

項目	(七) 資通安全防護及控制措施		
7.10	是否已確實 <b>設定</b> 防火牆並 <b>定期</b> 檢視防火牆規則，DNS 查詢是否僅限於 <b>指定</b> DNS 伺服器？ <b>有效</b> 掌握與管理防火牆連線部署？		
稽核 依據	資通安全責任等級分級辦法應辦事項：技術面之資通安全防護之網路防火牆		N20702
	110 年 12 月 7 日行政院國家資通安全會報第 38 次委員會議擴大會議紀錄		O01
	1. 資通安全管理法施行細則第 6 條第 1 項第 8 款：資通安全防護及控制措施 2. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：資通安全健診-目錄伺服器設定及防火牆連線設定檢視 A.資通安全防護-網路防火牆 B.資通安全防護-具有對外服務之核心資通系統者，應備應用程式防火牆		
稽核 重點	設定防火牆並定期檢視防火牆規則	佐證 資料	防火牆規則申請單、防火牆規則定期檢視紀錄
稽核 參考	1. 機關需掌握防火牆規則清單，並依法遵要求定期檢視。 2. 機關防火牆惡意中繼站名單宜定期更新，資安院每週公布一次該院掌握之 c2 清單，故建議至少每週更新 c2 清單。 3. 限制明碼傳輸 ( 如 telnet、FTP 等 )、任意連線，防火牆最後一條規則應建立 Denyall/any 等。 4. 檢視 DNS 查詢使用端口應納入防火牆規則清單。 5. 是否依機關風險評估結果建立連線行為黑名單 ( 例如有風險的網站、VPN 之使用、加密貨幣挖掘、不受信賴的來源等 )。		
FQA			