資安健診服務執行流程

前置作業

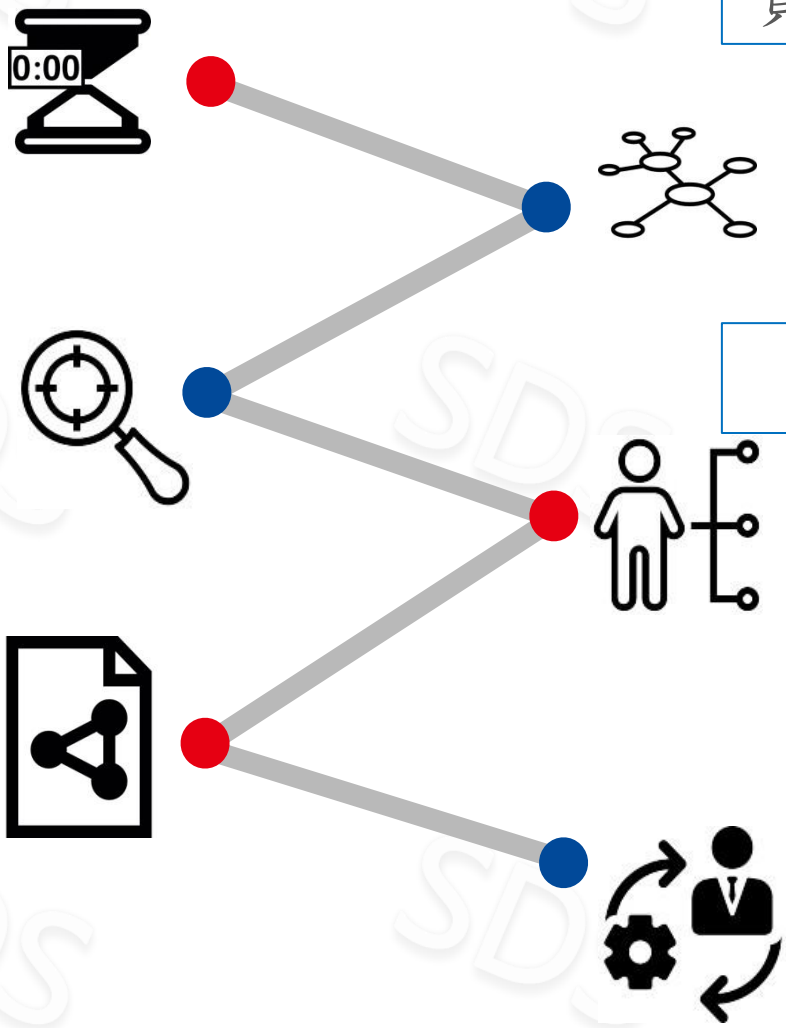
利用資安健診服務基本資料表，針對機關資安境服務範圍、執行時程及訪談調查等事項進行討論。

進行實地檢測

至單位進行實地檢測

健診結果分析與說明

利用資安健診結果提出書面執行報告，並向健診機關說明執行結果



資安現況分析

針對前置訪談作業所取得之資料與現有資料進行分析，規劃本次健診之重點檢視項目

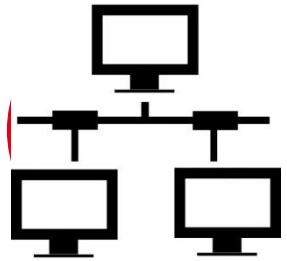
依檢測結果進行管理檢視

執行內部、外部之技術檢測與管理程序面之檢視，了解至機關落實資安防護部署之表現

資安健診服務管理系統

將機關執行結果歸檔，作為下次現狀分析參考

資安健診服務項目



網路架構檢視

針對網路架構圖進行安全性弱點檢視，檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠。

有線網路惡意活動檢視

針對有線網路適當位置架設側錄設備，觀察是否有異常連線或DNS查詢，並比對是否連線已知惡意IP、中繼站（Command and Control,C&C）或有符合惡意網路行為的特徵。

檢視防火牆、入侵偵測/防護系統等網路設備紀錄檔，分析過濾異常連線紀錄。

使用者端電腦檢視

針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

作業系統、Officc應用程式、防毒軟體、AdobeAcrobat及Adobe flashPlayer應用程式更新檢視。

伺服器主機檢視

針對伺服器主機進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

作業系統、Officc應用程式、防毒軟體、AdobeAcrobat及Adobe flashPlayer應用程式更新檢視。

安全設定檢視

檢視目錄伺服器中群組的密碼設定與帳號鎖定原則，例如AD伺服器有關群組原則（Group Policy）中之「密碼設定原則」與「帳號鎖定原則」設定。

檢視防火牆是否開啟具有安全性風險的通訊埠或非必要通訊埠，連線設定是否有安全性弱點。