時間	議程
13:30~14:00	報到
14:00~14:30	國家標準ISO / CNS 19086議題交流
14:30~15:00	雲端服務公開徵求議題交流
15:00~16:00	綜合討論

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

國家標準CNS19086介紹說明

數位發展部 數位產業署

2022 年 10 月 26 日

大　綱

一.介紹CNS 19086

二.測試規範技術說明

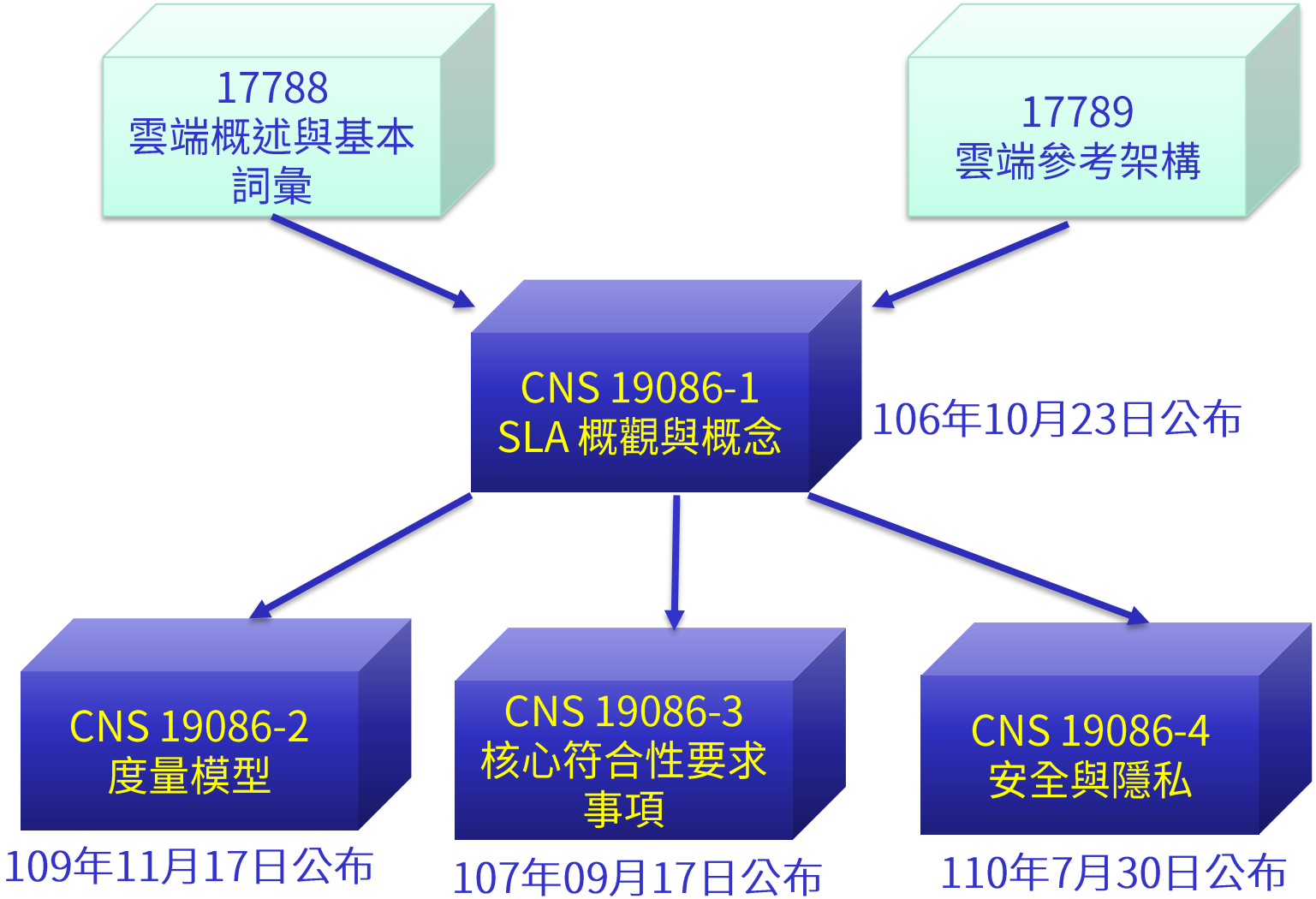
三.CNS 19086於共契後續推動時程

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，且需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促成公告。

CNS 19086 標準架構與制定進度



CNS 19086 四部簡介

- 19086-1是概觀及概念(Overview and concepts)，提供雲端SLA 框架概觀、基本概念及定義標準
- 19086-2是度量模型(Metric model)，提供度量模型用以建立供雲端服務水準目標(Cloud Service Level Objective, SLO)使用之度量項目
- 19086-3是要求事項(Requirements)，提供核心符合性要求事項，這些要求事項衍生自ISO/IEC 19086-1 所定義之SLO 與雲端服務定性目標(Cloud Service Qualitative Objective, SQO)
- 19086-4是資訊安全與個人可識別資訊保護之組成項目(Components of security and of protection of PII)，包含進行雲端服務委外時，擬定合約內容時資訊安全與個資保護之注意事項。

CNS 19086之認驗證制度期程

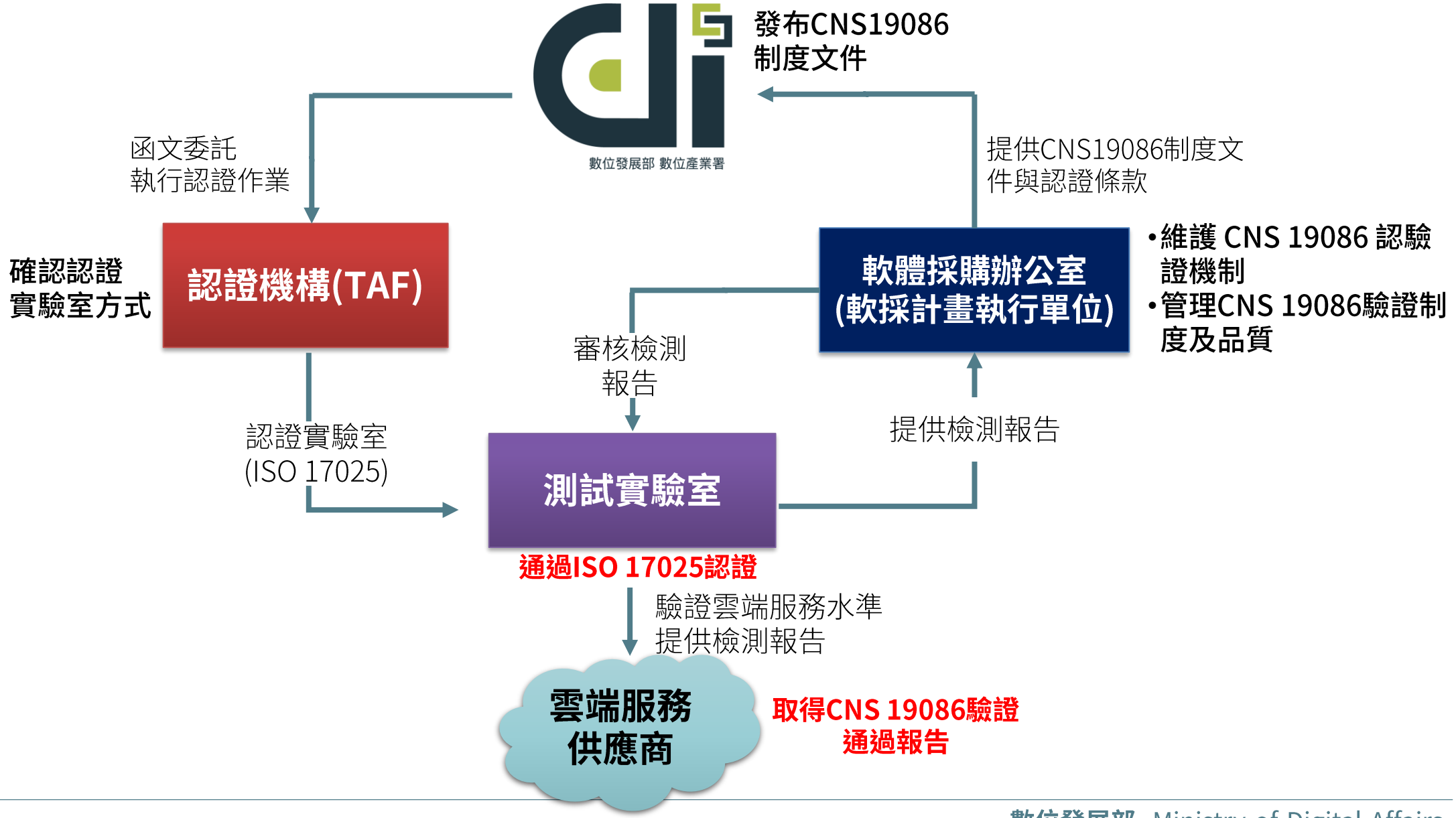
協助政府建立法規，透過認/驗證機制建構維持產業秩序

- 推動CNS 19086認驗證制度，透過共同供應契約採購將雲端業者帶入政府市場，以推動雲端業者積極取得驗證合格證明

- 與全國認證基金會(TAF)達成共識，TAF已於3月成立工作小組及啟動相關會議及教育訓練
- 由軟體採購辦公室提出「雲端服務水準驗測推動制度」、「雲端服務水準驗測規範」、「雲端服務水準驗測基準」三項認驗證機制規範文件，作為雲端服務水準認驗證機制基礎架構

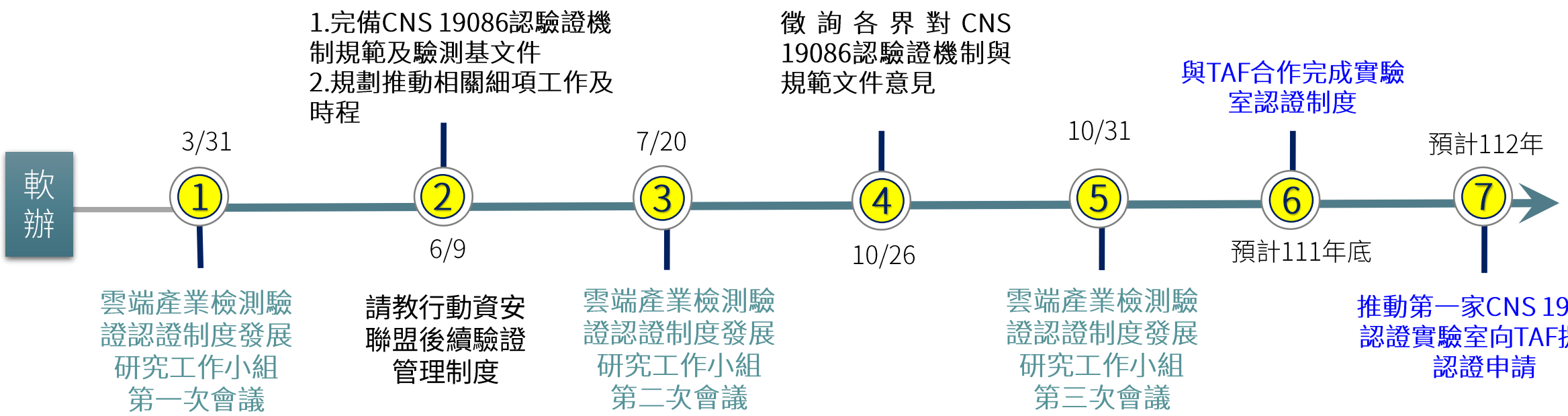
- 自106年依循ISO國際標準組織發布「ISO/IEC 19086雲端服務水準協議框架系列之國際標準」內容轉換制訂國家標準CNS 10986
- 與全國認證基金會(TAF)多次溝通後續CNS 19086之認驗證推動可行性
- 110年訪談未來有機會參與之驗證單位及業者對於CNS 19086之意見搜集

CNS 19086 認驗證架構



CNS 19086推動時程(1/2)

- 與財團法人全國認證基金會(TAF)合作召開3場專家委員工作小組會議，完成CNS 19086之：
  - 第三方實驗室認證管理制度
  - 第三方實驗室測試規範及測試基準



大　綱

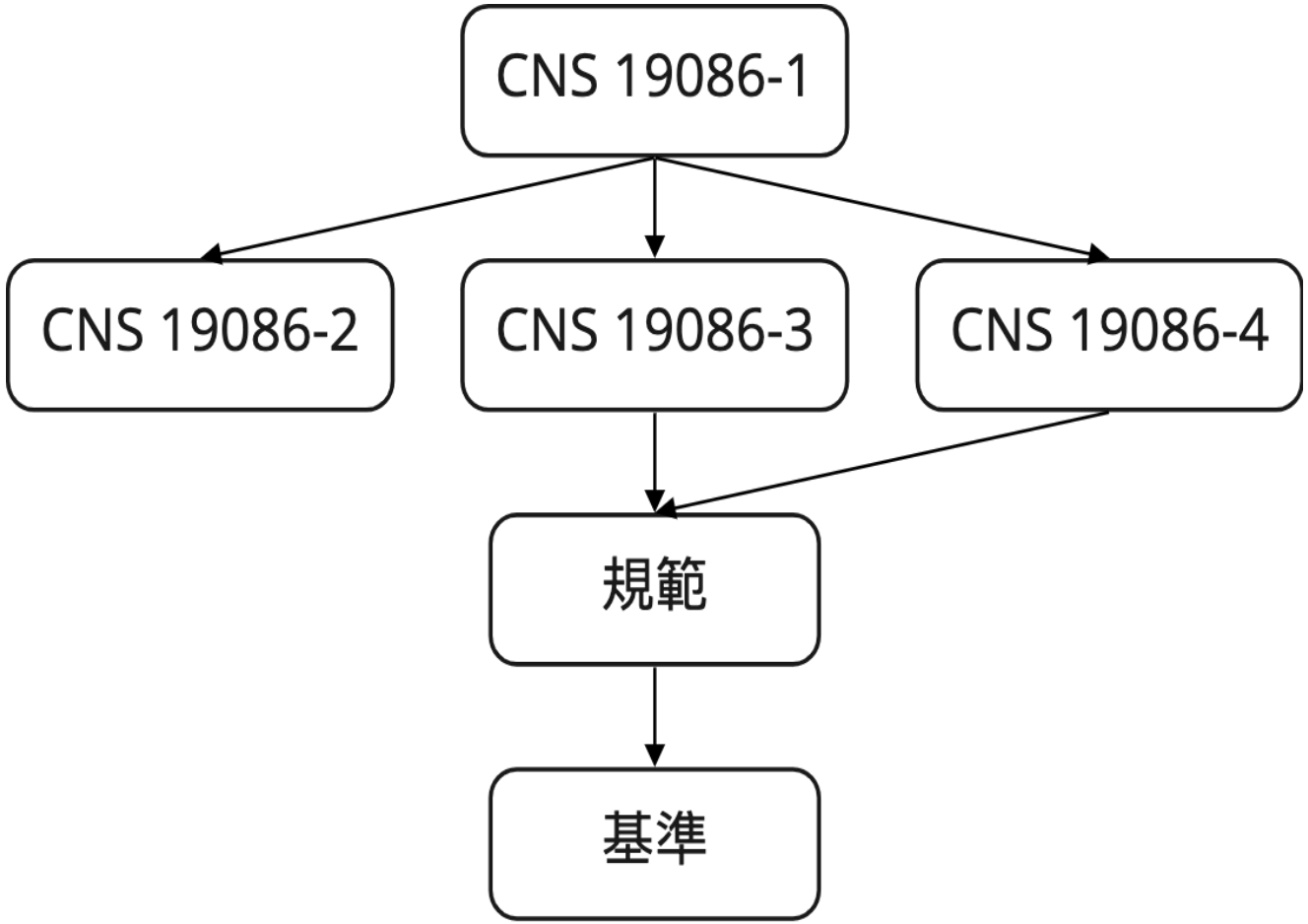
一.介紹CNS 19086

二.測試規範技術說明

三.CNS 19086於共契後續推動時程

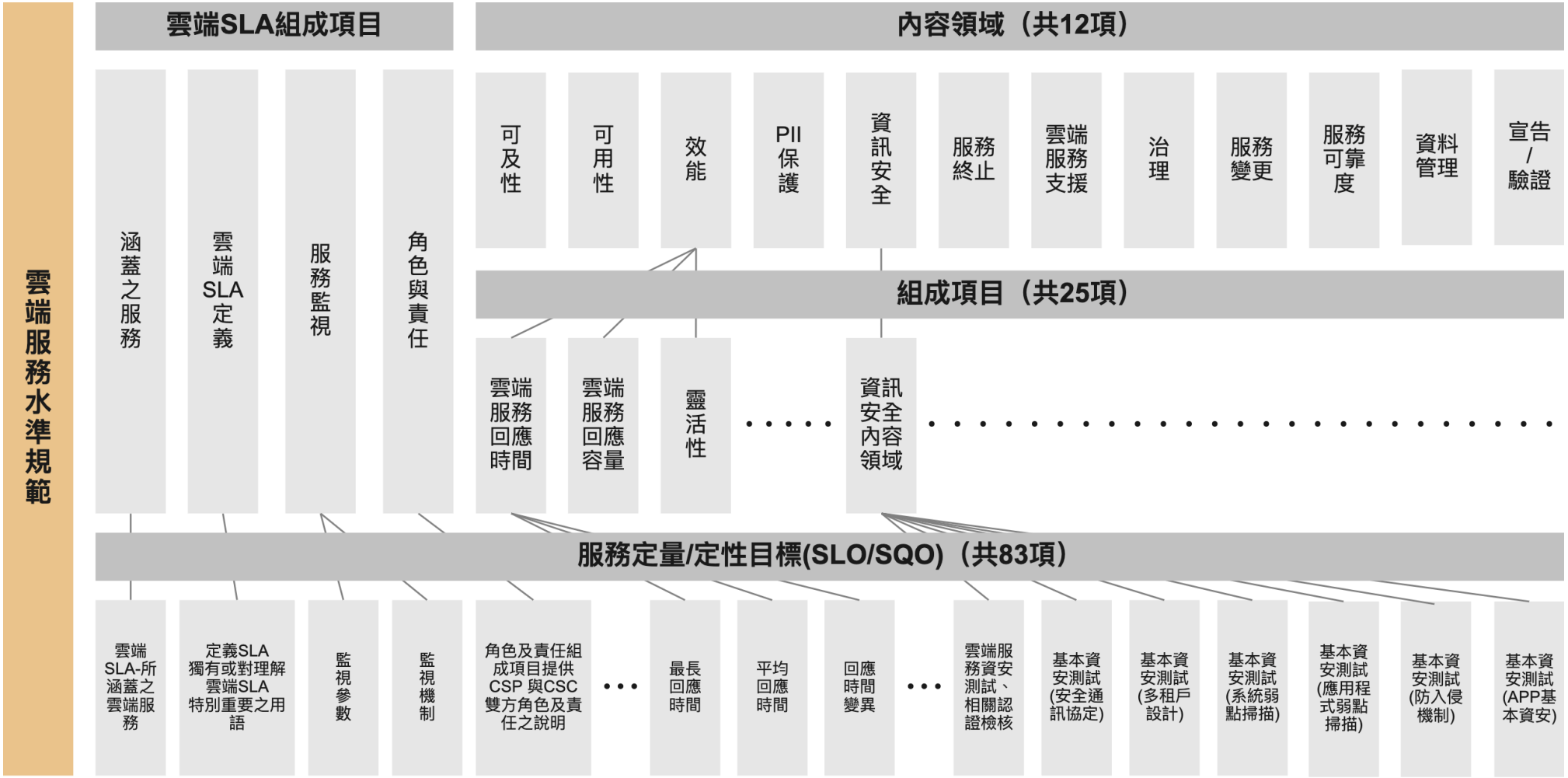
測試規範技術說明

- 驗測規範項目設計係依據CNS 19086-1、-3及-4，其100%涵蓋CNS 19086所有條款要求(參考附錄二)



測試規範項目說明

- 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：



測試規範的技術內容介紹(3/3)

- 各雲端服務領域之必測原則說明：
  - 雲端服務水準測試規範之領域分為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
    - 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

測試規範所有項目內容(1/4)

- 雲端服務水準測試規範之所有目標、項目與適用領域共83項如下圖

編號	領域	組成項目	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	雲端SLA-所涵蓋之雲端服務	檢視	V	V	V
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。	檢視	V	V	V
3		服務監視	監視參數(Monitoring Parameters)	檢視	V	V	V
4			監視機制(Monitoring Mechanisms)	檢視	V	V	V
5		角色與責任	角色及責任組成項目提供CSP 與CSC 雙方角色及責任之說明	檢視	(V)	(V)	(V)
6	可及	可及性	可及性標準(Accessibility Standards)	測試	V	V	V
7		可及性	可及性政策(Accessibility Policies)	檢視	(V)	(V)	(V)
8	可用	可用性(Availability)	可用性(Availability)	檢視	V	V	V
9	服務效能	雲端服務回應時間	最長回應時間(Maximum Response Time Observation)	測試	(V)	(V)	(V)
10			平均回應時間(Response Time Mean)	測試	V	V	V
11			回應時間變異(Response Time Variance)	測試	(V)	(V)	(V)
12		雲端服務容量	同時連線數之限制(Limit of Simultaneous Connections)	測試	(V)	V	V
13			可用資源上限(Limit of Available Resources)	測試	V	V	(V)
14			服務處理能量(Cloud Service Throughput)	測試	(V)	V	(V)
15			雲端服務頻寬(Cloud Service Bandwidth)	測試	(V)	(V)	(V)
16		靈活性(Elasticity)	靈活性速度(Elasticity Speed)	測試	V	V	V
17			靈活性精確度(Elasticity Precision)	測試	(V)	(V)	(V)
18	個資	個資保護(PII)	個資保護-相關認證檢核	檢視	V	V	V
19	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	檢視	V	V	V
20			基本資安測試(安全通訊協定)	測試	V	V	V

測試規範所有項目內容(2/4)

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)	測試方式	適用領域要求		
					IaaS	PaaS	SaaS
21	資訊安全	資訊安全內容領域	基本資安測試(多租戶設計)	測試	V	V	V
22			基本資安測試(系統弱點掃描)	測試	V	V	V
23			基本資安測試(應用程式弱點掃描)	測試	V	V	V
24			基本資安測試(防入侵機制)	檢視	V	V	V
25			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	資料留存期間(Data Retention Period)	檢視	(V)	(V)	(V)
27			日誌留存期間(Log Retention Period)	檢視	(V)	(V)	(V)
28			服務終止通知(Notification of Serv. Termination)	檢視	V	V	V
29			資產歸還(Return of Assets)	檢視	(V)	(V)	(V)
30	服務支援	雲端服務支援	支援時段(Support Hours)	檢視	V	V	V
31			服務事故支援時段(Service Incident Support Hours)	檢視	(V)	(V)	(V)
32			服務事故通知時限(Incident Notification Time)	檢視	(V)	(V)	(V)
33			首次支援回應時限(Max First Support Resp.Time)	檢視	(V)	(V)	(V)
34			事故解決最大時限(Maximum Incident Resolution Time)	檢視	(V)	(V)	(V)
35			支援計畫(Support Plans)	檢視	(V)	(V)	(V)
36			支援方法(Support Methods)	檢視	V	V	V
37			支援聯絡窗口(Support Contacts)	檢視	V	V	V
38			服務事故報告(Service Incident Reporting)	檢視	(V)	(V)	(V)
39			服務事故通知(Service Incident Notification)	檢視	(V)	(V)	(V)
40	治理	治理(Governance)	法規遵循Regulation Adherence)	檢視	V	V	V
41			標準遵循(Standards Adherence)	檢視	V	V	V
42			政策遵循(Policy adherence)	檢視	(V)	(V)	(V)
43			稽核時程(Audit Schedule)	檢視	(V)	(V)	(V)

測試規範所有項目內容(3/4)

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)	測試方式	適用領域要求		
					IaaS	PaaS	SaaS
44	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)	檢視	V	V	V
45			特性/功能下架前最短服務時間(Function Deprecation)	檢視	(V)	(V)	(V)
46			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 (resilience /fault tolerance)	服務復原時間(Time to Service Recovery /TTSR)	檢視	V	V	V
48			服務復原平均時間(Mean Time to Service Recovery)	檢視	(V)	(V)	(V)
49			服務復原最長時間(MaxTime to Serv Recovery MTTSR)	檢視	(V)	(V)	(V)
50			服務失效次數(Number of Service Failures)	檢視	(V)	(V)	(V)
51			服務韌性/容錯方法(Resiliency/Fault Tolerance)	檢視	V	V	V
52		客戶資料備份及回復	備份期間(Backup Interval)	檢視	V	V	V
53			備份資料留存期間(Retention Period)	檢視	V	V	V
54			備份版本數(Number of Backup Generations)	檢視	(V)	(V)	(V)
55			備份回復測試(Backup Restoration Testing)	檢視	(V)	(V)	(V)
56			備份方法(Backup Method)	檢視	V	V	V
57			備份查證(Backup Verification)	檢視	(V)	(V)	(V)
58			備份回復測試報告(Restoration Test Reporting)	檢視	(V)	(V)	(V)
59			資料回復替代方案(Alt. methods for Data Recovery)	檢視	(V)	(V)	(V)
60			資料備份儲存位置(Data Backup Storage Location)	檢視	V	V	V
61		災難復原	復原時間目標(Recovery Time Objective /RTO)	檢視	V	V	V
62			復原點目標(Recovery Point Objective/RPO)	檢視	V	V	V
63			服務提供者災難復原計畫(Disaster Recovery Plan)	檢視	(V)	(V)	(V)

測試規範所有項目內容(4/4)

編號	領域	組成項目	服務定量/定性目標 (SLO/SQO)	測試方式	適用領域要求		
					IaaS	PaaS	SaaS
64	資料管理	智慧財產權	智慧財產權(Intellectual Property Rights)	檢視	V	V	V
65		雲端服務客戶資料	客戶資料(Customer Data)	檢視	V	V	V
66			客戶資料使用(Cloud Serv Customer Data Usage)	檢視	V	V	V
67		雲端服務提供者資料	提供者資料(Provider Data)	檢視	V	V	V
68		帳戶資料	帳戶資料(Account data)	檢視	V	V	V
69		衍生資料	衍生資料(Derived Data)	檢視	V	V	V
70			衍生資料使用(Derived Data Usage)	檢視	V	V	V
71			衍生資料存取(Derived Data Access)	檢視	(V)	(V)	(V)
72		資料可攜性	資料可攜能力(Data Portability Capabilities)	檢視	V	V	V
73		資料刪除	資料刪除時限(Data Deletion Time)	檢視	V	V	V
74			資料刪除流程(Data Deletion Process)	檢視	(V)	(V)	(V)
75			資料刪除通知(Data Deletion Notification)	檢視	(V)	(V)	(V)
76		資料位置	資料位置(Data Location)	檢視	(V)	(V)	(V)
77			資料位置規定能力(Location Spec. Capability)	檢視	(V)	(V)	(V)
78			資料位置政策(Data Location Policy)	檢視	V	V	V
79		資料檢驗	資料檢驗(Data Examination)	檢視	V	V	V
80		法遵請求	法遵請求(Law Enforcement Requests)	檢視	V	V	V
81	驗證稽核	具結、驗證及稽核	雲端服務具結(Cloud Service Attestations)	檢視	(V)	(V)	(V)
82			雲端服務驗證(Cloud Service Certifications)	檢視	V	V	V
83			雲端服務稽核(Cloud Service Audits)	檢視	(V)	(V)	(V)

大　綱

一.介紹CNS 19086

二.測試規範技術說明

三.CNS 19086於共契後續推動時程

雲端特性檢測

雲端特性	檢測編號	檢測指標	檢測步驟
隨需自助服務 (On–demand Self-Service)	CL-001	具備賦予CSC 隨時隨需採取行動之能力	1.使用申請之使用者帳號登入系統 2.測試使用1項廠商所提供的雲端服務功能
多元網絡存取 (Broad Network Access)	CL-002	CSC 只要可存取網路，即可存取實體或虛擬資源	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)
多人共享資源池 (Resource Pooling)	CL-003	雲端服務提供者能支援多租用，藉以服務1或多個CSC	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)
快速且彈性佈署 (Rapid Elasticity)	CL-004	實體及虛擬資源能彈性增減資源	檢視雲端服務架構是否具備資源彈性增減設計
	CL-005	具有CSC資源彈性變更功能	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
服務可量測(Measured Service)	CL-006	具備區分使用者資源/服務度量與計費機制	雲端應用服務具有使用者端資源/服務度量與計費機制

註：採購規定，以公告文件為主

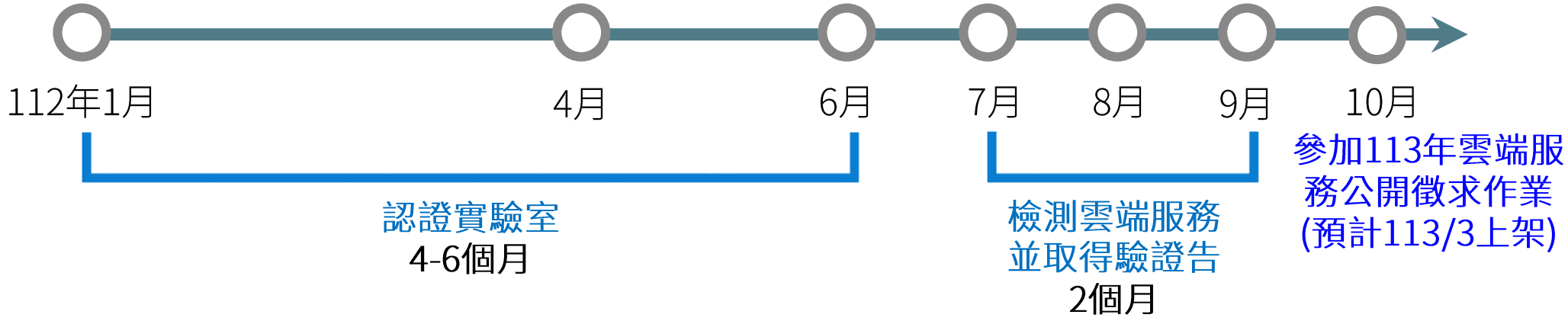
基本資安檢測

檢測編號	檢測指標	檢測項目
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	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
CS-002	OWASP TOP10 最新版應用程式弱點掃描	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 TOP 10 2017以上掃描內容選項)，需無中、高等級以上風險 2. 若廠商無法提供上述檢測報告，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，檢測結果無中、高等級以上風險
CS-003	系統弱點掃描	1.檢視廠商提供之3個月內第三方系統弱點掃描報告 2.檢測人員透過檢測工具Nessus針對系統弱點進行檢測
CS-004	雲端服務需有相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制。	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。
CS-005	若雲端服務包含APP產品，需通過「行動應用APP基本資安檢測實驗室」檢測之合格證書文件或國際獨立認驗證機構之APP資安檢測證明，APP通過檢測之版本應與參與投標之版本相符。	檢視廠商參與投標雲端服務之APP是否通過「行動應用APP基本資安檢測實驗室」檢測之合格證書文件或國際獨立認驗證機構之APP資安檢測證明，並比對APP通過檢測之版本應與參與投標之版本相符。

註：採購規定，以公告文件為主

CNS 19086於共契後續推動時程

- 經TAF公告測試實驗室認證流程，即可接收實驗室提出申請：
  - 視測試實驗室申請情況，TAF認證時程約4-6個月
  - 測試實驗室依測試規範及測試基準，針對雲端供應商驗證雲端服務，測試(初測+複測)及測試報告審查時程約2個月
  - 112年10月開始進行雲端服務公開徵求作業，以做113年4月雲端服務上架共契



報告完畢　敬請指教