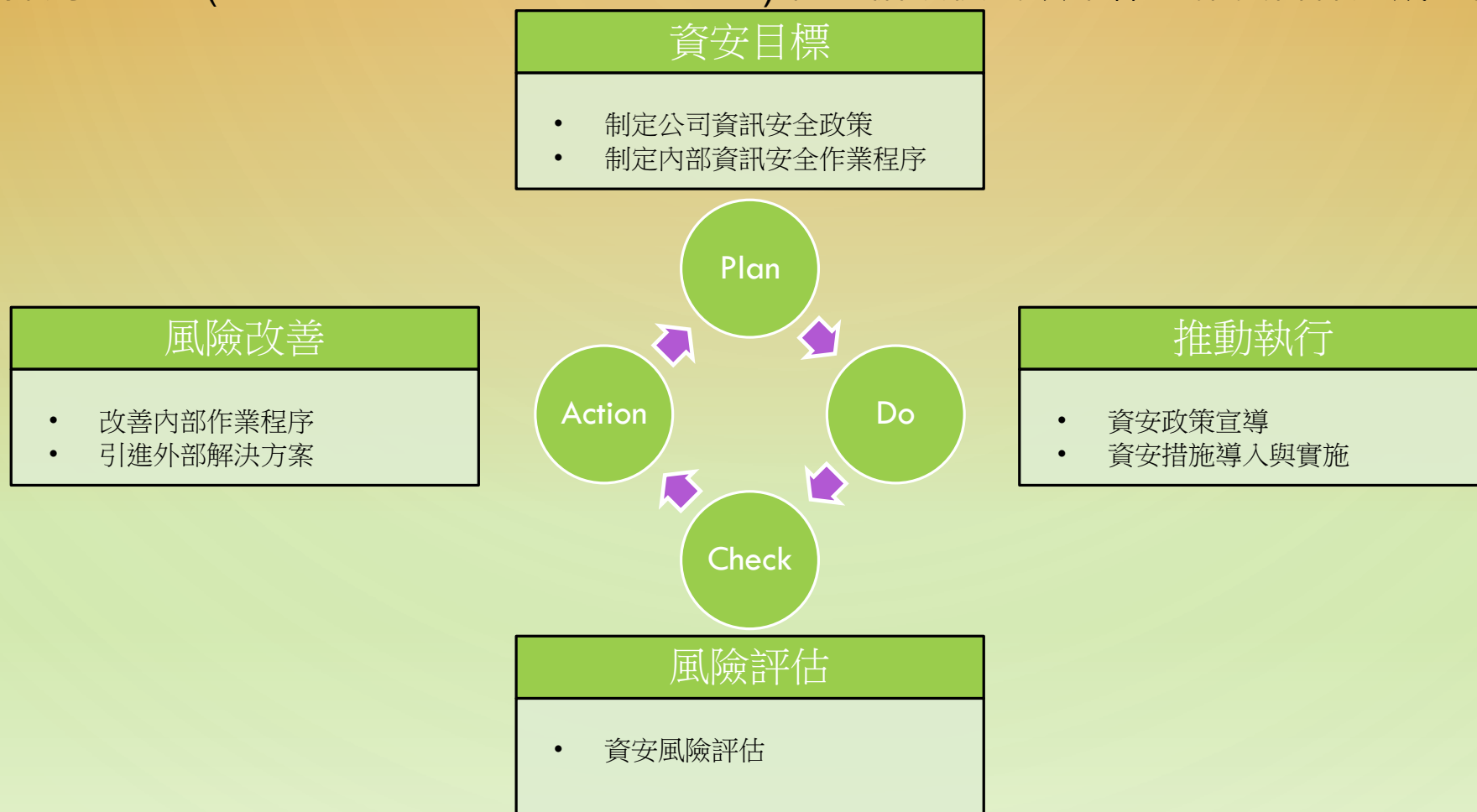
A decorative graphic on the left side of the slide, consisting of a network of light blue lines and small circles, resembling a circuit board or a stylized tree structure, extending from the top to the bottom.

# 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。



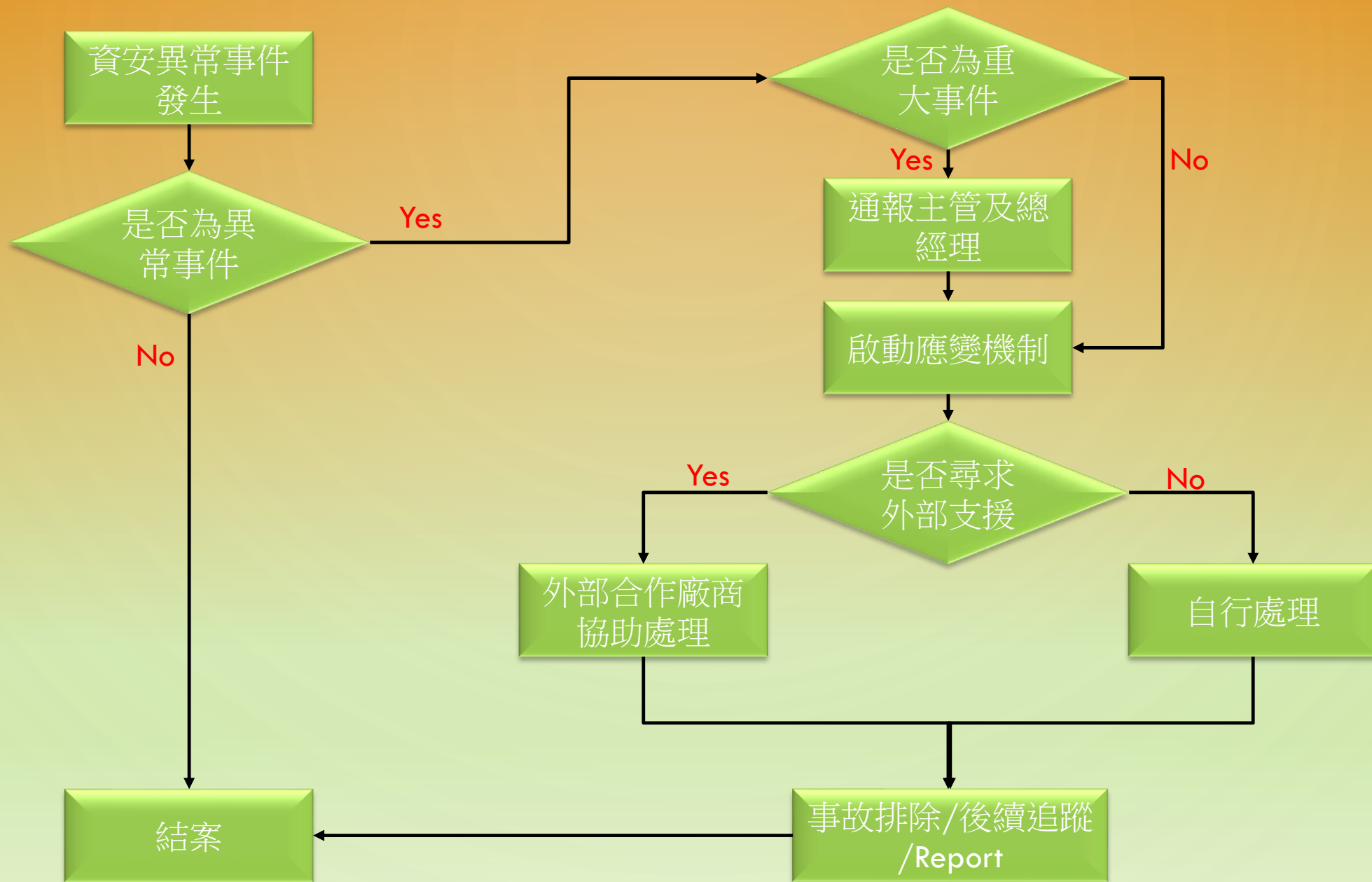
# 資通安全管理措施

- 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"> <li>資通安全宣導</li> </ul>	<ul style="list-style-type: none"> <li>預防降低中毒機率</li> </ul>	<ul style="list-style-type: none"> <li>定期對於員工進行國內外重大資安異常事件案例分享。</li> </ul>
裝置控管	<ul style="list-style-type: none"> <li>防毒軟體</li> <li>非信任裝置阻擋</li> </ul>	<ul style="list-style-type: none"> <li>預防中毒</li> </ul>	<ul style="list-style-type: none"> <li>系統判定符合規範之電腦才給與網路連接權限。</li> <li>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。</li> </ul>
權限管理	<ul style="list-style-type: none"> <li>專案權限控管</li> </ul>	<ul style="list-style-type: none"> <li>避免帳號冒用</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> </ul>
資料管理	<ul style="list-style-type: none"> <li>專業型儲存設備</li> <li>本地備援架構</li> <li>異地資料備份</li> </ul>	<ul style="list-style-type: none"> <li>避免資料遺失</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>公司研發資料有完整的定期備份機制。</li> <li>採取異地存放，以確保災難發生時的復原能力。</li> </ul>
輸出管理	<ul style="list-style-type: none"> <li>專用資料空間</li> <li>傳輸監控</li> </ul>	<ul style="list-style-type: none"> <li>避免資料外洩</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>對有異常行為之帳號進行監控，並複製存取紀錄。</li> <li>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。</li> </ul>

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