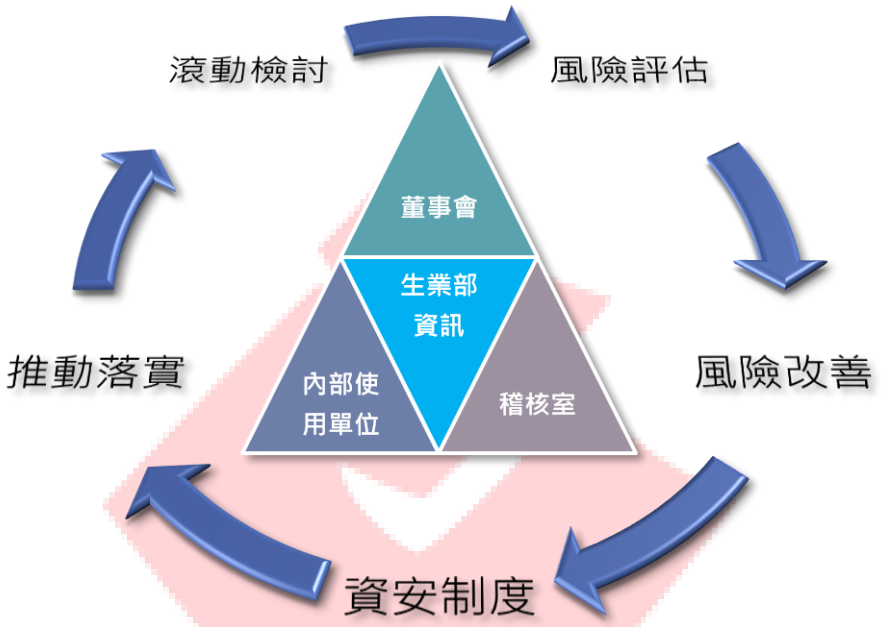
《資訊安全風險管理架構》

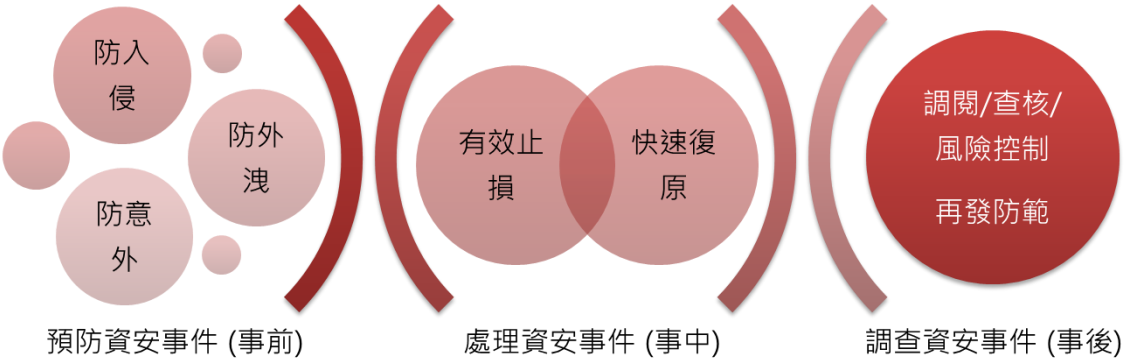
一、資訊安全風險管理架構

裕隆汽車資訊安全權責單位為生產業務部，配置資訊主管四名與專業人員數名，負責訂定資安政策、規劃暨執行資訊安全作業與資安措施推動與落實，並定期向裕隆汽車董事會及裕隆集團總管理處報告資安治理概況。



組織運作採 PDCA 循環式管理，確保可靠度目標之達成且持續改善。為掌握資訊安全風險管理，裕隆汽車自三面向來對應及預防風險事件發生：

1. 未發生前：定期自主盤點檢驗，從流程與技術多方面著手，主動預防資安事故。
    a) 防入侵：主動防禦來自內外網攻擊，侵入資訊系統造成破壞。
    b) 防外洩：主動防範公司機敏資訊及營業秘密遭外流外洩，影響裕隆永續營運。
    c) 防意外：主動預防環境內因素（故障/跳電／病毒／設備遺失）造成的生產損失。
2. 事件發生時：損害控制緊急應變
    a) 完善機制：建立有效的災害應變機制，迅速將損害控制止血。
    b) 落實演練：運用演練經驗，在最短時間內恢復正常，維持企業體持續營運。
3. 發生以後：追查並列入預防
    a) 避免問題發生：調閱系統紀錄追蹤問題原因，擬定對策成新預防措施。
    b) 查核方法再強化：引入外部顧問/弱點檢測團隊，低減查核盲點提高內控機制可靠性。



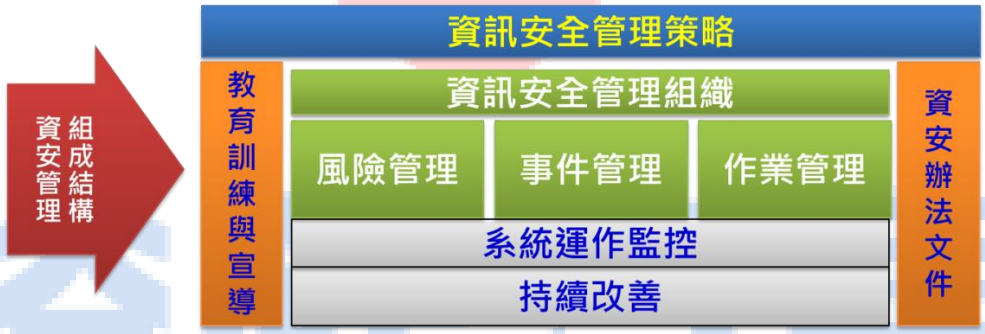
二、資訊安全政策

為提升資訊安全管理，本公司由生產業務部推動資訊安全風險內控，負責本公司資訊安全運作管理、監督及查核…等相關作業，並由稽核單位定期向董事會報告資安治理審查狀況。其涵蓋範疇包含下列三項：

（一）資安技術：依據產業特性及資訊安全新興科技發展，導入資訊安全管理設備，深化多層次縱深防禦，實施自動化防禦管制，落實資安管理措施。

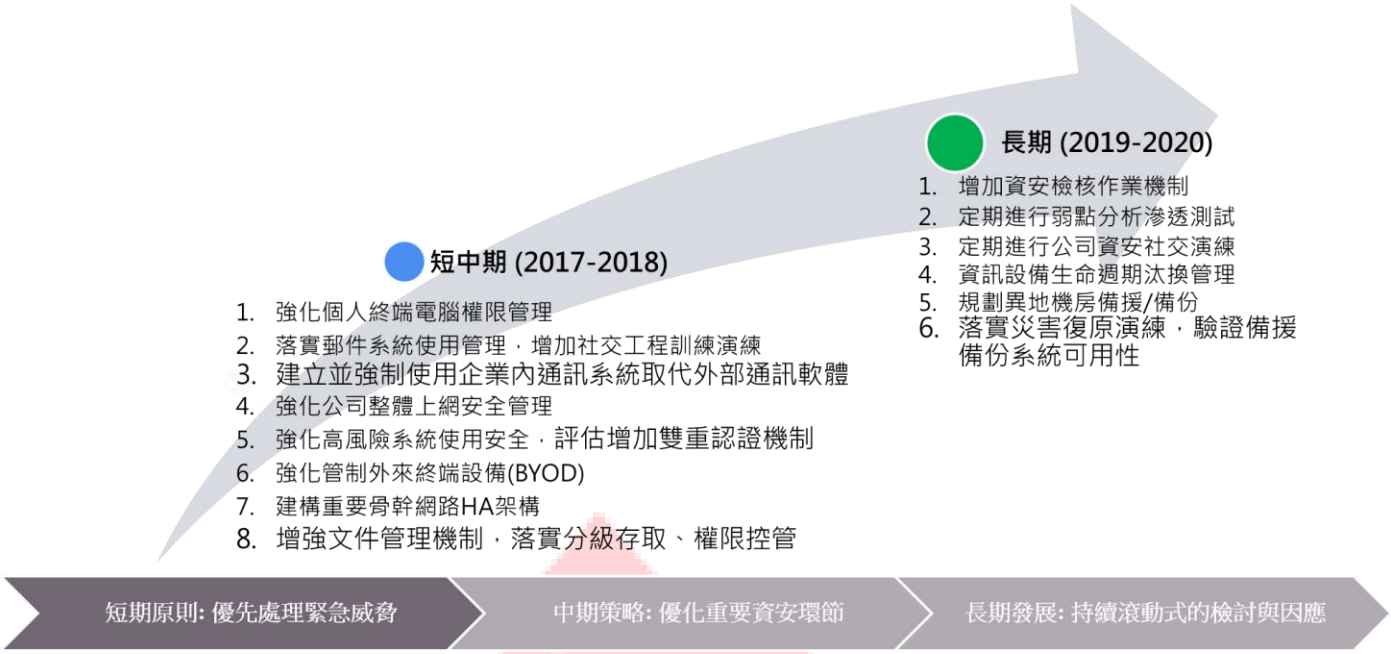
（二）制度辦法：本公司依「公開發行公司建立內部控制度處理準則」第九條「電腦化資訊系統處理」之規定制定相關內部作業規定，以降低新興資訊科技應用以及環境變遷所帶來未知的資安威脅風險。

（三）員工認知：不定時進行資安教育訓練/演練、創設風險行為內控提報獎懲、依時事週期性公告宣導，提昇全體同仁資安意識。



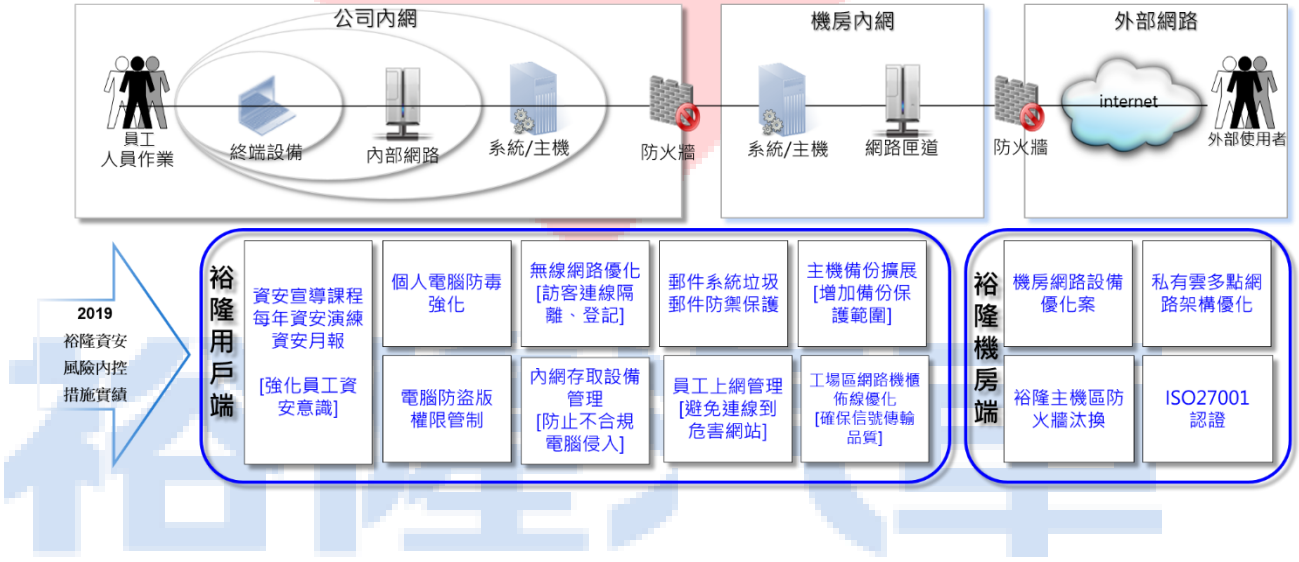
三、具體管理方案措施

1. 裕隆汽車持續對資訊安全完備其治理制度與提升防禦能力，各項資訊作業不僅須符合資安標準流程外，更要符合資訊安全法令法規。
2. 自 2017 年起依循集團【資訊安全發展藍圖】逐步精進，並於 2018 年完成【資安風險內控管理措施】規劃發布，深刻落實資訊安全風險管理。



3. **過去資訊安全規劃**

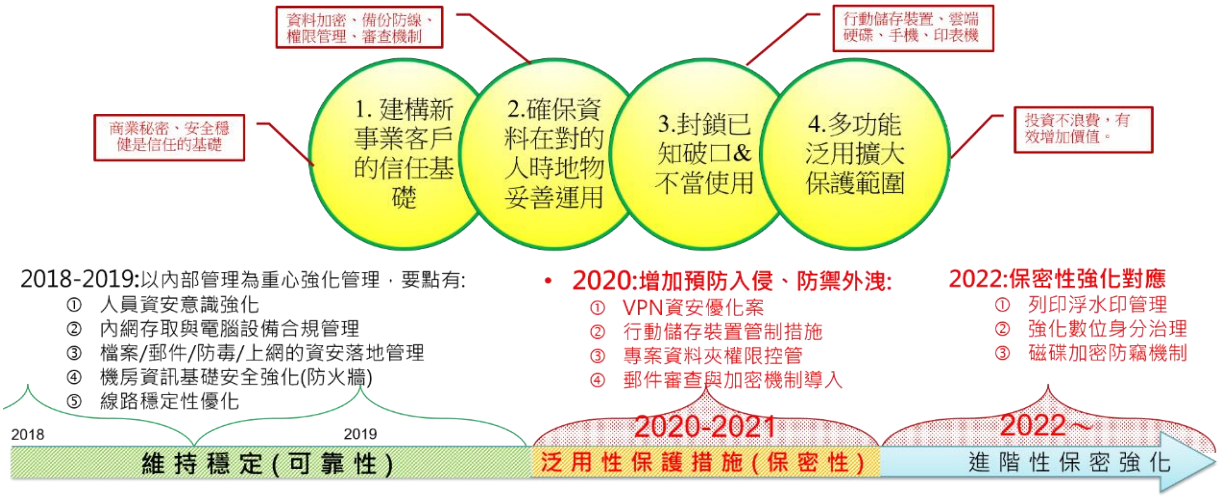
本公司為強化整體資訊安全，2019~2020 年具體進行多項資訊安全強化專案，範圍包含【內外傳輸網路防駭】、【員工資安意識提升】、【防範惡意網站管控】、【遠距工作連線保護】、【系統弱點改善強化】、【資料外洩保護(DLP)】、【跨公司異地機房強化】和【增強 IT 基礎架構】。



4. **未來資訊安全規劃**

本公司已規劃 2021 年~2023 年「資安風險內控管理措施」推動藍圖，穩健推展中長期整體資安、持續優化，包含基礎資訊建設、智慧製造防護、落實資安訓練。包含：

1. 2019 年起因應裕隆集團轉型，採「全面開放，爭取多元客戶，藉資源共享共用創規模/降成本」的情境下，從資訊安全三要素(保密性、完整性、可靠性)中分群，過往重於服務可靠性(穩定/不中斷使用)強化，將導引為【保密性風險】強化為主軸，提升資安等級與科技/國際業界接軌，獲取客戶信任度、防止機敏資料外洩發生。



2. 有關資訊安全管理執行現況及未來規劃報告，每年至少一次由稽核單位報告董事會，落實資訊安全風險管理。

本版次訂立於民國一〇七年十二月三十日
第一次修訂於民國一〇八年五月十五日
第二次修訂於民國一〇九年九月三十日