

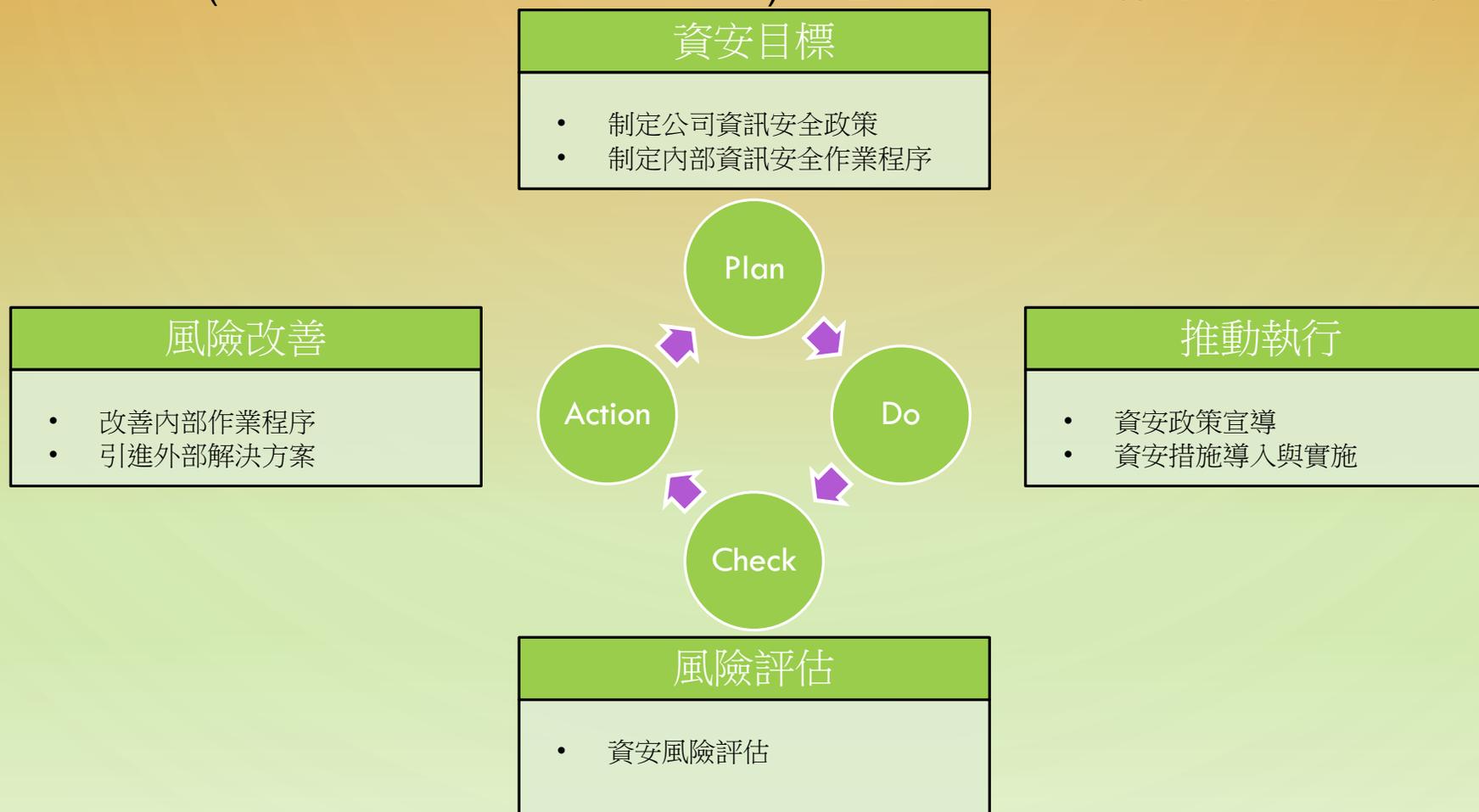


資通安全管理

2025/10

資通安全風險管理策略及架構

- 資通安全是本公司長期以來重視、關注的重要工作之一，為確保各項資通安全管理作業有效落實，並及早發現不正當之行為與安全漏洞威脅，早期識別可幫助阻止不法行為並盡可能減少潛在的風險。
- 公司採用PDCA (Plan → Do → Check → Action) 管理循環模式以確保可靠度目標達成且持續改善。



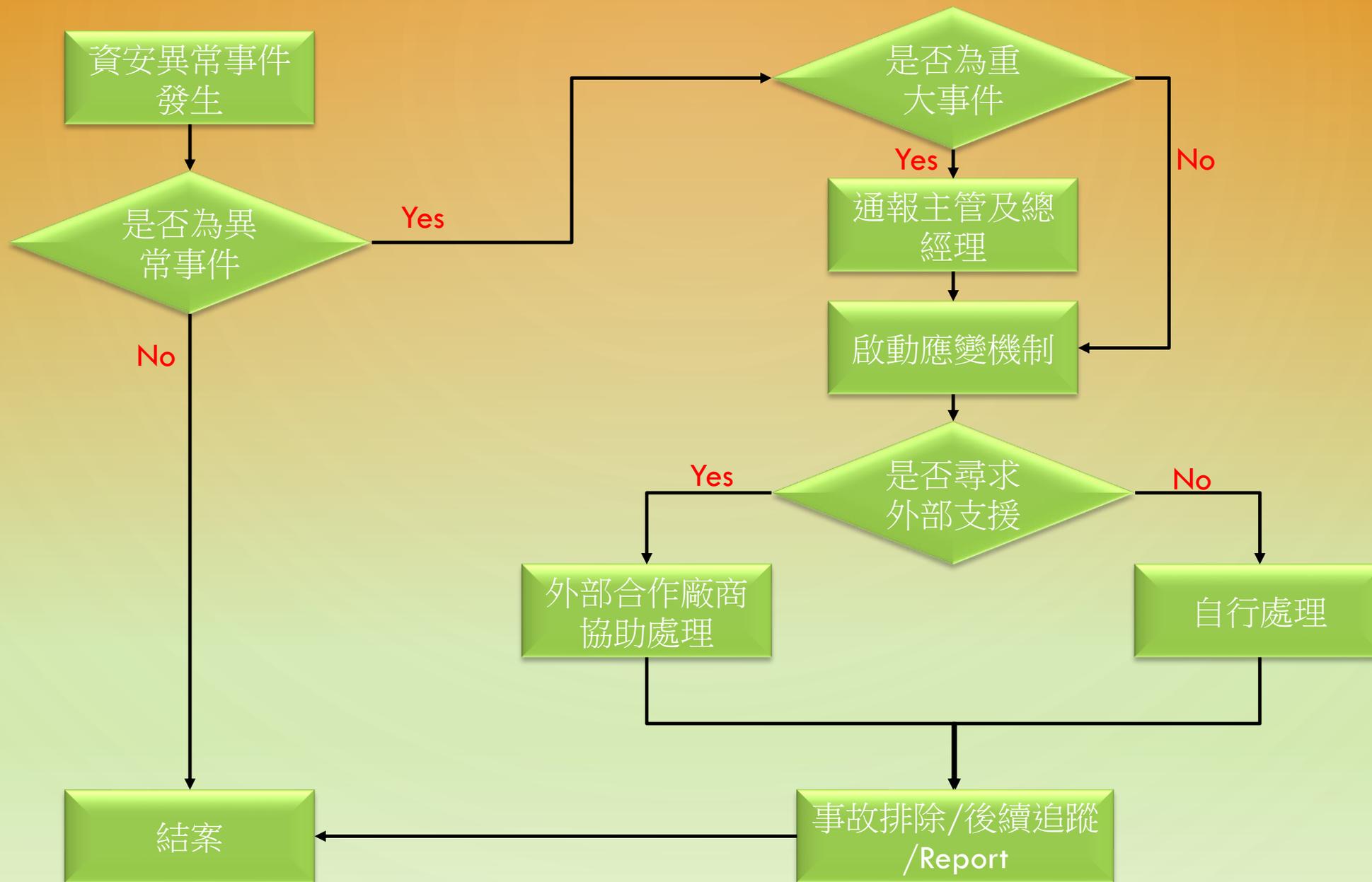
資通安全管理措施

- 本公司對於資通安全控管相當重視，在資通安全方面採行以下具體措施管理：



類型	項目	防範目的	相關作業說明
員工管理	<ul style="list-style-type: none"> 資通安全宣導 	<ul style="list-style-type: none"> 預防降低中毒機率 	<ul style="list-style-type: none"> 定期對於員工進行國內外重大資安異常事件案例分享。
裝置控管	<ul style="list-style-type: none"> 防毒軟體 非信任裝置阻擋 	<ul style="list-style-type: none"> 預防中毒 	<ul style="list-style-type: none"> 系統判定符合規範之電腦才給與網路連接權限。 非經公司許可之電腦設備嚴禁接入公司網路，如有未經許可之設備接入將無法使用網路。
權限管理	<ul style="list-style-type: none"> 專案權限控管 	<ul style="list-style-type: none"> 避免帳號冒用 	<ul style="list-style-type: none"> 各研發專案皆有嚴格權限控管，專案成員需提出表單申請，經主管同意後由資訊管理人員設定存取權限，並且每半年進行一次存取權限覆核，以確保權限管理之正確性。
資料管理	<ul style="list-style-type: none"> 專業型儲存設備 本地備援架構 異地資料備份 	<ul style="list-style-type: none"> 避免資料遺失 	<ul style="list-style-type: none"> 專業型儲存設備具有高可用性的備援能力，專案研發資料皆有權限控管，僅允許授權成員進行存取。 公司研發資料有完整的定期備份機制。 採取異地存放，以確保災難發生時的復原能力。
輸出管理	<ul style="list-style-type: none"> 專用資料空間 傳輸監控 	<ul style="list-style-type: none"> 避免資料外洩 	<ul style="list-style-type: none"> 提供予客戶的資料，由資訊人員上傳至專用空間，並限制僅由客戶所提供之特定IP做連線。 對有異常行為之帳號進行監控，並複製存取紀錄。 除特定需求且經過申請之人員外，嚴格封鎖相關網路磁碟與空間的存取。

資通安全異常事件處理程序



資訊安全規劃

類型	年度	項目	規劃目的
帳號管理	2026	<ul style="list-style-type: none">多因子驗證 (Multi-factor authentication, MFA)	<ul style="list-style-type: none">上市櫃公司資通安全管控指引及個資法，皆述明需導入多重驗證機制 (第五章 第十三條)降低帳號被盜及非法登入的風險最低資安管控標準
資料管理	2026	<ul style="list-style-type: none">資料遺失防護 (Data Loss Prevention, DLP)	<ul style="list-style-type: none">網路傳輸封包檢查監控和保護本地機敏資料資料存取完整記錄(第五章 第十三條)
資安認證	2026	<ul style="list-style-type: none">資訊安全管理國際標準 (ISO 27001)	<ul style="list-style-type: none">資安事件監控、識別、分析、告警與資訊安全情報集成，用以識別已知和未知的安全威脅(第六章 第十八條 第七項)
系統管理	2026	<ul style="list-style-type: none">弱點掃描 (Vulnerability Scanning)滲透測試 (Penetration Testing)	<ul style="list-style-type: none">定期辦理弱點掃描/滲透測試系統上線前執行源碼掃描安全檢測(第五章 第十六條)
訊息管理	2027	<ul style="list-style-type: none">安全資訊與事件管理 (Security Information and Event Management, SIEM)資安協調、自動化和響應 (Security Orchestration, Automation, and Response, SOAR)	<ul style="list-style-type: none">資安事件監控、識別、分析、告警與資訊安全情報集成，用以識別已知和未知的安全威脅(第六章 第十八條 第七項)