

項目	(九) 資通安全事件通報應變及情資評估因應		
9.12	針對日誌之是否進行存取控管，並有適當之保護控制措施？		
稽核 依據	資通安全責任等級分級辦法附表十資通系統防護基準：事件日誌與可歸責性之日誌資訊之保護	C0206	
	數位發展部 111 年 11 月 23 日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	O01	
	1. 資通安全責任等級分級辦法第 11 條第 2 項：應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表 10 所定資通系統防護基準執行控制措施 2. 資通安全責任等級分級辦法第 11 條第 2 項：資通系統防護基準之事件日誌與可歸責-日誌資訊之保護-對日誌之存取管理(普中高)；應運用雜湊或其他適當方式之完整性確保機制(中高)；定期備份日誌至原系統外之其他實體系統(高)。		
稽核 重點	確認機關是否依資通安全責任等級分級辦法附表十「事件日誌與可歸責性」及系統防護需求等級落實辦理相關法遵作業。	佐證 資料	相關佐證資料
稽核 參考	1. 對日誌之存取管理，僅限於有權限之使用者（如系統或資料庫管理者等存取日誌檔案或日誌主機）。依附表十辦理。 2. 宜運用雜湊或其他適當方式之完整性確保機制。 3. 日誌完整性防護又分為事前預防、事中監視及事後驗證等三種面向： (1) 事前預防：將日誌以 CD-ROM/DVD-ROM 或其他具唯獨（ReadOnly）特性之儲存媒體進行保存，或透過加密處理後保存或備份。 (2) 中監視：市面上推出多款針對檔案、目錄或資料庫專用之監控工具，其功能特性為可即時偵測檔案、目錄或資料庫欄位異動，並提出警示通知。 (3) 事後驗證：可利用 SHA-256 或 HMAC-SHA-256 等雜湊演算法計算雜湊值，或將日誌備份至原日誌系統不同之實體系統，亦可用來驗證資料完整性。		

	4. 防護等級高等級之系統定期備份日誌至與原系統外之其他實體系統。
FQA	