數位發展部

政府公有雲服務供應商檢核作業指引

文件版本：V5.0

中華民國 112 年 7 月

目　　錄

壹、 依據

數位發展部(以下簡稱本部) 順應國際發展趨勢，推動政府雲端基礎建設，為無縫移轉為民服務系統至政府公有雲，並確保服務效能與資訊安全，爰依前瞻基礎建設計畫第 3 期「強化公部門網路服務與運算雲端基礎設施計畫」之「雲世代雲端基礎建設」細部計畫實施重點「政府數位服務雲端環境優化」，訂定本檢核程序。

貳、 目的

一、 本檢核程序旨在協助機關確認「公有雲服務項目選用參考指引」之合規狀態，並了解CSP與機關雙方應配合事項，以利機關採用一致性基準檢核複雜多元的公有雲服務，達成資訊系統雲端化目標。

二、 本指引適用前瞻基礎建設計畫第 3 期「強化公部門網路服務與運算雲端基礎設施計畫」之「雲世代雲端基礎建設」細部計畫實施重點「政府數位服務雲端環境優化」相關試行機關，指引內容為參考性質，各機關可依業務需求選用或調整適用之要求項目。

參、 名詞定義

參閱「行政院及所屬各機關資料中心設置作業要點」及「國家標準-資訊技術－雲端運算－概述與基本詞彙(CNS 17788)」之定義如下：

一、 雲端服務提供者(Cloud Service Provider, CSP)：從事支援或輔助雲端服務提供者或雲端服務客戶之一，或二者的活動之當事者。

二、 雲端服務客戶(Cloud Service Consumer, CSC)：於營運關係中，目的在使用雲端服務之當事者。

備考：營運關係不必然須具備財務協議。

三、 基礎設施作為服務[1](Infrastructure as a Service, IaaS)：雲端服務種類之一，其中對雲端服務客戶提供之雲端能力型式係基礎設施能力型式。

四、 平台作為服務(Platform as a Service, PaaS)：雲端服務種類之一，其中

1 雲端服務客戶並部管理或控制下層實體及虛擬資源，但對使用實體及虛擬資源之作業系統、儲存體，以及所部署的應用系統有控制權。雲端服務客戶亦能對某些聯網組件(例：主機防火牆)具有有限控制能力。

對雲端服務客戶提供之雲端能力型式係平台能力型式。

五、 軟體作為服務(Software as a Service, SaaS)：雲端服務種類之一，其中對雲端服務客戶提供之雲端能力型式係應用能力型式。

肆、 管理項目類別

依「公有雲服務項目選用參考指引」，公有雲服務管理共區分為服務、營運、通訊及資安與隱私管理四個面向，共計 65 項管理要求，概述如下：

一、 服務管理面向，共計有 24 個要求項目：

(一)雲端服務共同基本要求，計有 8 個要求項目。

(二)IaaS 服務類型 ，計有 5 個要求項目。

(三)PaaS 服務類型 ，計有 6 個要求項目。

(四)SaaS 服務類型 ，計有 5 個要求項目。

二、 營運管理面向，共計有 25 個要求項目：

(一)資源需求，計有 1 個要求項目。

(二)維運管控，計有 7 個要求項目。

(三)資訊財產，計有 1 個要求項目。

(四)廠商選擇，計有 1 個要求項目。

(五)存取控制，計有 6 個要求項目。

(六)服務可用性，計有 6 個要求項目。

(七)雲端服務事故通報，計有 3 個要求項目。

三、 通訊管理面向，共計有 3 個要求項目：

(一)公有雲與政府網際服務網(Government Service Network, GSN)網路介接，計有 1 個要求項目。

(二)系統與通訊加密服務，計有 2 個要求項目。

四、 資安與隱私管理面向，共計有 13 個要求項目：

(一)資安技術面要求，計有 10 個要求項目。

(二)資安與隱私稽核，計有 3 個要求項目。

有關資安與隱私管理面向係參考我國現行法規所擬定之建議控制措

施，有關資訊系統上雲後資安合規最佳實踐做法，可參考國家資通安全研究院網站之共通規範專區所發布「政府機關雲端服務應用資安參考指引」[2]。

伍、 公有雲服務管理要求檢核程序

一、 檢核方法

為確認上揭管理要求之符合狀態，宜建立一致性之檢核程序，而檢核方式考量雲端特性、服務類型及責任分攤之不同，分為檢視及測試二種方式，說明如下：

(一)檢視：機關檢測人員依據 CSP 提供之佐證資料(文件、網站資訊或其它可證明之資料)判定是否符合，有關廠商提交予機關佐證資料之文件格式，可參考附件 1 及附件 2 之表格。

(二)測試：

1. 雙方應約定檢測時間，於約定區間執行。
2. 檢測人員依 CSP 提供之環境進行測試。
3. CSP 須提供檢測資源及技術支援窗口協助檢測人員測試，並按照檢測結果判斷是否符合。

二、 檢核程序

為利機關依服務類型檢核管理要求符合狀態，依 IaaS、PaaS、SaaS 分別彙整「IaaS 服務類型檢測項目表」、「PaaS 服務類型檢測項目表」及「SaaS 服務類型檢測項目表」如下，機關依雲端服務類型，選擇適用之檢核表，並依檢核表之「要求項目」及「要求項目檢測步驟」檢核「CSP 應提供之佐證資料」，確認管理要求之符合程度。

2 參考來源：https://www.nics.nat.gov.tw/CommonSpecification?lang=zh

表 1：IaaS 服務類型檢測項目表

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
服務管理	雲端服務共同基本要求	CC-1	CSP 須提供機關管理平臺服務介面/網站	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定服務管理平臺說明文件，且說明 CSP 具備專屬平臺供機關進行其服務配置與管理	CSP 提供機關租用服務範圍內之服務管理平臺說明文件
	雲端服務共同基本要求	CC-2	CSP 提供的網站與介面須可支援網站線上隨時進行申請，修改或退租所提供之雲端服務資源變更功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定後服務及資源變更說明文件，且說明使用者能夠隨時透過申請方式修改或退租雲端服務資源，並提供功能展示網站的畫面	CSP 提供機關租用服務範圍內之服務及資源變更說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	雲端服務共同基本要求	CC-3	CSP 提供之平台須支援至少 3 種主流瀏覽器的後台管理及服務使用機制(如：透過瀏覽器設定、遠端桌面管理、REST API 管理或 Console 管理等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務說明瀏覽器的廠牌與版本，且說明服務平台支援至少 3 種主流瀏覽器 2.後台管理服務使用機制支援(如：透過瀏覽器設定、遠端桌面管理、REST API 管理或 Console 管理等)	CSP 提供機關租用服務範圍內之後台服務管理機制說明文件
	雲端服務共同基本要求	CC-4	CSP 提供之平台須有多租戶設計，不同租戶帳號須有獨立作業環境及管理服務頁面，且操作資料不會相互影響	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定使用者身分認證與存取控制管理說明文件，且說明不同帳號登入系統，有獨立作業環境或管理頁面，使用者操作資料不會相互影響 (例如:於其中一個帳號新增一筆資	1.CSP 提供機關租用服務範圍內之使用者身分認證與存取控制管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				料，不會影響其他用戶帳號) 2.CSP 已於提供之內外部獨立稽核報告中說明使用者與租戶隔離管控之正確性與有效性	
	雲端服務共同基本要求	CC-5	CSP 提供之應用服務架構須具備資源彈性擴展/回收設計及使用者資源彈性變更功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂資源變更說明文件，且說明應用服務架構具備資源彈性擴展與回收設計，機關能夠依其需求變更資源配置 2.CSP 已於提供之內外部獨立稽核報告中說明服務資源變更功能之正確性與有效性	1.CSP 提供機關租用服務範圍內之資源變更說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	雲端服務共同基本要求	CC-6	CSP 提供之平台須具備各別租戶使用之資源(服務)度量功能，並以儀表板方式呈現	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定使	CSP 提供機關租用服務範圍內之使用者資源監控說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				用者資源監控說明文件，且說明將提供各別使用者以儀表板方式檢視資源(服務)度量	
	雲端服務共同基本要求	CC-7	CSP 提供之平台須具備即時檢視費用功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件，且說明具備即時檢視服務收費情形	CSP 提供機關租用服務範圍內之收費機制說明文件
	雲端服務共同基本要求	CC-8	CSP 所取得之 ISO 27001 第三方認證，範圍須包括機關選用服務所有項目	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供相關第三方認證報告，且認證範圍須保括選用服務所有項目	CSP 提供機關租用服務範圍內之第三方認證報告
	IaaS 服務類型	IS-1	CSP 須至少符合 ISO 27001 及 ISO 27017 (或 CSA STAR 等)標準的安	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備：	1.CSP 提供機關租用服務範圍內之 ISO 27001 及 ISO 27017 (或 CSA

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			全措施，CSP 處理資料若包含個資則須符合 ISO 27701(或 BS 10012)及 ISO 27018；CSP 若有通過其他國家雲端安全相關規範，可提供佐證資料	1.CSP 已針對租用範圍內之服務提供 ISO 27001 及 ISO 27017 (或 CSA STAR)驗證證書或報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內 2.CSP 已針對租用範圍內之服務提供 ISO 27701(或 BS 10012) 及 ISO 27018 驗證證書或報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內 3.CSP 已針對租用範圍內之服務提供他國雲端安全規範認證與報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內	STAR)驗證證書或報告 2.CSP 提供機關租用服務範圍內之 ISO 27701(或 BS 10012) 及 ISO 27018 驗證證書或報告 3.若 CSP 提供機關租用服務範圍內另有通過其他國家雲端安全相關規範，能夠提供其驗證證書或報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	IaaS 服務類型	IS-2	CSP 對提供之基礎設施須建立稽核與運作確保政策與程序，並至少每年審查與更新這些政策和程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂稽核與運作確保說明文件，且說明稽核與運作確保政策與程序將會每年定期審查與更新，並包含 CSP 應根據相關標準每年進行內外部稽核之評估作業相關佐證資料	CSP 提供機關租用服務範圍內之稽核與運作確保說明文件
	IaaS 服務類型	IS-3	CSP 須提供租用之虛擬機器相關維運與操作管理機制說明(例如：虛擬機器隔離、虛擬機器遷移、虛擬防火牆及虛擬機器更新管理)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂虛擬機器維運與操作管理政策與程序，並針對虛擬機器隔離、虛擬機器遷移、虛擬防火牆及虛擬機器更新管理提供相關配置與管理機制之說明	CSP 提供機關租用服務範圍內之虛擬機器維運與操作管理政策與程序

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	IaaS 服務類型	IS-4	CSP 須提供雲端服務維持運營持續性之相關佐證資料	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂運營持續管理政策與程序，並每年定期審查與更新運營持續管理政策與程序 2.CSP 已針對租用範圍內之服務制訂運營持續計劃與演練報告，並每年定期審查與更新運營持續計劃，且定期針對計畫進行演練	1.CSP 提供機關租用服務範圍內之運營持續管理政策和程序 2.CSP 提供機關租用服務範圍內之運營持續計劃 3.CSP 提供機關租用服務範圍內之運營持續計劃演練報告
	IaaS 服務類型	IS-5	CSP 須協助機關配合行政院秘書長院臺護長字第 1090201804A 號函之要求，確遵公務機關使用資通訊產品(含軟體、硬體及服務)相關原則，提供機關租用服務範圍內且涉及處理機關資料之設備，CSP 應聲明使用或未使用該等	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供承諾書聲明其服務範圍內且涉及處理機關資料之設備，使用或未使用該等「不得使用之資通訊產品」，且說明 CSP 了解並將協助	CSP 提供機關租用服務範圍內之承諾書說明了解行政院秘書長院臺護長字第 1090201804A 號函之要求事項

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			「不得使用之資通訊產品」；另機關可參考美國貿易局網站所公布之綜合審查清單(https://www.trade.gov/data-visualization/csl-search)或其他國家之標準進行風險評估	機關配合行政院秘書長院臺護長字第1090201804A 號函之要求事項	
營運管理	資源需求	OM-1	CSP 須至少提供虛擬機、容器、APP 及無伺服器等 4 種服務，並支援 IAM 機制協助機關進行權限控管作業(機關可視實際需求自行調整)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分與存取管理說明文件，且說明提供虛擬機、容器、APP 及無伺服器進行身分與存取服務的管理，機關能夠管理使用者生命週期包含帳號註冊、角色權限分配、角色權限變更及帳號刪除之管控，並均需有相應審核與管控過程 2.CSP 已於提供之	1.CSP 提供機關租用服務範圍內之身分與存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				內外部獨立稽核報告中說明虛擬機、容器、APP 及無伺服器身分與存取管理服務之正確性與有效性	
	維運管控	OM-2	CSP 須具有應用服務及系統資源(實體或虛擬資源)使用監控機制，亦應可依現有實體或虛擬資源動態調整分配	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定應用服務及系統資源(實體或虛擬資源)使用監控機制說明文件，且說明其使用之監控機制與監控範圍 2.CSP 已於提供之內外部獨立稽核報告中說明應用服務及系統監控機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之應用服務及系統資源(實體或虛擬資源)使用監控機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	維運管控	OM-3	CSP 須支援自機關登入服務後之相關操作及活動紀錄，並能按機關要求自動保存相關紀錄期限設定調整之功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定相關操作及活動紀錄保存說明文件，且說明機關能夠依照其需求自行調整相關紀錄保存期限之設定	CSP 提供機關租用服務範圍內之相關操作及活動紀錄保存說明文件
	維運管控	OM-4	政府公有雲儲存資料(含備援、備份資料)存放實體位置，以台灣為優先，不得以直接或間接方式存放於大陸、港澳地區	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供備援與備份資料的實際存放位置，且說明政府公有雲資料(含備援、備份資料)存放實體位置，將以台灣為優先，不得以直接或間接方式存放於大陸、港澳地區	CSP 提供機關租用服務範圍內之備援與備份資料的實際存放位置說明文件
	維運管控	OM-5	機關應自行選定公有雲服務之資料儲存地 CSP 須揭露機	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項	1.CSP 提供機關租用服務範圍內之公有雲資料處理與管

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			關選定公有雲資料儲存所在地點機關若選擇位於我國境外之資料儲存地，則該區域資安防護不得低於 ISO 27001	目是否具備： CSP 已針對租用範圍內之服務制定之公有雲資料處理與管理程序說明文件，且說明若選擇資料儲存地若非為我國境內，CSP 能夠提供當地相關雲端資安防護之檢核報告(該資安防護要求項目不得於 ISO 27001)	理程序說明文件 2.CSP 提供機關租用服務範圍內之他國當地相關雲端資安防護之檢核報告
	維運管控	OM-6	CSP 或其認證代理商須於我國具備 24 小時專業技術支援人員	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定技術支援服務說明文件，且說明於台灣或其認證代理商具備 24 小時專業技術支援人員，並提供專屬聯絡方式	CSP 提供機關租用服務範圍內之技術支援服務說明文件
	維運管控	OM-7	CSP 若使用特殊資料格式或儲存加密等技術致未來移轉不易時，須盡告知之義務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範	CSP 提供機關租用服務範圍內之安全互操作性與可移植性之管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				圍內之服務制定安全互操作性與可移植性之管理機制說明文件，且說明當 CSP 若使用特殊資料格式或儲存加密等技術須盡告知之義務	
	維運管控	OM-8	CSP 內部進行作業調整設定時應確保不影響客戶服務，若發生資安事件時，須主動通報機關並能於服務水準要求期限內恢復服務 CSP 須協助提供相關使用設定，協助機關能接獲有關服務異常的通知	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定服務水平管理說明文件，且說明若 CSP 內部進行作業調整設定時將確保不影響客戶服務，若發生資安事件時，將主動通報機關並能於服務水準要求期限內恢復服務，並協助機關能有效接獲有關服務異常的通知 2.CSP 已針對租用範圍內之服務制定資安事件管理制定應變計畫與演練報告，且針對資安事	1.CSP 提供機關租用服務範圍內之服務水平管理說明文件 2.CSP 提供機關租用服務範圍內之資安事件管理政策與程序 3.CSP 提供機關租用服務範圍內之資安事件應變計畫 4.CSP 提供機關租用服務範圍內之資安事件演練報告 5.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				件管理定期進行演練，演練過程包含當事件發生時能有效恢復至事件發生前之穩定設定檔 3.CSP 已於提供之內外部獨立稽核報告中說明資安事件通報機制之正確性與有效性	
	資訊資產	OM-9	CSP 應提供受委託雲端服務之清冊	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供完整的服務使用清冊供機關進行確認	CSP 提供機關租用服務範圍內之雲端服務使用清冊
	廠商選擇	OM-10	CSP 不得為大陸廠商，亦須符合國內對中資及港資限制之規範	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供公司申請註冊國家的相關佐證資料，且說 CSP 並非大陸廠商	CSP 提供機關租用服務範圍內之公司申請註冊國家的相關佐證資料

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	存取控制	OM-11	CSP 須支援至少 3 種多元身分識別機制(如雙因子及 OAuth2 等)進行存取授權	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分識別與存取管理說明文件，且說明其支援至少 3 種多元身分識別機制(如雙因子及 OAuth2 等)進行存取授權 2.CSP 已於提供之內外部獨立稽核報告中說明多元身分識別機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之身分識別與存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	存取控制	OM-12	CSP 須提供可支援機關遠端管理人員及設備之安全技術(例：來源 IP 限定、角色型存取控制、雙因素認證、端點設備及安全狀態等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定遠端服務存取管理說明文件，且說明能夠支援機關自行定義遠端管理人員及設備所需之安全技術(例：來源 IP 限定、角色型存取	1.CSP 提供機關租用服務範圍內之遠端服務存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				控制、雙因素認證、端點設備及安全狀態等) 2.CSP 已於提供之內外部獨立稽核報告中說明遠端服務存取之正確性與有效性	
	存取控制	OM-13	CSP 若需使用機關之相關稽核紀錄，雙方須訂定明確之權利與義務規定，並經機關同意後方可使用	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定身稽核紀錄管理機制說明文件，且說明相關稽核紀錄須經機關同意後方可使用，並已明確訂定雙方之權利與義務	CSP 提供於機關租用服務範圍內之稽核紀錄管理機制說明文件
	存取控制	OM-14	CSP 不得以任何理由限制機關可不受任何限制，於通過身分識別後，存取其使用服務之檔案、資料或文件	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定身分識別與存取管理機制說明文件，且說明當機關通過相關身分識別後將能	CSP 提供機關租用服務範圍內之身分識別與存取管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				不受限制存取其使用服務之檔案、資料或文件	
	存取控制	OM-15	CSP 須訂定對系統管理及維運人員之聘用與管理(含帳號權限)，且應制定保密協議，要求其員工、供應商均須確實遵守，未經同意不得瀏覽機關用戶儲存之資料及紀錄；另若有複委託之情形，其相關要求應等同於原合約	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分識別與存取管理機制說明文件與第三方供應商管理說明文件，且規範相關系統管理及維運人員的存取管理(含帳號權限)受到管控 2.CSP 已針對租用範圍內之服務要求相關員工、供應商須簽訂保密協議，協議內容須包含未經同意不得瀏覽機關儲存之資料及紀錄 3.CSP 已針對租用範圍內之服務規範如有複委託之情形，其相關要求應	1.CSP 提供機關租用服務範圍內之身分識別與存取管理機制說明文件 2.CSP 提供機關租用服務範圍內之第三方供應商管理說明文件 3.CSP 提供機關租用服務範圍內之員工、供應商簽訂之保密協議範本 4.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				等同於原合約 4.CSP 已於提供之內外部獨立稽核報告中說明委外與第三方供應商管理機制之正確性與有效性	
	存取控制	OM-16	CSP 須協助機關在存取控制方面設置 GCB 之技術支援	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資訊系統組態設定說明文件，且說明 CSP 能夠提供機關技術支援以配置政府組態基準(GCB)	CSP 提供機關租用服務範圍內之資訊系統組態設定說明文件
	服務可用性	OM-17	CSP 提供之機關相關服務(IaaS、PaaS 及 SaaS)服務可用率至少須達 99.9%以上	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定服務可用性管理說明文件，且說明租用範圍內之服務可用率至少達 99.9%以上	CSP 提供機關租用服務範圍內之服務可用性管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	服務可用性	OM-18	所採用雲服務 CSP 虛擬主機或容器異常時，在機關按照 CSP 虛擬機器/容器高可用性設定架構下，服務須能支援自動移轉至另一台備用機上繼續執行	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定設備備援機制說明文件，且說明當虛擬主機或容器異常時，服務能夠自動移轉至另一台備用機上繼續執行且不影響服務運行 2.CSP 已於提供之內外部獨立稽核報告中說明資訊系統備援機制管理之正確性與有效性	1.CSP 提供機關租用服務範圍內之資訊設備備援機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	服務可用性	OM-19	CSP 須依據機關選定之服務提供營運持續計畫，包含風險管理、災害管理、程式及設備管理、供應鏈管理、品質管理、緊急事件管理及相關管理之控管流程(生命週期)或具 ISO 22301 營運持續管理國際標準認證，以確保可達成服務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定營運持續計畫管理說明文件，且包含風險管理、災害管理、程式及設備管理、供應鏈管理、品質管理、緊急事件管理及相關營運	1.CSP 提供機關租用服務範圍內之營運持續計畫管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			水準要求	之控管流程(生命週期) 2.CSP 已於提供之內外部獨立稽核報告中說明提供之服務的營運持續計畫與管理機制之正確性與有效性	
	服務可用性	OM-20	對於災難復原資料的保全及復原，CSP 須提供完整復原機制服務，並依據委託機關之需求提供最佳實務與最符合經濟效益之建議方案	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定災難復原計畫管理政策與程序，且說明機關能依業務需求調整最大可容忍資料遺失時間與最大可容忍資訊服務復原時間	CSP 提供機關租用服務範圍內之災難復原計畫管理說明文件
	服務可用性	OM-21	CSP 是否同意如因機關公務預算編列問題發生延遲付款或付款額度不足之情況，可依機關需求展延既有服務，且不可影響服務水準	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件與服務水平協定範本，且說明如機	1.CSP 提供機關租用服務範圍內之收費機制說明文件 2.CSP 提供機關租用服務範圍內之服務水平協定範本

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				關因公務預算編列問題發生延遲付款或付款額度不足之情況，將能夠持續展延既有服務並維持服務水準	
	服務可用性	OM-22	各項收費制度應明定於契約內，非經雙方同意，不得任意變更資費及收費機制	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件與服務水平協定範本，且說明各項收費度已明訂於範本內並未經雙方同意不得任意變更資費及收費機制	1.CSP 提供機關租用服務範圍內之收費機制說明文件 2.CSP 提供機關租用服務範圍內之服務水平協定範本
	雲端服務事故通報	OM-23	CSP 提供之公有雲服務須具備偵測入侵嘗試警示服務，並自動發送警示給機關用戶	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定入侵偵測與通報機制說明文件，且說明其使用之入侵偵測機制、偵測之範圍、偵測通報流程	1.CSP 提供機關租用服務範圍內之入侵偵測與通報機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				及通報之後續處理方式 2.CSP 已於提供之內外部獨立稽核報告中說明入侵嘗試警示與通報機制之正確性與有效性	STAR)
	雲端服務事故通報	OM-24	如租用之公有雲發生資安或個資外洩事件，CSP 須於雙方合約時限內主動通報相關機關外，並應確認機關連繫窗口收到通知，並於事件處理完成後提出說明(雙方須訂定通報時限)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且說明當發生資安或個資外洩事件時，CSP 將主動聯繫機關窗口，並於事件發生後的依定期限內提出說明 2.CSP 已於提供之內外部獨立稽核報告中說明資安或個資外洩事件處理機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	雲端服務事故通報	OM-25	CSP 須提供資安事件通報標準作業程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且包含以下項目： –定義通報機關之資安事件範圍 –規範對於資安事件發生時，其可揭露程度與相關之應變流程 –規範當識別資安事件發生後之目標通報時限 –規範當識別資安事件發生後之通報流程與資安事件聯絡窗口 –規範針對不同資安事件發生，提供相對應之補救措施	CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件
通訊管理	公有雲與 GSN 網路介接	CM-1	CSP 須提供連接至機關(GSN 網路)安全連線建議	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網	CSP 提供機關租用服務範圍內之網路安全連線管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				路安全連線管理說明文件，且說明如須連接至 GSN 網路將提供相關安全連線供機關進行配置(例如：IPSec VPN、網路專線服務)	
	系統與通訊加密服務	CM-2	CSP 須提供資料傳輸(Data in Transit)及靜態資料(Data at Rest)儲存時加解密方案，以保障資料安全性	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定料傳輸及靜態資料加密管理說明文件，且說明機關能依其業務需求自行配置加解密方案 2.CSP 已於提供之內外部獨立稽核報告中說明資料加密機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之資料傳輸及靜態資料加密管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	系統與通訊加密服務	CM-3	CSP 提供金鑰保管服務與加密機制須符合第三方驗證(FIPS140-2 或 FedRAMP 等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務通過第	CSP 提供機關租用服務範圍內之金鑰管理機制第三方驗證報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				三方驗證其金鑰保管服務與機制，其驗證標準為 FIPS140-2、FedRAMP 其中之一	
資安與隱私管理	資安技術面要求	SP-1	配合「資通安全責任等級分級辦法」，CSP 須協助客戶自外部進行網站弱點掃描與系統滲透測試或提供相同服務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安檢測連線申請與檢測說明相關文件，或說明 CSP 能於平台提供相同服務	CSP 提供機關租用服務範圍內之相關資安檢測連線申請與檢測說明相關文件
	資安技術面要求	SP-2	雲端服務須具備 TLS v1.2 以上安全通訊協定	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網路安全連線作業說明文件，且說明於已使用 TLS v1.2 以上進行通訊協定加密	CSP 提供機關租用服務範圍內之網路安全連線作業說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	資安技術面要求	SP-3	CSP 須提供租用服務之整體資訊安全管理架構相關佐證資料，並提供可選用的安全強化管控方案	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定整體資訊安全管理架構或提供相關資安管理報告，說明 CSP 持續管理其資安控管情形	CSP 提供機關租用服務範圍內之整體資訊安全管理架構或相關持續維持資安管理之證明報告
	資安技術面要求	SP-4	CSP 須提供網路惡意活動檢視紀錄權限與管控機制	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網路惡意活動監控機制說明文件，且說明其內容包含監控機制、監控範圍及機關檢視監控紀錄流程與權限管理之說明	CSP 提供機關租用服務範圍內之網路惡意活動監控機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	資安技術面要求	SP-6	CSP 所提供之防毒軟體服務(可含原廠自有解決方案)：須包含於 3 大防毒軟體評鑑機構(AV-Comparatives 、AV-TEST 與 Virus Bulletin)所公布最新檢測清單之非大陸廠商，且病毒碼必須能即時更新之服務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定防毒軟體管理機制說明文件，且說明佈署之防毒軟體(可含原廠自有解決方案)：須包含於 3 大防毒軟體評鑑機構(AV-Comparatives、AV-TEST 與 Virus Bulletin)符合 3 大防毒軟體評鑑機構所公布之最新清單與提供病毒碼即時更新之服務	CSP 提供機關租用服務範圍內之防毒軟體管理機制說明文件
	資安技術面要求	SP-7	CSP 須提供機關租用範圍內防火牆之服務：機關可自行定義防火牆機制及規則(如設定目的虛擬機及特定連接埠)，設定防火牆規則	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定防火牆使用與管理機制說明文件，且說明機關能夠自行定義防火牆機制及規則(如設定目的虛	CSP 提供機關租用服務範圍內之防火牆使用與管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				擬機及特定連接埠)	
	資安技術面要求	SP-8	CSP 須提供 WAF 服務供機關選用	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供 WAF 服務供機關進行選擇與配置，且說明機關能夠自訂 WAF 服務規則(例如：SQL injection、Cross Site Scripting)	CSP 提供機關租用服務範圍內之 WAF 服務使用說明文件
	資安技術面要求	SP-9	CSP 須提供 IDS 或 IPS 相關服務供機關選用，且提供配置與管理 IDS 或 IPS 的功能或技術支援窗口	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定入侵偵測系統(IDS)或入侵防禦系統(IPS)使用與管理機制說明文件，且說明 CSP 將會提供機關配置入侵偵測系	CSP 提供機關租用服務範圍內之入侵偵測系統(IDS)或入侵防禦系統(IPS)使用與管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				統(IDS)或入侵防禦系統(IPS)之相關技術支援	
	資安技術面要求	SP-10	CSP 須提供(或委託第三方)7*24 SOC 服務，或配合機關 SOC 需求支援轉傳相關紀錄	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定(SOC 服務使用機制說明文件，且說明其使用之監控機制、監控之範圍及監控通報機制，或說明 CSP 能夠配合機關資安監控中心需求轉傳相關紀錄	CSP 提供機關租用服務範圍內之資安監控中心(SOC)服務使用機制說明文件
	資安與隱私稽核	SP-11	CSP 如發生資安事件、個資外洩或其他必要事項，CSP 須配合檢調單位調查	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且說明當發生資安事	CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				件、個資外洩或其他必要事項，CSP 應配合檢調單位進行調查	
	資安與隱私稽核	SP-12	CSP 須依照雙方契約約定，配合接受委辦公務機關(含委託查核單位)之稽核活動	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定稽核管理機制，且說明 CSP 會配合接受委辦公務機關(含委託查核單位)進行稽核活動	CSP 提供機關租用服務範圍內之稽核管理機制
	資安與隱私稽核	SP-13	CSP 除被要求遵循法律有效且具有約束力的命令（例如傳票、搜索令或法院命令），未經機關同意，不得披露或提供機關租用服務及儲存於 CSP 公有雲上任何資料	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資料保密協議，且說明除被要求遵循法律有效且具有約束力的命令（例如傳票、搜索令或法院命令），未經機關同意，不得披露或	CSP 提供機關租用服務範圍內之資料保密協議

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				提供機關租用服務及儲存於 CSP 公有雲上所有資料	

表 2：PaaS 服務類型檢測項目表

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
服務管理	雲端服務共同基本要求	CC-1	CSP 須提供機關管理平臺服務介面/網站	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定服務管理平臺說明文件，且說明 CSP 具備專屬平臺供機關進行其服務配置與管理	CSP 提供機關租用服務範圍內之服務管理平臺說明文件
	雲端服務共同基本要求	CC-2	CSP 提供的網站與介面須可支援網站線上隨時進行申請，修改或退租所提供之雲端服務資源變更功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定後服務及資源變更說明文件，且說明使用者能夠隨時透過申請方式修改或退租雲端服務資源，並提供功能展示網站的畫面	CSP 提供機關租用服務範圍內之服務及資源變更說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	雲端服務共同基本要求	CC-3	CSP 提供之平台須支援至少 3 種主流瀏覽器的後台管理及服務使用機制(如：透過瀏覽器設定、遠端桌面管理、REST API 管理或 Console 管理等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務說明瀏覽器的廠牌與版本，且說明服務平台支援至少 3 種主流瀏覽器 2.後台管理服務使用機制支援(如：透過瀏覽器設定、遠端桌面管理、REST API 管理或 Console 管理等)	CSP 提供機關租用服務範圍內之後台服務管理機制說明文件
	雲端服務共同基本要求	CC-4	CSP 提供之平台須有多租戶設計，不同租戶帳號須有獨立作業環境及管理服務頁面，且操作資料不會相互影響	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定使用者身分認證與存取控制管理說明文件，且說明不同帳號登入系統，有獨立作業環境或管理頁面，使用者操作資料不會相互影響 (例如:於其中一	1.CSP 提供機關租用服務範圍內之使用者身分認證與存取控制管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				個帳號新增一筆資料，不會影響其他用戶帳號) 2.CSP 已於提供之內外部獨立稽核報告中說明使用者與租戶隔離管控之正確性與有效性	
	雲端服務共同基本要求	CC-5	CSP 提供之應用服務架構須具備資源彈性擴展/回收設計及使用者資源彈性變更功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂資源變更說明文件，且說明應用服務架構具備資源彈性擴展與回收設計，機關能夠依其需求變更資源配置 2.CSP 已於提供之內外部獨立稽核報告中說明服務資源變更功能之正確性與有效性	1.CSP 提供機關租用服務範圍內之資源變更說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	雲端服務共同基本要求	CC-6	CSP 提供之平台須具備各別租戶使用之資源(服務)度量功能，並以儀表板方式呈現	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定使用者資源監控說明文件，且說明將提供各別使用者以儀表板方式檢視資源(服務)度量	CSP 提供機關租用服務範圍內之使用者資源監控說明文件
	雲端服務共同基本要求	CC-7	CSP 提供之平台須具備即時檢視費用功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件，且說明具備即時檢視服務收費情形	CSP 提供機關租用服務範圍內之收費機制說明文件
	雲端服務共同基本要求	CC-8	CSP 所取得之 ISO 27001 第三方認證，範圍須包括機關選用服務所有項目	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供相關第三方認證報告，且認證範圍須保括選用服務所有	CSP 提供機關租用服務範圍內之第三方認證報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				項目	
	IaaS 服務類型	IS-1	CSP 須至少符合 ISO 27001 及 ISO 27017 (或 CSA STAR 等)標準的安全措施，CSP 處理資料若包含個資則須符合 ISO 27701(或 BS 10012)及 ISO 27018；CSP 若有通過其他國家雲端安全相關規範，可提供佐證資料	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務提供 ISO 27001 及 ISO 27017 (或 CSA STAR)驗證證書或報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內 2.CSP 已針對租用範圍內之服務提供 ISO 27701(或 BS 10012) 及 ISO 27018 驗證證書或報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內 3.CSP 已針對租用範圍內之服務提供他國雲端安全規範認證與報告，且認證由標準機構	1.CSP 提供機關租用服務範圍內之 ISO 27001 及 ISO 27017 (或 CSA STAR)驗證證書或報告 2.CSP 提供機關租用服務範圍內之 ISO 27701(或 BS 10012) 及 ISO 27018 驗證證書或報告 3.若 CSP 提供機關租用服務範圍內另有通過其他國家雲端安全相關規範，能夠提供其驗證證書或報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內	
	IaaS 服務類型	IS-2	CSP 對提供之基礎設施須建立稽核與運作確保政策與程序，並至少每年審查與更新這些政策和程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂稽核與運作確保說明文件，且說明稽核與運作確保政策與程序將會每年定期審查與更新，並包含 CSP 應根據相關標準每年進行內外部稽核之評估作業相關佐證資料	CSP 提供機關租用服務範圍內之稽核與運作確保說明文件
	IaaS 服務類型	IS-3	CSP 須提供租用之虛擬機器相關維運與操作管理機制說明(例如：虛擬機器隔離、虛擬機器遷移、虛擬防火牆及虛擬機器更新管理)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂虛擬機器維運與操作管理政策與程序，並針對虛擬機器隔離、虛擬機器遷移、虛擬防火牆及虛擬機器更新管理	CSP 提供機關租用服務範圍內之虛擬機器維運與操作管理政策與程序

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				提供相關配置與管理機制之說明	
	IaaS 服務類型	IS-4	CSP 須提供雲端服務維持運營持續性之相關佐證資料	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂運營持續管理政策與程序，並每年定期審查與更新運營持續管理政策與程序 2.CSP 已針對租用範圍內之服務制訂運營持續計劃與演練報告，並每年定期審查與更新運營持續計劃，且定期針對計畫進行演練	1.CSP 提供機關租用服務範圍內之運營持續管理政策和程序 2.CSP 提供機關租用服務範圍內之運營持續計劃 3.CSP 提供機關租用服務範圍內之運營持續計劃演練報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	IaaS 服務類型	IS-5	CSP 須協助機關配合行政院秘書長院臺護長字第 1090201804A 號函之要求，確遵公務機關使用資通訊產品(含軟體、硬體及服務)相關原則，提供機關租用服務範圍內且涉及處理機關資料之設備，CSP 應聲明使用或未使用該等「不得使用之資通訊產品」；另機關可參考美國貿易局網站所公布之綜合審查清單(https://www.trade.gov/data-visualization/csl-search)或其他國家之標準進行風險評估	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供承諾書聲明其服務範圍內且涉及處理機關資料之設備，使用或未使用該等「不得使用之資通訊產品」，且說明 CSP 了解並將協助機關配合行政院秘書長院臺護長字第 1090201804A 號函之要求事項	CSP 提供機關租用服務範圍內之承諾書說明了解行政院秘書長院臺護長字第 1090201804A 號函之要求事項

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	PaaS 服務類型	PS-1	CSP 針對平台所使用之加密機制與金鑰管理，須建立並實施管理的政策、程序、角色和職責等，並定期審查且紀錄備查	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂加密機制與金鑰管理說明文件，且說明政策與程序將會每年定期審查與更新，並其包含以下項目： -定義並實施密碼、加密及金鑰管理的角色與職責 -依資料的機敏性、完整性及可用性與相關風險及加密技術的可行性，選擇適當加密演算法保護資料 -CSP 須為機關提供能夠自行管理資料加密金鑰的功能 -金鑰管理流程須涵蓋金鑰產生、更換、移除、銷毀、啟用、暫停、停用、備份、外洩及恢復	CSP 提供機關租用服務範圍內之加密機制與金鑰管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	PaaS 服務類型	PS-2	CSP 須提供服務之平台、軟體主動挖掘安全漏洞，並建立完善通報、修補或重新發佈等程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂威脅與漏洞管理規範與程序，且說明其具備主動發掘軟體安全漏洞的能力，並建立完善通報、修補或重新發佈等程序，並所有 CSP 使用之系統與應用程式，需定期進行 OWASP TOP10 應用程式弱點掃描以及 CVE 系統弱點掃描，並修補被掃描出之弱點，弱點檢測結果需無中、高等級以上風險，始能確實降低被駭客入侵機率 2.CSP 已於提供之內外部獨立稽核報告中說明威脅與漏洞管理機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之威脅與漏洞管理規範與程序 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	PaaS 服務類型	PS-3	CSP 於平台提供之服務，若有引用其他外部第三方之公用服務(例：防毒軟體、端點管控或其它服務)，除須確保傳輸之資料不涉及機關資訊外，亦須事先告知	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂第第三方服務管理機制說明文件，且說明如有引用其他內部或外部之公用服務(例：防毒軟體、端點管控或其它服務)，除傳輸之資料將不涉及機關敏感資訊，亦須事先告知機關	CSP 提供機關租用服務範圍內之第三方服務管理機制說明文件
	PaaS 服務類型	PS-4	CSP 須確實保存資安事件追查所須之平台、系統與網路等日誌資訊，當機關使用之服務發生資安事件並提出調閱需求時，可即時提供參考	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂紀錄監測與管理機制說明文件，且說明當服務發生資安事件時，機關能夠調閱平台、系統與網路等日誌資訊以供即時提供參考，並可提供使用者連	1.CSP 提供機關租用服務範圍內之紀錄監測與管理機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				線日誌紀錄，記錄使用者登錄資訊，包括系統標識、登錄使用者、登錄時間、登錄 IP 及登錄終端等 2.CSP 已於提供之內外部獨立稽核報告中說明資訊系統紀錄監測管理機制之正確性與有效性	
	PaaS 服務類型	PS-5	CSP 須建立紀錄與監測政策，並落實相關程序管控	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂紀錄監測與管理機制說明文件，並其包含以下項目： -定義紀錄監測的機制 -定義紀錄監測的範圍 -規範紀錄日誌的保護方式 -規範對於異常紀錄與事件的反應	CSP 提供機關租用服務範圍內之紀錄監測與管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	PaaS 服務類型	PS-6	CSP 須提供資料轉移之工具或必要協助，以提供機關資料下載使用	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂資料轉移機制說明文件，且說明當機關如需將雲端服務中的資料進行轉移時，CSP 將會提供相關資料轉移之工具或協助	CSP 提供機關租用服務範圍內之資料轉移機制說明文件
營運管理	資源需求	OM-1	CSP 須至少提供虛擬機、容器、APP 及無伺服器等 4 種服務，並支援 IAM 機制協助機關進行權限控管作業(機關可視實際需求自行調整)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分與存取管理說明文件，且說明提供虛擬機、容器、APP 及無伺服器進行身分與存取服務的管理，機關能夠管理使用者生命週期包含帳號註冊、角色權限分配、角色權限變更及帳號刪除之管控，並均	1.CSP 提供機關租用服務範圍內之身分與存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				需有相應審核與管控過程 2.CSP 已於提供之內外部獨立稽核報告中說明虛擬機、容器、APP 及無伺服器身分與存取管理服務之正確性與有效性	
	維運管控	OM-2	CSP 須具有應用服務及系統資源(實體或虛擬資源)使用監控機制，亦應可依現有實體或虛擬資源動態調整分配	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定應用服務及系統資源(實體或虛擬資源)使用監控機制說明文件，且說明其使用之監控機制與監控範圍 2.CSP 已於提供之內外部獨立稽核報告中說明應用服務及系統監控機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之應用服務及系統資源(實體或虛擬資源)使用監控機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	維運管控	OM-3	CSP 須支援自機關登入服務後之相關操作及活動紀錄，並能按機關要求自動保存相關紀錄期限設定調整之功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務制定相關操作及活動紀錄保存說明文件，且說明機關能夠依照其需求自行調整相關紀錄保存期限之設定	CSP 提供機關租用服務範圍內之相關操作及活動紀錄保存說明文件
	維運管控	OM-4	政府公有雲儲存資料(含備援、備份資料)存放實體位置，以台灣為優先，不得以直接或間接方式存放於大陸、港澳地區	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務提供備援與備份資料的實際存放位置，且說明政府公有雲資料(含備援、備份資料)存放實體位置，將以台灣為優先，不得以直接或間接方式存放於大陸、港澳地區	CSP 提供機關租用服務範圍內之備援與備份資料的實際存放位置說明文件
	維運管控	OM-5	機關應自行選定公有雲服務之資料儲存地 CSP 須揭露機	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下	1.CSP 提供機關租用服務範圍內之公有雲資料處理與管

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			關選定公有雲資料儲存所在地點機關若選擇位於我國境外之資料儲存地，則該區域資安防護不得低於 ISO 27001	項目是否具備： CSP 已針對租用範圍內之服務制定之公有雲資料處理與管理程序說明文件，且說明若選擇資料儲存地若非為我國境內，CSP 能夠提供當地相關雲端資安防護之檢核報告(該資安防護要求項目不得於 ISO 27001)	理程序說明文件 2.CSP 提供機關租用服務範圍內之他國當地相關雲端資安防護之檢核報告
	維運管控	OM-6	CSP 或其認證代理商須於我國具備 24 小時專業技術支援人員	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定技術支援服務說明文件，且說明於台灣或其認證代理商具備 24 小時專業技術支援人員，並提供專屬聯絡方式	CSP 提供機關租用服務範圍內之技術支援服務說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	維運管控	OM-7	CSP 若使用特殊資料格式或儲存加密等技術致未來移轉不易時，須盡告知之義務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定安全互操作性與可移植性之管理機制說明文件，且說明當 CSP 若使用特殊資料格式或儲存加密等技術須盡告知之義務	CSP 提供機關租用服務範圍內之安全互操作性與可移植性之管理機制說明文件
	維運管控	OM-8	CSP 內部進行作業調整設定時應確保不影響客戶服務，若發生資安事件時，須主動通報機關並能於服務水準要求期限內恢復服務 CSP 須協助提供相關使用設定，協助機關能接獲有關服務異常的通知	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定服務水平管理說明文件，且說明若 CSP 內部進行作業調整設定時將確保不影響客戶服務，若發生資安事件時，將主動通報機關並能於服務水準要求期限內恢復服務，並協助機關能有效接獲有關服務	1.CSP 提供機關租用服務範圍內之服務水平管理說明文件 2.CSP 提供機關租用服務範圍內之資安事件管理政策與程序 3.CSP 提供機關租用服務範圍內之資安事件應變計畫 4.CSP 提供機關租用服務範圍內之資安事件演練報告 5.CSP 提供機關租用服務範圍內之內外部獨立稽核報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				異常的通知 2.CSP 已針對租用範圍內之服務制定資安事件管理制定應變計畫與演練報告，且針對資安事件管理定期進行演練，演練過程包含當事件發生時能有效恢復至事件發生前之穩定設定檔 3.CSP 已於提供之內外部獨立稽核報告中說明資安事件通報機制之正確性與有效性	(例如：ISO 27001、ISO27018、CSA STAR)
	資訊資產	OM-9	CSP 應提供受委託雲端服務之清冊	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供完整的服務使用清冊供機關進行確認	CSP 提供機關租用服務範圍內之雲端服務使用清冊
	廠商選擇	OM-10	CSP 不得為大陸廠商，亦須符合國內對中資及港資限制之規範	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供公	CSP 提供機關租用服務範圍內之公司申請註冊國家的相關佐證資料

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				司申請註冊國家的相關佐證資料，且說 CSP 並非大陸廠商	
	存取控制	OM-11	CSP 須支援至少 3 種多元身分識別機制(如雙因子及 OAuth2 等)進行存取授權	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分識別與存取管理說明文件，且說明其支援至少 3 種多元身分識別機制(如雙因子及 OAuth2 等)進行存取授權 2.CSP 已於提供之內外部獨立稽核報告中說明多元身分識別機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之身分識別與存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	存取控制	OM-12	CSP 須提供可支援機關遠端管理人員及設備之安全技術(例：來源 IP 限定、角色型存取控制、雙因素認證、端點設備及安全狀態等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定遠端服務存取管理說明文件，且說明能夠支援機關自行定義遠端管理人員及設備所需之安全技術(例：來源 IP 限定、角色型存取控制、雙因素認證、端點設備及安全狀態等) 2.CSP 已於提供之內外部獨立稽核報告中說明遠端服務存取之正確性與有效性	1.CSP 提供機關租用服務範圍內之遠端服務存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	存取控制	OM-13	CSP 若需使用機關之相關稽核紀錄，雙方須訂定明確之權利與義務規定，並經機關同意後方可使用	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定身稽核紀錄管理機制說明文件，且說明相關稽核紀錄須經	CSP 提供於機關租用服務範圍內之稽核紀錄管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				機關同意後方可使用，並已明確訂定雙方之權利與義務	
	存取控制	OM-14	CSP 不得以任何理由限制機關可不受任何限制，於通過身分識別後，存取其使用服務之檔案、資料或文件	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定身分識別與存取管理機制說明文件，且說明當機關通過相關身分識別後將能不受限制存取其使用服務之檔案、資料或文件	CSP 提供機關租用服務範圍內之身分識別與存取管理機制說明文件
	存取控制	OM-15	CSP 須訂定對系統管理及維運人員之聘用與管理(含帳號權限)，且應制定保密協議，要求其員工、供應商均須確實遵守，未經同意不得瀏覽機關用戶儲存之資料及紀錄；另若有複委託之情形，其相關要	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分識別與存取管理機制說明文件與第三方供應商管理說明文件，且規範相關系統管理及維運人員的存取管理	1.CSP 提供機關租用服務範圍內之身分識別與存取管理機制說明文件 2.CSP 提供機關租用服務範圍內之第三方供應商管理說明文件 3.CSP 提供機關租用服務範圍內之員工、供應商簽訂之保密協議範本

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			求應等同於原合約	(含帳號權限)受到管控 2.CSP 已針對租用範圍內之服務要求相關員工、供應商須簽訂保密協議，協議內容須包含未經同意不得瀏覽機關儲存之資料及紀錄 3.CSP 已針對租用範圍內之服務規範如有複委託之情形，其相關要求應等同於原合約 4.CSP 已於提供之內外部獨立稽核報告中說明委外與第三方供應商管理機制之正確性與有效性	4.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	存取控制	OM-16	CSP 須協助機關在存取控制方面設置 GCB 之技術支援	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資訊系統組態設定說明文件，且說明 CSP 能夠提供機關	CSP 提供機關租用服務範圍內之資訊系統組態設定說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				技術支援以配置政府組態基準(GCB)	
	服務可用性	OM-17	CSP 提供之機關相關服務(IaaS、PaaS 及 SaaS)服務可用率至少須達 99.9%以上	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定服務可用性管理說明文件，且說明租用範圍內之服務可用率至少達 99.9%以上	CSP 提供機關租用服務範圍內之服務可用性管理說明文件
	服務可用性	OM-18	所採用雲服務 CSP 虛擬主機或容器異常時，在機關按照 CSP 虛擬機器/容器高可用性設定架構下，服務須能支援自動移轉至另一台備用機上繼續執行	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定設備備援機制說明文件，且說明當虛擬主機或容器異常時，服務能夠自動移轉至另一台備用機上繼續執行且不影響服務運行	1.CSP 提供機關租用服務範圍內之資訊設備備援機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				2.CSP 已於提供之內外部獨立稽核報告中說明資訊系統備援機制管理之正確性與有效性	
	服務可用性	OM-19	CSP 須依據機關選定之服務提供營運持續計畫，包含風險管理、災害管理、程式及設備管理、供應鏈管理、品質管理、緊急事件管理及相關管理之控管流程(生命週期)或具 ISO 22301 營運持續管理國際標準認證，以確保可達成服務水準要求	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定營運持續計畫管理說明文件，且包含風險管理、災害管理、程式及設備管理、供應鏈管理、品質管理、緊急事件管理及相關營運之控管流程(生命週期) 2.CSP 已於提供之內外部獨立稽核報告中說明提供之服務的營運持續計畫與管理機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之營運持續計畫管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	服務可用性	OM-20	對於災難復原資料的保全及復原，CSP 須提供完整復原機制服務，並依據委託機關之需求提供最佳實務與最符合經濟效益之建議方案	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定災難復原計畫管理政策與程序，且說明機關能依業務需求調整最大可容忍資料遺失時間與最大可容忍資訊服務復原時間	CSP 提供機關租用服務範圍內之災難復原計畫管理說明文件
	服務可用性	OM-21	CSP 是否同意如因機關公務預算編列問題發生延遲付款或付款額度不足之情況，可依機關需求展延既有服務，且不可影響服務水準	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件與服務水平協定範本，且說明如機關因公務預算編列問題發生延遲付款或付款額度不足之情況，將能夠持續展延既有服務並維持服務水準	1.CSP 提供機關租用服務範圍內之收費機制說明文件 2.CSP 提供機關租用服務範圍內之服務水平協定範本

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	服務可用性	OM-22	各項收費制度應明定於契約內，非經雙方同意，不得任意變更資費及收費機制	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件與服務水平協定範本，且說明各項收費度已明訂於範本內並未經雙方同意不得任意變更資費及收費機制	1.CSP 提供機關租用服務範圍內之收費機制說明文件 2.CSP 提供機關租用服務範圍內之服務水平協定範本
	雲端服務事故通報	OM-23	CSP 提供之公有雲服務須具備偵測入侵嘗試警示服務，並自動發送警示給機關用戶	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定入侵偵測與通報機制說明文件，且說明其使用之入侵偵測機制、偵測之範圍、偵測通報流程及通報之後續處理方式 2.CSP 已於提供之內外部獨立稽核報告中說明入侵嘗試警示與通報機制之	1.CSP 提供機關租用服務範圍內之入侵偵測與通報機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				正確性與有效性	
	雲端服務事故通報	OM-24	如租用之公有雲發生資安或個資外洩事件，CSP 須於雙方合約時限內主動通報相關機關外，並應確認機關連繫窗口收到通知，並於事件處理完成後提出說明(雙方須訂定通報時限)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且說明當發生資安或個資外洩事件時，CSP 將主動聯繫機關窗口，並於事件發生後的依定期限內提出說明 2.CSP 已於提供之內外部獨立稽核報告中說明資安或個資外洩事件處理機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	雲端服務事故通報	OM-25	CSP 須提供資安事件通報標準作業程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且包含以下項目： –定義通報機關之資安事件範圍 –規範對於資安事件發生時，其可揭露程度與相關之應變流程 –規範當識別資安事件發生後之目標通報時限 –規範當識別資安事件發生後之通報流程與資安事件聯絡窗口 –規範針對不同資安事件發生，提供相對應之補救措施	CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
通訊管理	公有雲與GSN網路介接	CM-1	CSP 須提供連接至機關(GSN 網路)安全連線建議	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網路安全連線管理說明文件，且說明如須連接至 GSN 網路將提供相關安全連線供機關進行配置(例如：IPSec VPN、網路專線服務)	CSP 提供機關租用服務範圍內之網路安全連線管理說明文件
	系統與通訊加密服務	CM-2	CSP 須提供資料傳輸及靜態資料儲存時加解密方案，以保障資料安全性	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定料傳輸及靜態資料加密管理說明文件，且說明機關能依其業務需求自行配置加解密方案 2.CSP 已於提供之內外部獨立稽核報告中說明資料加密機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之資料傳輸及靜態資料加密管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	系統與通訊加密服務	CM-3	CSP 提供金鑰保管服務與加密機制須符合第三方驗證(FIPS140-2 或 FedRAMP 等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務通過第三方驗證其金鑰保管服務與機制，其驗證標準為 FIPS140-2、FedRAMP 其中之一	CSP 提供機關租用服務範圍內之金鑰管理機制第三方驗證報告
資安與隱私管理	資安技術面要求	SP-1	配合「資通安全責任等級分級辦法」，CSP 須協助客戶自外部進行網站弱點掃描與系統滲透測試或提供相同服務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安檢測連線申請與檢測說明相關文件，或說明 CSP 能於平台提供相同服務	CSP 提供機關租用服務範圍內之相關資安檢測連線申請與檢測說明相關文件
	資安技術面要求	SP-2	雲端服務須具備 TLS v1.2 以上安全通訊協定	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網	CSP 提供機關租用服務範圍內之網路安全連線作業說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				路安全連線作業說明文件，且說明於已使用 TLS v1.2 以上進行通訊協定加密	
	資安技術面要求	SP-3	CSP 須提供租用服務之整體資訊安全管理架構相關佐證資料，並提供可選用的安全強化管控方案	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定整體資訊安全管理架構或提供相關資安管理報告，說明 CSP 持續管理其資安控管情形	CSP 提供機關租用服務範圍內之整體資訊安全管理架構或相關持續維持資安管理之證明報告
	資安技術面要求	SP-4	CSP 須提供網路惡意活動檢視紀錄權限與管控機制	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網路惡意活動監控機制說明文件，且說明其內容包含監控機制、監控範圍及機關檢視監控紀錄流程與權限管理之	CSP 提供機關租用服務範圍內之網路惡意活動監控機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				說明	
	資安技術面要求	SP-5	CSP 須提供伺服器主機惡意活動檢視紀錄權限與管控機制	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定伺服器主機惡意活動監控機制說明文件，且說明其內容包含監控機制、監控範圍及機關檢視監控紀錄流程與權限管理之說明	CSP 提供機關租用服務範圍內之伺服器主機惡意活動監控機制說明文件
	資安技術面要求	SP-6	CSP 所提供之防毒軟體服務(可含原廠自有解決方案)：須包含於 3 大防毒軟體評鑑機構(AV-Comparatives、AV-TEST 與 Virus Bulletin)所公布最新檢測清單之非大陸廠商，且病毒碼必須能即時更新之服務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定防毒軟體管理機制說明文件，且說明佈署之防毒軟體(可含原廠自有解決方案)：須包含於 3 大防毒軟體評鑑機構(AV-Comparatives、	CSP 提供機關租用服務範圍內之防毒軟體管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				AV-TEST 與 Virus Bulletin)符合 3 大防毒軟體評鑑機構所公布之最新清單與提供病毒碼即時更新之服務	
	資安技術面要求	SP-7	CSP 須提供機關租用範圍內防火牆之服務：機關可自行定義防火牆機制及規則(如設定目的虛擬機及特定連接埠)，設定防火牆規則	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定防火牆使用與管理機制說明文件，且說明機關能夠自行定義防火牆機制及規則(如設定目的虛擬機及特定連接埠)	CSP 提供機關租用服務範圍內之防火牆使用與管理機制說明文件
	資安技術面要求	SP-8	CSP 須提供 WAF 服務供機關選用	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供 WAF 服務供機關進行選擇與配置，且說明機關能夠自訂 WAF 服務規則(例如：SQL	CSP 提供機關租用服務範圍內之 WAF 服務使用說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				injection、Cross Site Scripting)	
	資安技術面要求	SP-9	CSP 須提供 IDS 或 IPS 相關服務供機關選用，且提供配置與管理 IDS 或 IPS 的功能或技術支援窗口	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定入侵偵測系統(IDS)或入侵防禦系統(IPS)使用與管理機制說明文件，且說明 CSP 將會提供機關配置入侵偵測系統(IDS)或入侵防禦系統(IPS)之相關技術支援	CSP 提供機關租用服務範圍內之入侵偵測系統(IDS)或入侵防禦系統(IPS)使用與管理機制說明文件
	資安技術面要求	SP-10	CSP 須提供(或委託第三方)7*24 SOC 服務，或配合機關 SOC 需求支援轉傳相關紀錄	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定 SOC 服務使用機制說明文件，且說明其使用之監控機制、監控之範圍及監控通報機制，或說明 CSP 能夠配合機關資安監控中	CSP 提供機關租用服務範圍內之資安監控中心(SOC)服務使用機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				心需求轉傳相關紀錄	
	資安與隱私稽核	SP-11	CSP 如發生資安事件、個資外洩或其他必要事項，CSP 須配合檢調單位調查	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且說明當發生資安事件、個資外洩或其他必要事項，CSP 應配合檢調單位進行調查	CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件
	資安與隱私稽核	SP-12	CSP 須依照雙方契約約定，配合接受委辦公務機關(含委託查核單位)之稽核活動	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務制定稽核管理機制，且說明 CSP 會配合接受委辦公務機關(含委託查核單位)進行稽核活動	CSP 提供機關租用服務範圍內之稽核管理機制

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	資安與隱私稽核	SP-13	CSP 除被要求遵循法律有效且具有約束力的命令（例如傳票、搜索令或法院命令），未經機關同意，不得披露或提供機關租用服務及儲存於 CSP 公有雲上任何資料	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務制定資料保密協議，且說明除被要求遵循法律有效且具有約束力的命令（例如傳票、搜索令或法院命令），未經機關同意，不得披露或提供機關租用服務及儲存於 CSP 公有雲上所有資料	CSP 提供機關租用服務範圍內之資料保密協議

表 3：SaaS 服務類型檢測項目表

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
服務管理	雲端服務共同基本要求	CC-1	CSP 須提供機關管理平臺服務介面/網站	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定服務管理平臺說明文件，且說明 CSP 具備專屬平臺供機關進行其服務配置與管理	CSP 提供機關租用服務範圍內之服務管理平臺說明文件
	雲端服務共同基本要求	CC-2	CSP 提供的網站與介面須可支援網站線上隨時進行申請，修改或退租所提供之雲端服務資源變更功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定後服務及資源變更說明文件，且說明使用者能夠隨時透過申請方式修改或退租雲端服務資源，並提供功能展示網站的畫面	CSP 提供機關租用服務範圍內之服務及資源變更說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	雲端服務共同基本要求	CC-3	CSP 提供之平台須支援至少 3 種主流瀏覽器的後台管理及服務使用機制(如：透過瀏覽器設定、遠端桌面管理、REST API 管理或 Console 管理等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務說明瀏覽器的廠牌與版本，且說明服務平台支援至少 3 種主流瀏覽器 2.後台管理服務使用機制支援(如：透過瀏覽器設定、遠端桌面管理、REST API 管理或 Console 管理等)	CSP 提供機關租用服務範圍內之後台服務管理機制說明文件
	雲端服務共同基本要求	CC-5	CSP 提供之應用服務架構須具備資源彈性擴展/回收設計及使用者資源彈性變更功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂資源變更說明文件，且說明應用服務架構具備資源彈性擴展與回收設計，機關能夠依其需求變更資源配置 2.CSP 已於提供之內外部獨立稽核報告中說明服務資源	1.CSP 提供機關租用服務範圍內之資源變更說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				變更功能之正確性與有效性	
	雲端服務共同基本要求	CC-6	CSP 提供之平台須具備各別租戶使用之資源(服務)度量功能，並以儀表板方式呈現	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定使用者資源監控說明文件，且說明將提供各別使用者以儀表板方式檢視資源(服務)度量	CSP 提供機關租用服務範圍內之使用者資源監控說明文件
	雲端服務共同基本要求	CC-7	CSP 提供之平台須具備即時檢視費用功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件，且說明具備即時檢視服務收費情形	CSP 提供機關租用服務範圍內之收費機制說明文件
	雲端	CC-8	CSP 所取得之 ISO	由機關檢測人員檢	CSP 提供機關租用

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	服務共同基本要求		27001 第三方認證，範圍須包括機關選用服務所有項目	視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供相關第三方認證報告，且認證範圍須保括選用服務所有項目	服務範圍內之第三方認證報告
	IaaS 服務類型	IS-1	CSP 須至少符合 ISO 27001 及 ISO 27017 (或 CSA STAR 等)標準的安全措施，CSP 處理資料若包含個資則須符合 ISO 27701(或 BS 10012)及 ISO 27018；CSP 若有通過其他國家雲端安全相關規範，可提供佐證資料	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務提供 ISO 27001 及 ISO 27017 (或 CSA STAR)驗證證書或報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內 2.CSP 已針對租用範圍內之服務提供 ISO 27701(或 BS 10012) 及 ISO 27018 驗證證書或報告，且認證由標準機構(如:BSI、SGS)提供，另該	1.CSP 提供機關租用服務範圍內之 ISO 27001 及 ISO 27017 (或 CSA STAR)驗證證書或報告 2.CSP 提供機關租用服務範圍內之 ISO 27701(或 BS 10012) 及 ISO 27018 驗證證書或報告 3.若 CSP 提供機關租用服務範圍內另有通過其他國家雲端安全相關規範，能夠提供其驗證證書或報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				認證仍處於有效時程範圍內 3.CSP 已針對租用範圍內之服務提供他國雲端安全規範認證與報告，且認證由標準機構(如:BSI、SGS)提供，另該認證仍處於有效時程範圍內	
	IaaS 服務類型	IS-2	CSP 對提供之基礎設施須建立稽核與運作確保政策與程序，並至少每年審查與更新這些政策和程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂稽核與運作確保說明文件，且說明稽核與運作確保政策與程序將會每年定期審查與更新，並包含 CSP 應根據相關標準每年進行內外部稽核之評估作業相關佐證資料	CSP 提供機關租用服務範圍內之稽核與運作確保說明文件
	IaaS 服務類型	IS-4	CSP 須提供雲端服務維持運營持續性之相關佐證資料	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用	1.CSP 提供機關租用服務範圍內之運營持續管理政策和程序 2.CSP 提供機關租

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				範圍內之服務制訂運營持續管理政策與程序，並每年定期審查與更新運營持續管理政策與程序 2.CSP 已針對租用範圍內之服務制訂運營持續計劃與演練報告，並每年定期審查與更新運營持續計劃，且定期針對計畫進行演練	用服務範圍內之運營持續計劃 3.CSP 提供機關租用服務範圍內之運營持續計劃演練報告
	PaaS 服務類型	PS-2	CSP 須提供服務之平台、軟體主動挖掘安全漏洞，並建立完善通報、修補或重新發佈等程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂威脅與漏洞管理規範與程序，且說明其具備主動發掘軟體安全漏洞的能力，並建立完善通報、修補或重新發佈等程序，並所有 CSP 使用之系統與應用程式，需定期進行 OWASP TOP10 應用程式弱點掃描以及	1.CSP 提供機關租用服務範圍內之威脅與漏洞管理規範與程序 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				CVE 系統弱點掃描，並修補被掃描出之弱點，弱點檢測結果需無中、高等級以上風險，始能確實降低被駭客入侵機率 2.CSP 已於提供之內外部獨立稽核報告中說明威脅與漏洞管理機制之正確性與有效性	
	PaaS 服務類型	PS-3	CSP 於平台提供之服務，若有引用其他外部第三方之公用服務(例：防毒軟體、端點管控或其它服務)，除須確保傳輸之資料不涉及機關資訊外，亦須事先告知	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂第第三方服務管理機制說明文件，且說明如有引用其他內部或外部之公用服務(例：防毒軟體、端點管控或其它服務)，除傳輸之資料將不涉及機關敏感資訊，亦須事先告知機關	CSP 提供機關租用服務範圍內之第三方服務管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	PaaS 服務類型	PS-4	CSP 須確實保存資安事件追查所須之平台、系統與網路等日誌資訊，當機關使用之服務發生資安事件並提出調閱需求時，可即時提供參考	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂紀錄監測與管理機制說明文件，且說明當服務發生資安事件時，機關能夠調閱平台、系統與網路等日誌資訊以供即時提供參考，並可提供使用者連線日誌紀錄，記錄使用者登錄資訊，包括系統標識、登錄使用者、登錄時間、登錄 IP 及登錄終端等 2.CSP 已於提供之內外部獨立稽核報告中說明資訊系統紀錄監測管理機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之紀錄監測與管理機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	PaaS 服務類型	PS-5	CSP 須建立紀錄與監測政策，並落實相關程序管控	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂紀	CSP 提供機關租用服務範圍內之紀錄監測與管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				錄監測與管理機制說明文件，並其包含以下項目： -定義紀錄監測的機制 -定義紀錄監測的範圍 -規範紀錄日誌的保護方式 -規範對於異常紀錄與事件的反應	
	SaaS 服務類型	SS-1	CSP 須根據組織定義的安全要求，於變更過程中的測試及部署均應有完善管理作為及安全管控，服務若有重大調整(例：調整導致服務中斷等)須提前告知	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂變更管理機制說明文件，且說明若租用之服務有重大調整(例：調整導致服務中斷等)將提前告知，並其變更過程中的測試及部署應包含以下項目： -定義變更風險管理流程，相關變便包含應用程式、系統、基礎設施配置等	1.CSP 提供機關租用服務範圍內之變更管理機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				-規範變更品質控管流程與測試流程 -規範變更異常管理流程 -定義變更復原管理流程 -規範重大變更通報機制 2.CSP 已於提供之內外部獨立稽核報告中說明變更管理機制之正確性與有效性	
	SaaS 服務類型	SS-2	CSP 須具備 SSDLC 機制，確保不同應用程序間安全運作，並可提供機關相關佐證資料	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂 SSDLC 機制，且包含以下項目： -根據業務目標、安全需求及合規義務定義應用程式安全基線與指標 -依據 CSP 定義之安全要求，為應用程式的設計、開發、部署及運行定義並實施 SSDLC 流程	1.CSP 提供機關租用服務範圍內之 SSDLC 機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				-規範應用程式資訊安全測試流程，包括新開發、更新及新版本的應用程式 2.CSP 已於提供之內外部獨立稽核報告中說明 SSDLC 機制之正確性與有效性	
	SaaS 服務類型	SS-3	CSP 須確保機關資料、帳號權限與其他機關彼此區隔	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制訂公有雲多租戶管理機制說明文件，且說明 CSP 能夠提供相關保護機制以確保不會受到其他機關租戶或來自網際網路的攻擊，以保持租戶之間資料、帳號權限與系統運作之獨立性與安全性	CSP 提供機關租用服務範圍內之公有雲多租戶管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	SaaS 服務類型	SS-4	CSP 須提供明確之資料儲存、網路及其他相關資源使用監測資訊，並於達設定之容量門檻時，提供機關告警介面	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制訂資料儲存、網路及其他相關資源使用監控機制說明文件，且包含以下項目： -定義監控的機制 -定義監控的範圍 -規範監控紀錄的保護方式 -規範當到達機關設定之監控容量門檻時，將提供機關告警介面 2.CSP 已於提供之內外部獨立稽核報告中說明資訊系統資源使用監控機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之資料儲存、網路及其他相關資源使用監控機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	SaaS 服務類型	SS-5	CSP 須提供機關租用 SaaS 服務產品支援規格清單	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供 SaaS 服務之產品	CSP 提供機關租用服務範圍內之 SaaS 服務之支援裝置清單(或限制清單)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				支援規格清單(或限制清單)，且包含以下項目： -支援存取 SaaS 服務的裝置的種類 -支援存取 SaaS 服務的裝置版本 -支援存取 SaaS 服務裝置的安全防護措施要求	
營運管理	維運管控	OM-2	CSP 須具有應用服務及系統資源(實體或虛擬資源)使用監控機制，亦應可依現有實體或虛擬資源動態調整分配	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定應用服務及系統資源(實體或虛擬資源)使用監控機制說明文件，且說明其使用之監控機制與監控範圍 2.CSP 已於提供之內外部獨立稽核報告中說明應用服務及系統監控機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之應用服務及系統資源(實體或虛擬資源)使用監控機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	維運管控	OM-3	CSP 須支援自機關登入服務後之相關操作及活動紀錄，並能按機關要求自動保存相關紀錄期限設定調整之功能	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定相關操作及活動紀錄保存說明文件，且說明機關能夠依照其需求自行調整相關紀錄保存期限之設定	CSP 提供機關租用服務範圍內之相關操作及活動紀錄保存說明文件
	維運管控	OM-4	政府公有雲儲存資料(含備援、備份資料)存放實體位置，以台灣為優先，不得以直接或間接方式存放於大陸、港澳地區	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供備援與備份資料的實際存放位置，且說明政府公有雲資料(含備援、備份資料)存放實體位置，將以台灣為優先，不得以直接或間接方式存放於大陸、港澳地區	CSP 提供機關租用服務範圍內之備援與備份資料的實際存放位置說明文件
	維運管控	OM-5	機關應自行選定公有雲服務之資料儲存地 CSP 須揭露機	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下	1.CSP 提供機關租用服務範圍內之公有雲資料處理與管

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			關選定公有雲資料儲存所在地點機關若選擇位於我國境外之資料儲存地，則該區域資安防護不得低於 ISO 27001	項目是否具備：CSP 已針對租用範圍內之服務制定之公有雲資料處理與管理程序說明文件，且說明若選擇資料儲存地若非為我國境內，CSP 能夠提供當地相關雲端資安防護之檢核報告(該資安防護要求項目不得於 ISO 27001)	理程序說明文件 2.CSP 提供機關租用服務範圍內之他國當地相關雲端資安防護之檢核報告
	維運管控	OM-6	CSP 或其認證代理商須於我國具備 24 小時專業技術支援人員	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務制定技術支援服務說明文件，且說明於台灣或其認證代理商具備 24 小時專業技術支援人員，並提供專屬聯絡方式	CSP 提供機關租用服務範圍內之技術支援服務說明文件
	維運管控	OM-7	CSP 若使用特殊資料格式或儲存加密等技術致未來移轉不易時，須盡告知之義務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範	CSP 提供機關租用服務範圍內之安全互操作性與可移植性之管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				圍內之服務制定安全互操作性與可移植性之管理機制說明文件，且說明當 CSP 若使用特殊資料格式或儲存加密等技術須盡告知之義務	
	維運管控	OM-8	CSP 內部進行作業調整設定時應確保不影響客戶服務，若發生資安事件時，須主動通報機關並能於服務水準要求期限內恢復服務 CSP 須協助提供相關使用設定，協助機關能接獲有關服務異常的通知	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定服務水平管理說明文件，且說明若 CSP 內部進行作業調整設定時將確保不影響客戶服務，若發生資安事件時，將主動通報機關並能於服務水準要求期限內恢復服務，並協助機關能有效接獲有關服務異常的通知 2.CSP 已針對租用範圍內之服務制定資安事件管理制定應變計畫與演練報告，且針對資安事	1.CSP 提供機關租用服務範圍內之服務水平管理說明文件 2.CSP 提供機關租用服務範圍內之資安事件管理政策與程序 3.CSP 提供機關租用服務範圍內之資安事件應變計畫 4.CSP 提供機關租用服務範圍內之資安事件演練報告 5.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				件管理定期進行演練，演練過程包含當事件發生時能有效恢復至事件發生前之穩定設定檔 3.CSP 已於提供之內外部獨立稽核報告中說明資安事件通報機制之正確性與有效性	
	資訊資產	OM-9	CSP 應提供受委託雲端服務之清冊	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供完整的服務使用清冊供機關進行確認	CSP 提供機關租用服務範圍內之雲端服務使用清冊
	廠商選擇	OM-10	CSP 不得為大陸廠商，亦須符合國內對中資及港資限制之規範	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供公司申請註冊國家的相關佐證資料，且說 CSP 並非大陸廠商	CSP 提供機關租用服務範圍內之公司申請註冊國家的相關佐證資料

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	存取控制	OM-11	CSP 須支援至少 3 種多元身分識別機制(如雙因子及 OAuth2 等)進行存取授權	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分識別與存取管理說明文件，且說明其支援至少 3 種多元身分識別機制(如雙因子及 OAuth2 等)進行存取授權 2.CSP 已於提供之內外部獨立稽核報告中說明多元身分識別機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之身分識別與存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	存取控制	OM-12	CSP 須提供可支援機關遠端管理人員及設備之安全技術(例：來源 IP 限定、角色型存取控制、雙因素認證、端點設備及安全狀態等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定遠端服務存取管理說明文件，且說明能夠支援機關自行定義遠端管理人員及設備所需之安全技術(例：來源 IP 限定、角色型存取	1.CSP 提供機關租用服務範圍內之遠端服務存取管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				控制、雙因素認證、端點設備及安全狀態等) 2.CSP 已於提供之內外部獨立稽核報告中說明遠端服務存取之正確性與有效性	
	存取控制	OM-13	CSP 若需使用機關之相關稽核紀錄，雙方須訂定明確之權利與義務規定，並經機關同意後方可使用	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定身稽核紀錄管理機制說明文件，且說明相關稽核紀錄須經機關同意後方可使用，並已明確訂定雙方之權利與義務	CSP 提供於機關租用服務範圍內之稽核紀錄管理機制說明文件
	存取控制	OM-14	CSP 不得以任何理由限制機關可不受任何限制，於通過身分識別後，存取其使用服務之檔案、資料或文件	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定身分識別與存取管理機制說明文件，且說明當機關通過相關身分識別後將能	CSP 提供機關租用服務範圍內之身分識別與存取管理機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				不受限制存取其使用服務之檔案、資料或文件	
	存取控制	OM-15	CSP 須訂定對系統管理及維運人員之聘用與管理(含帳號權限)，且應制定保密協議，要求其員工、供應商均須確實遵守，未經同意不得瀏覽機關用戶儲存之資料及紀錄；另若有複委託之情形，其相關要求應等同於原合約	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定身分識別與存取管理機制說明文件與第三方供應商管理說明文件，且規範相關系統管理及維運人員的存取管理(含帳號權限)受到管控 2.CSP 已針對租用範圍內之服務要求相關員工、供應商須簽訂保密協議，協議內容須包含未經同意不得瀏覽機關儲存之資料及紀錄 3.CSP 已針對租用範圍內之服務規範如有複委託之情形，其相關要求應	1.CSP 提供機關租用服務範圍內之身分識別與存取管理機制說明文件 2.CSP 提供機關租用服務範圍內之第三方供應商管理說明文件 3.CSP 提供機關租用服務範圍內之員工、供應商簽訂之保密協議範本 4.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				等同於原合約 4.CSP 已於提供之內外部獨立稽核報告中說明委外與第三方供應商管理機制之正確性與有效性	
	存取控制	OM-16	CSP 須協助機關在存取控制方面設置 GCB 之技術支援	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資訊系統組態設定說明文件，且說明 CSP 能夠提供機關技術支援以配置政府組態基準(GCB)	CSP 提供機關租用服務範圍內之資訊系統組態設定說明文件
	服務可用性	OM-17	CSP 提供之機關相關服務(IaaS、PaaS 及 SaaS)服務可用率至少須達 99.9%以上	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定服務可用性管理說明文件，且說明租用範圍內之服務可用率至少達 99.9%以上	CSP 提供機關租用服務範圍內之服務可用性管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	服務可用性	OM-19	CSP 須依據機關選定之服務提供營運持續計畫，包含風險管理、災害管理、程式及設備管理、供應鏈管理、品質管理、緊急事件管理及相關管理之控管流程(生命週期)或具 ISO 22301 營運持續管理國際標準認證，以確保可達成服務水準要求	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定營運持續計畫管理說明文件，且包含風險管理、災害管理、程式及設備管理、供應鏈管理、品質管理、緊急事件管理及相關營運之控管流程(生命週期) 2.CSP 已於提供之內外部獨立稽核報告中說明提供之服務的營運持續計畫與管理機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之營運持續計畫管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	服務可用性	OM-20	對於災難復原資料的保全及復原，CSP 須提供完整復原機制服務，並依據委託機關之需求提供最佳實務與最符合經濟效益之建議方案	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定災難復原計畫管理政策與程序，且說明機關能依業務需求調整最大可容忍資	CSP 提供機關租用服務範圍內之災難復原計畫管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				料遺失時間與最大可容忍資訊服務復原時間	
	服務可用性	OM-21	CSP 是否同意如因機關公務預算編列問題發生延遲付款或付款額度不足之情況，可依機關需求展延既有服務，且不可影響服務水準	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件與服務水平協定範本，且說明如機關因公務預算編列問題發生延遲付款或付款額度不足之情況，將能夠持續展延既有服務並維持服務水準	1.CSP 提供機關租用服務範圍內之收費機制說明文件 2.CSP 提供機關租用服務範圍內之服務水平協定範本
	服務可用性	OM-22	各項收費制度應明定於契約內，非經雙方同意，不得任意變更資費及收費機制	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定收費機制相關說明文件與服務水平協定範本，且說明各項收費度已明訂於範	1.CSP 提供機關租用服務範圍內之收費機制說明文件 2.CSP 提供機關租用服務範圍內之服務水平協定範本

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				本內並未經雙方同意不得任意變更資費及收費機制	
	雲端服務事故通報	OM-23	CSP 提供之公有雲服務須具備偵測入侵嘗試警示服務，並自動發送警示給機關用戶	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定入侵偵測與通報機制說明文件，且說明其使用之入侵偵測機制、偵測之範圍、偵測通報流程及通報之後續處理方式 2.CSP 已於提供之內外部獨立稽核報告中說明入侵嘗試警示與通報機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之入侵偵測與通報機制說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	雲端服務事故通報	OM-24	如租用之公有雲發生資安或個資外洩事件，CSP 須於雙方合約時限內主動通報相關機關外，並應確認機關連繫窗口收到通知，並	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定資安或個資外洩事	1.CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
			於事件處理完成後提出說明(雙方須訂定通報時限)	件管理說明文件，且說明當發生資安或個資外洩事件時，CSP 將主動聯繫機關窗口，並於事件發生後的依定期限內提出說明 2.CSP 已於提供之內外部獨立稽核報告中說明資安或個資外洩事件處理機制之正確性與有效性	(例如：ISO 27001、ISO27018、CSA STAR)
	雲端服務事故通報	OM-25	CSP 須提供資安事件通報標準作業程序	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且包含以下項目： –定義通報機關之資安事件範圍 –規範對於資安事件發生時，其可揭露程度與相關之應變流程 –規範當識別資安事件發生後之目標通報時限	CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				–規範當識別資安事件發生後之通報流程與資安事件聯絡窗口 –規範針對不同資安事件發生，提供相對應之補救措施	
通訊管理	公有雲與GSN網路介接	CM-1	CSP 須提供連接至機關(GSN 網路)安全連線建議	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網路安全連線管理說明文件，且說明如須連接至 GSN 網路將提供相關安全連線供機關進行配置(例如：IPSec VPN、網路專線服務)	CSP 提供機關租用服務範圍內之網路安全連線管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
	系統與通訊加密服務	CM-2	CSP 須提供資料傳輸及靜態資料儲存時加解密方案，以保障資料安全性	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定料傳輸及靜態資料加密管理說明文件，且說明機關能依其業務需求自行配置加解密方案 2.CSP 已於提供之內外部獨立稽核報告中說明資料加密機制之正確性與有效性	1.CSP 提供機關租用服務範圍內之資料傳輸及靜態資料加密管理說明文件 2.CSP 提供機關租用服務範圍內之內外部獨立稽核報告(例如：ISO 27001、ISO27018、CSA STAR)
	系統與通訊加密服務	CM-3	CSP 提供金鑰保管服務與加密機制須符合第三方驗證(FIPS140-2 或 FedRAMP 等)	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務通過第三方驗證其金鑰保管服務與機制，其驗證標準為 FIPS140-2、FedRAMP 其中之一	CSP 提供機關租用服務範圍內之金鑰管理機制第三方驗證報告

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
資安與隱私管理	資安技術面要求	SP-1	配合「資通安全責任等級分級辦法」，CSP 須協助客戶自外部進行網站弱點掃描與系統滲透測試或提供相同服務	由機關檢測人員檢視 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定資安檢測連線申請與檢測說明相關文件，或說明 CSP 能於平台提供相同服務	CSP 提供機關租用服務範圍內之相關資安檢測連線申請與檢測說明相關文件
	資安技術面要求	SP-2	雲端服務須具備 TLS v1.2 以上安全通訊協定	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網路安全連線作業說明文件，且說明於已使用 TLS v1.2 以上進行通訊協定加密	CSP 提供機關租用服務範圍內之網路安全連線作業說明文件
	資安技術面要求	SP-4	CSP 須提供網路惡意活動檢視紀錄權限與管控機制	由機關檢測人員檢視與測試 CSP 提供之佐證資料，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定網	CSP 提供機關租用服務範圍內之網路惡意活動監控機制說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				路惡意活動監控機制說明文件，且說明其內容包含監控機制、監控範圍及機關檢視監控紀錄流程與權限管理之說明	
	資安技術面要求	SP-7	CSP 須提供機關租用範圍內防火牆之服務：機關可自行定義防火牆機制及規則(如設定目的虛擬機及特定連接埠)，設定防火牆規則	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定防火牆使用與管理機制說明文件，且說明機關能夠自行定義防火牆機制及規則(如設定目的虛擬機及特定連接埠)	CSP 提供機關租用服務範圍內之防火牆使用與管理機制說明文件
	資安技術面要求	SP-8	CSP 須提供 WAF 服務供機關選用	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務提供 WAF 服務供機關進行選擇與配置，且說明機關能夠自訂 WAF 服務規則	CSP 提供機關租用服務範圍內之 WAF 服務使用說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				(例如：SQL injection、Cross Site Scripting)	
	資安技術面要求	SP-10	CSP 須提供(或委託第三方)7*24 SOC 服務，或配合機關 SOC 需求支援轉傳相關紀錄	由機關檢測人員依 CSP 提供之佐證資料測試，確認以下項目是否具備： CSP 已針對租用範圍內之服務制定 SOC 服務使用機制說明文件，且說明其使用之監控機制、監控之範圍及監控通報機制，或說明 CSP 能夠配合機關資安監控中心需求轉傳相關紀錄	CSP 提供機關租用服務範圍內之資安監控中心(SOC)服務使用機制說明文件
	資安與隱私稽核	SP-11	CSP 如發生資安事件、個資外洩或其他必要事項，CSP 須配合檢調單位調查	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備： 1.CSP 已針對租用範圍內之服務制定資安或個資外洩事件管理說明文件，且說明當發生資安事件、個資外洩或其他必要事項，	CSP 提供機關租用服務範圍內之資安或個資外洩事件管理說明文件

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				CSP 應配合檢調單位進行調查	
	資安與隱私稽核	SP-12	CSP 須依照雙方契約約定，配合接受委辦公務機關(含委託查核單位)之稽核活動	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備：1.CSP 已針對租用範圍內之服務制定稽核管理機制，且說明 CSP 會配合接受委辦公務機關(含委託查核單位)進行稽核活動	CSP 提供機關租用服務範圍內之稽核管理機制
	資安與隱私稽核	SP-13	CSP 除被要求遵循法律有效且具有約束力的命令（例如傳票、搜索令或法院命令），未經機關同意，不得披露或提供機關租用服務及儲存於 CSP 公有雲上任何資料	由機關檢測人員於租用服務範圍內，檢視 CSP 提供之佐證資料，確認以下項目是否具備：CSP 已針對租用範圍內之服務制定資料保密協議，且說明除被要求遵循法律有效且具有約束力的命令（例如傳票、搜索令或法院命令），未經機關同意，不得披露或	CSP 提供機關租用服務範圍內之資料保密協議

管理面向	管理類別	編號	要求項目	要求項目檢測步驟	CSP 應提供之佐證資料(以下為參考說明)
				提供機關租用服務及儲存於 CSP 公有雲上所有資料	

附件 1、CSP 基本資料表

CSP 名稱(中文)*			
CSP 名稱(英文)			
統一編號*		**負責人***	
電話*		**傳真**	
登記地址*			
聯絡地址			
公司網址			
聯絡人*		**職稱***	
聯絡人電話*		**聯絡人電郵***	
行動電話			
備註			

附件 2、CSP 提供佐證資料表

管理類別		編號	
檢測方式		廠商自評結果	□符合 □不符合
1. 要求項目			
雲端服務應具備 TLS v1.2 以上安全通訊協定			
2. 要求項目檢測步驟			
由機關檢測人員測試雲端服務連線是否具備 TLS v1.2(含)以上安全通訊協定			
3. CSP 應提供之佐證資料(以下為範本)			
CSP 提供之雲端服務連線均具備 TLS v1.2(含)以上安全通訊協定			
4. CSP 實際提供之佐證資料與說明			
例： 1.網址： 2.使用者名稱： 3.密碼： 4.佐證畫面 5.補充說明 6.技術服務人員電話：			