

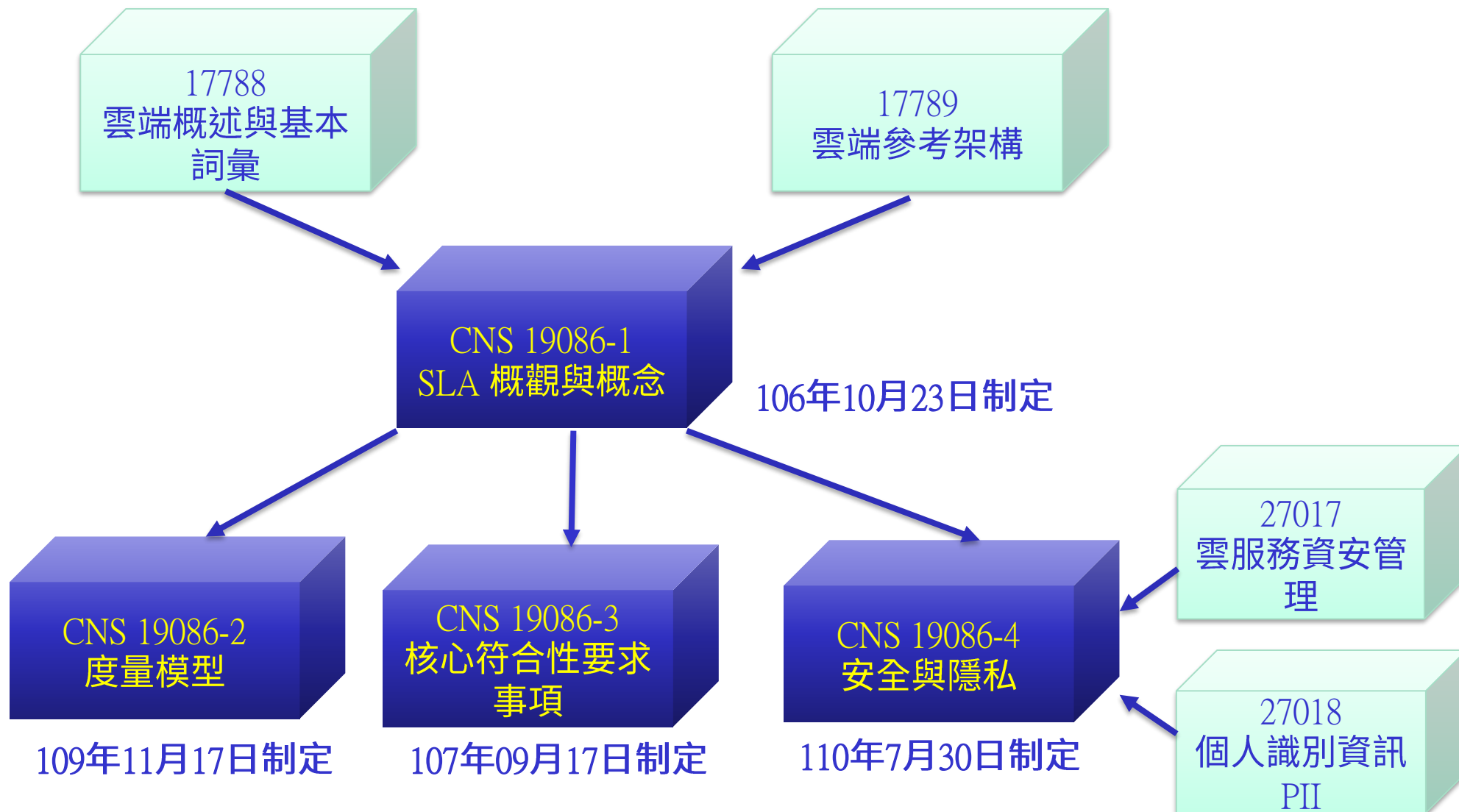


數位發展部 數位產業署
Administration for
Digital Industries, moda

CNS 19086雲端檢測說明

2024

CNS 19086 標準架構與制定進程



為何產生CNS 19086 (1/2)

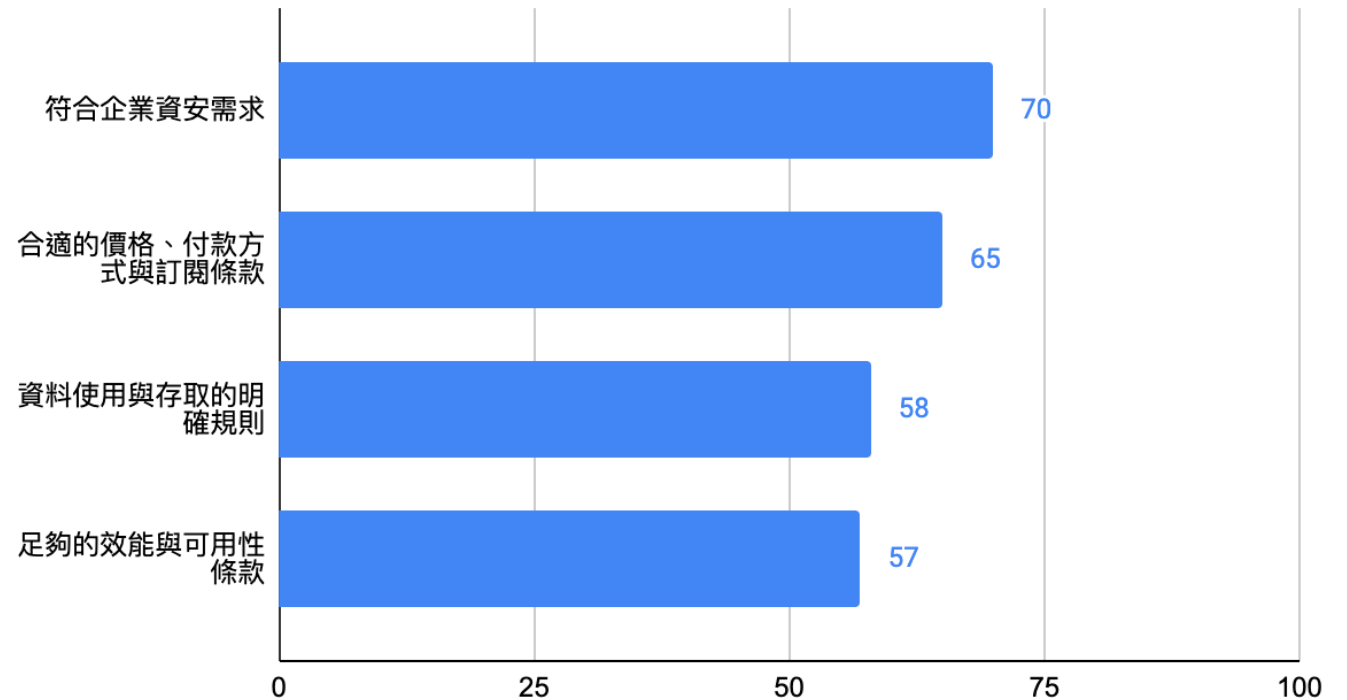
➤ 企業選擇CSP時應自我檢視的三大項目：

➤ 對於技術與選擇過程的專業知識

➤ 整合該APP的能力

➤ 產業經驗

雲端服務購買者在意的SLA要素(%)



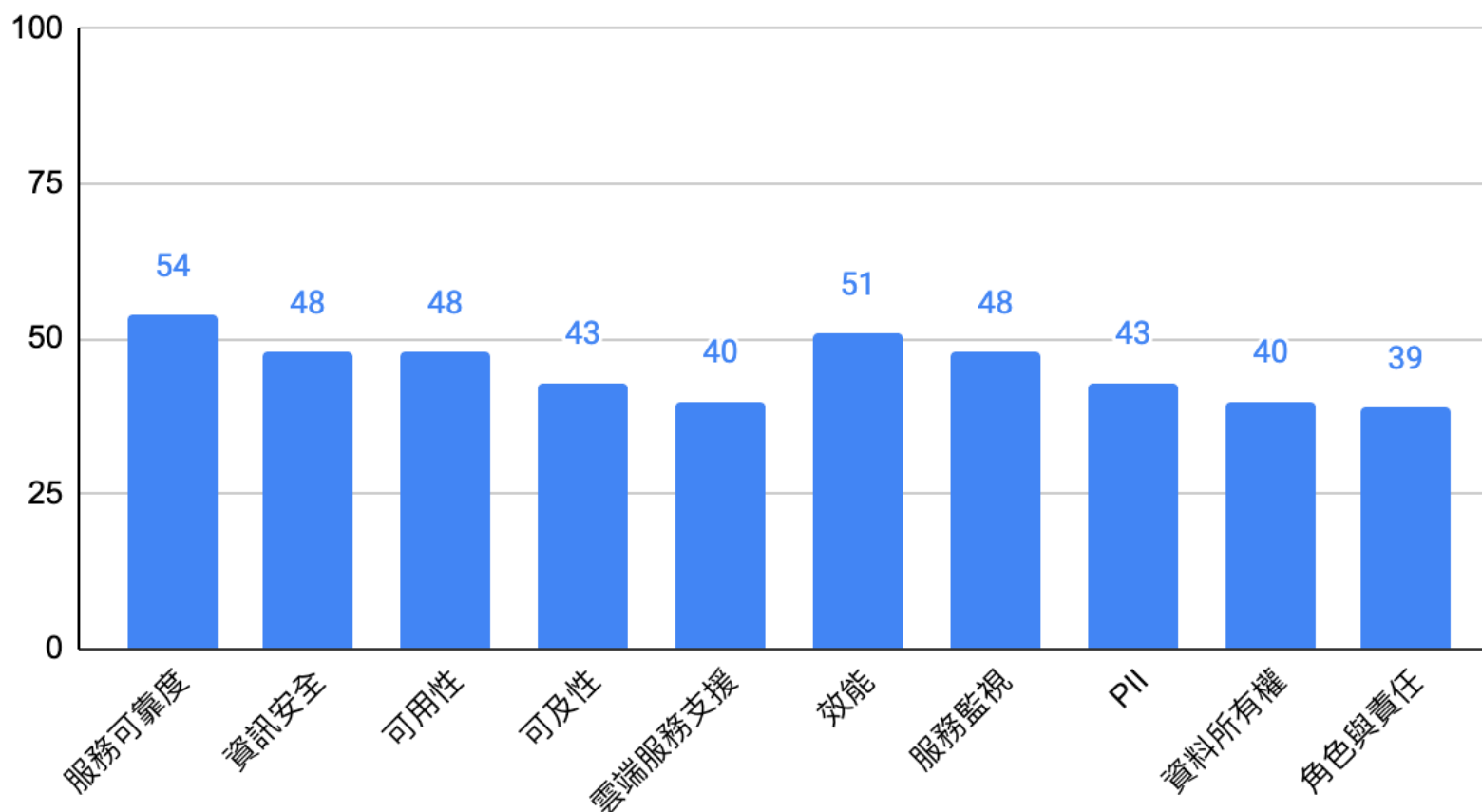
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft

為何產生CNS 19086 (2/2)



現行SLA內常忽略各種CNS 19086內的關鍵要素

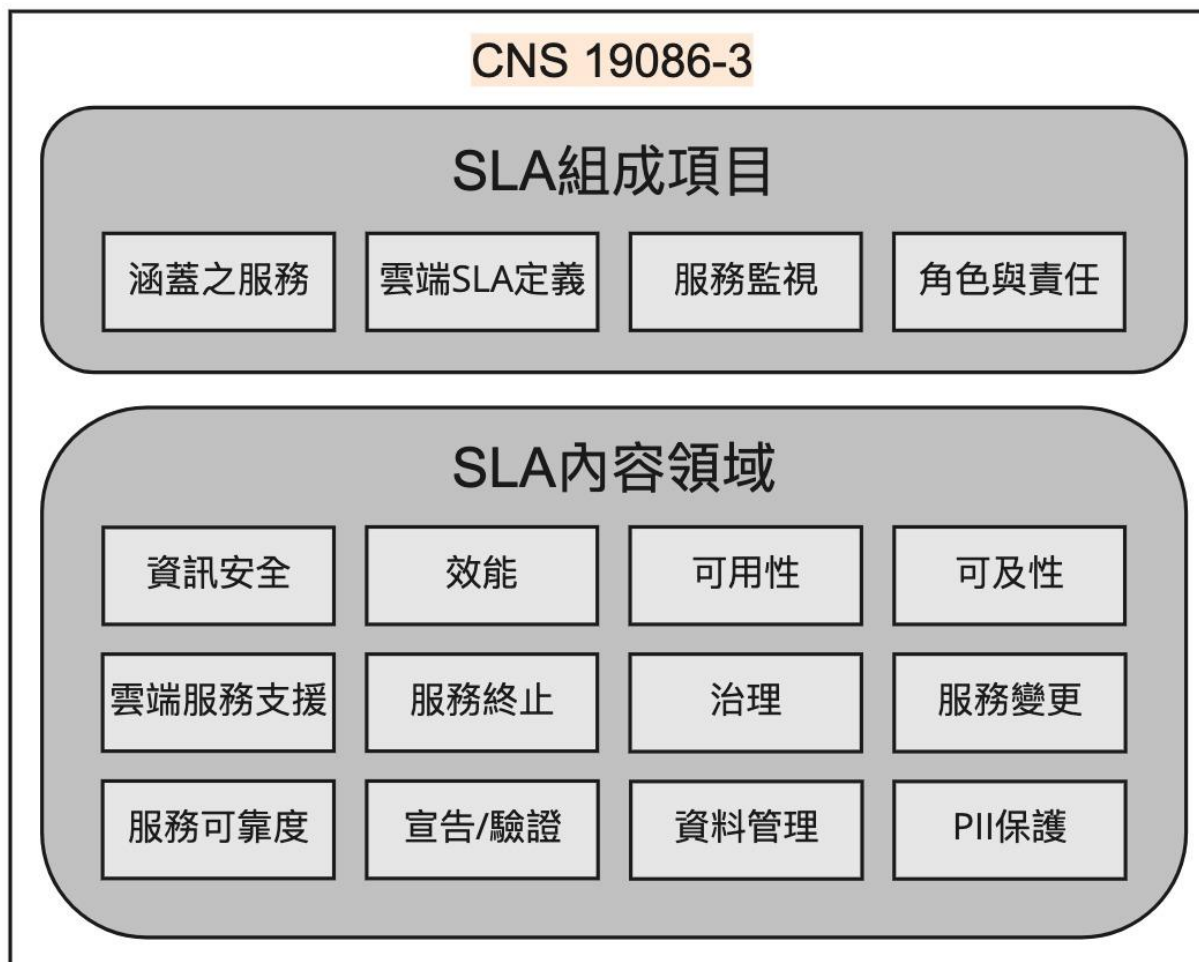
關鍵要素包含於SLA的比例(%)



Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft

CNS 19086 測試規範與架構 – 必要項目

➤ 依19086-3規範，可分為16大必要項目：



測試規範的技術內容介紹

- 雲端服務水準測試規範之雲端服務領域分為IaaS、PaaS及SaaS，針對不同雲端服務領域有不同的測試項目。
- 雲端服務水準測試規範項目**共為83項**，**47項**為(IaaS, PaaS, SaaS)任一領域之**必測項目**，餘**36項**為**選測項目**。
- 雲端服務水準測試規範之測試方式分為：
 - SQO定性目標：根據受測對象提供之資料**檢視**是否符合定性目標要求之測試方式。(Cloud Service Qualitative Objective, SQO)
 - SLO定量目標：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。(Cloud Service Level Objective, SLO)

IaaS領域測試必測項目

IaaS領域驗測之必測項目為45項

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)
1	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
2		雲端SLA定義	定義SLA 獨有或對理解雲端SLA 特別重要之用語。
3		服務監視	監視參數(Monitoring Parameters)
4		服務監視	監視機制(Monitoring Mechanisms)
5	可及	可及性(Accessibility)	可及性標準(Accessibility Standards)
6	可用	可用性(Availability)	可用性(Availability)
7	服務效能	雲端服務回應時間	平均回應時間(Response Time Mean)
8		雲端服務容量	可用資源上限(Limit of Available Resources)
9		靈活性(Elasticity)	靈活性速度(Elasticity Speed)
10	個資	個資保護(PII)	個資保護-相關認證檢核，如ISO 27001/ BS10012/
11	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
12			基本資安測試(安全通訊協定)
13			基本資安測試(多租戶設計)
14			基本資安測試(系統弱點掃描)
15			基本資安測試(應用程式弱點掃描)
16			基本資安測試(防入侵機制)
17			基本資安測試(APP基本資安)
18	服務終止	服務終止	服務終止通知(Notification of Serv. Termination)
19	服務支援	雲端服務支援	支援時段(Support Hours)
20			支援方法(Support Methods)
21			支援聯絡窗口(Support Contacts)
22	治理	治理(Governance)	法規遵循Regulation Adherence) 個資法、資安法..
23			標準遵循(Standards Adherence) ISO...
24	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)

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)
25	服務可靠性	服務韌性/容錯 (resilience/fault tolerance)	服務復原時間(Time to Service Recovery /TTSR)
26			服務韌性/容錯方法(Resiliency/Fault Tolerance)
27		客戶資料備份及回復	備份期間(Backup Interval)
28			備份資料留存期間(Retention Period)
29			備份方法(Backup Method)
30			資料備份儲存位置(Data Backup Storage Location)
31		災難復原	復原時間目標(Recovery Time Objective /RTO)
32			復原點目標(Recovery Point Objective/RPO)
33	資料管理	智慧財產權	智慧財產權(Intellectual Property Rights)
34		雲端服務客戶資料	客戶資料(Customer Data)
35			客戶資料使用(Cloud Serv Customer Data Usage)
36		雲端服務提供者資料	提供者資料(Provider Data)
37		帳戶資料	帳戶資料(Account data)
38		衍生資料	衍生資料(Derived Data)
39			衍生資料使用(Derived Data Usage)
40		資料可攜性	資料可攜能力(Data Portability Capabilities)
41		資料刪除	資料刪除時限(Data Deletion Time)
42		資料位置	資料位置政策(Data Location Policy)
43		資料檢驗	資料檢驗(Data Examination)
44		法遵請求	法遵請求(Law Enforcement Requests)
45	驗證稽核	具結、驗證及稽核	雲端服務驗證(Cloud Service Certifications)

PaaS領域測試必測項目

➤ PaaS領域驗測之必測項目為47項

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)
1	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
2		雲端SLA定義	定義SLA 獨有或對理解雲端SLA 特別重要之用語。
3		服務監視	監視參數(Monitoring Parameters)
4			監視機制(Monitoring Mechanisms)
5	可及	可及性(Accessibility)	可及性標準(Accessibility Standards)
6	可用	可用性(Availability)	可用性(Availability)
7	服務效能	雲端服務回應時間	平均回應時間(Response Time Mean)
8		雲端服務容量	同時連線數之限制(Limit of Simultaneous Connection)
9			可用資源上限(Limit of Available Resources)
10			服務處理能量(Cloud Service Throughput)
11		靈活性(Elasticity)	靈活性速度(Elasticity Speed)
12	個資	個資保護(PII)	個資保護-相關認證檢核，如ISO 27001/ BS10012/ T
13	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
14			基本資安測試(安全通訊協定)
15			基本資安測試(多租戶設計)
16			基本資安測試(系統弱點掃描)
17			基本資安測試(應用程式弱點掃描)
18			基本資安測試(防入侵機制)
19			基本資安測試(APP基本資安)
20	服務終止	服務終止	服務終止通知(Notification of Serv. Termination)
21	服務支援	雲端服務支援	支援時段(Support Hours)
22			支援方法(Support Methods)
23			支援聯絡窗口(Support Contacts)
24	治理	治理(Governance)	法規遵循(Regulation Adherence) 個資法、資安法..
25			標準遵循(Standards Adherence) ISO...
26	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)

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)
27	服務可靠性	服務韌性/容錯 (resilience/fault tolerance)	服務復原時間(Time to Service Recovery /TTSR)
28			服務韌性/容錯方法(Resiliency/Fault Tolerance)
29		客戶資料備份及回復	備份期間(Backup Interval)
30			備份資料留存期間(Retention Period)
31			備份方法(Backup Method)
32			資料備份儲存位置(Data Backup Storage Location)
33		災難復原	復原時間目標(Recovery Time Objective /RTO)
34			復原點目標(Recovery Point Objective/RPO)
35	資料管理	智慧財產權	智慧財產權(Intellectual Property Rights)
36		雲端服務客戶資料	客戶資料(Customer Data)
37			客戶資料使用(Cloud Serv Customer Data Usage)
38		雲端服務提供者資料	提供者資料(Provider Data)
39		帳戶資料	帳戶資料(Account data)
40		衍生資料	衍生資料(Derived Data)
41			衍生資料使用(Derived Data Usage)
42		資料可攜性	資料可攜能力(Data Portability Capabilities)
43		資料刪除	資料刪除時限(Data Deletion Time)
44		資料位置	資料位置政策(Data Location Policy)
45		資料檢驗	資料檢驗(Data Examination)
46		法遵請求	法遵請求(Law Enforcement Requests)
47		具結、驗證及稽核	雲端服務驗證(Cloud Service Certifications)

SaaS領域測試必測項目

➤ SaaS領域驗測之必測項目為45項

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)
1	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
2		雲端SLA定義	定義SLA 獨有或對理解雲端SLA 特別重要之用語。
3		服務監視	監視參數(Monitoring Parameters)
4			監視機制(Monitoring Mechanisms)
5	可及	可及性(Accessibility)	可及性標準(Accessibility Standards)
6	可用	可用性(Availability)	可用性(Availability)
7	服務效能	雲端服務回應時間	平均回應時間(Response Time Mean)
8		雲端服務容量	同時連線數之限制(Limit of Simultaneous Connections)
9		靈活性(Elasticity)	靈活性速度(Elasticity Speed)
10	個資	個資保護(PII)	個資保護-相關認證檢核，如ISO 27001/ BS10012/ TPIF
11	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
12			基本資安測試(安全通訊協定)
13			基本資安測試(多租戶設計)
14			基本資安測試(系統弱點掃描)
15			基本資安測試(應用程式弱點掃描)
16			基本資安測試(防入侵機制)
17			基本資安測試(APP基本資安)
18	服務終止	服務終止	服務終止通知(Notification of Serv. Termination)
19	服務支援	雲端服務支援	支援時段(Support Hours)
20			支援方法(Support Methods)
21			支援聯絡窗口(Support Contacts)
22	治理	治理(Governance)	法規遵循(Regulation Adherence) 個資法、資安法..
23			標準遵循(Standards Adherence) ISO...
24	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)

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)
25	服務可靠性	服務韌性/容錯 (resilience/fault tolerance)	服務復原時間(Time to Service Recovery /TTSR)
26			服務韌性/容錯方法(Resiliency/Fault Tolerance)
27		客戶資料備份及回復	備份期間(Backup Interval)
28			備份資料留存期間(Retention Period)
29			備份方法(Backup Method)
30			資料備份儲存位置(Data Backup Storage Location)
31		災難復原	復原時間目標(Recovery Time Objective /RTO)
32			復原點目標(Recovery Point Objective/RPO)
33	資料管理	智慧財產權	智慧財產權(Intellectual Property Rights)
34		雲端服務客戶資料	客戶資料(Customer Data)
35			客戶資料使用(Cloud Serv Customer Data Usage)
36		雲端服務提供者資料	提供者資料(Provider Data)
37		帳戶資料	帳戶資料(Account data)
38		衍生資料	衍生資料(Derived Data)
39			衍生資料使用(Derived Data Usage)
40		資料可攜性	資料可攜能力(Data Portability Capabilities)
41		資料刪除	資料刪除時限(Data Deletion Time)
42		資料位置	資料位置政策(Data Location Policy)
43		資料檢驗	資料檢驗(Data Examination)
44		法遵請求	法遵請求(Law Enforcement Requests)
45	驗證稽核	具結、驗證及稽核	雲端服務驗證(Cloud Service Certifications)

方法1: SLO 定量目標

• 針對效能測試、安全測試等項目

AC-AC-01	可及性標準		CSC可以隨時使用任何硬體平台透過網路存取CSP的雲端運算資源。	使用任2個ISP搭配任1組硬體(手機&電腦)測試任一該雲端服務之功能，產生4張測試結果截圖，證明4種情況下皆能使用該雲端服務
PF-RT-01	最長回應時間		CSP應載明至少一個雲端服務使用情境(scenario)，該情境至少需包含： 1. 該情境之持續時間 2. 在前項之持續時間內，持續使用該雲端服務的使用者數量 3. 前項之使用者對該雲端服務進行之相同操作	CSP要給情境、最長回應時間、平均回應時間、標準差。
PF-RT-02	平均回應時間		經過該情境之持續時間後，透過統計可以得到一組關於回應時間的樣本，並存在多個統計量，CSP至少應載明： 1. 最長回應時間(Maximum Response Time) 2. 平均回應時間(Average Response Time) 3. 標準差(Standard Deviation)	例如： 情境：10個使用者在10分鐘內連續查詢清潔用品類別的商品。 最長回應時間：8秒 平均回應時間：5秒 標準差：2秒
PF-RT-03	回應時間變異		備註：從CSC端發出請求(request)到獲得CSP雲端服務的回應(response)所經過的時間，稱為回應時間(Response Time)。	

方法2: SQO 定性目標

• 檢視廠商SLA合約內容及所提供佐證資料與項目符合度

SA-CS-01	涵蓋服務		CSP應載明受測範圍之雲端服務項目清單，清單內容至少包含雲端服務名稱、版本號碼。	CSP應列出該SLA對應之一個或多個雲端服務名稱及其版本號碼。 例如： 本服務水準協議適用於 XYZ 公司所提供之下列服務 <ul style="list-style-type: none"> • XYZ 線上郵件 • XYZ BLOB 儲存
SA-SD-01	用語定義		CSP應對SLA內獨有用語或對理解該SLA特別重要之用語進行定義，且應盡可能採用產業標準所使用之定義，不應重新定義用語。	應定義該SLA獨有或對理解該SLA特別重要之用語，且應盡可能採用產業標準所使用之定義，不應重新定義用語。
SA-SM-01	監視參數		CSP應載明監視參數表列(list of Monitoring Parameters)及監視機制表列(list of Monitoring Mechanisms)，該監視參數表列是由CSP進行監視且資料提供予CSC；而監視機制表列應包含所監視參數之說明，以及所有相關條款與條件之說明。	CSP應載明CSP監視CSC哪些項目(該項目之監視資料需為CSC會收到的)，並提供對於該項目的說明，以及所有相關條款與條件之說明。
SA-SM-02	監視機制			例如： 監視參數：服務運行狀況、資源使用量等 監視機制：資源使用量達00%後即採用更低的收費標準
SA-RR-01	角色與責任		CSP得載明與受測雲端服務有關之角色表列(含CSP及CSC雙方)及該角色之責任說明。	CSP得載明CSP與CSC雙方各角色及其應負責之事項 例如：保密義務、侵權行為之法律責任、資訊安全責任等

➤ 採用專業測試工具，驗證廠商驗測內容，例壓力測試、安全性測試等

採用專業工具

為求測試效果精準，採用測試工具應為業界常用且口碑的工具為主，摘要如下：

- LoadRunner-提供壓力測試、測試腳本錄製工具、測試結果分析圖表，可同時模擬數千個使用者的上線工作量。
- WebInspect-針對Web網站進行黑箱測試，於開發中或完成上線前進行掃描作業，確保無中高風險。
- Nessus-針對主機作業系統進行黑箱測試，包括網路裝置、虛擬主機等無中高風險。

測試工具規劃

效能	壓力測試	LoadRunner
	容量測試	LoadRunner
資安	網頁弱掃	WebInspect
	系統弱掃	Nessus

雲端標(雲端特性)與實驗室測試項目對應表 (1/2)

雲端標(特性)				實驗室			
編號	執行方式	測試內容		編號	執行方式	測試內容	
CL-001	測試	1. 使用申請之使用者帳號登入系統 2. 測試申請或使用一項廠商所提供的雲端服務功能	可及性	AC-AC-01	測試	1. 使用申請之帳號測試申請或使用一項廠商所提供的雲端服務功能，確認可成功操作 2. 使用個人電腦或行動裝置透過兩個(含)以上網際網路環境(ISP)測試使用雲端服務，確認可正常連線操作。	
CL-002	測試/檢視	使用個人電腦或行動裝置透過兩個(含)以上網際網路環境(ISP)測試使用雲端服務或檢視雲端服務是否具備服務組織控制報告(SOC2)					
CL-003	測試	使用2個(含)以上不同CSC帳戶登入系統，有各自獨立之作業介面，且不同使用者間操作不會相互影響或檢視雲端服務是否具備服務組織控制報告(SOC2)	多租戶	IS-IS-03	測試	1. CSP 雲端服務是否具備多租戶管理之設計，且提供各租戶專屬頁面，請以文件佐證，例系統畫面及系統架構。 2. 使用 2 個以上不同帳號模擬不同 CSC 登入系統，有獨立作業環境或管理頁面，測試兩個帳號間，使用者操作資料不會相互影響(例如：於其中一個帳號新增一筆資料，不會影響其他用戶帳號)。	
CL-004	檢視	由廠商揭露，檢視其雲端服務架構是否具備資源彈性增減設計	靈活性速度	PF-EL-01	測試	1. 針對資源彈性調度機制，確認CSP是否具備資源彈性調度機制與數值指標之(手動調整或自動調整情境的做法說明)。 (1) 由 CSC 提出資源重新配置請求(手動調整之情境)。 (2) 由工作負荷(如 CPU、網路等)之變化觸發(自動調整之情境)。 2. 確認系統服務能力符合靈活性速度值之數值指標。	
			靈活性精確度	PF-EL-02	測試	1. 針對系統資源彈性調度之靈活性精確度，要求如下： (1) 於手動情況下，精確度係不要求量測之雲端服務技術特性(亦即無相關聯之度量)。 (2) 於自動情況下，確認 CSP 是否有資源需求量測的機制，並訂有回應資源請求之配置資源量與實際需要資源量(最佳狀態)間差異的靈活性精確度數值指標及其作法。 2. 針對使用者資源彈性變更，是否具有相關機制及能力。	
CL-005	測試	以CSC帳戶新增/異動/刪除1項廠商所提供的雲端應用服務，測試是否成功完成					
CL-006	測試	測試是否具有使用者端資源/服務度量與計費機制	監視參數	SA-SM-01	檢視	1. 確認CSP針對雲端服務，是否訂有所涵蓋服務之參數表列，請提供相關文件 佐證，例網站或文件。 2. 所涵蓋服務之參數表列，確認雲端服務水準協議，是否明確載明，CSP監視且 該資料係提供予 CSC，至少包含下列項目。 A. 是否能夠提供客戶判斷服務水準目標，是否符合合約規定之參數項目 B. 雲端應用服務具有使用者端資源/服務度量資訊參數 C. 雲端服務具有資源/服務之使用量及計費資訊參數	
			監視機制	SA-SM-02	檢視	1. 確認CSP針對雲端服務，是否訂有監視機制之作法，並具有統計及報表功能，例如日誌，其包括受監視之參數的說明，以及治理此等機制可用性之所有條款及條件的說明，監視機制項目至少包含如下。 A. 是否能夠提供客戶判斷服務水準目標，是否符合合約規定之參數項目 B. 雲端應用服務具有使用者端資源/服務度量及計費機制資訊 2. 確認CSP針對雲端服務，是否訂有監視機制之聲明，例網站、合約。	

雲端標(資安)與實驗室測試項目對應表 (2/2)

雲端標(資安)				實驗室		
編號	執行方式	測試內容		編號	執行方式	測試內容
CS-001	測試	由檢測人員端服務是否具備 TLS v1.2 以上安全通訊協定	安全通訊協定	IS-IS-02	測試	雲端服務之安全通訊協定須採 TLS1.2(含) 以上(Transport Layer Security)。
CS-002	檢視/測試	1.檢視廠商提供之一年內應用程式弱點掃描報告(掃描報告須可呈現包含 OWASP TOP10 最新版以上掃描內容選項) 2.若廠商無法提供上述檢測報告,軟體採購辦公室檢測人員將透過檢測工具 MICRO FOCUS WebInspect 針對 OWASP TOP 10 最新版進行檢測	應用程式弱點掃描	IS-IS-05	測試	CSP 應提供1年內之網頁弱點掃描報告(須使用 OWASP TOP 10 2017 或 2021 進行掃描),以證明該雲端服務無中等級(含)以上之風險;若 CSP 未提供該報告,則由實驗室進行網頁弱點掃描。
CS-003	檢視/測試	1. 檢視廠商提供之一年內系統弱點掃描報告 2. 若廠商無法提供上述檢測報告,軟體採購辦公室檢測人員將透過檢測工具 Nessus 針對系統弱點進行檢測	系統弱點掃描	IS-IS-04	測試	CSP 應提供1年內之系統弱點掃描報告(須使用 CVE 進行掃描),以證明該雲端服務無中等級(含)以上之風險;若 CSP 未提供該報告,則由實驗室進行系統弱點掃描。
CS-004	檢視	檢視廠商之佐證資料,雲端服務是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。	防入侵機制	IS-IS-06	測試	CSP 應提供 SOC 2 報告及 ISO 27001 認證。 : CSP 若無 SOC 2 報告及 ISO 27001 認證,則 CSP 之雲端服務應提供以下機制之說明並提供佐證: 1. 網路入侵防護 2. 實體入侵防護 3. 監測活動管理或防毒機制

CNS 19086 雲端檢測項目 (1/3)

➤ 領域分為IaaS, PaaS, SaaS，共83個測試項

編號	內容領域	組成項目	測試編號	服務定量/定性目標 (SLO/SQO)	測試方式	適用領域要求		
						IaaS	PaaS	SaaS
1	雲端SLA組成項目	所涵蓋雲端服務	SA-CS-01	雲端SLA-所涵蓋之雲端服務	檢視	V	V	V
2	雲端SLA組成項目	雲端SLA定義	SA-SD-01	定義SLA 獨有或對理解雲端SLA 特別重要之用語。	檢視	V	V	V
3	雲端SLA組成項目	服務監視	SA-SM-01	監視參數(Monitoring Parameters)	檢視	V	V	V
4	雲端SLA組成項目	服務監視	SA-SM-02	監視機制(Monitoring Mechanisms)	檢視	V	V	V
5	雲端SLA組成項目	角色與責任	SA-RR-01	角色及責任組成項目提供CSP 與CSC 雙方角色及責	檢視	(V)	(V)	(V)
6	可及	可及性	AC-AC-01	可及性標準(Accessibility Standards)	測試	V	V	V
7	可及	可及性	AC-AC-02	可及性政策(Accessibility Policies)	檢視	(V)	(V)	(V)
8	可用	可用性(Availability)	AV-AV-01	可用性(Availability)	檢視	V	V	V
9	服務效能	雲端服務回應時間	PF-RT-01	最長回應時間(Maximum Response Time Observation)	測試	(V)	(V)	(V)
10	服務效能	雲端服務回應時間	PF-RT-02	平均回應時間(Response Time Mean)	測試	V	V	V
11	服務效能	雲端服務回應時間	PF-RT-03	回應時間變異(Response Time Variance)	測試	(V)	(V)	(V)
12	服務效能	雲端服務容量	PF-CP-01	同時連線數之限制(Limit of Simultaneous Connections)	測試	(V)	V	V
13	服務效能	雲端服務容量	PF-CP-02	可用資源上限(Limit of Available Resources)	測試	V	V	(V)
14	服務效能	雲端服務容量	PF-CP-03	服務處理能量(Cloud Service Throughput)	測試	(V)	V	(V)
15	服務效能	雲端服務容量	PF-CP-04	雲端服務頻寬(Cloud Service Bandwidth)	檢視	(V)	(V)	(V)
16	服務效能	靈活性(Elasticity)	PF-EL-01	靈活性速度(Elasticity Speed)	測試	V	V	V
17	服務效能	靈活性(Elasticity)	PF-EL-02	靈活性精確度(Elasticity Precision)	測試	(V)	(V)	(V)
18	個資	個資保護(PII)	PI-PI-01	個資保護-相關認證檢核，如ISO 27001/ BS10012/	檢視	V	V	V
19	資訊安全	資訊安全內容領域	IS-IS-01	雲端服務資安測試、相關認證檢核	檢視	V	V	V
20	資訊安全	資訊安全內容領域	IS-IS-02	基本資安測試(安全通訊協定)	測試	V	V	V
21	資訊安全	資訊安全內容領域	IS-IS-03	基本資安測試(多租戶設計)	測試	V	V	V
22	資訊安全	資訊安全內容領域	IS-IS-04	基本資安測試(系統弱點掃描)	測試	V	V	V
23	資訊安全	資訊安全內容領域	IS-IS-05	基本資安測試(應用程式弱點掃描)	測試	V	V	V
24	資訊安全	資訊安全內容領域	IS-IS-06	基本資安測試(防入侵機制)	檢視	V	V	V
25	資訊安全	資訊安全內容領域	IS-IS-07	基本資安測試(APP基本資安)	檢視	V	V	V
26	服務終止	服務終止	ST-ST-01	資料留存期間(Data Retention Period)	檢視	(V)	(V)	(V)
27	服務終止	服務終止	ST-ST-02	日誌留存期間(Log Retention Period)	檢視	(V)	(V)	(V)

CNS 19086 雲端檢測項目 (2/3)

➤ 領域分為IaaS, PaaS, SaaS，共83個測試項

編號	內容領域	組成項目	測試編號	服務定量/定性目標 (SLO/SQO)	測試方式	適用領域要求		
						IaaS	PaaS	SaaS
28	服務終止	服務終止	ST-ST-03	服務終止通知(Notification of Serv. Termination)	檢視	V	V	V
29	服務終止	服務終止	ST-ST-04	資產歸還(Return of Assets)	檢視	(V)	(V)	(V)
30	服務支援	雲端服務支援	SP-SP-01	支援時段(Support Hours)	檢視	V	V	V
31	服務支援	雲端服務支援	SP-SP-02	服務事故支援時段(Service Incident Support Hours)	檢視	(V)	(V)	(V)
32	服務支援	雲端服務支援	SP-SP-03	服務事故通知時限(Incident Notification Time)	檢視	(V)	(V)	(V)
33	服務支援	雲端服務支援	SP-SP-04	首次支援回應時限(Max First Support Resp.Time)	檢視	(V)	(V)	(V)
34	服務支援	雲端服務支援	SP-SP-05	事故解決最大時限(Maximum Incident Resolution Time)	檢視	(V)	(V)	(V)
35	服務支援	雲端服務支援	SP-SP-06	支援計畫(Support Plans)	檢視	(V)	(V)	(V)
36	服務支援	雲端服務支援	SP-SP-07	支援方法(Support Methods)	檢視	V	V	V
37	服務支援	雲端服務支援	SP-SP-08	支援聯絡窗口(Support Contacts)	檢視	V	V	V
38	服務支援	雲端服務支援	SP-SP-09	服務事故報告(Service Incident Reporting)	檢視	(V)	(V)	(V)
39	服務支援	雲端服務支援	SP-SP-10	服務事故通知(Service Incident Notification)	檢視	(V)	(V)	(V)
40	治理	治理(Governance)	GV-GV-01	法規遵循Regulation Adherence)	檢視	V	V	V
41	治理	治理(Governance)	GV-GV-02	標準遵循(Standards Adherence)	檢視	V	V	V
42	治理	治理(Governance)	GV-GV-03	政策遵循(Policy adherence)	檢視	(V)	(V)	(V)
43	治理	治理(Governance)	GV-GV-04	稽核時程(Audit Schedule)	檢視	(V)	(V)	(V)
44	變更管理	雲端服務特性及功能變更	CM-CM-01	服務變更通知期限(Minimum Notification Period)	檢視	V	V	V
45	變更管理	雲端服務特性及功能變更	CM-CM-02	特性/功能下架前最短服務時間(Function Deprecation Notice Period)	檢視	(V)	(V)	(V)
46	變更管理	雲端服務特性及功能變更	CM-CM-03	服務變更通知方法(Change Notification Method)	檢視	(V)	(V)	(V)
47	服務可靠性	服務韌性/容錯	RL-FT-01	服務復原時間(Time to Service Recovery /TTSR)	檢視	V	V	V
48	服務可靠性	服務韌性/容錯	RL-FT-02	服務復原平均時間(Mean Time to Service Recovery)	檢視	(V)	(V)	(V)
49	服務可靠性	服務韌性/容錯	RL-FT-03	服務復原最長時間(MaxTime to Serv Recovery MTTR)	檢視	(V)	(V)	(V)
50	服務可靠性	服務韌性/容錯	RL-FT-04	服務失效次數(Number of Service Failures)	檢視	(V)	(V)	(V)
51	服務可靠性	服務韌性/容錯	RL-FT-05	服務韌性/容錯方法(Resiliency/Fault Tolerance)	檢視	V	V	V
52	服務可靠性	客戶資料備份及回復	RL-BK-01	備份期間(Backup Interval)	檢視	V	V	V
53	服務可靠性	客戶資料備份及回復	RL-BK-02	備份資料留存期間(Retention Period)	檢視	V	V	V
54	服務可靠性	客戶資料備份及回復	RL-BK-03	備份版本數(Number of Backup Generations)	檢視	(V)	(V)	(V)

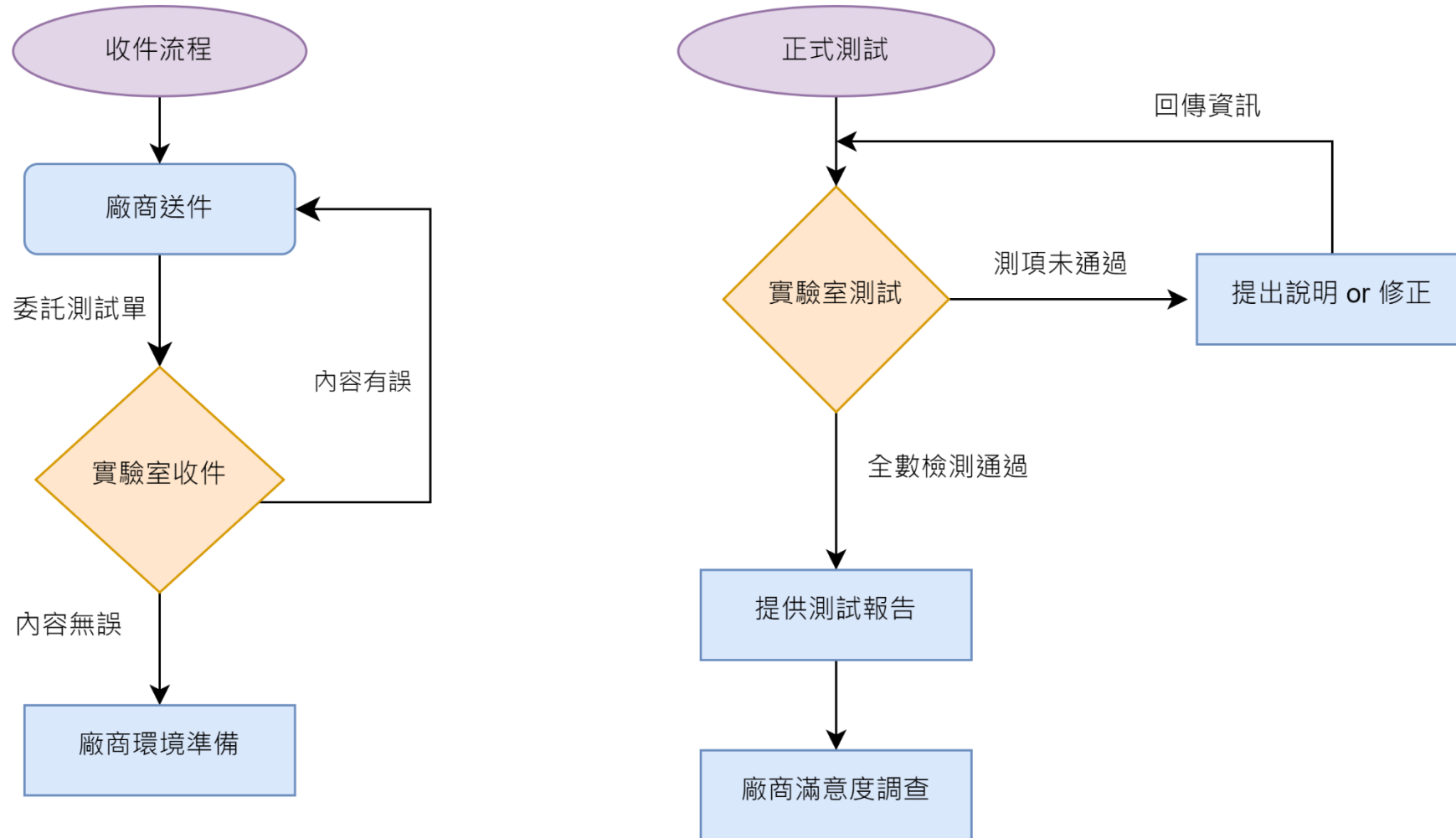
CNS 19086 雲端檢測項目 (3/3)

➤ 領域分為IaaS, PaaS, SaaS，共83個測試項

編號	內容領域	組成項目	測試編號	服務定量/定性目標 (SLO/SQO)	測試方式	適用領域要求		
						IaaS	PaaS	SaaS
55	服務可靠性	客戶資料備份及回復	RL-BK-04	備份回復測試(Backup Restoration Testing)	檢視	(V)	(V)	(V)
56	服務可靠性	客戶資料備份及回復	RL-BK-05	備份方法(Backup Method)	檢視	V	V	V
57	服務可靠性	客戶資料備份及回復	RL-BK-06	備份查證(Backup Verification)	檢視	(V)	(V)	(V)
58	服務可靠性	客戶資料備份及回復	RL-BK-07	備份回復測試報告(Restoration Test Reporting)	檢視	(V)	(V)	(V)
59	服務可靠性	客戶資料備份及回復	RL-BK-08	資料回復替代方案(Alt. methods for Data Recovery)	檢視	(V)	(V)	(V)
60	服務可靠性	客戶資料備份及回復	RL-BK-09	資料備份儲存位置(Data Backup Storage Location)	檢視	V	V	V
61	服務可靠性	災難復原	RL-DR-01	復原時間目標(Recovery Time Objective /RTO)	檢視	V	V	V
62	服務可靠性	災難復原	RL-DR-02	復原點目標(Recovery Point Objective/RPO)	檢視	V	V	V
63	服務可靠性	災難復原	RL-DR-03	服務提供者災難復原計畫(Disaster Recovery Plan)	檢視	(V)	(V)	(V)
64	資料管理	智慧財產權	DM-IP-01	智慧財產權(Intellectual Property Rights)	檢視	V	V	V
65	資料管理	雲端服務客戶資料	DM-CD-01	客戶資料(Customer Data)	檢視	V	V	V
66	資料管理	雲端服務客戶資料	DM-CD-02	客戶資料使用(Cloud Serv Customer Data Usage)	檢視	V	V	V
67	資料管理	雲端服務提供者資料	DM-PD-01	提供者資料(Provider Data)	檢視	V	V	V
68	資料管理	帳戶資料	DM-AD-01	帳戶資料(Account data)	檢視	V	V	V
69	資料管理	衍生資料	DM-DR-01	衍生資料(Derived Data)	檢視	V	V	V
70	資料管理	衍生資料	DM-DR-02	衍生資料使用(Derived Data Usage)	檢視	V	V	V
71	資料管理	衍生資料	DM-DR-03	衍生資料存取(Derived Data Access)	檢視	(V)	(V)	(V)
72	資料管理	資料可攜性	DM-DP-01	資料可攜能力(Data Portability Capabilities)	檢視	V	V	V
73	資料管理	資料刪除	DM-DD-01	資料刪除時限(Data Deletion Time)	檢視	V	V	V
74	資料管理	資料刪除	DM-DD-02	資料刪除流程(Data Deletion Process)	檢視	(V)	(V)	(V)
75	資料管理	資料刪除	DM-DD-03	資料刪除通知(Data Deletion Notification)	檢視	(V)	(V)	(V)
76	資料管理	資料位置	DM-DL-01	資料位置(Data Location)	檢視	(V)	(V)	(V)
77	資料管理	資料位置	DM-DL-02	資料位置規定能力(Location Spec. Capability)	檢視	(V)	(V)	(V)
78	資料管理	資料位置	DM-DL-03	資料位置政策(Data Location Policy)	檢視	V	V	V
79	資料管理	資料檢驗	DM-DE-01	資料檢驗(Data Examination)	檢視	V	V	V
80	資料管理	法遵請求	DM-LE-01	法遵請求(Law Enforcement Requests)	檢視	V	V	V
81	驗證稽核	具結、驗證及稽核	CA-CA-01	雲端服務具結(Cloud Service Attestations)	檢視	(V)	(V)	(V)

工作項目	工作內容	需要時程
1.啟動會議	<ul style="list-style-type: none"> ●邀請公司高階長官出席，說明CNS19086驗測表內容及驗測個案 ●初步篩選是否具有雲端服務SLA關鍵要素 ●討論驗測配合事項，如驗測腳本及環境 	半天
1.1.廠商受測環境整備	●受測廠商依據測試個案準備受測系統，由本實驗室先行錄製驗測腳本，以利驗測	視廠商時程(含實驗室進行測試腳本錄製1天)
2.驗測會議 -進行驗測	依據驗測表進行驗測，包含檢視及驗測2大項 <ul style="list-style-type: none"> ●本實驗室於執行驗測個案，請廠商現地配合驗測，以利排除驗測時所發生之例外狀況立即改善必免中斷驗測 ●本實驗室執行驗測表中檢視項目驗測，並取得佐證資料，予以記錄 	2~3天(需視廠商配合狀況)
2.1驗測會議 -初測結果說明	<ul style="list-style-type: none"> ●本實驗室針對初步初測結果向廠商說明，進行討論或確認是否為誤判 ●廠商依據結果，視廠商需求是否“複測”，本實驗室提供複測1次(限1個月內使用) 	<ul style="list-style-type: none"> ■ 初測結果說明半天 ■ 若，廠商擬修正進行複測，其時程，依廠商作業時程
3.結案會議 -驗測結果說明	●邀請公司高階長官出席，最終報告說明，針對驗測數據進行結果分析，所找出問題或瓶頸，進行討論或改善建議	半天(另含平台彙整報告3天)

CNS19086 檢測流程



CNS19086 廠商配合事項與時程

作業階段	廠商進行作業	實驗室進行作業	時程
1. 廠商送件	<ul style="list-style-type: none"> ➤ 準備受測雲端服務SLA合約及服務版本。 ➤ 確認受測SLA項目(IaaS、PaaS、SaaS)必要及選測項目 	<ul style="list-style-type: none"> ➤ 檢視送件雲端服務版本及SLA合約符合性 ➤ 確認受測項目(必要與選測) 	1-2週
2. 廠商環境準備	<ul style="list-style-type: none"> ➤ 檢視項目準備相關佐證資料 ➤ 測試項目如採實驗室進行測試,準備相關測試環境如效能測試及資安測試環境,環境設定及準備 	<ul style="list-style-type: none"> ➤ 檢視項目:確認檢測項目是否都有提供佐證資料或需廠商補充說明 ➤ 測試項目:進行受測環境確認,確認環境可進行測試 	1-2週
3. 測試進行階段	<ul style="list-style-type: none"> ➤ 檢視項目:測訂期間如測人員對SLA定義如有疑問或不名地方提供協助解釋說明,以達成雙方共識·避免誤判。 ➤ 測試項目:進行測試如因環境因素導致無法進行測試,協助排除問題 	<ul style="list-style-type: none"> ➤ 檢視項目:依據受測項目逐項檢視佐證資料及說明,如有不符合或佐證資料不足之處,與受測方說明及確認資料、補充或修正佐證資料 ➤ 測試項目:以工具進行測試、初測提供受測方測試結果與數據、如受測方對結果或數據有進行修正,進行複測結果確認。 	4週

附件1：廠商配合提供之項目

- SLA
- SLA各服務之程式版本截圖及/或佐證文件
- SLA對應表（測試編號與SLA頁數對應表）
- 可用資源最大容量之佐證、最大對外頻寬之佐證，如磁碟空間：50TB／記憶體：32GB、最大對外網路頻寬：500Mbps
- 相關(證書)佐證，如ISO 27001、ISO 27701、ISO 27018、ISO 27017
- 請提供2組測試帳號密碼
- 請提供壓力測試情境，如10個使用者在10分鐘內連續查詢清潔用品類別的商品，最長回應時間：8秒、平均回應時間：5秒、標準差：2秒
- 請提供可進行壓測時段，如5/1~5/10號可進行壓力測試
- 請提供設定之資源彈性調度，並提供相關佐證
如本雲端服務同時具有手動調整及自動調整之功能
 1. 手動調整時：系統將在10分鐘內自動調整資源
 2. 自動調整時：系統將在5分鐘內自動調整資源
- 災難復原計畫
- 資安風險掃描佐證資料，須使用OWASP TOP 10 2017或2021進行掃描
- 資安掃描IP是否須設定白名單
- 可掃描之時段，如5/1~5/10號可進行資安掃描

附件2：廠商委託申請單

- 廠商名稱
- 雲端服務名稱
- 聯絡人
- 雲端服務URL
- 電話
- 雲端服務版本
- 手機
- 顧客需求
- email
- 選測項目
- 受測SLA名稱(檔名)
- 領域