**113年第六次電腦軟體共同供應契約採購-雲端服務**

**(1130206)** **雲端服務檢核表**

雲端微服務（SaaS）套裝型

共通性資通安全基本要求

以下為「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(112.9.25版)」中，要求【普】、【中】及【高】類型之資料或系統類型應建議辦理之各項控制措施。

請投件廠商依本檢核表就所提之雲端服務產品實際情形勾選為【普級】或【中】、【高】資料或系統類型，併於廠商說明欄填覆相關對應措施，**本表格內容後續將公告於資訊服務採購網中。**

**服務名稱：**Caloudi CRP雲端資源規劃解決方案

**□**符合【普級】資料或系統類型(所有「高、中、普」標記●項目，皆須符合並進行說明，標記「高、中」標記●項目，則為選填)

**🗹**符合【中】、【高】資料或系統類型(所有項目皆須符合並進行說明)

填寫說明：

1. 圖示表示：● 建議辦理，◎ 經訂購機關評估個案有必要辦理時，▲ 依訂購機關機關資通安全責任等級辦理。
2. 普、中、高皆標示◎項目(橘色項目)，為所有廠商選填項目，提供機關個別評估時參考。

| **項目** | **子項** | **資料或系統類型** | | | **請廠商自我檢視並填寫相關說明**  填寫日期： 113年 07 月 11 日 |
| --- | --- | --- | --- | --- | --- |
| **高** | **中** | **普** |
| 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 | ● | ● | ● | **🗹符合要求：**  卡洛地提供之 CRP 雲端資源規劃解決方案，全部都架設在 Microsoft Azure 的雲端資料中心上頭，Microsoft Azure 通過 ISO 27001 / 27017 / 27018 稽核的相關證書，詳見附件：   1. Microsoft Azure, Dynamics and Online Services - ISO 27001 Certificate (with UKAS) (5.30.2023).pdf 2. Microsoft Azure, Dynamics and Online Services - ISO 27017 Certificate (5.18.2023).pdf 3. Microsoft Azure, Dynamics and Online Services - ISO 27018 Certificate (5.18.2023).pdf |
| 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  (提供服務項目涉及個資時機關應納入要求) | ◎ | ◎ | ◎ | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫或提供，有證書提供者將於資訊服務採購網中揭露) |
| 不得為大陸地區廠商或第三地區含陸資成分廠商 | ● | ● | ● | **🗹符合要求：**   1. 雲端服務原廠不得為「中國大陸（含港、澳）地區廠商」或「經濟部投資審議司列為陸資來台投資事業名錄之廠商」者。 2. 經數位發展部資通安全署、國家安全會議及其他資安、國安等機關通知有資安疑慮，例如投件廠商、投件代理商所提供產品之原廠屬「第三地區含陸資成分廠商」。 |
| 身分鑑別/傳輸機密性與完整性 | 廠商提供機關帳號控管措施 | ◎ | ◎ | ◎ | (為機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 廠商提供機關資料傳輸措施 | ◎ | ◎ | ◎ | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 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 | ● | ● | ● | 卡洛地提供之 CRP 雲端資源規劃解決方案，是透過用戶的授權，將客戶原先存放在公有雲上的用戶資料，包括費用與使用記錄，透過API呼叫取得，重新整理之後，方便用戶查詢檢視。CRP 雲端資源規劃解決方案無法新增、刪除、修改客戶原始資料，也不提供這些功能。  但是，考量到客戶對於資安的疑慮與需求，CRP 雲端資源規劃解決方案因為支援 Microsoft 與 Google 的 Single Sign-On，所以同樣因為客戶的授權，可以提供客戶的使用者存取記錄，包括**活動時間**、**來源** (Microsoft Azure AD / Google Sign-in / Local)、**活動** (動作內容)、與**狀態** (成功與否) 等資訊 (如下圖)：    搭配 Microsoft 或 Google 的 Sign-in Log，可以進一步追蹤到 **Date** (日期時間)、**User** (使用者帳號)、**Status** (成功與否)、**IP Address**、**Location** 等登入資訊 (如下圖)：    CRP 雲端資源規劃解決方案也是採前後端分離的 Cloud-Native 方式開發，底層 API Server 因為是使用 Microsoft Azure 提供的 Azure Kubernetes Service (AKS) 架設，所以用戶操作 CRP 所呼叫的相對應 API，也有Microsoft Azure 提供的 Activity Log，可以追蹤到 **Operation Name** (活動內容)、**Status** (成功與否)、**Time Stamp** (日期時間)、**Event Initiated By** (使用者帳號) 等重要資訊 (如上圖)。  Microsoft Azure 提供的 Activity Log 預設只會記錄 90 天，所以我們另外建置 Azure Storage Account 儲存這些相關日誌，以滿足客戶資料保存年限至少六個月的需求。  **CRP雲端資源規劃解決方案亦能記錄下列雲端API使用資訊（計費、資源管理等）**  **Cloud API end point**  **Cloud API version**  **Cloud API payload**  **Cloud API call start time**  **Cloud API call end time**  **Cloud API result status**  **Cloud API result**  **這些記錄能夠確保完整與正確性，並符合機關保存年限的要求。** |
| 供應商及產品安全要求 | 針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險  1.供應商安全：符合以下任一條件。  (1)廠商有公開漏洞回報應變機制  (2)廠商有第三方檢測團隊執行檢測  2.產品安全：符合以下任一條件。  (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告  (2)提供經商用弱點檢測軟體未含\_\_\_等級風險之掃描報告  (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 | ● | ● | ● | **🗹符合要求：**  關於供應商安全的部分 卡洛地股份有限公司本身通過 ISO 27001 稽核，明文規定資通安全政策：  4.4 條即說明「本公司全體同仁、委外服務廠商及資料使用者(含保管者)均有責任透過適當通報機制，通報資通安全事件或弱點。」在官網「卡洛地股份有限公司資通安全及隱私權政策聲明」頁面上，也提供聯絡方式 (如下圖) (<https://caloudi.com/zh/security-privacy-zh/>)。    也可以透過 CRP 雲端資源規劃解決方案的雲端平台，提出支援要求 (如上圖)。  關於產品安全的部分，CRP 雲端資源規劃解決方案有Tenable弱點掃描工具的檢測報告，未含 OWASP Top 10 相關弱點，如附件：  [卡洛地\_弱掃\_應用程式\_Website\_Scan\_1222.pdf](https://caloudi-my.sharepoint.com/:b:/p/teresa_hung/EXdfKlDwWV9Ep1UNIiZSbHoBW2yS1xLm1pbi0s6kr5jO-w?e=LGLHk4) [卡洛地\_弱掃\_系統\_Network, SSL Scan.pdf](https://caloudi-my.sharepoint.com/:b:/p/teresa_hung/EXdfKlDwWV9Ep1UNIiZSbHoBW2yS1xLm1pbi0s6kr5jO-w?e=LGLHk4) |
| 廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC) | ◎ | ◎ | - | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 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 | ● | ● | ● | **🗹符合要求：**  雲端服務資料儲存所在地於本國境內者，未經機關審查同意不得隨意變更至本國境外。 |
| 資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。 | ● | ● | ● | **🗹符合要求：**  雲端服務資料存取、備份及備援的位置，都不在大陸地區(含香港及澳門地區)，也不會跨該等境內傳輸相關資料。 |
| 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 | ● | ● | ◎ | CRP 雲端資源規劃解決方案的底層使用 Microsoft Azure 提供的 Azure Kubernetes Service (AKS)，Node Pool 裡面各個 Node 所使用的，都是由 AKS 本身經過檢測所提供的 Image，如下圖：  Image 所有詳細資訊，Microsoft 都有公佈在 [AgentBaker/vhdbuilder/release-notes/AKSUbuntu/gen2/2204containerd at master · Azure/AgentBaker · GitHub](https://github.com/Azure/AgentBaker/tree/master/vhdbuilder/release-notes/AKSUbuntu/gen2/2204containerd) 這個 GitHub網頁，如果 NIST 發佈了有關 Kubernetes 或 Ubuntu 特定版本的漏洞，AKS 也會第一時間通知我們更新。 |