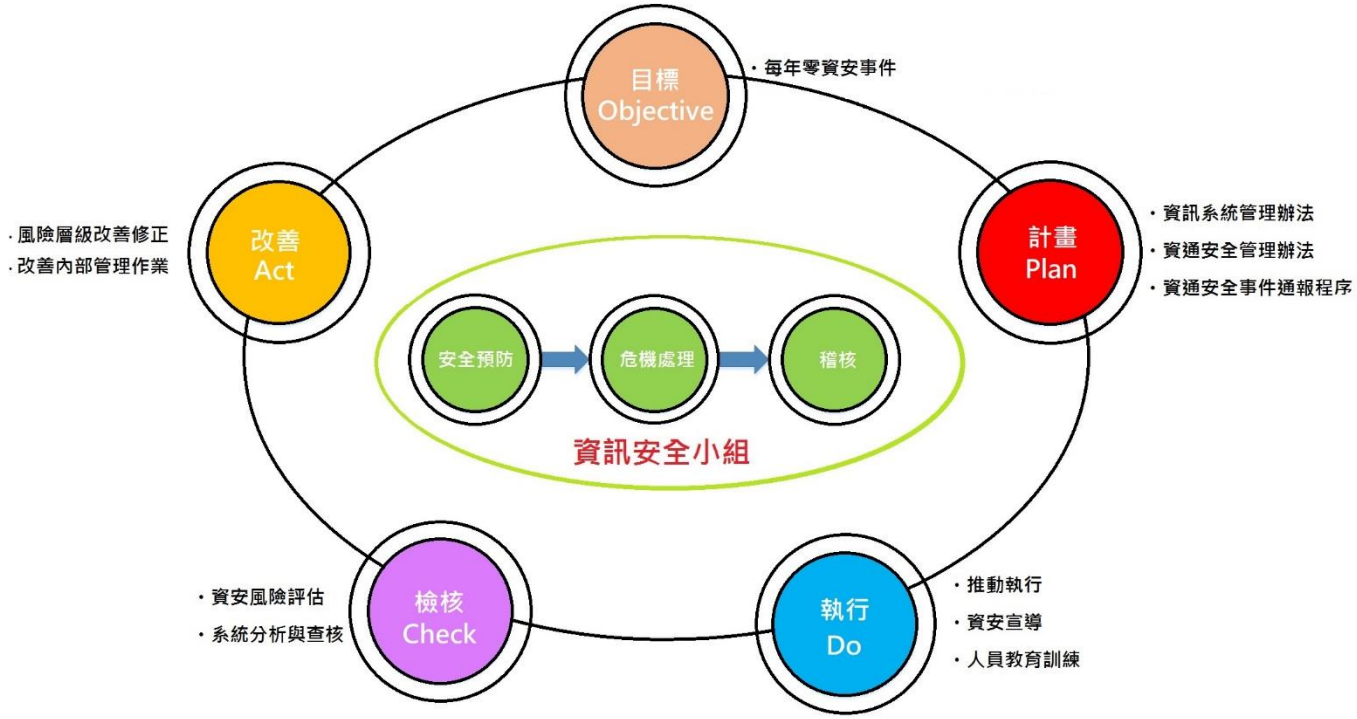
一、資訊安全風險管理架構

本公司資訊安全由管理部資訊權責人員負責，設置資訊人員二名，負責制訂落實資訊系統與資通安全辦法推動。

公司資訊安全運作模式採用 OPDCA（Objective-Plan-Do-Check-Act）循環式方管理方式，確保制定的目標達成且持續改善。



二、資通安全政策

為確保順天建設股份有限公司（以下簡稱本公司）所屬之資訊資產機密性、完整性、可用性及資訊系統之安全維運，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，本公司資通安全管理機制，包含以下三個面向：

（一）訂立制度規範：制訂公司資通安全管理辦法、資訊系統管理辦法，規範人員作業行為。

（二）系統設備建置：建置端點安全防護系統、網路資安設備，監控設備、網路運作，防範各種資安威脅。

（三）人員意識訓練：不定期發佈資安通報及資訊安全教育訓練，加強全體同仁資安意識

三、資通安全防護及控制措施

01.伺服器管理：為確保伺服器主機運作正常，建置資訊安全管控機制。

02.防火牆管理：建置企業防火牆，依網路使用性質設立連線規範，保護公司資訊環境及資料。

03.郵件安全管理：建置郵件過濾系統進行郵件掃描，事先防護攻擊威脅、釣魚郵件、垃圾郵件、不安全附件及惡意連結。

04.網站安全管理：網站服務的資料傳輸導入安全協定，傳輸資料過程使用 SSL/TLS 進行加密。

05.實體安全管理：內部重要之資訊設備應妥善放置於獨立機房，予以有效地保護，連接資訊設施的電源及通信線路，應採取適當的保護措施 並定期檢查。

06.環境安全管理：機房設置進出管制及維持內部環境適當之溫濕度，確保系統設備正常運作。

07.存取控制管理：對於重要之資訊資產(包含網路、作業系統等)或資訊服務等項目之機密等級資料，訂定存取控制作業程序，明定使用者及管理者之存取權限。

08.備份備援管理：伺服器及端點設備皆定期執行備份程序，以確保資料安全及回復資訊作業。

09.病毒防護系統管理：每部端點皆安裝防毒軟體及端點防護系統，以有效維護資訊作業安全。

10.入侵偵測系統管理：建置入侵偵測系統，以有效監控網路連線狀況，遏止外部攻擊。

11.電子資料、媒體銷毀：電子資料、媒體銷毀程序執行前，應先進行清查作業，確認資料之保存年限、性質及價值，後續由管理單位人員會同相關資訊人員及單位，全程檢視過程，確保完全清除或毀滅。

四、資安事件通報程序

1.資訊安全事件包括，任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、、設備資安漏洞以及通訊中斷等。

2.資訊安全事件通報程序，如下圖所示。