# 雲端服務共同供應契約調整說明

## 報告人：數位發展部數位產業署

113年 01 月

# 大綱

1 公開徵求作業調整內容說明

2 招標及契約作業調整內容說明

3 後續廠商配合事項

# 雲端服務共同供應契約採購作業說明


**01**

- 由**原廠或原廠授權之代理商**提供雲端服務產品規格資料，並依要求提供相關佐證文件。
- 依IaaS、PaaS、SaaS三類進行「**雲端共通特性檢測**」及「**雲端服務安全性檢測**」。

**02**

- 依「共同供應契約實施辦法」規定辦理機關需求調查，各項產品**須有二以上機關表示有需求**，始納入採購品項。
- 若**連續近二標上架且有銷售實績者**，可不辦理機關需求調查，直接納入本次採購品項。

**03**

- 委請**中華軟協會進行各項規格市場詢價**，如網路價格、市場銷售價、促銷價等。

**04**

- 依據本署之「訂價暨規格審查會」決議之訂價原則，參考本署辦理之**共契以往決標價**、機關提供**非共契決標價**及軟協詢得之**市場價格**，訂定合理底價。

**05**

- 以符合政府採購法規定，採用**公告底價最低價決標**，及依廠商報價由低至高排列取前90%之複數決標。
- 廠商應具備**雲端服務之製造、供應或承做**之能力證明

**06**

- **中央及地方機關、其所屬機構、學校、議會、公營事業及受政府補助之法人或團體**，可於工程會政府電子採購網訂購。
- 上架品項**契約價格含依級距不同併計1%及1.1%作業服務費**，履約期限到期後依訂單向立約廠商收取。

# 雲端服務共契整體調整說明

➢ **參考依據：**

- 工程會公布之「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」(112年9月25日工程企字第1120022701號)，其中之**『雲端微服務(SaaS)套裝型』**、**『雲端微服務(SaaS)辦公生產力工具(含郵件、行事曆、雲端硬碟、即時通訊等)』**及**『雲端平台(PaaS或IaaS) 』**
- 本部公布之「政府公有雲服務供應商檢核作業指引V5.0」(112年 7 月)
- 共通性資通安全基本要求參考一覽表對象名詞對照：

| 共通性資通安全基本要求參考一覽表 | 雲端服務共契參與對象 |
|---|---|
| 供應商 | 雲端服務原廠（公開徵求階段） |
| 提供服務商<br>提供平台服務商 | 立約商（投標履約階段） |

# 1 公開徵求作業調整內容說明

# 雲端服務公開徵求調整說明

## ➢ 雲端服務公開徵求流程：


### 廠商資格

投件廠商及雲端服務原廠不得為：
- 中國大陸(含港、澳)地區廠商
- 第三地區含陸資成分廠商
- 經濟部投資審議司列為陸資來台投資事業名錄之廠商

### 採購規格

- 雲端服務**資料存取、備份及備援**之實體機房所在地**不得位於中國大陸(含港、澳)**，且**不得跨該等境內傳輸**相關資料。
- **不得為「各機關對危害國家資通安全產品限制使用原則」之廠牌或產品**

### 國際或國家標準驗證證書

- **雲端服務之資訊機房(Data center)**具備要求之**資訊安全管理制度及雲端服務個人資訊保護相關國際或國家標準驗證**
- 通過驗證之證明文件須顯示出**雲端服務資訊機房在驗證範圍內**，且**公開徵求階段及未來產品上架期間應維持證明文件之有效性**

### 檢測作業

- 雲端共通特性檢測：共6項檢測項目
- 雲端服務安全性檢測：共4項檢測項目

# 雲端服務共契徵求調整說明(1/4)

➢ 針對「雲端服務原廠」資訊安全管理制度及個人資訊保護相關國際或國家標準驗證調整如下：

| 國際標準驗證類別 | 雲端服務共契現行要求 | 政府公有雲服務供應商檢核作業指引 | 共通性資通安全基本要求參考一覽表 | 調整後要求 |
|---|---|---|---|---|
| ISO/IEC27001 | 雲端服務之資訊機房須具備ISO27001，或CNS27001 | CSP提供機關租用服務範圍內之ISO27001 | 無 | 雲端服務提供者(CSP)須具備ISO27001或CNS27001 |
| ISO/IEC27701 | 無 | CSP提供機關租用服務範圍內之ISO27701或BS10012 | 無 | 雲端服務提供者(CSP)須具備ISO27701或BS10012 |
| ISO/IEC27017 | 雲端服務之資訊機房須具備ISO27017，或CSA Star（等級不限） | CSP提供機關租用服務範圍內之ISO27017或CSA Star | 無 | 雲端服務提供者(CSP)須具備ISO27017或CSA Star（等級不限） |
| ISO/IEC27018 | 雲端服務之資訊機房須具備ISO27018 | CSP提供機關租用服務範圍內之ISO27018 | 無 | 雲端服務提供者(CSP)須具備ISO27018 |

共契要求: 如分階段實施, 詳第16頁

# 雲端服務共契徵求調整說明(1/4)

➢ 針對「雲端服務產品」檢測規範調整如下：

| 檢測編號 | 檢測指標 | 雲端服務共契現行要求 | 政府公有雲服務供應商檢核作業指引 | 共通性資通安全基本要求參考一覽表 | 調整後要求 |
|---|---|---|---|---|---|
| CS-002 | OWASP TOP10 最新版應用程式弱點掃描 | 1.檢視廠商提供之一年內應用程式弱點掃描報告(掃描報告須可呈現包含OWASP TOP 10 2017以上掃描內容選項)，須無中、高等級以上風險<br>2.若廠商無法提供上述檢測報告，檢測人員將透過檢測工具Opentext WebInspect針對OWASP TOP 10 最新版進行檢測，檢測結果無中、高等級以上風險 | 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 | 產品安全：符合以下任一條件。<br>(1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告<br>(2)提供經商用弱點檢測軟體未含___等級風險之掃描報告<br>(3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證 | 1.檢視廠商提供之一年內**經第三方檢測單位**應用程式弱點掃描報告(掃描報告須可呈現包含OWASP TOP 10 2021以上掃描內容選項)，須無中等級以上風險<br>2.若廠商無法提供上述檢測報告，檢測人員將透過檢測工具Opentext WebInspect針對OWASP TOP 10 最新版進行檢測，檢測結果無中等級以上風險 |
| CS-003 | 系統弱點掃描 | 1.檢視廠商提供之一年內系統弱點掃描報告，無中等級以上風險<br>2.若廠商無法提供上述檢測報告，軟體採購辦公室檢測人員將透過檢測工具Nessus針對系統弱點進行檢測，檢測結果無中、高等級以上風險 | | | 1.檢視廠商提供之一年內**經第三方檢測單位**系統弱點掃描報告，無中等級以上風險<br>2.若廠商無法提供上述檢測報告，軟體採購辦公室檢測人員將透過檢測工具Nessus針對系統弱點進行檢測，檢測結果無中等級以上風險 |

共契要求: 如分階段實施, 詳第16頁

# 雲端服務共契徵求調整說明(3/4)

➢ **針對「雲端服務產品」其他新增之資安要求項目：**

圖示：●建議辦理 ◎經機關評估個案有必要辦理時

| 類別 | 項目 | 子項 | 高 | 中 | 普 |
|---|---|---|---|---|---|
| 雲端微服務（SaaS）辦公室生產力工具(含郵件、行事曆、雲端硬碟、即時通訊等) | 傳輸機密性與完整性 | 廠商提供機關資料傳輸措施 | ● | ● | ● |
| | 防惡意軟體 | 靜態分析 | ● | ● | ● |
| | | 動態沙箱分析 | ● | ● | ◎ |
| | 防惡意連結 | 靜態分析 | ● | ● | ● |
| | | 動態沙箱分析 | ● | ● | ◎ |
| | 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● |
| | | 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ |
| | 資料與個資安全 | 資料分類與標籤 | ● | ● | ● |
| | | 資料外洩防護 | ● | ● | ◎ |
| | 身分驗證與存取控制 | 多因子認證 | ● | ● | ● |
| | | 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ |

共契要求: 如分階段實施, 詳第16頁

# 雲端服務共契徵求調整說明(4/4)

| 類別 | 項目 | 子項 | 高 | 中 | 普 |
|---|---|---|---|---|---|
| 雲端平台(PaaS或IaaS) | 弱點管理 | 雲端應用系統平台具備定期檢視PaaS 之應用、組件或 Web 服務是否存在漏洞並進行更新修補 | ● | ● | ● |
| | 存取控制 | 須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制 | ● | ● | ◎ |
| | 營運持續計畫 | 檢視廠商平台營運持續、資料復原計畫及執行情形 | ● | ● | ● |
| | 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ |
| | | 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● |
| | 資料安全 | 廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證 | ● | ● | ◎ |
| | | 雲端應用系統平台內如存有機密或個人資料應依相關法令強化資料安全防護措施 | ● | ● | ● |
| | 資安檢測 | 滲透測試掃描(由檢測人員測試雲端服務是否具備TLS v1.2 以上安全通訊協定) | ● | ◎ | ◎ |
| | | 雲端服務之APP取得行動應用 App 基本資安標章 | ● | ● | ◎ |
| | | 資安健診 | ● | ● | ● |

共契要求: 如分階段實施, 詳第16頁

# 2 招標及契約作業調整內容說明

# 雲端服務共契招標文件調整說明

➢ **參考依據：「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」(112年9月25日工程企字第1120022701號)**

**針對「投標廠商(立約商)」要求：**

| 類型 | 項目 | 子項 | 高 | 中 | 普 |
|---|---|---|---|---|---|
| 雲端微服務(SaaS)套裝型 | 提供服務商 | 須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準 | ● | ● | ● |
| 雲端微服務(SaaS)辦公室生產力 | | | | | |
| 雲端平台(PaaS或IaaS) | | 須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準 | ◎ | ◎ | ◎ |

| 投標須知-現況 | 投標須知-配合調整 |
|---|---|
| **四十八、其他須知：**<br>(一)得標廠商：<br>1. 應於政府電子採購網公告之決標日為起始日起算14日(日曆天)內繳納加蓋公司大小章之保密同意書(格式詳契約條款第40頁)，以納入本案契約之附件。<br>2. 「招標、投標及簽約三用文件」經本署於簽約欄以電子簽章方式簽署後即完成簽約，不必再經過得標廠商簽章。 | **四十八、其他須知：**<br>(一)得標廠商：<br>1. 應於政府電子採購網公告之決標日為起始日起算14日(日曆天)內繳納加蓋公司大小章之保密同意書(格式詳契約條款第40頁)，以納入本案契約之附件。<br>2. 「招標、投標及簽約三用文件」經本署於簽約欄以電子簽章方式簽署後即完成簽約，不必再經過得標廠商簽章。<br>**3. 已取得ISO27001或ISO27701證書之廠商，請繳交證書影本作為三用文件附件，本署軟體採購辦公室將揭露於之「資訊服務採購網」供機關訂購時參酌。** |

共契要求: 113年新標案(1130202案號)起實施

# 雲端服務共契招標文件調整說明

➢ **參考依據：「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」(112年9月25日工程企字第1120022701號)**
**針對「訂購機關&立約商(含原廠)」要求：**

| 類型 | 項目 | 子項 | 高 | 中 | 普 |
|---|---|---|---|---|---|
| 雲端微服務(SaaS)套裝型 | 資料安全 | 未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區 | ● | ● | ● |
| 雲端微服務(SaaS)辦公室生產力 | | | | | |
| 雲端平台(PaaS或IaaS) | | | | | |

| 契約條款-現況 | 契約條款-配合調整 |
|---|---|
| **第四條　訂購方式**<br>.....(略)<br>(三)訂購機關因故需取消原訂單，請先洽廠商同意，須至行政院公共工程委員會政府電子採購網(網址：https://web.pcc.gov.tw)電子採購系統「訂單管理」執行退件功能，並登載退件原因，系統會將此一訂單交由本署裁定可否取消。<br>(四)訂購機關同意廠商取消原訂單，並經本署裁定取消，廠商不負違約之責。 | **第四條　訂購方式**<br>.....(略)<br>**(六)請機關訂購前先行確認雲端服務資料儲存所在地：**<br>**機關於訂購、使用雲端產品功能前，應先考量其雲端資訊系統或資料儲存之實體所在地是否為我國境外地區，以及機關所屬資料之機敏性。廠商資料儲存之實體以位於我國境內為原則，雲端資訊系統或資料儲存之儲存實體設置於我國境外者，其資料之蒐集、處理及利用應符合我國相關法令規定，並使機關具有儲存資料內容完整控制權，以維護機關資料安全需求。爰請機關於訂購前自行審查，並與該類產品之廠商為確認。** |

共契要求: 113年新標案(1130202案號)起實施

# 雲端服務共契招標文件調整說明

➢ **參考依據：「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」(112年9月25日工程企字第1120022701號)**
**針對「投標廠商(立約商)」要求：**

| 類型 | 項目 | 子項 | 高 | 中 | 普 |
|---|---|---|---|---|---|
| 雲端微服務(SaaS)套裝型 | 事件日誌保存與可歸責性 | 應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求 | ● | ● | ● |
| 雲端微服務(SaaS)辦公室生產力 | | | | | |
| 雲端平台(PaaS或IaaS) | | | | | |

| 契約條款-現況 | 契約條款-配合調整 |
|---|---|
| **第十五條　權利及責任**<br>(十七)資通安全責任：<br>3.契約履約或終止後，廠商應依約定或機關指示，刪除或銷毀或返還或移交執行服務所持有機關之相關資料，並依機關指定之期間通知執行結果及保留執行紀錄。廠商因執行服務所生之有關日誌，於契約終止、解除後，應至少保存90日。 | **第十五條　權利及責任**<br>(十七)資通安全責任：<br>3.契約履約或終止後，廠商應依約定或機關指示，刪除或銷毀或返還或移交執行服務所持有機關之相關資料，並依機關指定之期間通知執行結果及保留執行紀錄。廠商因執行服務所生之有關日誌，於契約終止、解除後，應至少保存六個月。 |

共契要求: 113年新標案(1130202案號)起實施

# 3 後續廠商配合事項

# 後續廠商配合事項

➢ **採漸進式協助業界依循合規**

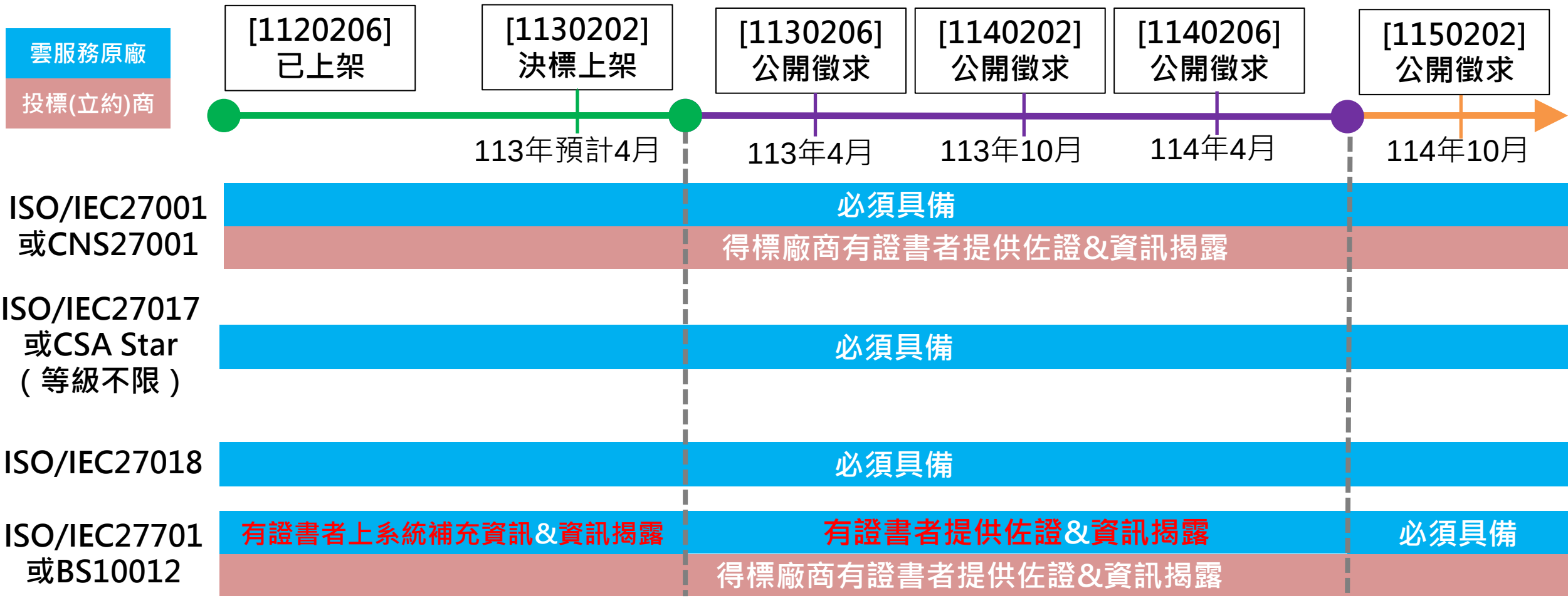
- **因應「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」113年3月1日起正式施行，公開徵求資料提供者(雲端服務原廠或原廠授權之代理商)配合事項如下：**

| 共契適用處理階段 | 作業內容說明 |
| --- | --- |
| 1. 已上架(112年第六次電腦軟體共同供應契約採購 - 雲端服務)<br>2. 113年4月決標(113年第二次電腦軟體共同供應契約採購 - 雲端服務) | **軟體採購辦公室將另行通知，並開放公開徵求系統補充，並做資料揭露：**<br>1. 國際標準驗證：提供雲端服務之資訊機房ISO/IEC 27701證書。<br>2. 新增資安項目提供相關資料：提供新增項目之相關佐證資料。 |
| 1. 113年4月公開徵求(113年第六次電腦軟體共同供應契約採購 - 雲端服務)<br>2. 113年10月公開徵求(114年第二次電腦軟體共同供應契約採購 - 雲端服務)<br>3. 114年4月公開徵求(114年第六次電腦軟體共同供應契約採購 - 雲端服務) | **於公開徵求期間須提供要求項目之相關佐證資料：**<br>1. 國際標準驗證：提供雲端服務之資訊機房國際標準證書，其中ISO/IEC 27701做資料揭露。<br>2. 各類資安項目提供相關資料：由原廠提供相關佐證資料，提供資料揭露供機關參考 |
| 114年10月後雲端服務共契案之公開徵求 | 於公開徵求期間須提供要求項目之相關佐證資料，**不符合公開徵求要求，其所提供之產品，將逕不納入採購。** |

# 後續廠商配合事項

➢ **採漸進式協助業界依循合規**

- 有關資訊安全管理制度及個人資訊保護相關國際或國家標準驗證證書要求：



# 感謝您的聆聽

Thank You