



數位發展部 數位產業署
Administration for
Digital Industries, moda

113年體驗符合國家標準之雲端服務水準暨資通安全檢測推動介紹

2024年7月3日

➤ 目的

- 隨著雲端服務的蓬勃發展，政府與產業採購雲端服務的比例也逐年增加，共同供應契約後續也將更開放雲端服務進入政府市場，因此如何為雲端服務的品質把關是當前的一大課題。
- 鑒於雲端服務的品質需要一套制度來規範以有效保證買賣雙方的權益，「軟體採購辦公室」於105年起參採ISO 19086推動CNS 19086標準的制定，作為雲端服務水準認證制度的發展基礎。

➤ 期待

- 111年已與全國認證基金會(TAF)完成檢測實驗室的評鑑制度規劃。
- 112年起提供具備雲端服務檢測能量之**驗證機構取得合格實驗室認證資格**。
- 113年起視實驗室整備度，**促成實驗室驗證雲端業者其CNS 19086項目之符合性**，逐步穩固雲端服務水準認證生態系，以確保雲端業者的服務水準，將來政府與產業也可據以評估雲端服務提供者，建立可信賴的雲端服務採購環境。

什麼是CNS 19086標準？

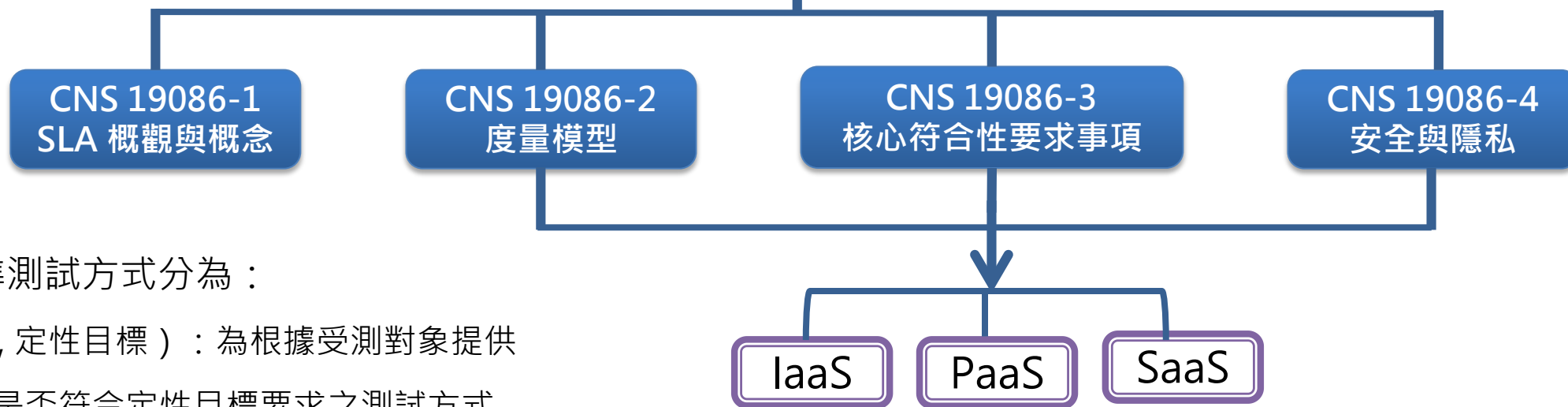
- CNS 19086標準全名為「**雲端運算 - 服務水準協議 (SLA) 框架**」(Cloud computing – Service Level Agreement Framework)，建構於標準17788與17789之上，主要目的為提供任何參與建立、修訂或了解雲端服務水準協議之組織或個人參考使用。雲端SLA 宜考量雲端服務之關鍵特性，本標準能協助促進雲端服務提供者與雲端服務使用者之間的共識，標準共分為四部。
- 軟體採購辦公室從105年開始即陸續依據ISO 19086各部的發行狀況，緊密同步提出CNS制定建議書與中文化草案，協助標檢局技術審查並於110年前完成四部公告。

雲端服務國家標準(1/4)

自106年依循ISO國際標準組織
發布「ISO/IEC 19086 Cloud
computing-Service level
agreement (SLA) framework」
內容轉換制訂國家標準
CNS 19086



雲端運算 - 服務水準協議(SLA)框架 Cloud computing – Service Level Agreement Framework (CNS 19086)



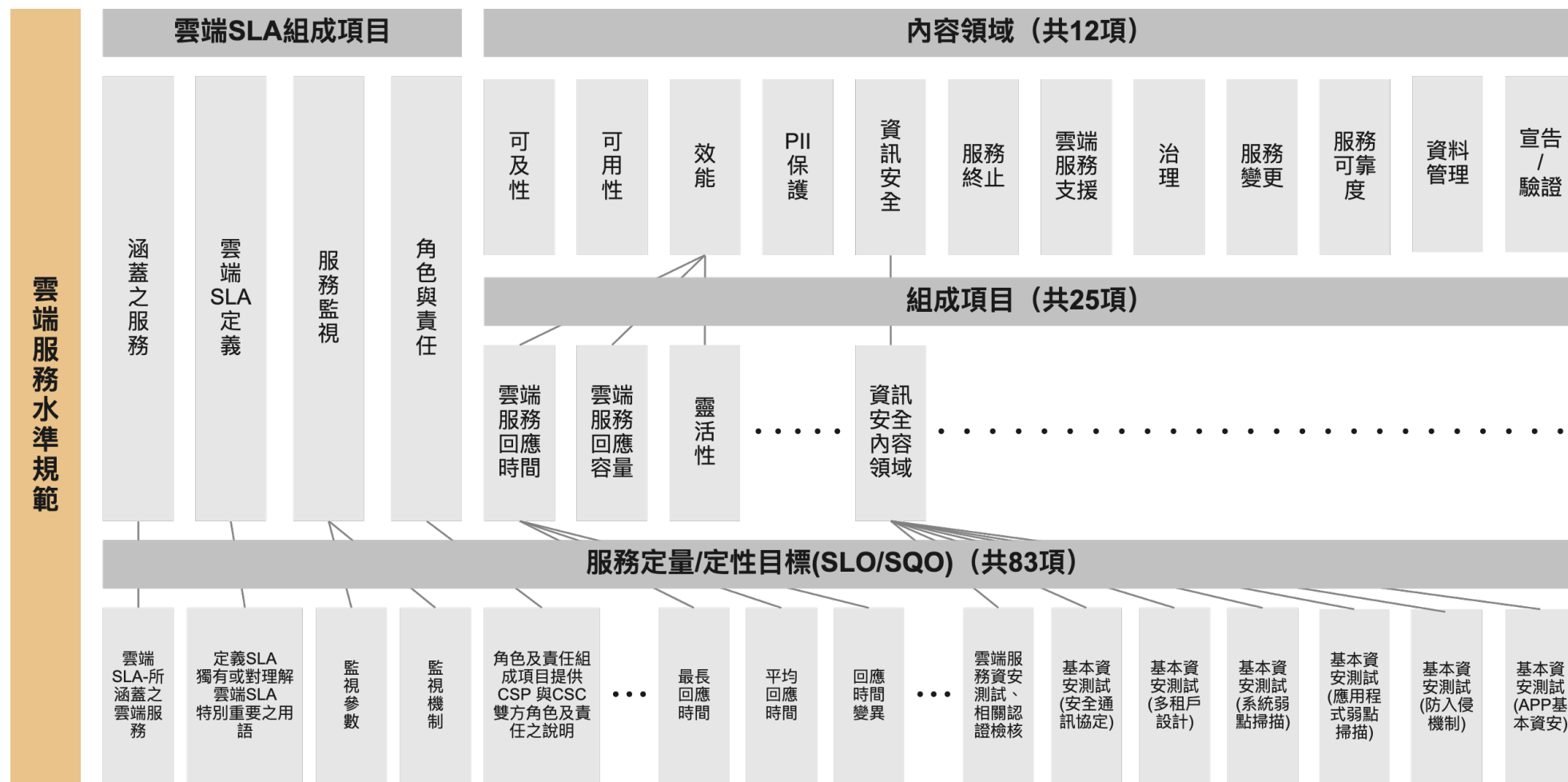
雲端服務水準測試方式分為：

- 檢驗 (SQO, 定性目標)：為根據受測對象提供之資料判斷是否符合定性目標要求之測試方式
- 測試 (SLO, 定量目標)：為使用工具或手動測試來判斷是否符合定量目標要求之測試方式

依條文要求規劃**三領域(IaaS、PaaS及SaaS)**
計83項測試項目
其中**47項為任一領域必測項目**

雲端服務國家標準(2/4)

- 雲端服務水準測試規範主要是依據4項雲端SLA組成項目及12項內容領域所發展，其架構如下圖：



雲端服務國家標準(3/4)

- 以SaaS檢測為例：必要測試之定量 / 定性目標共45項如下所示：

領域	組成項目	服務定量/定性目標 (SLO/SQO)
雲端SLA組成項目	所涵蓋雲端服務	雲端SLA-所涵蓋之雲端服務
雲端SLA組成項目	雲端SLA定義	定義SLA 獨有或對理解雲端SLA 特別重要之用語。
雲端SLA組成項目	服務監視	監視參數(Monitoring Parameters)
雲端SLA組成項目	服務監視	監視機制(Monitoring Mechanisms)
可及	可及性	可及性標準(Accessibility Standards)
可用	可用性(Availability)	可用性(Availability)
服務效能	雲端服務回應時間	平均回應時間(Response Time Mean)
服務效能	雲端服務容量	同時連線數之限制(Limit of Simultaneous Connections)
服務效能	靈活性(Elasticity)	靈活性速度(Elasticity Speed)
個資	個資保護(PII)	個資保護-相關認證檢核，如ISO 27001/ BS10012/
資訊安全	資訊安全內容領域	雲端服務資安測試、相關認證檢核
資訊安全	資訊安全內容領域	基本資安測試(安全通訊協定)
資訊安全	資訊安全內容領域	基本資安測試(多租戶設計)
資訊安全	資訊安全內容領域	基本資安測試(系統弱點掃描)
資訊安全	資訊安全內容領域	基本資安測試(應用程式弱點掃描)
資訊安全	資訊安全內容領域	基本資安測試(防入侵機制)
資訊安全	資訊安全內容領域	基本資安測試(APP基本資安)
服務終止	服務終止	服務終止通知(Notification of Serv. Termination)
服務支援	雲端服務支援	支援時段(Support Hours)
服務支援	雲端服務支援	支援方法(Support Methods)
服務支援	雲端服務支援	支援聯絡窗口(Support Contacts)
治理	治理(Governance)	法規遵循Regulation Adherence)
治理	治理(Governance)	標準遵循(Standards Adherence)

領域	組成項目	服務定量/定性目標 (SLO/SQO)
治理	治理(Governance)	標準遵循(Standards Adherence)
變更管理	雲端服務特性及功能變更	服務變更通知期限(Minimum Notification Period)
服務可靠性	服務韌性/容錯	服務復原時間(Time to Service Recovery /TTSR)
服務可靠性	服務韌性/容錯	服務韌性/容錯方法(Resiliency/Fault Tolerance)
服務可靠性	客戶資料備份及回復	備份期間(Backup Interval)
服務可靠性	客戶資料備份及回復	備份資料留存期間(Retention Period)
服務可靠性	客戶資料備份及回復	備份方法(Backup Method)
服務可靠性	客戶資料備份及回復	資料備份儲存位置(Data Backup Storage Location)
服務可靠性	災難復原	復原時間目標(Recovery Time Objective /RTO)
服務可靠性	災難復原	復原點目標(Recovery Point Objective/RPO)
資料管理	智慧財產權	智慧財產權(Intellectual Property Rights)
資料管理	雲端服務客戶資料	客戶資料(Customer Data)
資料管理	雲端服務客戶資料	客戶資料使用(Cloud Serv Customer Data Usage)
資料管理	雲端服務提供者資料	提供者資料(Provider Data)
資料管理	帳戶資料	帳戶資料(Account data)
資料管理	衍生資料	衍生資料(Derived Data)
資料管理	衍生資料	衍生資料使用(Derived Data Usage)
資料管理	資料可攜性	資料可攜能力(Data Portability Capabilities)
資料管理	資料刪除	資料刪除時限(Data Deletion Time)
資料管理	資料位置	資料位置政策(Data Location Policy)
資料管理	資料檢驗	資料檢驗(Data Examination)
資料管理	法遵請求	法遵請求(Law Enforcement Requests)
驗證稽核	具結、驗證及稽核	雲端服務驗證(Cloud Service Certifications)

雲端服務國家標準(4/4)

- 必測試之定量/定性目標相對應的SaaS測試項目如右圖：

領域	組成項目	服務定量/定性目標 (SLO/SQO)
雲端SLA組成項目	所涵蓋雲端服務	雲端SLA-所涵蓋之雲端服務
雲端SLA組成項目	雲端SLA定義	定義SLA 獨有或對理解雲端SLA 特別重要之用語。
雲端SLA組成項目	服務監視	監視參數(Monitoring Parameters)
雲端SLA組成項目	服務監視	監視機制(Monitoring Mechanisms)
可及	可及性	可及性標準(Accessibility Standards)
可用	可用性(Availability)	可用性(Availability)
服務效能	雲端服務回應時間	平均回應時間(Response Time Mean)
服務效能	雲端服務容量	同時連線數之限制(Limit of Simultaneous Connections)
服務效能	靈活性(Elasticity)	靈活性速度(Elasticity Speed)
個資	個資保護(PII)	個資保護-相關認證檢核，如ISO 27001/ BS10012/ TIS
資訊安全	資訊安全內容領域	雲端服務資安測試、相關認證檢核
資訊安全	資訊安全內容領域	基本資安測試(安全通訊協定)
資訊安全	資訊安全內容領域	基本資安測試(多租戶設計)
資訊安全	資訊安全內容領域	基本資安測試(系統弱點掃描)
資訊安全	資訊安全內容領域	基本資安測試(應用程式弱點掃描)
資訊安全	資訊安全內容領域	基本資安測試(防入侵機制)
資訊安全	資訊安全內容領域	基本資安測試(APP基本資安)
服務終止	服務終止	服務終止通知(Notification of Serv. Termination)
服務支援	雲端服務支援	支援時段(Support Hours)
服務支援	雲端服務支援	支援方法(Support Methods)
服務支援	雲端服務支援	支援聯絡窗口(Support Contacts)
治理	治理(Governance)	法規遵循Regulation Adherence)
治理	治理(Governance)	標準遵循(Standards Adherence)



驗測項目	驗測指標	指標說明	驗測方式
網路安全	傳輸層安全之設計	傳輸層通道安全須採 TLS1.2 以上(Transport Layer Security)並不得採用 SSL V3.0 或其他版本機制(參考依據 NIST Publication 800-52)	檢視
	傳輸資料數據之加密	資料數據本身於傳輸過程時是否加密 (例: 採國際編碼 AES256)	檢視
	上傳傳輸安全設計 (新增項目)	網頁是否具有檔案上傳功能，傳輸過程時是否具有安全設計 (例: 採國際編碼 AES256)	檢視
程式碼安全	程式碼設計安全弱點 風險(Code Review)	針對程式碼進行白箱測試，無中高風險 (使用工具 Fortify)	測試
網頁安全(弱點)	Web 網站安全弱點風險	針對 Web 網站進行黑箱測試，無中高風險 (使用工具 WebInspect)	測試
網站系統安全	網站主機作業系統安全 弱點風險	針對網站主機作業系統進行黑箱測試，無中高風險 (使用工具 Nessus)	測試
開源元件安全 (open Source)	第三方開源元件安全 及授權	針對第三方開源元件安全及授權進行掃描測試，無中高風險 (使用工具 Black Duck Software)	測試
人工滲透測試	滲透測試	進行複合式滲透測試，包含 Web 網頁、主機系統、網路環境，無滲透成功 (人工滲透)	測試
多租戶設計	權限安全設計	帳號權限管理功能是否具備多租戶管理之設計，且提供各租戶帳號權限管理功能	檢視
	資料庫安全設計	資料庫是否考量個資法安全要求，針對機敏欄位資料儲存，具加強安全性設計 (例: 編碼加密)	檢視

➤ 益處

- 可減少檢測成本，由本辦公室委託之專業實驗室協助測試及輔導說明。
- 未來將於數位發展部數產署軟體採購辦公室共契網站，適當的揭露相關資訊，可供採購機關挑選採用產品之評估因素之一，提升機關的服務效率與品質。
- 凡配合通過本次測試之雲端服務商，可獲得於展會展示攤位機會，向與會機關進行產品推廣。
- 如取得CNS19086測試通過，於數位發展部數位產業署軟體採購辦公室，所辦理之雲端服務標，僅需提出效期內證明文件，無須進行檢測作業。
- 可藉雲端服務之檢驗通過，因資訊揭露取得服務認同，提升雲端服務市場之能見度，有利於業界推廣行銷，擴大商機。

感謝您的聆聽

Thank You



數位發展部 數位產業署
Administration for
Digital Industries, moda

