**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：Google Cloud Platform - Cloud VPN 雲端虛擬專用網路

⬜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 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 | ● | ● | ● | **Ｖ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。   Google Cloud 符合 ISO/IEC 27001 標準，參考資料連結：https://cloud.google.com/security/compliance/iso-27001?hl=zh-tw   1. 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   Google Cloud 符合 ISO/IEC 27017 標準，參考資料連結：https://cloud.google.com/security/compliance/iso-27017?hl=zh-tw   1. 雲端服務個人資訊保護管理國際標準(ISO/IEC 27018)。   Google Cloud 符合 ISO/IEC 27018 標準，參考資料連結：https://cloud.google.com/security/compliance/iso-27018?hl=zh-tw |
| 廠商不得為大陸地區廠商第三地區含陸資成分廠商 | ● | ● | ● | **Ｖ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」。   Google是總部位於美國加州山景城的跨國科技公司，為Alphabet的子公司 |
| 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) Google Cloud PaaS 如 Cloud SQL 服務，作為托管式服務，Cloud SQL 會自動更新實例，以確保底層硬件、操作系統和數據庫引擎可靠、高性能、安全且為最新版本。其中大部分更新都在 Cloud SQL 實例啟動和運行期間執行。持續監控操作系統中新發現的安全漏洞。發現漏洞後，Google 會盡快進行修補，以防範新風險。參考資料連結：https://cloud.google.com/sql/docs/mysql/maintenance |
| 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。  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。   * 帳號安全認證：Google Cloud 支持使用兩步驟身份驗證來增強帳號的安全性，防止未經授權的訪問。參考資料連結：<https://support.google.com/cloudidentity/answer/9176657?hl=zh-Hant> * 帳號安全認證：Google Cloud IAM 允許細粒度的權限控制，幫助管理誰可以訪問哪些資源以及他們能夠執行哪些操作。參考資料連結：<https://cloud.google.com/security/products/iam?hl=zh-tw> * 網路安全傳輸：Google Cloud Load Balancing 支援 TLS 1.2 安全通訊協定。參考資料連結：<https://cloud.google.com/load-balancing/docs/ssl-policies-concepts> |
| 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)  [BeyondCorp](https://cloud.google.com/beyondcorp?hl=zh-tw) 是 Google 實作的零信任網路架構，不需要任何傳統 VPN，即可從任何裝置或網路安全地進行存取。BeyondCorp 使用各種 Google Cloud 工具，例如[單一登入](https://cloud.google.com/architecture/identity/single-sign-on?hl=zh-tw)、[Access Context Manager](https://cloud.google.com/access-context-manager/docs?hl=zh-tw) 和 [Identity-Aware Proxy](https://cloud.google.com/iap?hl=zh-tw)，將範圍從網路延伸到個別裝置和使用者。  BeyondCorp 提供一組存取權控管，透過驗證和授權工作流程來驗證身分，藉此授予資源的存取權，讓機構在不影響生產力的情況下持續驗證信任關係。參考資料連結：  https://cloud.google.com/learn/what-is-zero-trust?hl=zh-tw |
| 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 | ● | ● | ● | **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)**   Google Cloud IaaS 如 Compute Engine, 可以透過安裝 Ops Agent, 將 AP 如 IIS, SAP HANA 等 Log 儲存到 Cloud Logging，且日誌可保留至少六個月。參考資料連結：  https://cloud.google.com/logging/quotas#logs\_retention\_periods   1. 登入日誌(logon log)**(必要)**   Google Cloud IaaS 如 Compute Engine Linux Based VM, 可透過查看 OS 登錄審計日誌來監控對已啟用 OS 登錄和 OS 登錄雙重身份驗證 (2FA) 的虛擬機器 (VM) 實例的連接嘗試，且日誌可保留至少六個月。參考資料連結：  https://cloud.google.com/logging/quotas#logs\_retention\_periods   1. 網站日誌(web log)**(必要)**   Google Cloud PaaS 如 Cloud Run, Cloud Run 日誌會自動發送到 Cloud Logging，如記錄發送到 Cloud Run 網頁服務的請求，且日誌可保留至少六個月。參考資料連結：  https://cloud.google.com/run/docs/logging   1. 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。) Google Cloud IaaS 如 Compute Engine 可提供系統事件日誌，如  * On host maintenance * Instance preemption * Automatic restart * Instance reset * Serial port connect/disconnect   且日誌可保留至少六個月，參考資料連結：  https://cloud.google.com/compute/docs/logging/audit-logging#audited\_operations  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)。 |
| 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) Google Cloud 的全球資料中心網路是世界上最安全和最節能的設施之一，能以最高的速度和可靠性，全年無休地執行服務。資料中心採用多層式安全防護機制，內建備援和容錯功能。  參考資料連結：  https://cloud.google.com/infrastructure?hl=zh-TW |
| 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) Google Cloud 提供了多種工具和服務來支援變更管理制度。以下是一些關鍵功能和工具：   * Cloud Deployment Manager: 用於自動化基礎設施的部署和管理，幫助使用者以代碼的形式定義、管理和配置雲資源。 * Operations Suite：提供監控、記錄和錯誤報告功能，幫助你監視和管理應用程序和基礎設施的變更。 * Cloud Source Repositories: 提供基於 Git 的代碼存儲庫，允許版本控制和變更跟踪。 * Cloud Build: 用於持續集成和持續部署（CI/CD）的工具，幫助自動化構建、測試和部署流程。 * Identity and Access Management (IAM): 管理用戶和服務賬戶的權限，確保只有授權用戶可以進行變更。 |
| 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) Google Cloud 提供了一系列工具和功能來幫助設置和管理安全制度，確保雲環境安全可靠。以下是一些關鍵功能和服務：   * Identity and Access Management (IAM): 允許精細控制誰可以訪問 Google Cloud 資源以及可以執行哪些操作。你可以創建和管理用戶、群組和服務賬戶，並分配具體的角色和權限。 * VPC Service Controls: 幫助建立安全邊界，保護 Google Cloud 資源免受來自外部和內部的威脅。可以定義和管理受控資源的範圍，限制數據的移動和訪問。 * Cloud Identity: 提供單一登錄 (SSO)、多因素認證 (MFA) 和設備管理，幫助確保用戶身份和設備安全。 * Cloud Security Command Center (SCC): 提供一個統一的安全管理平台，幫助檢測、管理和響應安全威脅。SCC 可以整合來自多個安全產品的數據，提供綜合的安全態勢視圖。 * Cloud Audit Logs: 記錄對 Google Cloud 資源進行的所有管理操作和數據訪問，幫助實現合規性和審計要求。 * Data Loss Prevention (DLP): 幫助識別、分類和保護敏感數據。DLP 工具可以掃描數據存儲和流量，識別並掩蔽敏感信息。 * Encryption: 提供靜態和傳輸中的數據加密，確保數據始終受到保護。Google Cloud 內建加密功能，並支持自帶密鑰（BYOK）。 * Security Health Analytics: 提供安全配置分析和建議，幫助你識別和修復安全配置問題，提升整體安全性。 |
| 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 | ● | ● | ● | **Ｖ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。Google Cloud 可將 IaaS 與 PaaS雲端資料儲存所在地設定於 Asia-east1 台灣，可配合機關規範進行配置。參考資料連結：  https://cloud.google.com/about/locations?hl=zh-tw#asia-pacific |
| 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。 | ● | ● | ● | **Ｖ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。Google Cloud 雲端服務資料存取、備份及備援之實體機房設定於 Asia-east1 台灣。參考資料連結：  https://cloud.google.com/about/locations?hl=zh-tw#asia-pacific |
| 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) 針對 Google Cloud 儲存與使用安全措施  使用安全：   * 受控環境：啟動虛擬機時，可以使用受控環境（如虛擬私有雲 VPC）來確保映像檔只在受信任的網路環境中運行。 * 鏡像完整性驗證：使用 Binary Authorization 來確保只有經過簽名和驗證的映像檔才能部署到您的環境中，防止未經授權的變更和惡意軟件。 * 自動修復：透過設定自動修復機制，當虛擬機遇到問題時，系統會自動替換損壞的映像檔，以保持服務的高可用性。   佐證：   * 審計日誌：Google Cloud 提供詳盡的審計日誌，記錄所有對虛擬機映像檔的存取和操作。這些日誌可以用來進行安全審查和合規性檢查。 * 合規認證：Google Cloud 遵循多項國際和行業標準的合規要求（如 ISO/IEC 27001、PCI DSS），並可以提供相應的合規報告作為佐證。 |
| 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 | ● | ● | ● | (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) Google Cloud 可使用以下方式強化資料安全   * Cloud Key Management Service (KMS) 來管理加密密鑰，確保密鑰的安全性和完整性。 * 定期輪換密鑰 並且遵循最佳實踐來保護密鑰。 * 身份與訪問管理 (IAM)：設置嚴格的訪問控制策略，確保只有授權用戶可以訪問機密或個人資料。使用多因素身份驗證 (MFA) 增強登錄安全性。 * 角色型訪問控制 (RBAC)：根據用戶角色分配適當的權限，確保遵循最小特權原則 (Principle of Least Privilege)。 * 虛擬私有雲 (VPC)：使用 VPC 提供隔離的網路環境，並設置防火牆規則控制進出流量。 * 身份感知代理 (Identity-Aware Proxy, IAP)：使用 IAP 管理應用和虛擬機的安全訪問控制。 * VPC Service Controls：擴展 VPC 的安全性，防止數據從 Google Cloud Services 無意中暴露到互聯網。 * 堡壘主機 (Bastion Host)：使用堡壘主機管理對內部網路的遠端存取，增加一層安全防護。 |
| 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) Google Cloud 可選用 Google Security Operations 結合低程式碼自動化功能和強大的協作機制，以現代化、快速且有效的方式 7x24 全面候監控應對威脅。整合資安營運活動，輕鬆產生有助於改善成效的洞察資料，並評估長期進度。   * 追蹤即時 SOC 指標和 KPI。透過立即可用的互動式報表和資訊主頁範本，查看團隊在重要指標上的表現，例如偵測率、結案數量和進步趨勢。 * 運用商業智慧有效評估及管理作業。串連、檢查並以視覺化方式呈現資料，藉此找出不足之處、重新分配資源、改良現有程序，或判斷要將哪些手動作業自動化。 * 自動擷取、記錄及回報所有 SOC 活動。在可供搜尋及稽核的單一存放區中，擷取所有分析師案件活動，包括所有自動化操作、手動作業、即時通訊、工作和上傳的檔案。   參考資料連結：  https://cloud.google.com/security/products/security-orchestration-automation-response?hl=zh-TW |
| 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) Google Security Operations 整合 SIEM、SOAR 和威脅情報等功能，可提升機構的偵測、調查和應變能力。您可以收集安全性遙測資料、運用威脅情報找出需優先處理的威脅，並透過應對手冊自動化、案件管理和協作功能提高應變能力。參考資料連結：  https://cloud.google.com/security/products/security-orchestration-automation-response?hl=zh-TW |
| 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) Google Cloud Armor 提供完善的應用程式和網站保護機制，防範阻斷服務和網路攻擊。   * 享有 Google 級分散式阻斷服務 (DDoS) 防護機制與網路應用程式防火牆 (WAF) * 偵測並緩解針對 Cloud Load Balancing 工作負載或 VM 的攻擊 * Adaptive Protection 機器學習型機制，協助偵測及封鎖第 7 層 DDoS 攻擊 * 防範 OWASP 機構所彙整的十大資安風險，保護地端部署或雲端環境中的工作負載 * 透過與 reCAPTCHA Enterprise 原生整合的機器人管理功能，防止邊緣詐欺。參考資料連結：   <https://cloud.google.com/security/products/armor?hl=zh-TW>  Google Cloud NGFW:   * Cloud NGFW 的完全分散式防火牆具備有狀態的檢查機制，並原生內建於我們的軟體定義網路架構中，會在各個工作負載強制執行。 * 採用 Palo Alto Networks 技術，提供領先業界且容易部署的雲端優先入侵預防系統，內嵌防護機制可保護您的網路免受惡意軟體、間諜軟體和指令與控制攻擊。 * 根據預設，網路防火牆政策為全球性，並適用於所有區域。使用階層式防火牆政策在機構、資料夾和專案層級定義政策。 * 運用以 IAM 控管的標記，跨虛擬私有雲與機構，針對單一 VM 定義南北向與東西向流量的精細控管機制。 * 政策物件，例如 Google Cloud Threat Intelligence 清單、網域名稱 (FQDN) 物件和地理位置物件，提供防火牆規則的進階保護功能。這些物件是由 Google 收錄、會持續更新，並自動套用到呼叫這些物件的防火牆規則。參考資料連結：   https://cloud.google.com/security/products/firewall?hl=zh-TW |
| 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) Google Cloud Marketplace 提供多種 EDR 解決方案選擇，如Sophos Intercept X |
| 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)  Security Command Center 整合了主動式和被動安全防護機制，提供防護機制管理和威脅偵測功能，保護程式碼、身分和資料。內建補救措施可簡化安全應變流程。全部採用 Google 的創新技術，並在全球規模的資料湖泊中運作。參考資料連結：  <https://cloud.google.com/security/products/security-command-center?hl=zh-TW>  Security Command Center 提供相關的 API 串接服務，亦可結合 Pub/Sub 來做告警訊息的推送。參考資料連結：  <https://cloud.google.com/security-command-center/docs/how-to-api-manage-notifications> |
| 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。 |
| 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) |
| 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) |
| 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。Google Cloud 委託 Coalfire System 進行滲透測試，針對 Google Cloud Console 及 Google Cloud 各個主要服務進行檢測。  GCP 主機弱點掃描：  GCP 提供多種內建工具和第三方整合方式，協助您進行主機弱點掃描。這些工具能有效地檢測並修復潛在的漏洞，確保您的雲端環境安全。  Cloud Security Command Center (SCC): 先主動找出多雲端環境中的安全漏洞和錯誤設定，以免攻擊者利用這些弱點存取機密雲端資源。然後使用攻擊路徑和遭受攻擊風險分數來優先排序風險最大的安全性問題。監控業界標準的遵循情形，如 CIS、PCI-DSS、NIST 等。將結果匯出至風險和法規遵循團隊。此外，也可透過第三方工具如 Tenable 整合提供 Nessus 等知名主機漏洞掃描工具。  網站弱點掃描：  GCP 提供了專門針對網站的弱點掃描工具，協助您檢測常見的Web應用程式漏洞。 Web Security Scanner: 自動掃描網頁應用程式，找出常見的漏洞，如SQL注入、XSS、檔案上傳漏洞等。  滲透測試掃描:  GCP內建功能 Cloud Load Balancing 可以設定TLS版本和加密套件，以及Cloud CDN 支持TLS 1.3。此外，也可透過第三方工具如 nmap 掃描SSL/TLS服務 |
| 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 | ● | ● | ◎ | **Ｖ**本雲端服務提供App，並取得行動應用App基本資安標章。這個應用程式已根據全球安全性標準完成獨立驗證  App名稱：Google Cloud Platform - Cloud VPN 雲端虛擬專用網路  **Ｖ** Android：1.24.prod.638802256 ⬜ iOS：1.28.259 |
| 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。  可配合機關規劃與需求執行資安健診，在此先提供健診執行的可能方式與工具：  1. Cloud Security Command Center (SCC): 提供全面的安全狀態檢視，並提出改善建議。  2. Security Health Analytics: 自動化識別配置錯誤和安全風險。 Vulnerability Scanner: 定期掃描漏洞。  3. Web Security Scanner: 掃描Web應用程式漏洞。 |