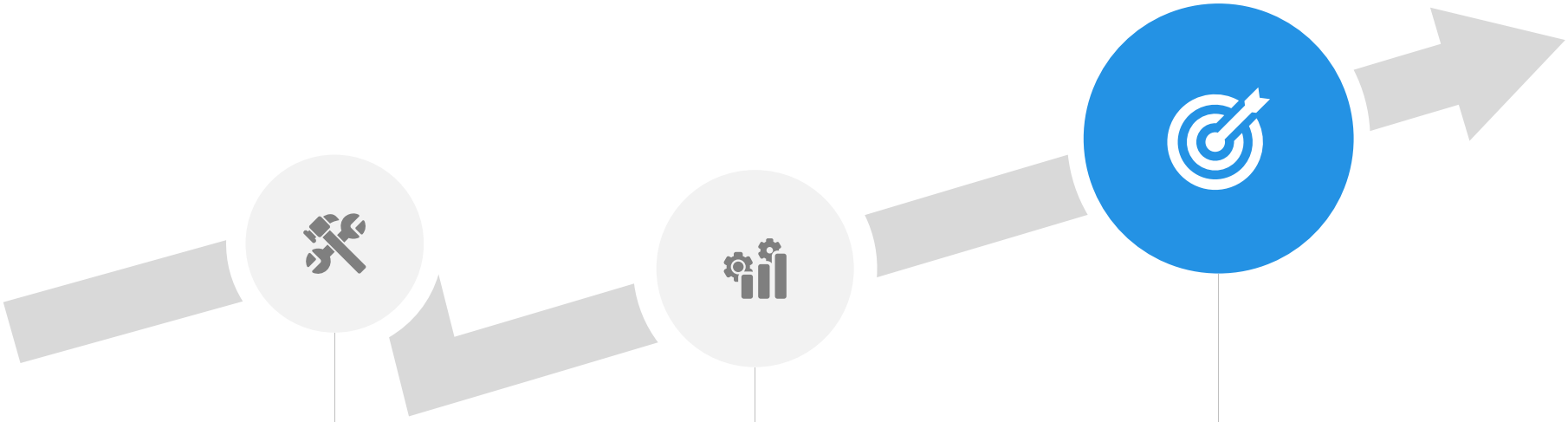
持續改善 (Act)
- 重新審視新的資安風險
- 引進外部解決方案



資訊安全風險管理架構


預防資安事件(事前)
處理資安事件(事中)
調查資安事件(事後)
預防入侵
預防外洩
停損措施
災難復原
資安鑑識
再發防止
資安架構檢視
強化權限管理
資安防禦機制導入
啟動災難應變機制
確認損失範圍，進行停損措施
進行損害復原
系統日誌分析
攻擊來源識別
漏洞彌補與系統更新

資訊安全風險管理架構



短期

優先處理緊急項目

- 資料存取依權責區分設立權限。
- 網路攻擊設置防火牆阻擋。
- 各端點防毒
- 資料備份與存放管理。
- 補系統漏洞。

中期

強化重要資安架構

- 建立系統異地備援機制。
- 系統與網路監控機制建立。
- 建立災難復原機制。
- 高風險系統導入雙因子驗證機制。
- 機敏資料分級與存取稽核。

長期

持續檢討與改善

- 定期資安健診並依結果改善。
- 人員資安意識教育訓練。
- 資訊安全檢核作業與標準。
- 持續改善。

- 藍色代表已執行
- 綠色代表執行中
- 黑色代表未來計畫執行