**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**

雲端平台(PaaS或IaaS)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：　　 AWS 雲端虛擬服務

**☑**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 07 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:  AWS 文檔說明:  (參考連結：<https://aws.amazon.com/tw/compliance/iso-27001-faqs/>)  AWS ISO/IEC 27001:2022 認證:  (參考連結：<https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf>)  ISO/IEC 27001:2022 標準  (參考連結：<https://www.iso.org/standard/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Amazon Web Services (AWS) 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AWS雲端服務目前可選擇之地理區域，請詳AWS Regions and Availability Zones 說明(參考連結：<https://aws.amazon.com/tw/about-aws/global-infrastructure/regions_az/>) 雖有提供中國地理區域資料中心，但使用中國區域的客戶需要另外註冊中國服務專屬的帳戶登入資料。客戶將無法使用現有 AWS 登入資料存取中國區域的資源。 |
| 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:  AWS 會在多個層級管理OS修補，包括實體伺服器、虛擬機器（EC2）、以及應用服務。AWS提供一系列的服務來管理和修補弱點：  Amazon Inspector(參考連結：<https://aws.amazon.com/tw/inspector/>)自動化安全評估服務，可幫助提升AWS上的應用安全性和合規性。Amazon Inspector會定期掃描應用，並提供安全漏洞的詳細報告。  AWS Systems Manager Patch Manager(參考連結：<https://docs.aws.amazon.com/zh_tw/systems-manager/latest/userguide/patch-manager.html>)允許客戶自動化操作系統修補程序，包括Windows和Linux伺服器。Patch Manager會定期應用補丁，以確保系統保持最新。  AWS Trusted Advisor(參考連結：<https://aws.amazon.com/tw/premiumsupport/technology/trusted-advisor/>)提供實踐建議，包括安全性、節約成本和性能提升，會檢查環境中的安全漏洞並提供修補建議。 |
| 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，請廠商依據左列說明) 1. 雲端服務帳號權限管理機制。   1. 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:  所有 AWS 使用者都有安全認證。有帳戶擁有者 (root 使用者) AWS IAM Identity Center 的使用者、聯合身分使用者和 IAM 使用者。使用者擁有長期或暫時安全憑證。根使用者、IAM 使用者和存取金鑰具有不會過期的長期安全憑證。若要保護長期憑證，您應有現成的程序以管理存取金鑰、變更密碼和啟用 MFA。  (參考連結：<https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/security-creds.html>)  AWS全面支援TLS 1.2 安全通訊協定  (參考連結：<https://aws.amazon.com/tw/blogs/security/tls-1-2-required-for-aws-endpoints/>) |
| 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:  AWS 的零信任架構（Zero Trust Architecture, ZTA）是一種安全模型，其核心理念是「永遠不要信任，始終驗證」。這意味著不管是內部網路還是外部網路的請求，都需要經過嚴格的驗證和授權。零信任架構旨在減少內部和外部威脅，確保僅授權的用戶和設備能夠訪問資源。(參考連結：<https://aws.amazon.com/tw/security/zero-trust/>)  AWS支持符合AAL2的多因素身份驗證機制，確保用戶身份驗證的高安全性要求  (參考連結：<https://docs.aws.amazon.com/zh_tw/singlesignon/latest/userguide/mfa-types.html>) |
| 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:  AWS CloudTrail：  AWS CloudTrail 是一項專為追蹤 AWS 資源 API 調用和活動設計的服務，簡單來說就是幫您記錄誰在何時對您的 AWS 資源做了什麼。它會自動記錄所有操作，並將這些記錄儲存在您指定的 S3 儲存桶中。這些詳細的事件歷史記錄讓您可以了解所有的操作細節，增強系統的安全性和合規性。  除了記錄操作外，CloudTrail 還允許您設置警報和報告，當有特定活動發生時，它會自動通知您。例如，如果有人嘗試未經授權地存取您的資源，CloudTrail 可以立即發出警報，提醒您進行處理。此外，它還有查詢和分析功能，讓您能迅速識別並應對可疑活動或潛在的安全威脅。  舉個例子，CloudTrail 就像是一個監控系統，幫您記錄所有的操作行為，並在需要時提供詳細的活動報告，讓您能輕鬆地進行故障排除和安全檢查。這使得管理和保護您的 AWS 環境變得更加簡單和有效。  提供詳細的操作審計日誌，記錄所有AWS賬戶中的API活動，包括帳號與權限變更、登入名稱、時間、IP地址等。CloudTrail日誌自動保存6個月，客戶可將日誌存入Amazon S3以便長期保存。  (參考連結：<https://docs.aws.amazon.com/zh_tw/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>) |
| 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:  高可用性和災害復原：  AWS 的雲基礎設施設計為高可用性和容錯，利用多個地理上分散的數據中心（稱為區域和可用區域），確保服務的連續性和災害復原能力。  (參考連結：<https://docs.aws.amazon.com/en_us/wellarchitected/2022-03-31/framework/reliability.html>)  資料備份和復原：  AWS 提供一系列備份和復原解決方案，如Amazon S3、Amazon Glacier和AWS Backup，確保數據在災害發生時能夠迅速恢復。  (參考連結：<https://docs.aws.amazon.com/zh_tw/prescriptive-guidance/latest/backup-recovery/welcome.html>)  業務連續性和災害復原標準：  AWS 符合多項國際標準，包括ISO 22301:2012業務連續性管理標準，並且提供相關的合規證書和獨立稽核報告。  (參考連結：<https://aws.amazon.com/tw/compliance/iso-22301-faqs/>) |
| 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，請廠商依據左列說明雲端服務變更管理制度做法)  **☑符合要求：**  廠商說明:  AWS Management Console：  AWS 提供的入口網站，幫助用戶在線上隨時進行申請、修改或退租所使用的AWS雲端服務資源。用戶可以通過管理控制台進行各種資源的管理，包括配置、更改、監控等操作。  (參考連結：<https://aws.amazon.com/tw/console/>) |
| 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，請廠商依據左列說明雲端服務具備設定安全管理)  **☑符合要求：**  廠商說明:  AWS Identity and Access Management (IAM)：  提供細粒度的訪問控制和權限管理，確保只有授權的用戶才能對資源進行操作，保障資源的安全性。  (參考連結：<https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/id.html>)  AWS Well-Architected Framework：  提供最佳實踐指導，幫助客戶設計和運營可靠的、可擴展的和高效的雲基礎設施。  (參考連結：<https://aws.amazon.com/tw/architecture/well-architected/?ref=wellarchitected-wp>) |
| 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：**  AWS VM Import/Export：  AWS VM Import/Export 允許客戶將現有的虛擬機器映像檔匯入AWS EC2中進行使用。匯入的映像檔可以利用AWS的安全功能來保護，包括加密存儲和訪問控制。  (參考連結：<https://aws.amazon.com/tw/ec2/vm-import/>)  AWS Elastic Block Store (EBS)：  EBS 提供持久性塊存儲卷，用於Amazon EC2實例。EBS卷可以進行加密，以保護靜態數據的安全性，並確保只有授權的用戶和實例能夠訪問這些數據。  (參考連結：<https://docs.aws.amazon.com/zh_tw/ebs/latest/userguide/ebs-encryption.html>) |
| 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:  資料加密：  靜態資料加密：AWS 提供多種靜態資料加密選項，包括透過AWS Key Management Service (KMS) 進行的自動加密，以及客戶管理的加密密鑰。AWS存儲服務如Amazon S3、Amazon EBS和Amazon RDS都支持加密，確保靜態資料的安全性。  (參考連結：<https://docs.aws.amazon.com/zh_tw/prescriptive-guidance/latest/encryption-best-practices/services-best-practices.html>)  傳輸資料加密：AWS 服務支持使用TLS/SSL協議來保護資料在傳輸過程中的安全性，防止未經授權的訪問和竊聽。  安全管理工具：  AWS Identity and Access Management (IAM)：  提供細粒度的訪問控制和權限管理，確保只有授權的用戶才能對資源進行操作，保障資源的安全性。  (參考連結：<https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/id.html>)  Amazon Macie：  自動化資料分類和保護：使用機器學習技術自動發現、分類和保護Amazon S3中的敏感資料（如PII、財務數據）。  持續監控和威脅檢測：持續監控S3桶，檢測資料變更和潛在的資料洩露，並提供安全報告和警報。  (參考連結：<https://docs.aws.amazon.com/macie/latest/user/data-classification.html>) |
| 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:  AWS CloudWatch：  CloudWatch 提供全天候的監控和管理功能，幫助客戶收集和追蹤其AWS資源和應用程序的指標和日誌文件，設置警報，並自動響應特定狀況。  (參考連結：<https://docs.aws.amazon.com/zh_tw/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>) |
| 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:  AWS 安全事件回應指南:  本指南概述了回應客戶的 Amazon Web Services (AWS) 雲端環境中的安全事件的基礎知識。它概述了雲端安全性和事件回應概念，並確定了可供回應安全問題的客戶使用的雲端功能、服務和機制。  (參考連結：<https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html>) |
| 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:  Amazon Virtual Private Cloud (VPC)：  隔離和控制：Amazon VPC 允許客戶在AWS雲中啟動資源到虛擬網絡中，提供隔離和控制網絡設置的能力。客戶可以完全控制虛擬網絡環境，包括選擇自己的IP地址範圍、子網配置和路由表。  網路安全控制：VPC 支持多種安全功能，包括網絡ACL和安全組，用於控制入站和出站流量。這些安全功能確保只有授權的流量能夠進出VPC。  (參考連結：<https://docs.aws.amazon.com/zh_tw/vpc/latest/userguide/infrastructure-security.html>)  AWS Shield：  DDoS 防護：AWS Shield 是一項DDoS防護服務，分為標準版和進階版。標準版提供自動DDoS防護，進階版提供進階的威脅檢測和快速緩解。  (參考連結：<https://docs.aws.amazon.com/zh_tw/waf/latest/developerguide/ddos-overview.html>)  AWS WAF (Web Application Firewall)：  Web應用防火牆：AWS WAF 幫助保護Web應用免受常見的網絡攻擊，如SQL注入和跨站腳本攻擊。用戶可以定義自訂的規則來過濾不必要的流量。  (參考連結：https://docs.aws.amazon.com/zh\_tw/waf/latest/developerguide/how-aws-waf-works.html)  Amazon GuardDuty：  威脅檢測：GuardDuty 提供持續的威脅檢測服務，使用機器學習和威脅情報來識別潛在的安全問題。它可以監控和分析VPC流量記錄、AWS CloudTrail事件和DNS記錄。  (參考連結：<https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>) |
| 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:  AWS 提供多種工具和服務來支援端點偵測與回應（EDR）功能，幫助客戶保護其雲端環境中的端點安全。  Amazon GuardDuty：  威脅檢測：GuardDuty 提供持續的威脅檢測服務，使用機器學習和威脅情報來識別潛在的安全問題。它可以監控和分析VPC流量記錄、AWS CloudTrail事件和DNS記錄。  (參考連結：<https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>)  AWS Systems Manager：  AWS Systems Manager 提供對EC2實例和其他AWS資源的集中管理，包括安全修補管理、自動化操作和合規性檢查。它可以幫助客戶快速檢測和修復端點的安全問題。  (參考連結：<https://docs.aws.amazon.com/zh_tw/systems-manager/latest/userguide/quick-setup-patch-manager.html>)  AWS Security Hub：  AWS Security Hub 提供一個統一的安全檢查視圖，幫助客戶整合和分析來自多個AWS安全服務的警報，協助快速識別和回應安全威脅。  (參考連結：<https://docs.aws.amazon.com/zh_tw/securityhub/latest/userguide/what-is-securityhub.html>)  AWS Config：  AWS Config 持續監控和記錄AWS資源配置的變更，幫助檢測和通知配置中的漏洞，確保符合安全和合規要求。  (參考連結：<https://docs.aws.amazon.com/zh_tw/config/latest/developerguide/WhatIsConfig.html>) |
| 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:  Amazon Inspector：  自動化安全評估服務，幫助識別和修復AWS上的安全漏洞。  (參考連結：<https://docs.aws.amazon.com/zh_tw/inspector/latest/user/scanning-resources.html>) |
| 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:  AWS Artifact：  提供訪問AWS合規性報告和文檔，幫助客戶實現和維護符合政府配置基線的要求。  (參考連結：<https://docs.aws.amazon.com/zh_tw/artifact/latest/ug/what-is-aws-artifact.html>) |
| 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:  DDoS (Distributed Denial of Service) 模擬測試  AWS 提供多種工具和服務來防禦DDoS攻擊，並支援相關的演練活動。  (參考連結：<https://aws.amazon.com/tw/security/ddos-simulation-testing/?nc1=h_ls>) |
| 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)  **☑符合要求：**  廠商說明:  AWS 滲透測試  滲透測試是指模擬真實攻擊情境，以評估和強化系統和應用程序安全性的一種方法。AWS 支持客戶在其 AWS 環境中進行滲透測試，以確保其雲端資源的安全。  (參考連結：<https://aws.amazon.com/tw/security/penetration-testing/>) |
| 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:  AWS 滲透測試和弱點掃描  AWS 支持客戶在其 AWS 環境中進行滲透測試和弱點掃描，以確保其雲端資源的安全性和合規性。AWS 提供多種工具和服務來幫助客戶進行這些安全檢測活動。  (備註: 所有模擬事件請求都必須在開始日期前，至少提前兩 (2) 週提交至 AWS。)  (參考連結：<https://aws.amazon.com/tw/security/penetration-testing/>)  AWS全面支援TLS 1.2 安全通訊協定  (參考連結：<https://aws.amazon.com/tw/blogs/security/tls-1-2-required-for-aws-endpoints/>) |
| 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。  (AWS安全性和合規性文件，參考連結：<https://docs.aws.amazon.com/zh_tw/artifact/latest/ug/what-is-aws-artifact.html>)  App名稱：AWS Console  □ Android：3.4.5 □ iOS：3.4.7 |
| 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。 |