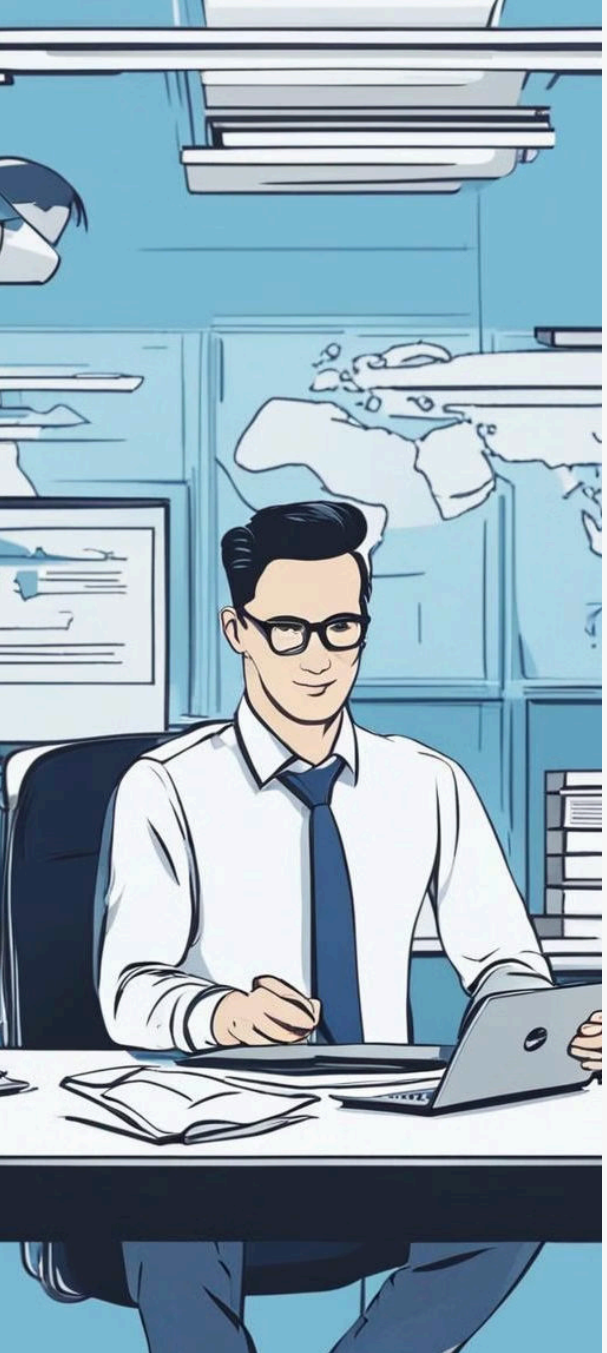


中華電信學院 資通安全講座

政府資訊作業委外安全管理

亞洲大學 陳偉嵩 博士

講師介紹

陳偉嵩，亞洲大學資訊工程博士

現職/亞洲大學資訊發展處擔任技正/組長

資訊專長/網路系統規畫建置和資料中心規劃建置

其他/各級機關內部稽核作業、舉辦資安講座及教育訓練

證照

ISO 27001、ISO 27701:2019、ISO 29100:2011

BS 10012:2017、ITE 網路通訊專業人員、乙級電腦硬體技術士

資安相關經歷

行政院資通安全稽核團隊稽核委員

教育部資安稽核團隊稽核委員

教育部國教署資安輔導團委員

教育機構資安驗證中心主導稽核員

衛生福利部資安稽核團隊稽核委員

國家文官學院講座

教育體系資安職能證照課程講師

相關規範與文件

- 政府資訊服務採購作業指引(1120925)
- 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(1120925)
- 資通安全管理法及六大子法
- 資通系統籌獲各階段資安強化措施
- 資訊服務採購契約範本

資通安全管理法及六大子法

資通安全責任等級分級辦法附表9 資通系統防護需求分級原則

資通安全責任等級分級辦法附表9涵蓋了資通系統防護需求的分級原則，包括機密性、完整性、可用性和法律遵循性。

資通系統分級原則、核心與非核心資通系統定義

資通安全責任等級分級辦法附表10 資通系統防護基準

確認資通系統各等級之防護基準原則

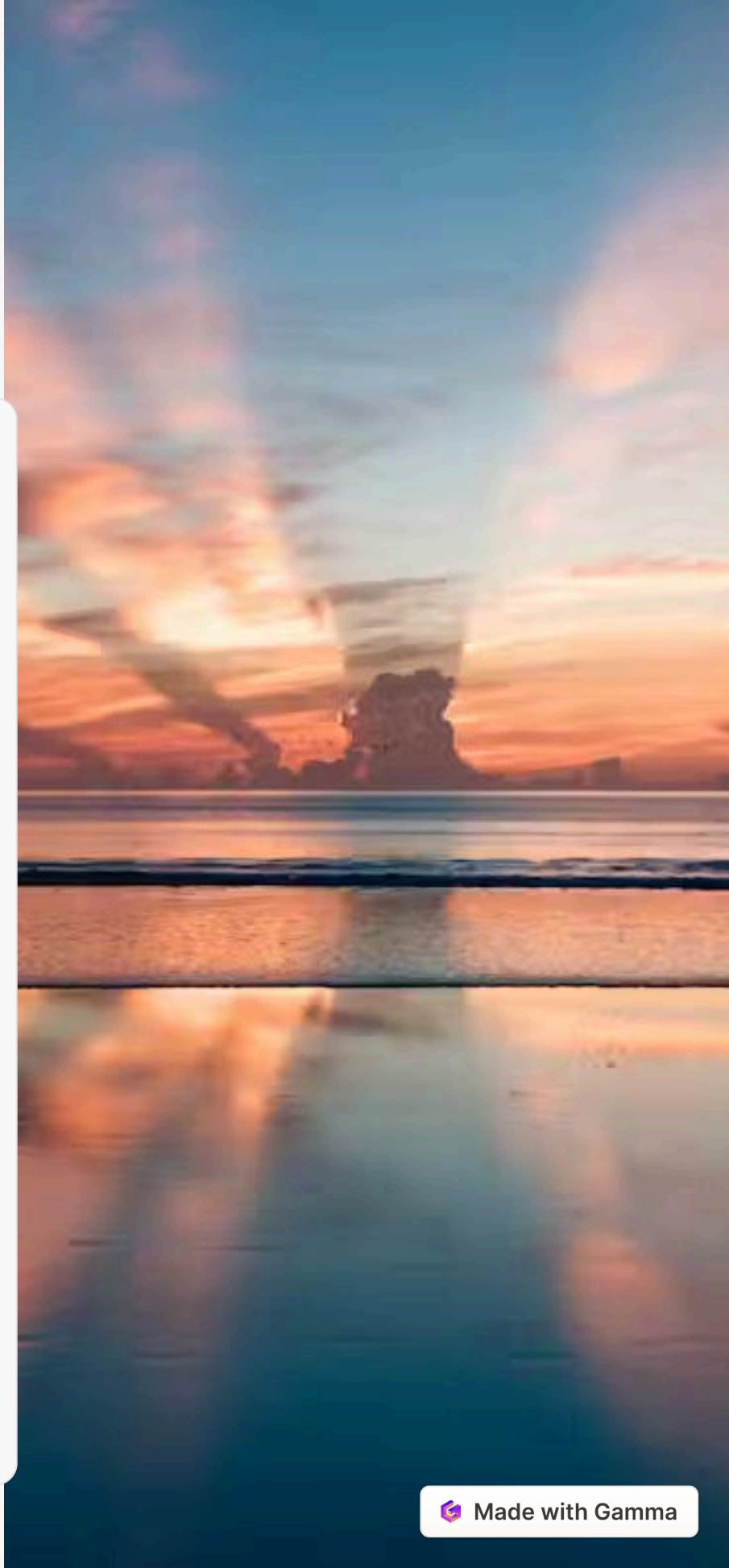
系統開發過程自規劃、設計、執行、維運均應參照SSDLC落實資安要求，並留存紀錄以確保資安要求的落實。

資通系統防護基準

資通系統防護基準是確保資通系統安全的重要標準，規範各等級資通系統之資安要求。

Google Docs

附表十資通系統防護基準.pdf



資通系統籌獲各階段資安強化措施

需求階段

系統防護需求等級標註(普、中、高)

資安作業經費5%

受託者資安作業應納入評選項目10%

資安評選委員至少一位

建置階段

核心資通系統則應聘請外部資安專家協助檢視資安管理作為

核心資通系統且委託金額達1千萬元以上，應評估獨立驗證與認證(IV&V)

維運階段

請資安人員二線協助確認系統維運之資安作業

應對高防護等級之資通系統廠商辦理資安稽核

受託業務發生重大資安事件，機關應辦理廠商資安稽核，並將結果送交主管機關

共通性資通安全基本要求參考

雲端微服務（SaaS）套裝型

雲端微服務（SaaS）辦公室生產力工具

既有雲端微服務（SaaS）客製化需求更版

雲端平台(PaaS或IaaS)

資訊系統規劃服務

資訊安全類規劃服務

應用軟體或系統開發服務

既有系統功能後續擴充

應用軟體或系統維運服務

資訊服務採購契約範本

資訊服務採購契約範本

投標須知範本

請參考資訊服務採購契約範本(含投標須知範本)之資安檢核事項

政府資訊服務採購作業指引

1 預算編列

精確評估所需資金和資源，以確保符合預算要求。

2 廠商資格

確保潛在廠商符合標準和資格，符合採購需求。

3 需求文件

編制清晰明確的需求檔案，以明確說明所需的服務和產品。

4 招、決標作業

透明公平的招標和決標程序，確保最佳選擇。

5 契約執行

執行過程中確保合約中的條款和條件得到遵守和履行。

6 爭議處理

有效處理任何爭議，以確保公平公正和有效的解決。

7 服務等級協議(SLA)

確定和訂立明確的服務等級協議，以確保服務質量。

預算編列

按比例編列資安預算並單獨列項

依「六大核心戰略產業推動方案」項下「資安卓越產業」

依數位發展部(下簡稱數位部)「資通系統籌獲各階段資安強化措施」之要求達一定經費比例；如因實務作業無法達成上開要求，應敘明原因及擬採行之資安作為

必要時先行辦理系統整體規劃

規劃系統架構、分析功能需求、開發資料底層等前置工作，並納入安全系統開發生命周期(SSDLC)規劃，後續再另案委託其他廠商辦理應用層及使用者介面開發

預算編列

依個案特性編列預備費、物價調整費及檢測費。

另考量相關資訊系統開發於履約及驗收時，機關要求廠商辦理檢測，應預估檢測所需費用，編列檢測費，依契約給付檢測費。

如屬逾1年之長期服務契約，機關得於契約載明每年服務費用因應物價(如：軟體授權費用)或薪資指數調整之計算方式。

依法得洽廠商提供意見。

機關應就廠商履約工作內容、各類履約人員成本（得參考行政院主計總處薪情平臺、勞動部職類別薪資資料、政府電子採購網資訊人員薪資資料等）、軟體維護、軟體授權費等項目，並參酌市場行情（包含國際市場）、物價水準等核實編列預算；編列後得依政府採購法（下稱採購法）第34條第1項但書規定，於政府電子採購網公開向廠商說明，並請廠商提供意見及參考資料。

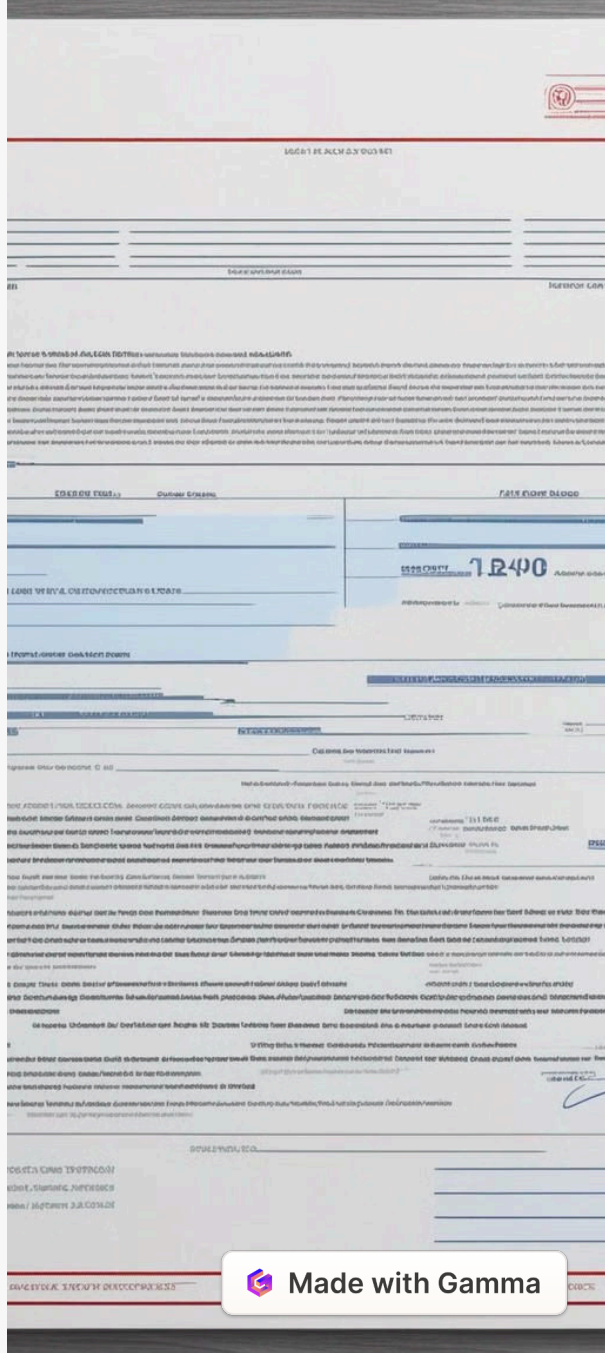
廠商資格

評估是否允許陸資廠商參與

機關應妥適訂定相應之投標廠商資格，如涉及國家安全或資通安全之採購，機關應於招標文件規定不允許陸資廠商(含其分包廠商)及陸籍人士參與；陸資廠商包含大陸地區廠商、第三地區陸資廠商及在臺陸資廠商。請參閱行政院公共工程委員會(下簡稱工程會)107年12月20日工程企字第10700501311號函。

必要時限制廠商資金來源比例

依「機關辦理涉及國家安全採購之廠商資格限制條件及審查作業辦法」，機關辦理涉及國家安全之採購，得依採購案件之特性及實際需要擇定廠商資格限制條件。



需求文件

詳列機關招標需求

資通系統或軟體開發前，應依個案性質於招標文件載明服務之項目及工作範圍，以明確描述系統需求

載明服務水準及資安要求

機關應依資通安全管理法相關規定、數位部相關規範與政策要求擇定資通系統防護需求(高、中、普)

「附表十、資通系統防護基準」

「各類資訊(服務)採購共通性資通安全基本要求參考一覽表」

需求文件

使用政府資料傳輸平臺及納入零信任架構

數位部以政府骨幹網路（GSN）為基礎，已建置跨機關資料傳輸專屬通道（T-Road）管理平臺

「政府資料傳輸平臺管理規範」

資通安全責任等級A級公務機關應依數位部規劃進程導入零信任架構

要求廠商投標時載明執行規劃

廠商載明執行規劃方式，例如：需求訪談、系統分析、系統設計、開發、測試作法及預計時程等，並於開標後審視及評估廠商是否確實了解及符合機關需要

妥適訂定招標文件所載之主要部分

採購契約載明應由得標廠商自行履行之全部或主要部分，不得轉包(由其他廠商代為履行)。因資訊服務採購涉及多項專業分工，部分特定服務依市場慣例有分包予其他專業廠商辦理之必要時，機關於訂定招標文件主要部分時應妥為考量，不宜逕明列所有工作項目均為主要部分。

招、決標作業

1

載明固定價格決標者議價時不議減價格

依採購法第52條第2項規定，公告金額以上資訊服務採購以不訂底價最有利標為原則，請機關於招標文件明定以固定費用決標，不議減價格。請參閱工程會112年5月16日工程企字第11200030081號函及「最有利標作業手冊」

2

評選項目考量廠商資安實績及作為

應將「投標廠商資安作為」納入採購評選項目，且有一定比率之配分(如：10%，依採購個案中資通系統或服務占比合理考量)，如屬依政府採購法規定無須辦理評選之採購或採其他執行方式者，應以適當方式檢視受託者之資安作為。

3

評選項目不得列「回饋」項目

為提升採購效益及評選廠商服務之差異，評選項目得列「創意」項目，但不得列「回饋」項目

契約執行

依契約約定內容協助履約及落實管理

另亦應落實要求廠商依約履行義務並交付成果(包含原始碼)

強化履約使用產品及履約人員之管理

不得提供或使用大陸廠牌之資通訊產品，履約人員不得為大陸籍人員

仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位部)核定

反覆檢視需求訪談結果，確認後始進行開發

為深化及細化需求，辦理需求訪談時應反覆檢視及要求廠商展示(例如：示意圖、流程圖或雛型等)，確認符合需要再允許廠商進行程式開發

契約執行

開發過程設定查核點，反覆檢視執行成果

定期(開會)追蹤檢討，查核時間不列入工期計算；如經查核有不符合契約約定及機關需要者，應即要求廠商配合改善，非可歸責於廠商者，應依查核狀態調整履約期間

機關新增需求應合理增加經費及期程

履約過程如確屬機關需求改變或增加情形，應辦理契約變更，給予必要之履約期間與費用

機關以取得授權利用為原則

機關應儘量以取得著作財產權之授權利用為優先，包括轉授權或再製權等

履約及驗收得請具資訊、資安專業人員協助確認

得邀請具資訊專業之專家學者協助確認

如履約內容涉及機關之核心資通系統，並應優先考量聘請外部資安專家為顧問或委員

爭議處理

善用契約雙方約定之處理機制。現行工程會提供之「資訊服務採購契約範本」第19條已載明多元之爭議處理方式，機關可善用爭議處理小組機制，並選擇具有資訊、資安專業之專家學者擔任小組委員，協助協調爭議。

機關成立採購工作及審查小組提供意見。依採購法第11條之1，機關辦理資訊服務採購得依採購特性及實際需要成立採購工作及審查小組，協助審查採購需求與經費、採購策略、招標文件等事項，及提供與採購有關事務之諮詢，開會時並得邀請具資訊、資安專業之專家學者列席，協助審查及提供諮詢。

服務等級協議(SLA)

服務等級協議(SLA)是指雙方就服務水準、品質、責任等內容所達成的協議。SLA通常包括了服務的範圍、回應時間、可用性、維護時間、問題解決時間等內容，以確保雙方對服務達成一致的期望。

一、 系統及服務可用性

(一)環境面						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	服務韌性:電力、水、網路、空調、濕度調節之備援與調節方式，確保系統正常運作於發生異常時有足夠之應變緩衝時間。		0
		v	v	對外網路環境：骨幹網路、交換器、路由器異常故障，造成連線與服務中斷，其累計時間每月不得超過____小時(約為____%可用率)。		0
(二)服務面						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	服務可用性(Service Availability)：該指標衡量服務對用戶可用的時間百分比，其計算應考慮到其他須排除之因素，如計畫中維護和升級；例如，SLA 可能規定該服務必須 99.9%的時間可用。(計算公式： 服務可用性 =（本月總小時數-停機時間）/ 本月總小時數 × 100%)	0	
v	v	v	v	正常運行時間百分比(Uptime percentage)：正常運行時間通常按每個日曆月或結算週期進行追蹤及報告。	0	

資訊服務採購作業指引之SLA

政府資訊服務採購作業指引(1120925).pdf

資訊服務採購作業重點整理

1 產出RFP

確保RFP（請求提案）文件清晰明瞭，包含所有必要的資訊，以便廠商能夠準確理解機關的需求和期望。

2 訂定資訊服務採購契約

確保採購契約充分規範了機關與廠商之間的權利義務，並明確了服務水準、資訊安全要求、履約期限等重要內容。

RFP資安需求範例說明

.參考 「Web網站建置與個人資料管理維運」RFP資安需求範例

專案概述	系統環境現況說明	專案建置需求	交付文件與產品
驗收	建議書製作規定	評選辦法	附件

專案建置需求

參考「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」連結

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

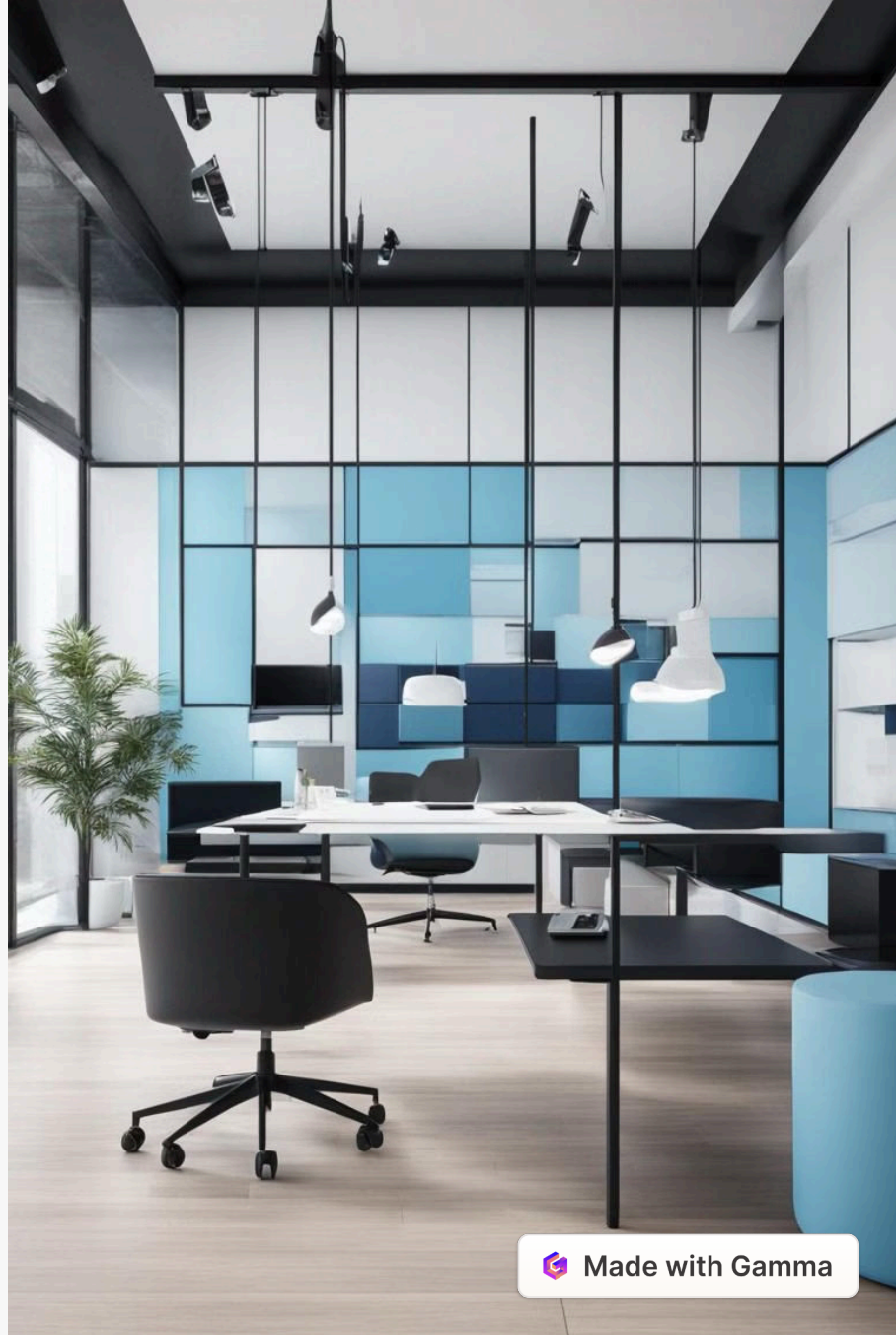
112年9月25日

雲端微服務（SaaS）辦公室生產力工具 （含郵件、行事曆、雲端硬碟、即時通訊等）							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
		提供服務商	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	●	●	●	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準	◎	◎	◎	提供服務項目涉及個資時應納入要求。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		傳輸機密性與完整性	廠商提供機關資料傳輸措施	●	●	●	
		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	●	●	●	

基礎環境需求

投標廠商背景資格限制

參照作業指引-廠商資格



介面需求

1. 參照作業指引-需求文件-使用政府資料傳輸平臺及納入零信任架構
2. 參照作業指引-資料交換之格式、介接之方式等

安全需求

1 **3.5.1 資安技術功能需求**

依資通系統等級 參考-附表十 資通系統防護基準表

2 **3.5.2 安全服務需求**

包含漏洞修補、資安改善建議、安全傳輸需求、行動APP開發安全等

3 **3.5.3 滲透測試服務**

依機關資安責任等級及核心系統定義

4 **3.5.4 事件緊急應變處理與鑑識需求**

依通報應變辦法定義

5 **3.5.5 資安攻防演練服務**

依機關資安責任等級之要求定義

6 **3.5.6 資安稽核需求**

依資安法要求合約廠商有配合機關執行監督作業

專案管理

1 3.6.1 專案組織與職掌

參考指引-契約執行-強化履約使用產品及履約人員之管理

2 3.6.2 交付項目與交付日期

參考指引-契約執行-反覆檢視需求訪談結果，確認後始進行開發

3 3.6.3 建構管理

參考指引-契約執行-開發過程設定查核點，反覆檢視執行成果

4 3.6.4 品質管理

5 3.6.5 需求異動管理

參考指引-契約執行-機關新增需求應合理增加經費及期程

6 3.6.6 服務水準協定

參考指引-服務等級協議SLA

安全管理需求

1 **3.8.1 資訊安全管理計畫**

合約廠商依專案執行之法規要求訂定相關資安管理計畫

2 **3.8.2 服務終止之措施**

合約之終止定義與終止後之權利義務，資料文件之處理原則

3 **3.8.3 所有權與智慧財產之保障**

參考指引-契約執行-機關以取得授權利用為原則

4 **3.8.4 遵循適法性作法**

其他相關法規之遵循，個資法、機關資安規範等

5 **3.8.5 資安測試與驗證**

參考指引-契約執行-履約及驗收得請具資訊、資安專業人員協助確認

總結

與資訊系統、服務相關之採購案件，應以資訊服務採購契約範本為主

共約採購項目應視其必要性另簽定服務協議要求

資訊系統及服務應自需求階段開始即納入各項資安要求評估，並留存相關紀錄

感謝聆聽 敬請指教