**114年第二次電腦軟體共同供應契約採購-雲端服務**

**(1140202)雲端服務檢核表**

雲端平台(PaaS或IaaS)共通性資通安全基本要求

|  |  |
| --- | --- |
| 雲端服務名稱 | 雲端零信任資訊安全強化包 |
| 資料或系統類型 | **☑**符合【普】資料或系統類型(所有【普】標示為●之項目皆須符合並進行說明，其他則為選填)  **☑**符合【中】、【高】資料或系統類型(所有項目須符合並說明) |

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】或【中】、【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【普】或【中】、【高】資料或系統類型，並於「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。**

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時辦理，▲ 依訂購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：中華民國 113年 月 日 |
| **高** | **中** | **普** |
| 提供平台服務商 | 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：**  雲端服務應具備以下三項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在驗證範圍內，雲端服務原廠得以合作之公有雲業者通過驗證證書代之)：   1. 資訊安全管理系統國際標準(ISO/IEC 27001)或國家標準(CNS 27001)，二者擇一。 2. 雲端服務資訊安全管理國際標準，如ISO/IEC 27017或雲端安全聯盟CSA Star(等級不限)等，二者擇一 3. 雲端服務個人資訊保護管理國際標準(ISO/IEC 27018)。   廠商說明:  Microsoft Compliance Offering (英文網站): <https://docs.microsoft.com/en-us/compliance/>  微軟合規性方案網站: 客戶可參閱所有合規性標準  <https://docs.microsoft.com/zh-tw/compliance/regulatory/offering-home>  Azure ISO/IEC 27001:2022 認證:  <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001> |
| 廠商不得為大陸地區廠商第三地區含陸資成分廠商 | ● | ● | ● | **☑符合符合要求：**   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」。   廠商說明:  客戶使用Micosoft Azure 時，得自行選擇資料存放之地理區域，按該等選擇權既屬客戶自行決定且控制之事項，雲端服務廠商無從處理之。有關微軟雲端服務目前可選擇之地理區域，請詳Azure geographies中英文網站(https://azure.microsoft.com/en-us/global-infrastructure/geographies/#overview)，或微軟信任中心網站。Microsoft Azure 雖有提供中國地理區域資料中心，但僅限服務中國境內之客戶，且此地理區域是與其他地理區域實體上隔離之地理區域，併此說明。請造訪Azure geographies中英文網站(https://azure.microsoft.com/en-us/global-infrastructure/geographies/#overview)，選擇「中國」之地理區域以閱讀「Availalbe to (customers)」(可提供(客戶))欄位。客戶可在自身租戶環境內了解其選擇之資料儲存地。 |
| 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 | ● | ● | ● | (**符合【普】、【中】、【高】者必填**，請廠商依據左列具體說明雲端服務定期檢視漏洞與漏洞修補機制)  **☑符合要求：**  廠商說明:  Azure 會在兩個層級管理 OS 修補，分別是實體伺服器和執行 App Service 資源的客體虛擬機器 (VM)。 兩者皆會每月更新，以配合每月的 [Patch Tuesday](https://learn.microsoft.com/zh-tw/security-updates/) 排程。 這些更新會以能夠保證 Azure 服務具有高可用性 SLA 的方式自動套用。  微軟作業系統OS 和執行階段修補:  <https://learn.microsoft.com/zh-tw/azure/app-service/overview-patch-os-runtime#how-does-azure-deal-with-significant-vulnerabilities> |
| 存取控制 | 雲端應用系統平台提供帳號安全認證、權限管理、網路安全傳輸及遠端存取控管佐證 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明) 1. 雲端服務帳號權限管理機制。  2. 請詳閱雲端服務安全性檢測個案編號CS-001：雲端服務均須具備「傳輸層安全通訊協定(Transport Layer Security-TLS)」的安全通訊協定v1.2以上。  **☑符合要求：**  廠商說明:  Microsoft Azure 採用多租戶設計，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。<https://docs.microsoft.com/zh-tw/azure/security/fundamentals/isolation-choices>  Microsoft Azure 支援TLS 1.2 安全通訊協定  <https://azure.microsoft.com/zh-tw/updates/azuretls12/> |
| 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 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明說明雲端服務之零信任防護與多因子認證機制)  **☑符合要求：**  廠商說明:  Microsoft Azure 以Azure Active Directory 為微軟雲端平台之身分驗證機制，Azure Active Directory 提供下列多種多因素驗證機制，包含Microsoft Authenticator 應用程式，OATH 硬體權杖，SMS，語音通話等驗證方式。  <https://docs.microsoft.com/zh-tw/azure/active-directory/authentication/concept-mfa-howitworks> |
| 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 | ● | ● | ● | **☑符合要求：**  **依雲端服務共契採購契約要求**，雲端服務與履約標的相關之日誌保存項目如下：   1. 應用程式日誌(AP log)**(必要)** 2. 登入日誌(logon log)**(必要)** 3. 網站日誌(web log)**(必要)** 4. 作業系統日誌(OS event log)：若無法提供請提出說明(例如:因服務底層採用Serverless等架構，無直接管理作業系統，故無法提供作業系統日誌。)   上述日誌項目保存期限：自資料產生起保存**至少6個月**(含契約終止或解除或期滿後)。  廠商說明:  微軟依據 Microsoft Online Services 資料保護增補合約(Microsoft Online Services Data Protection Addendum)(2020/12/9版本)內「資料處理之性質: 所有權」(Nature of Data processing; Ownership)、資料保留及刪除(Data Retention and Deletion) 段落詳述資料保存規則。自用戶開始登入Microsoft Azure 服務後之相關操作及活動，將透過Azure Active Logs 自動保存相關紀錄，並搭配Azure Blob Storage保存至6個月以上。  Azure Entra ID 以及 log analytics 將記錄的資訊包含登入名稱、時間、IP 位址、操作狀態、操作標的目標、應用程式紀錄、網頁伺服器紀錄、錯誤訊息、部署狀態及重要安全性事件等。  微軟監視紀錄規則及樣態:  <https://docs.microsoft.com/zh-tw/azure/azure-monitor/essentials/activity-log>  登入日誌:  <https://learn.microsoft.com/zh-tw/azure/active-directory/reports-monitoring/concept-sign-ins>  應用程式日誌:  <https://learn.microsoft.com/zh-tw/azure/app-service/troubleshoot-diagnostic-logs>  Azure 監視器查詢 VM os log 以及 AP log:  <https://learn.microsoft.com/zh-tw/azure/azure-monitor/vm/vminsights-log-query> |
| 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 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明具備營運持續、資料復原計畫與執行情形)  **☑符合要求：**  廠商說明:  Azure提供高可用性、災害復原和備份功能可與您的應用程式搭配使用。  https://azure.microsoft.com/zh-tw/features/reliability/#featuresMicrosoft Azure雲端服務符合ISO 22301:2012 Business Continuity Management Standard，且可存取證書及獨立稽核報告。  <https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-22301> |
| 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明雲端服務變更管理制度做法)  **☑符合要求：**  廠商說明:  Microsoft Azure 提供Azure 入口網站(Azure Portal) 協助用戶線上隨時進行申請，修改或退租所使用之Azure 雲端服務資源。  <https://docs.microsoft.com/zh-tw/azure/azure-portal/azure-portal-overview> |
| 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明雲端服務具備設定安全管理)  **☑符合要求：**  廠商說明:  資訊安全是CSP 與用戶共同承擔責任，Microsoft Azure 提供機關承辦人租用服務之整體資訊安全管理架構，並透過Azure Security Center 評分機制讓租用戶隨著部署的服務類型與數量，隨時掌握目前雲端服務當前安全分數和最佳安全分數的差距，並提供可執行的安全改善與補救步驟建議。相關功能可參閱Azure 資訊安全中心  <https://azure.microsoft.com/zh-tw/services/security-center/#overviewAzure>  資訊安全中心的安全分數  <https://docs.microsoft.com/zh-tw/azure/security-center/secure-score-security-controls> |
| 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：**  **依雲端服務共契採購契約要求**，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：**  **依雲端服務共契採購契約要求**，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。 |
| 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 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列分別說明雲端服務於虛擬主機平台內之虛擬主機映像檔強化儲存與使用安全做法)  **☑符合要求：**  廠商說明:  透過微軟雲端平台內建工具 Azure VM Image Builder 協助確保安全性 (包括修補和更新) 和自訂映像的完整控制。連線到現有虛擬網路，以存取可路由傳送的資源、伺服器和服務，包括 Chef、Puppet 和 Desired State Configuration (DSC) 等設定伺服器。與[共用映像庫](https://go.microsoft.com/fwlink/?linkid=2212439)整合，輕鬆管理映像並在全域複寫。  <https://azure.microsoft.com/zh-tw/products/image-builder> |
| 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 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列說明雲端服務機密或個人資料依相關法令強化資料安全防護措施)  **☑符合要求：**  廠商說明:  保護靜態資料的安全使用資料加密是資料隱私權、合規性及資料主權的必要步驟。整理Microsoft Azure 資料傳輸與靜態資料加密之最佳做法:最佳做法：套用磁碟加密來協助保護您的資料。詳細資料：使用Azure 磁碟加密。它可讓IT 系統管理員加密Windows 和Linux IaaS VM 磁碟。磁碟加密結合業界標準的Windows BitLocker 功能和Linux dm-crypt 功能，為OS 和資料磁碟提供磁碟區加密。Azure 儲存體和Azure SQL Database 預設會加密待用資料，且許多服務會提供加密選項。您可以使用Azure Key Vault 控管存取和加密資料的金鑰。若要深入瞭解，請參閱Azure 資源提供者加密模型支援。  <https://azure.microsoft.com/zh-tw/products/key-vault> |
| 資安防護建置持續監控 | 資安監控(SOC)機制，廠商須提供 7x24 小時全天候監控 | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  **☑符合要求：**  廠商說明:  「適用於雲端的 Microsoft Defender」是一個雲端原生應用程式保護平台 (CNAPP)，由旨在保護雲端式應用程式免受各種網路威脅和弱點攻擊的安全性措施和做法所組成。 適用於雲端的 Defender 結合了以下功能：   * 一套開發安全性作業 (DevSecOps) 解決方案，可跨多雲端和多管線環境統一程式碼層級的安全性管理 * 雲端安全性態勢管理 (CSPM) 解決方案，可呈現您可以採取的動作來防止缺口 * 雲端工作負載保護平台 (CWPP) 具有伺服器、容器、儲存體、資料庫和其他工作負載的特定保護   <https://www.microsoft.com/zh-tw/security/business/solutions/cloud-security> |
| 須提供資安事件應變服務(Emergency Response Service) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  **☑符合要求：**  廠商說明:  Microsoft Azure 若發生服務安全問題將依據 Microsoft Online Services資料保護增補合約(Microsoft Online Services Data Protection Addendum)(2020/12/9版本)有關「安全性事件通知」(Security Incident Notification)段落及附錄A-安全措施(Appendix A-Security measures) 內合約條文通知用戶。  <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA> |
| 具備相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制(DDoS 防護服務、防毒、防火牆、IPS/IDS、WAF、APT等) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  **☑符合要求：**  廠商說明:  Microsoft Azure 與 Microsoft 365 提供各式 Defender 偵測入侵並依據戶用設定以電子郵件通知以保護您的雲端工作負載。  Microsoft Azure Defender  <https://docs.microsoft.com/zh-tw/azure/security-center/azure-defender>  Azure DDoS 保護:  <https://learn.microsoft.com/zh-tw/azure/ddos-protection/ddos-protection-overview>  Azure 防火牆:  <https://azure.microsoft.com/zh-tw/products/azure-firewall>  Azure 的網路安全性最佳做法  <https://learn.microsoft.com/zh-tw/azure/security/fundamentals/network-best-practices> |
| 導入端點偵測與回應機制(Endpoint Detection and Respons, EDR) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  **☑符合要求：**  廠商說明:  您可以使用「適用於伺服器的 Microsoft Defender」，存取[適用於端點的 Microsoft Defender](https://learn.microsoft.com/zh-tw/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint) 並將其部署到伺服器資源。  適用於端點的 Microsoft Defender 是全面性雲端端點安全性解決方案。 主要功能包括：   * 風險型的弱點管理和評量 * 攻擊面縮減 * 雲端式的行為型保護 * 端點偵測及回應 (EDR) * 自動化調查和補救 * 受控搜捕服務   <https://learn.microsoft.com/zh-tw/azure/defender-for-cloud/integration-defender-for-endpoint> |
| 導入VANS (Vulnerability Alert and Notification System, VANS) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  **☑符合要求：**  廠商說明:  透過微軟Azure 資訊安全中心可在您的 Azure 虛擬機器、容器映射及 SQL 伺服器上執行弱點評定、掃描及自動修補。  <https://learn.microsoft.com/zh-tw/security/benchmark/azure/security-control-vulnerability-management>  Microsoft Azure 內建提供Azure Defender 弱點掃描服務<https://docs.microsoft.com/zh-tw/azure/security-center/defender-for-servers-introduction>  用戶無需額外使用外部弱點掃描服務。  若需要外部弱點掃描與入侵測試用戶需依據以下規範進行弱點掃描與滲透測試  <https://docs.microsoft.com/zh-tw/azure/security/fundamentals/pen-testing>  滲透測試運作規則  <https://www.microsoft.com/zh-tw/msrc/pentest-rules-of-engagement>  在Azure 上開發安全的應用程式  <https://docs.microsoft.com/zh-tw/azure/security/develop/secure-develop> |
| 導入GCB(Government Configuration Baseline) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  如有不適用規則，應擬具管理或替代作為，並提請機關資安長確認風險。  **☑符合要求：**  廠商說明:  客戶選用微軟虛擬機器時，可自行在虛擬機器上安裝 GCB 組態。  客戶可自行於 Azure IaaS 曾調整及安裝組態。 |
| 資安演練 | DDoS (Distributed Denial of Service)攻防演練 | ◎ | ◎ | ◎ | (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)  **☑符合要求：**  廠商說明:  Azure DDoS 攻防演練及模擬測試  <https://learn.microsoft.com/en-us/azure/ddos-protection/test-through-simulations> |
| 入侵與攻擊模擬 (Breach and Attack Simulation)演練  (涉及重要對外服務之系統建議評估辦理) | ◎ | ◎ | ◎ | (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)  廠商說明:  Azure 滲透測試  <https://learn.microsoft.com/zh-tw/azure/security/fundamentals/pen-testing>  Azure安全性控制：滲透測試和紅藍隊攻防練習  <https://learn.microsoft.com/zh-tw/security/benchmark/azure/security-control-penetration-tests-red-team-exercises> |
| 紅藍隊演練  (涉及重要對外服務之系統建議評估辦理) | ◎ | ◎ | ◎ |
| 資安檢測 | 主機弱點掃描 | ● | ● | ● | 該服務屬訂購機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測。  廠商說明:  Microsoft Azure 內建提供Azure Defender 弱點掃描服務<https://docs.microsoft.com/zh-tw/azure/security-center/defender-for-servers-introduction>  用戶無需額外使用外部弱點掃描服務。若需要外部弱點掃描與入侵測試用戶需依據以下規範進行弱點掃描與滲透測試<https://docs.microsoft.com/zh-tw/azure/security/fundamentals/pen-testing>  滲透測試運作規則  <https://www.microsoft.com/zh-tw/msrc/pentest-rules-of-engagement>  在Azure 上開發安全的應用程式  <https://docs.microsoft.com/zh-tw/azure/security/develop/secure-develop> |
| 網站弱點掃描 | ● | ● | ● |
| 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 基本資安標章或其他具有同等級認證 | ● | ● | ◎ | □本雲端服務提供App，並取得行動應用App基本資安標章。  App名稱：Microsoft Azure  **☑** Android：6.6.2.2024.07.05-22.46.27 **☑** iOS：6.6.2 |
| 資安健診 | ● | ● | ● | 依委託機關需求執行資安檢測，或依機關規劃另案配合執行。 |