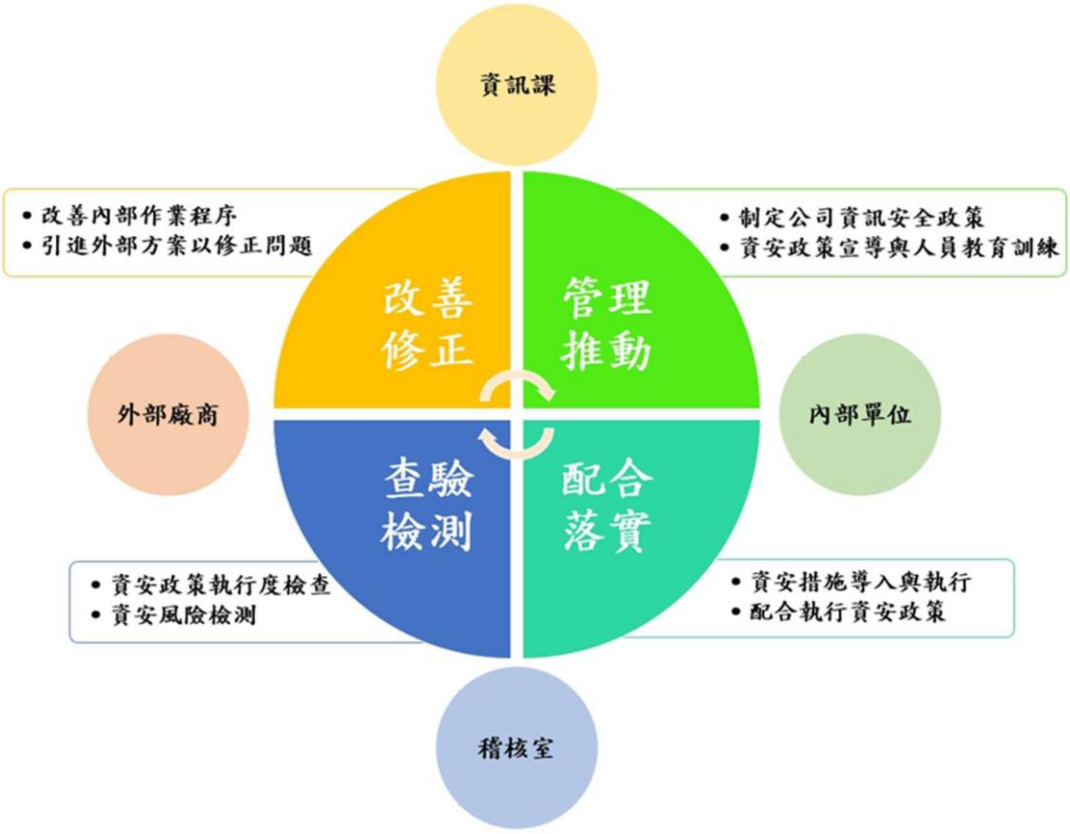
資訊安全政策及管理方案

- 資訊安全風險管理架構

1. 本公司資訊安全之權責單位為資訊課，該單位設置資訊主管1名，與專業資訊人員2名，負責訂定內部資訊安全政策、規劃資訊安全作業與資安政策推動與落實。每年稽核室會定期查核，若查核發現缺失，旋即要求受查單位提出改善措施， 且定期追蹤改善結果，以降低內部資安風險。
2. 本公司資訊課採用PDCA（Plan-Do-Check-Act）循環流程管理模式，確保可靠度目標之達成且持續改善。



- 資訊安全政策及具體管理方案

1. 本公司資訊安全管理機制，包含以下三個面向：
(1)制度規範：訂定公司資訊安全管理制度，規範人員作業行為。
(2)科技運用：建置資訊安全管理設備，落實資安管理措施。 (3)人員訓練：進行資訊安全教育訓練，提昇內部同仁資安意識。

2. 管理措施說明如下：

(1)制度規範：本公司訂有員工使用電腦同意書，內含員工資訊使用安全行為，每年定期檢視相關規定是否符合營運環境變遷，並依需求適時調整。

(2)科技運用：本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦導入資安系統工具， 落實人員資訊安全管理措施。

(3)人員訓練:本公司每年定期實施內部人員資訊安全教育訓練實務課程，並建置數堂線上學習 (E-Learining)資訊安全課程，藉以提昇內部人員資安知識與專業技能。

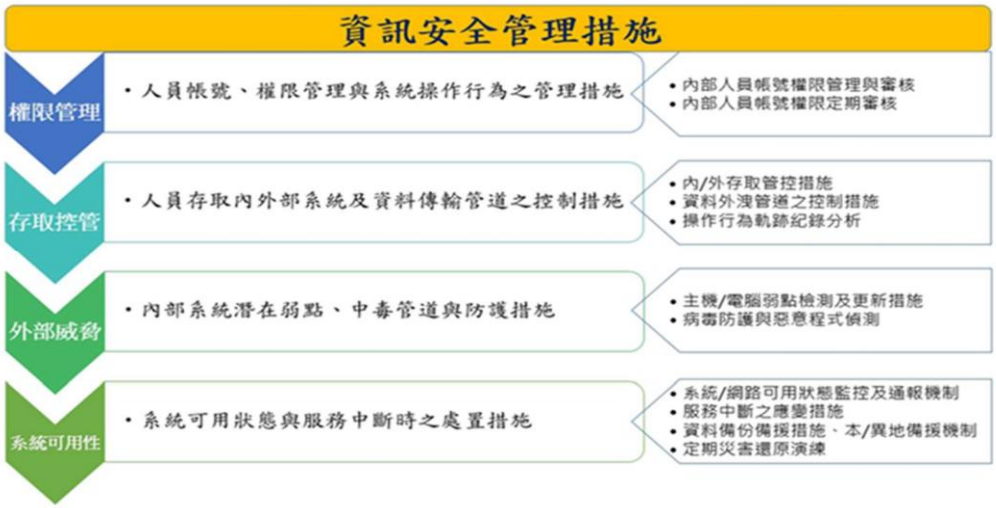
2022年10月12日及18日實施資訊安全講習，並於課後測驗，計185人次，平均97分。

- 資訊安全管理措施

本公司定期審視內部資訊安全規範，根據資產價值、弱點、威脅與影響性，分析內部風險水平，並以此風險評估結果制定安全措施強化項目，精進且提升整體資訊安全環境。

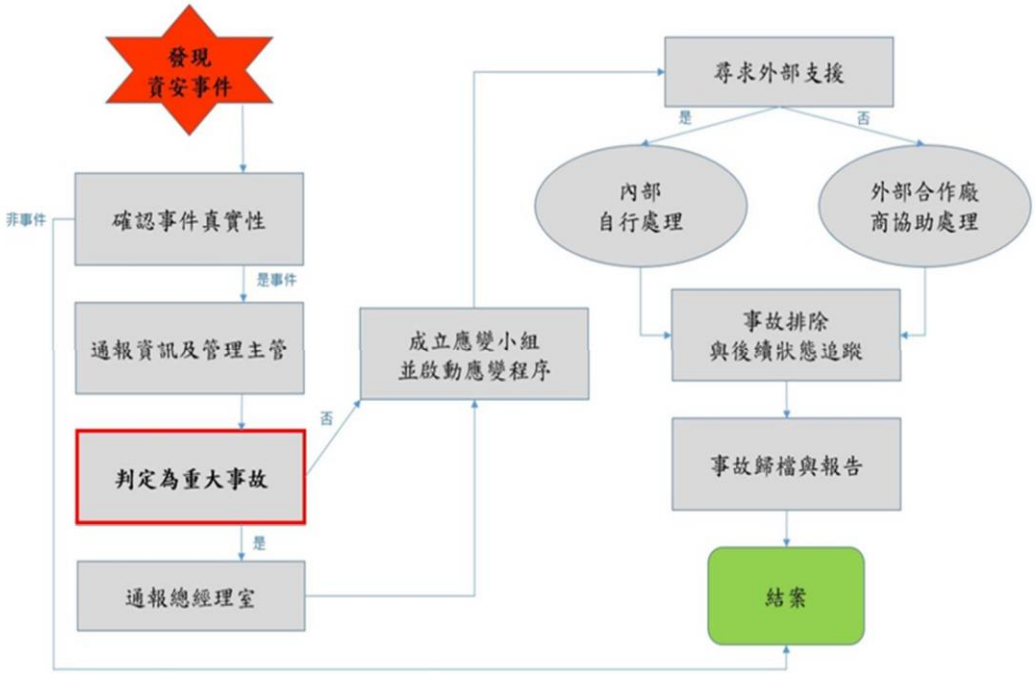
1. 本公司資訊風險評估程序如下：

2. 本公司實施之資訊安全管理措施，包含如下：



・資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。



・2022 年資安專案執行實績

分類	專案名稱	內容	執行方式	推展時間	執行情形
系統導入	導入資安軟體（IDE xpert、DDI）	• 配合客戶由遠端登入電腦採多因子認證，導入 IDExpert，除原有帳號密碼認證、增加手機接收推播驗證，達成兩步雙重驗證。 • 導入 DDI 系統，監控內網所有流量、內部網路通訊協定來發掘針對性攻擊，可縮短資安回應時間及利於察覺異常。	系統增購	2022.05.25	2022.06.16 驗收完成 2022.06.23 驗收完成
設備汰換	DELL 儲存伺服器	於子公司架構三層式之儲存設備，添購 DELL EMC 儲存設備，並進行資料轉移，確保資訊安全。	硬體增購	2022.08.23	2022.10.17 驗收完成
專案輔導	BPR(IBM)	檢討目前現有工作流程並提出改善建議，後續出具報告評估如採用SAP 之效益。	IBM 輔導	2022.01	2022.07 完成並交付報告給勝一化工
專案輔導	ERP（鼎新 T100）	更新ERP 系統升級鼎新T100 並調整相關內部作業流程。	鼎新輔導	2022.11~2023.12	延續至 2023 年持續建置及規劃人員教育訓練。