數位發展部

政府公有雲服務項目選用參考指引

文件版本：V5.1

中華民國112年7月

目錄

圖目錄

表目錄

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」，訂定本指引。

貳、 目的

一、 本指引之目的，係希望機關能透過本文件，了解雲端特性及服務類型，同時參考本指引維運其服務、營運、通訊及法遵等作業，完備機關雲端管理機制及政府雲端服務發展環境。

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「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(CNS17788CNS 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。

三、 備考：營運關係不必然須具備財務協議。

四、 隨需自助服務(On-demand self-service)：一種雲端服務之特性，指 CSC 需要時，能自動地或與 CSP 以最少互動方式提供運算能力。此關鍵特性聚焦於雲端運算賦予使用者隨時隨需採取行動之能力，相對節省成本、時間及工作量，而無須使用者額外之互動或負擔。

五、 多元網絡存取(Broad network access)：一種雲端服務之特性，指實體及虛擬資源可經網路使用，並透過標準機制存取之，而此等機制推廣經異質客戶端平台之使用。此關鍵特性聚焦於雲端運算可提供更高之便利性，使用者只要可存取網路，可使用包括諸如行動電話、平板電腦、筆電及工作站之各式各樣客戶端設備，即可由其需工作之處所，存取實體及虛擬資源。

六、 多人共享資源池(Resource pooling)：一種雲端服務之特徵，指 CSP 之實體及虛擬資源的聚合，藉以服務1或多個 CSC。此關鍵特性聚焦於 CSP 能支援多租用，而同時使用抽象畫對客戶遮蔽處理複雜度。就客戶之觀點而言，其僅需知悉服務工作，而通常不需控制或知悉資源如何提供或資源為於何處。此將客戶原有之某些工作負擔(諸如維護要求)卸除予提供者。宜注意，即使於此抽象層級，使用者仍可於較高抽象層級規定位置(例：國家、州或資料中心)。

七、 快速且彈性佈署(Rapid elasticity)：一種雲端服務之特性，指實體及虛擬資源能快速且靈活地調整(某些情況中自動進行)，以迅速增減資源。就 CSC 而言，於服務協議限制下，可用實體或虛擬資源之供應通常似乎無限，且能於任何時間自動採購任何數量。因此，此關鍵特性聚焦於雲端運算意旨客戶不需再擔心受限之資源，且可不需擔心容量規劃。

八、 服務可量測(Measured service)：一種雲端服務之特性，指計量所交付之雲端服務，使得其使用能被監視、控制、報告及計費。此係最佳化及驗核所交付之雲端服務所需的重要特性。此關鍵特性聚焦於客戶可僅就其所使用之資源付費。就客戶之觀點而言，雲端運算能藉由將資產利用率營運模型(asset utilization business model)由低效率切換至高效率，提供予使用者價值。

九、 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 CSC 提供之雲端能力型式係基礎設施能力型式。

十、 平台作為服務(Platform as a Service, PaaS)：雲端服務種類之一，其中對 CSC 提供之雲端能力型式係平台能力型式。

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

[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。CSC 亦能對某些聯網組件(例：主機防火牆)具有有限控制能力。

肆、 雲端特性與服務類型

雲端運算是透過網際網路的運算方式，CSP 依 CSC 需求提供資源，共享軟硬體資源和資訊。

雲端服務之5大特性包含隨需自助服務、多元網路存取、多人共享資源池、快速且彈性佈署及服務可量測，說明如下：

一、 隨需自助服務：雲端運算賦予使用者隨時隨需採取行動之能力，相對節省成本、時間及工作量，而無須使用者額外之互動或負擔。

二、 多元網絡存取：CSC 只要可存取網路，可由其需工作之處所，存取實體及虛擬資源，提供更高之便利性。

三、 多人共享資源池：CSP 能聚合實體及虛擬資源，服務1或多個 CSC。

四、 快速且彈性佈署：實體及虛擬資源能快速且靈活地調整，以迅速增減資源，CSC 不需再擔心受限之資源。

五、 服務可量測：計量所交付之雲端服務，CSC 可僅就其所使用之資源付費。

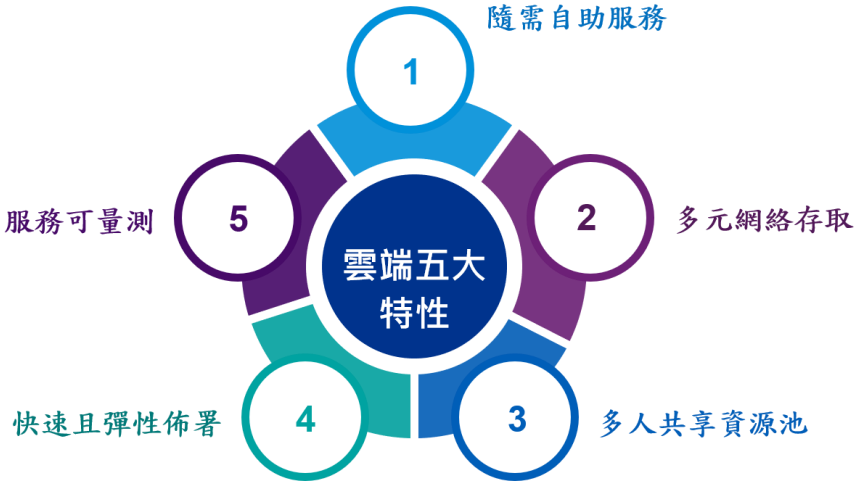

圖 1雲端五大特性

雲端運算依提供的服務類型可分為3種，IaaS、 PaaS 及 SaaS ，說明如下：

1. IaaS 服務類型： CSP 直接提供硬體及網路給用戶使用，主要服務對象為 IT 管理人員。
2. PaaS 服務類型： CSP 提供 CSC 可運算程式的平台， 主要服務對象為軟體開發人員。
3. SaaS 服務類型：CSP 提供 CSC 網路軟體應用，用戶只需要打開瀏覽器即可操作，主要服務對象為終端使用者。

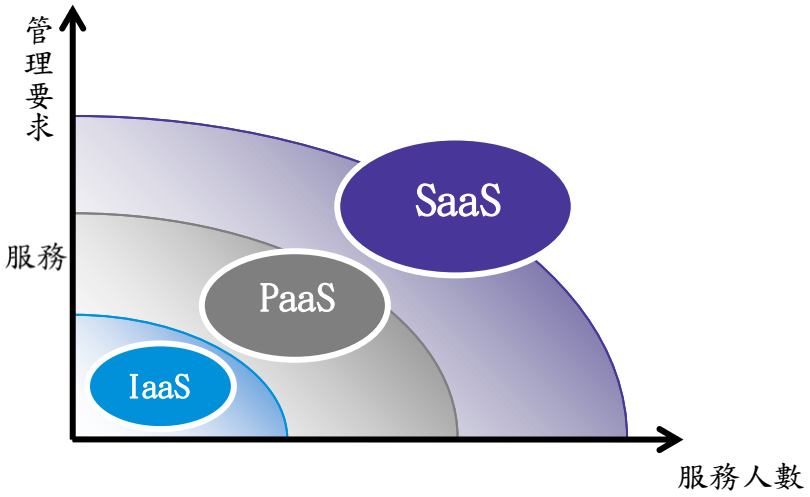

圖 2雲端服務類型

伍、 公有雲服務管理

鑑於機關發展公有雲服務，其資訊系統之架構、網路及維運模式已與往昔大不相同，為利機關健全雲端管理機制，本章節以服務管理、營運管理、通訊管理及資安與隱私管理等4大領域，分析公有雲服務管理要求，以期透過適當之管理機制，強化機關、CSP 及各項服務間之連結，確保雲端運算之服務效能及適法性。

一、 服務管理

有關雲端5大特性，在服務管理上，無論何種服務類型（IaaS、PaaS、SaaS）皆應符合共同基本要求。各服務類型，須在滿足共同基本要求之前題下，再依其特性堆疊服務要求。本節就雲端服務共同基本要求、IaaS、PaaS 及 SaaS 等4個面向，分述管理要求如下：

1. 雲端服務共同基本要求

(1) 對於雲端使用者隨需自助服務特性，CSP 須提供機關管理平臺服務介面/網站。

(2) 須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。

(3) 對於多元網路存取特性，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、表現層狀態轉移應用程式介面[Representational State Transfer

Application Programming Interface ,REST API]管理或控制台[Console]管理等)。

(4) 對於多人共享資源池特性，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。

(5) 對於快速且彈性佈署特性，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。

(6) 對於服務可量測特性，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。

(7) CSP 提供之平台須具備即時檢視費用功能。

(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。

2. IaaS 服務類型

(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。

(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。

(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)。

(4) CSP 須提供雲端服務維持運營持續性之相關佐證資料。

(5) CSP 須協助機關配合行政院院臺護長字第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。

3. PaaS 服務類型

(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。

(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。

(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。

(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。

(5) CSP 須建立紀錄與監測政策，並落實相關程序管控。

(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。

4. SaaS 服務類型

(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。

(2) CSP 須具備安全軟體開發生命週期(Secure Software Development Life Cycle,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。

(3) CSP 須確保機關資料、帳號權限與其他機關彼此區隔。

(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。

(5) CSP 須提供機關租用 SaaS 服務產品支援規格清單。

二、 營運管理

機關資訊系統從既有的IT環境跨入雲端環境，最佳之營運管理方式，

即參考 ISO 27001之控制項目，同時增列雲端環境特性要求，本節以資源需求、維運管控、資訊資產、廠商選擇、存取控制、服務可用性、費用及雲端服務事故通報等8個面向，分析說明雲端營運應具備之管理要求如下：

1. 資源需求

CSP 須至少提供虛擬機、容器、APP 及無伺服器等4種服務，並支援身分與存取管理服務(Identity and Access Management,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)。

2. 維運管控

(1) 隔離環境與多租戶管理

A. 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。

B. 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。

(2) 資料儲存位置

A. 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。

B. 機關應自行選定公有雲服務之資料儲存地 CSP 須揭露機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

(3) 服務專線

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。

(4) 資料移轉

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。

(5) 組態設定

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。

3. 資訊資產

CSP 應提供受委託雲端服務之清冊。

4. 廠商選擇

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。

5. 存取控制

(1) CSP 須支援至少3種多元身分識別機制(如雙因子及開放授權2[The OAuth 2.0 Authorization Framework,OAuth2]等)進行存取授權。

(2) 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)。

(3) 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。

(4) 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。

(5) 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。

(6) CSP 須協助機關在存取控制方面設置政府組態基準(Government Configuration Baseline,GCB)之技術支援。

6. 服務可用性

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

7. 雲端服務事故通報

(1) 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。

(2) 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)。

(3) CSP 須提供資安事件通報標準作業程序。

三、 通訊管理

各機關使用公有雲服務時，除須規劃機關與 CSP 資料中心之網路連接方式外，亦須考量我國政府網際服務網(Government Service Network,

GSN) 之管理規範，本節就公有雲與 GSN 網路介接及系統與通訊加密服務等2個面向，分述管理要求如下：

(一) 公有雲與 GSN 網路介接：CSP 須提供連接至機關(GSN 網路)安全連線建議。

(二) 系統與通訊加密服務

1. 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。

2. 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)。

四、 資安與隱私管理

機關使用公有雲服務，須事先進行移轉評估，了解存放於公有雲資料重要性、敏感性及其價值。

移轉上雲之資訊系統或服務，仍須考量我國資通安全管理法、個人資料保護法及國際標準適用於雲端管理之相關要求，說明如下：

(一) 資通安全責任等級 A 級之公務機關應辦事項技術面要求：

1. 安全性檢測

(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。

(2) 雲端服務須具備傳輸層安全性協定(Transport Layer Security,TLS)

v1.2以上安全通訊協定。

2. 資通安全健診

(1) 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。

(2) CSP 須提供網路惡意活動檢視紀錄權限與管控機制。

(3) CSP 須提供伺服器主機惡意活動檢視紀錄權限與管控機制。

3. 資通安全威脅偵測及防護管理機制

(1) 提供防毒、防火牆、Web 應用程式防火牆(WebApplication Firewall,WAF)、入侵偵測系統(Intrusion Detection Systems,IDS)(或入侵防禦系統[Intrusion Prevention Systems,IPS])、進階持續性滲透攻擊（Advanced Persistent Threat, APT）等資安防護機制之服務。

A. 防毒軟體服務：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。

B. 防火牆服務：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。

C. WAF 服務：CSP 須提供 WAF 服務供機關選用。

D. 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。

(2) CSP 須提供(或委託第三方)7*24資安監控中心(Security Operation Center, SOC)服務，或配合機關 SOC 需求支援轉傳相關紀錄。

(二) 資安與隱私稽核

1. 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。

2. 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。

3. 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。

本小節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，可參考本部資通安全署委國家資通安全

研究院網站之共通規範專區所公布「政府機關雲端服務應用資安參考指引」[2]。

陸、 實務應用指引

鑑於國內、外CSP提供之雲端服務繁多，加深機關選用及管理之困難，為利機關或相關資訊人員實務應用本指引，了解 IaaS、PaaS、SaaS相對於服務管理、營運管理、通訊管理及資安與隱私管理四大面向所需之管理條件，爰分別彙整「IaaS服務類型管理項目表」、「PaaS服務類型管理項目表」及「SaaS服務類型管理項目表」如下，便利機關依雲端服務類型，選擇適用之要求，完備管理機制。

表 1：IaaS服務類型管理項目表

管理面向	管理類別	編號	要求項目	備註
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	
	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	
	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)	

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

管理面向	管理類別	編號	要求項目	備註
	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	
	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	
	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	
	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	
	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	
	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	
	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	
	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)	

管理面向	管理類別	編號	要求項目	備註
	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	
	服務類型	IS-5	CSP 須協助機關配合行政院院臺護長字第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	
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)	
	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	
	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	
	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	

管理面向	管理類別	編號	要求項目	備註
	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	
	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	
	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	
	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	
	資訊資產	OM-9	CSP 應提供受委託雲端服務之清冊	
	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	
	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	
	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)	

管理面向	管理類別	編號	要求項目	備註
	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	
	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	
	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	
	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	
	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	
	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	

管理面向	管理類別	編號	要求項目	備註
	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	
	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	
	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	
	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	
	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	
	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)	
	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	

管理面向	管理類別	編號	要求項目	備註
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	
	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	
	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)	
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	
	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	
	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	
	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	
	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	

管理面向	管理類別	編號	要求項目	備註
	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	
	資安技術面要求	SP-8	CSP 須提供 WAF 服務供機關選用	
	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	
	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	
	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	
	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	
	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	

表 2：PaaS 服務類型管理項目表

管理面向	管理類別	編號	要求項目	備註
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	
	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	
	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)	
	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	
	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	
	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	
	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	
	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	
	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	
	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	
	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)	
	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	
	服務類型	IS-5	CSP 須協助機關配合行政院院臺護長字第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	
	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	
	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	
	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	
	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	
	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	
	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	
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)	
	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	
	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	
	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	
	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	
	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	
	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	
	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	
	資訊資產	OM-9	CSP 應提供受委託雲端服務之清冊	
	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	
	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	
	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)	
	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	
	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	
	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	
	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[3]	

[3] 機關若無實際需求可排除

	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	
	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	
	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	
	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	
	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	
	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	
	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	
	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)	

	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	
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	
	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	
	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)	
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	
	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	
	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	
	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	
	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	
	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	
	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	

	資安技術面要求	SP-8	CSP 須提供 WAF 服務供機關選用	
	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	
	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	
	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	
	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	
	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	

表 3：SaaS 服務類型管理項目表

管理面向	管理類別	編號	要求項目	備註
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	
	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	
	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)	
	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	
	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	
	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	
	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	
	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	

管理面向	管理類別	編號	要求項目	備註
	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	
	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	
	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	
	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	
	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	
	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	
	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	
	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	
	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	
	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	

管理面向	管理類別	編號	要求項目	備註
	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	
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	
	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	
	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	
	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	
	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	
	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	
	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	
	資訊資產	OM-9	CSP 應提供受委託雲端服務之清冊	
	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	

管理面向	管理類別	編號	要求項目	備註
	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	
	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)	
	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	
	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	
	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	
	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[4]	
	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	
	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	

[4] 機關若無實際需求可排除

管理面向	管理類別	編號	要求項目	備註
			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	
	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	
	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	
	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	
	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	
	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)	
	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	
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	
	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	
	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)	

管理面向	管理類別	編號	要求項目	備註
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	
	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	
	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	
	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	
	資安技術面要求	SP-8	CSP 須提供 WAF 服務供機關選用	
	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	
	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	
	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	
	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	