

項目	(九)資通安全事件通報應變及情資評估因應		
9.7	針對所有資安事件，是否保留完整紀錄，並與其他相關管理流程連結，應依自身機關資通安全責任等級保存日誌，詳各機關資通安全事件通報及應變處理作業程序表二，且落實執行後續檢討及改善？		
稽核 依據	資通安全管理法施行細則第 6 條：資通安全事件通報、應變及演練相關機制		P9
	資通安全管理法施行細則第 8 條		L1110082308
	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.資通安全管理法施行細則 (1) 第 6 條第 1 項第 9 款：資通安全事件通報、應變及演練相關機制 (2) 第 8 條第 1 項：本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告		
	2.資通安全事件通報及應變辦法 (1) 第 10 條第 1 項第 5 款：公務機關應訂定通安全事件應變作業規範，其內容應包括五、事件相關紀錄之保全。 (2) 第 16 條第 1 項第 5 款：特定非公務機關應訂定資通安全事件應變作業規範，其內容應包括五、事件相關紀錄之保全。		
稽核 重點	3.各機關資通安全事件通報及應變處理作業程序(表二)		
稽核 重點	機關應依資通安全管理法施行細則第 8 條落實辦理法遵作業。	佐證 資料	事件報告、保存紀錄。
稽核 參考	1. 資安事件相關文件的管理。 2. 負責應變之權責人員或緊急處理小組，辦理應變事務並留存應變之紀錄，包括： (1) 資安事件之衝擊及損害控制作業。 (2) 資安事件所造成損害之復原作業。 (3) 資安事件相關鑑識及其他調查作業。 (4) 資安事件之調查與處理及改善報告之方式。 (5) 資安事件後續發展及與其他事件關聯性之監控。 3. 機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中		

	斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。4.若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。
FQA	