



導入 ANCHOR能迅速消弭資安風險

透過ANCHOR系統有助於IT部門進行帳號管理時消弭下列可能風險：

■ 帳密被盜取：

透過ANCHOR管控高度敏感的特權帳號，以避免特權帳號被取得而遭受利用，造成入侵事件。

■ 多重系統權限：

組織中人員因為職務輪調或職務代理人的需求，往往會獲得多個系統的特殊權限，假使人員職務調動卻忘了將之權限回收，就有可能帶來風險。

■ 共享帳密：

諸如Administrator、root、或SA等帳號，為了業務及維運需求，經常多人持有這些帳號的登入，導致產生資安風險時難以究責。

符合 ISO 精神與最佳實務經驗的思維出發，

ANCHOR 為 (Ark of Network, Cyber Hamper for Operations Reliability) 之縮寫，從帳號生命週期中的每個管理環節（認證、申請、審核、啟用、通知、連線、監控、停用、報告、稽核）對應出符合管理流程與稽核要求等各項功能，構成一集中化的管理平台，省卻傳統上所需的高額建置費用與人力時間成本，將管理工作化繁為簡，讓IT人員提升工作效率，系統仍保有必要的稽核紀錄，並符合資安內控與法規查核。

特權帳號生命週期管理流程



ANCHOR提供各種角色定義之使用者，提供整合式入口網站方便針對受管理設備/服務等進行帳號集中控管、單一簽入及操作稽核等管理作業

Privileged Security Goals	帳號生命週期	駭客入侵防禦	風險威脅警示			
Definable Role Functions	雙重認證	存取管制	連線申請	連線審核		
	連線開通	單一簽入	軌跡紀錄	即時監控		
	連線回收	密碼變更	工作報告	稽核流程		
	密碼存取	帳號清查	密碼檢查	報表訂閱		
Shared Infra-mods	OTP	SSO	Credential Vault/TPM	SR	A2A	
	AM	IDM		BPM	VDI	
Adapter Framework						
	作業系統	資料庫	虛擬化	網路/資安	雲端服務	
				郵件	AD/目錄	SIEM