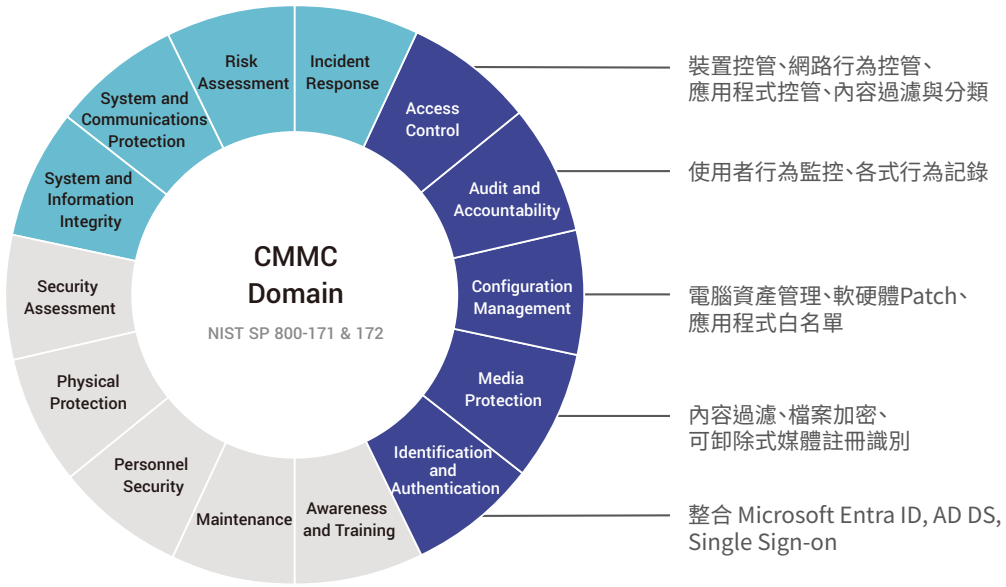
CMMC 實務說明

為遵循 CMMC 的要求，國防供應鏈業者需要確保其資訊安全措施。利用端點 DLP 資料控管機制，可以協助實踐 CMMC 規範的領域包含存取控制、稽核與歸責、組態管理、身分驗證與授權、媒體保護等。



對照 CMMC 控制措施與 X-FORT 控管

控制措施	控制項目	X-FORT 功能說明
Access Control	檔案管制	• 內容過濾與分類，依內容關鍵字(CUI標籤)，在檔案寫出記錄加註分類標籤 • 檔案寫出至隨身碟、網路傳輸前，依內容過濾結果放行或阻擋 • 檔案寫出可依主管審核結果放行 • 限制檔案傳輸，如：(1)唯讀隨身碟、(2)可瀏覽網頁，但禁止上傳檔案 • 安全傳輸：檔案加密，記錄檔案寫出或上傳
	連線管制	• 限制電腦連線的目的地，如：禁止使用雲端硬碟 • 限制可連線的WiFi AP，僅可連結公司核可的WiFi
	系統管理	• 多種管理者角色：系統管理員、系統稽核員、群組(部門)管理員及稽核等 • 系統閒置將自動登出用戶端電腦
Audit and Accountability	操作記錄	• 記錄使用者檔案操作行為，包含檔案新增、複製、搬移、刪除等 • 記錄寫出隨身碟、透過網路傳出檔案等行為 • 保留電腦登出登入記錄、WiFi連線記錄、裝置連結電腦記錄
	記錄與報表	• 用戶端記錄存放於隱藏區域，受保護無法被刪除；記錄上傳至伺服器完成後刪除 • 限制用戶端記錄儲存空間上限，硬碟空間不足提出告警；伺服器空間使用率告警 • 自訂篩選條件，搭配整合查詢記錄及寄送報表， 排程自動寄送報表給管理員
Configuration Management	資產管理	• 蒐集軟硬體資產，管理軟體資產與授權 • 掃描用戶端機碼(Registry)設定、本機使用者帳號等
	應用程式控管	• 電腦裝置控管白名單，可限制所有新增裝置，如藍牙、外接無線網卡等 • 應用程式白名單，控管不允許使用的應用程式，如FTP、 P2P軟體 • 除了禁止安裝或執行軟體，亦可遠端反安裝不需要的軟體
Identification and Authentication	控管政策	• 針對人員或電腦制定資安控管政策，如預設禁用外接儲存裝置，例外開放唯讀 • 提供註冊碟機制，並可指定使用人員
Media Protection	檔案加密	• 含CUI的檔案可加密保護，檔案加密後，依然具備內容過濾的出口管制保護 • 加密檔案，限制存取人員