政府資訊作業委外資安參考指引
(V6.4)

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	95/1/3	新編
2	V2.0	97/6/30	依機關導入過程中之發現修訂文件。第 4 章以「實務範例」取代「情境範例」
3	V3.0	100/3/14	第 4 章刪除，改於附件提供「政府資訊作業委外資安檢核表」、「政府 Web 應用程式委外開發 RFP 資安需求範例」及工程會有關契約書之範本等。安全檢核表內容依採購流程依序呈現
4	V4.0	105/3/9	第 2 章刪除參考法規乙節，並增列委外生命週期等章節。第 3 章調整內容，並於附件增列「Web 網站建置與個人資料管理維運」、「Infrastructure 基礎設施建置與維運管理」及「雲端服務商提供資訊系統部署、託管及維運服務」RFP 資安需求範例
5	V4.0	105/3/9	已依審查意見，於 P.3 與 P.7 補充說明停止適用法規參考為何，並調整表 4 位置
6	V4.1	106/3/7	修正陸資企業之規範與刪除附件 03 第 8 章未盡事宜
7	V5.0	108/1/1	▪ 參考國內外相關文獻修訂資訊作業委外之定義 ▪ 依據資通安全管理法與相關子法，修訂委外作業原則
8	V5.1	108/1/24	補充說明涉及全國性民眾服務或跨公務機關共用性資通系統開發與維護(如戶役政系統)，應要求加入技術審查，詳見 P.70 補充說明 GDPR 相關內容請參閱國發會歐盟一般資料保護規則專區網站，詳見 P.17

項次	版次	修訂日期	說明
9	V5.3	108/9/30	配合資通安全管理法及其子法今年度施行，並檢視相關國內外之標準，更新本參考指引之內容，詳見 P.11 等處
10	V6.0	110/2/3	▪第 1 章調整本次修訂重點 ▪第 2 章新增「資通安全管理法」及施行細則之內容，新增「2.5 資訊委外關係管理資安要求」簡介 CNS 27036-2 架構 ▪第 3 章引入供應者關係資訊安全最佳實務與深化資安管控事項 ▪第 4 章增訂常見資訊委外作業資安注意事項 ▪新增資訊委外資安管理相關實施文件，詳見附件
11	V6.1	110/8/1	▪修正第 2 章之資訊委外類別與型態與其相關內容
12	V6.2	110/12/31	▪更新附件 8~附件 11 至最新版本
13	V6.3	111/08/30	▪更新投標廠商專案人員之專業資格限制 ▪更新監控範圍與有效性 ▪更新附件 7、附件 10 及附件 11
14	V6.4	112/11/29	▪新增「2.3.1 政府資訊業務委外原則」之「資通系統籌獲各階段資安強化措施」及「資通安全自主產品採購原則」 ▪新增「3.1 計畫作業階段」之「政府資訊服務採購作業指引」及「3.2.3.1 採購契約」之「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」 ▪更新附件 9、附件 10、附件 11、附件 13 及新增附件 8、附件 12 ▪因應組織變動進行相應調整

摘要

報告名稱	政府資訊作業委外資安參考指引
資訊等級	☐機密　☐密　☐敏感　☐內部公開　☒普通

內容摘要：

本指引主要協助政府機關相關人員，如何依據政府資安政策、風險管理、相關法規及機關具體資安需求辦理資訊委外服務(以下簡稱資訊委外)，並依資訊委外採購程序與觀點，說明資訊委外各階段應注意之資通安全控制措施與作法，同時做好績效控管並監督資訊委外遂行，達成政府機關資訊委外資安要求目標。

為此本指引說明資訊委外之基礎概念與理論架構，包含資訊委外定義、類別與型態、資安策略及生命週期，除介紹一般常見資訊委外風險與處理原則外，亦簡要說明個人資料委外管理與雲端服務委外風險注意事項，最後說明資訊委外時，各利害關係人之角色、權責分工及溝通管理方式。

在資訊委外資安要求部分，依採購作業各階段流程，包含「計畫作業」、「招標」、「決標」、「履約管理」、「驗收」及「保固作業」等，提出各項資安要求與控制措施建議，以確保資訊委外安全遂行。

關鍵詞	資訊委外、資通安全、雲端服務、個資保護

目　次

圖 目 次

表 目 次

1. 前言

1.1 目的

本指引為協助政府機關相關人員於辦理各類資訊委外時，以一般通用採購作業流程為架構，參照政府頒訂之各項資安相關法規命令，導入 CNS 27036-1：2017(資訊技術－安全技術－供應者關係資訊安全－第 1 部：概觀及概念)、CNS 27036-2：2018(資訊技術－安全技術－供應者關係資訊安全－第 2 部：要求事項)等國際標準之委外管理最佳實務，提出於資訊委外各階段應注意之資安事項，以確保機關之資訊作業安全。政府機關得參考本指引，強化資訊委外之資安管理，本指引係屬建議性質，但不以此為限，以符合各機關資安管理規範之要求。

1.2 適用對象

本指引適用於政府機關運用資訊科技從事委外業務之所有人員，為便於閱讀與使用，茲將適用對象區分為「一般主管」、「資訊人員(含資訊主管)」、「資安人員」及「一般使用者」，針對不同對象建議閱讀之重點，適用對象對照表詳見表 1。

表1 「政府資訊作業委外資安參考指引」適用對象對照表

章	節	一般主管	資訊人員	資安人員	一般使用者
2.資訊委外介紹	2.1 資訊委外定義	○	○	○	△
	2.2 資訊委外類別與形態	○	○	○	△
	2.3 資訊委外資安策略	○	○	○	△
	2.4 資訊技術安全服務生命週期	○	○	○	△
	2.5 資訊委外關係管理資安要求	○	○	○	△
	2.6 資訊委外風險說明與風險處理原則	○	○	○	△

章	節	一般主管	資訊人員	資安人員	一般使用者
	2.7 資訊委外利害關係人分工與風險溝通	○	○	○	△
3.資訊委外各階段資安要求	3.1 計畫作業階段	△	○	○	
	3.2 招標階段	△	○	○	
	3.3 決標階段	△	○	○	
	3.4 履約管理階段	△	○	○	
	3.5 驗收階段	△	○	○	
	3.6 保固作業階段	△	○	○	
4.資訊委外資安注意事項	4.1 常見機關資訊委外類型資安注意事項	○	○	○	
	4.2 資訊委外情境探討－以維運管理類為例	△	○	○	
附記	各項符號代表意義說明如下： ○：詳閱；△：參考				

資料來源：本計畫整理

1.3 本次修訂重點

本次指引修訂主要方向如下：

- 導入 CNS 27036-1:2017 與 CNS 27036-2:2018 供應者關係資通安全之最佳實務，藉由「需求協議」、「專案啓動」、「專案執行」及「技術應用」等專案過程，貫穿現行資訊委外資安管理，以期提升與委外廠商於「規劃」、「選擇」、「協議」、「管理」及「終止」階段之評估方式與資安要求。

- 依據上述範疇，強化第 3 章內容，並擴展附件 2 之檢核問項。
- 增訂兩項 RFP 資安需求範例，即「政府機關資訊安全管理系統(ISMS)顧問輔導」與「政府機關資訊安全管理系統(ISMS)第三方驗證」。
- 本指引內容提及之資訊委外類別與形態，將適時聯結至現有之相關法令、作業規範及參考指引。
- 增訂第 4 章「資訊委外資安注意事項」，彙整機關常見 6 種資訊委外類型之資安管控注意事項。常見 6 種資訊委外類型包含「系統開發」、「系統維護」、「系統檢測」、「系統監控」、「顧問輔導」及「稽核審查」等。並以一維運管理類型為案例，說明如何參照本指引進行委外作業與需注意之資安要求，以加強機關對指引內容之理解。
- 補充資安法令之資訊委外要求事項、行政院公共工程委員會(以下簡稱工程會)採購資安規範，以及政府軟體採購共契之雲端服務資安機制等法令與作業規範，使本參考指引得與之呼應。

1.4 使用建議

本指引係依資訊採購作業各階段說明資通安全需求。使用者如已熟悉資訊採購作業，建議直接參閱附件 1 政府資訊委外資安注意事項或常見缺失」，檢視以往資訊委外是否有相同缺失，以便改善；或於完成資訊委外各階段作業時，參閱附件 2 政府資訊委外資安檢核表」，以便快速檢視各階段作業或所擬之文件內容，於資安方面是否仍有疏漏，適時予以補強。

如為 Web 應用程式委外開發案，涉及個人資料保護之問題，建議參閱附件 3「Web 網站建置與個人資料管理維運」RFP 資安需求範例」；如為內部網路基礎設施之網路與伺服器設備等重要元件建置，建議參閱附件 4「Infrastructure 基礎設施建置與維運管理」RFP 資安需求範例」；如為將應用程式服務或基礎設施以雲端服務方式建置或轉移，建議參閱附件 5

「雲端服務供應商提供資訊系統部署、託管及維運服務」RFP 資安需求範例」；如為顧問輔導類型，建議參閱附件 6「政府機關資訊安全管理系統(ISMS)顧問輔導」RFP 資安需求範例」；如為稽核審查類型，建議參閱附件 7「政府機關資訊安全管理系統(ISMS)公正第三方驗證」RFP 資安需求範例」；可協助機關涵蓋基本資安需求，加速相關文件之完成，並可減少資安方面之疏漏。

1.5 章節架構

- 第 1 章「前言」說明本文之目的、適用對象及章節架構。
- 第 2 章「資訊委外介紹」，本章係針對資訊委外之定義、類別及形態、資安策略、資訊技術安全服務生命週期、風險說明與處理，以及利害關係人分工與風險溝通等，提供整體性概念，並輔以資訊委外採購程序，期能有助於使用者認知政府機關資訊委外資安之相關威脅與處理方式。
- 第 3 章「資訊委外各階段資安要求」，本章係依一般通用之採購作業程序，參考 CNS 27036-1 與 CNS 27036-2，提供機關發展資訊委外管理之參考，以符合機關資安防護水準之要求。為便於作業過程進行中檢視執行細節，另提供附件 2 政府資訊委外資安檢核表」，做為資訊委外資安管理工作之檢查重點項目，章節內容包含「3.1 計畫作業階段」、「3.2 招標階段」、「3.3 決標階段」、「3.4 履約管理階段」、「3.5 驗收階段」及「3.6 保固作業階段」，針對資訊委外衍生之資通安全議題與應注意事項，提出建議作業模式與控制措施。
- 第 4 章「資訊委外資安注意事項」，本章彙整機關常見 6 種資訊委外類型之資安管控注意事項，並以一資訊委外類型為例，說明如何參照本指引進行資訊委外與需注意之資安要求，以加強機關對指引內容之理解。
- 第 5 章「結論」，說明本指引對使用者之幫助與重點提示。

- 第 6 章「參考文獻」，詳列本指引所參考之文件或資料。
- 第 7 章「附件」則詳列本指引所納編之附件內容。

2. 資訊委外介紹

本章節包含資訊委外之定義、類別與形態、資安策略、資訊技術安全服務生命週期、風險說明與處理，以及利害關係人分工與風險溝通。

2.1 資訊委外定義

參考過往文獻對資訊委外之定義，詳見表 2。

表2　資訊委外之定義

學者	年代	定義
Grover, Cheon & Teng[1]	1996	將組織中部分或全部資訊系統功能，轉交給外部服務供應商去完成，如應用系統開發與維護、系統操作、網路管理、系統規劃及應用系統軟體採購等
Lee & Kim[2]	1999	將組織中資訊相關活動，部分或全部由組織外之資訊服務提供者來完成
Kishore et al. [3]	2003	將資訊系統之功能以契約方式委託外部廠商，如資料中心管理與操作、硬體支援、軟體維護、網路管理及應用系統開發

資料來源：本計畫整理

綜整各學者對資訊委外之定義，本指引將政府資訊委外定義為，將政府機關之資訊服務所有相關活動，部分或全部由機關外之資訊服務提供者完成。

2.2 資訊委外類別與形態

依據工程會 106 年 9 月 11 日修訂之機關委託資訊服務廠商評選及計費辦法[4]第 3 條規定，所稱資訊服務，係指提供與電腦軟體或硬體有關之服務形態，包含系統整合、軟體開發、軟體維護、整體委外、設備操作、硬體

維護、機房設施管理、備份與備援服務、網路與資安服務、網路管理、資料處理、資料登錄、人力支援、顧問諮詢、整體規劃、系統稽核、軟體驗證、教育訓練、軟體即服務(SaaS)、平台即服務(PaaS)或基礎設施即服務(IaaS)等。

為提供承辦人員辦理資訊委外之方便，爰將資訊委外類別區分為系統發展類、維運管理類、顧問訓練類及雲端服務類等 4 類，分述如下：

2.2.1 系統發展類

2.2.1.1 系統開發

依機關所訂之規格需求開發設計一套應用系統程式(含資料庫建置)，並於開發設計完成後進行測試、訓練、製作技術文件及上線之專案。其作業範圍包含新系統開發設計、系統汰舊換新、系統架構更改、系統移轉訓練及系統保固等工作。

2.2.1.2 系統維護

應用軟體(含資料庫)之維護服務與功能增修，包含軟體版本更新、應用程式錯誤與漏洞之排除及更正服務等。

2.2.1.3 系統整合

提供一套完整解決方案(Total Solution)之資通系統，涵蓋範圍包含整合網路、通訊及硬體設備，加上訂製軟體(Tailor-made Software)、套裝軟體及新資訊系統教育訓練等項目。

2.2.2 維運管理類

2.2.2.1 設備操作

機關委由委外廠商派員前來操作其資源設備，並依一定程序處理產出媒體資訊或報告。

2.2.2.2 硬體維護

硬體維護係指設備保固期滿後，為維持原硬體之功能與正常運作，所提供之定期維護契約工作，統稱為硬體維護。機關購買之硬體設備(如系統主機、終端機、工作站、個人電腦、印表機、繪圖機及連線設備等)於保固期限內，應由委外廠商依購買時之契約規定，提供各項售後服務，非屬硬體維護範圍，惟目前部分機關考量經常門預算編列不易，將設備維護費用一併納入採購案中，保固期限則由 1 年延長至 3~5 年不等。

2.2.2.3 機房設施管理

機房設施管理指電腦設備、機房設施及機房相關業務，運用外界提供之專業技術，協助執行設施管理任務。包含管理制度之規劃與執行，提供運作環境與軟硬體設備之規劃或管理等。

2.2.2.4 備份與備援服務

備援指機關透過本地端備用之儲存空間與設備、遠端備用儲存空間、設備與網路，保存重要資訊資產與恢復系統正常作業。備援服務指委廠商提供資料儲存空間、主機運算能力、網路頻寬及備援場所(含辦公場所)等方式，協助機關保存重要之資訊資產與恢復正常作業。

備援服務可大致分為資料備份、主機資源備份、網路資源備份及備援場所支援等。依機關之資安政策與資訊系統之急迫性與重要性，決定各系統之備援方式與作法。

資訊委外之備援服務可有效降低機關資訊系統無法運作之風險與成本，同時可降低災害復原所投資成本，減低因人員操作疏失造成資料遺失，或系統被攻擊造成系統網路無法運作等風險，並可縮短系統回復作業時間。

2.2.2.5 網路與資安服務

網路服務包含提供機關外部網路連線服務、私有網路服務、其他網路加值服務(含系統與應用)；資安服務則包含「資安健診服務」、「資安監控服務」、「弱點掃描服務」、「滲透測試服務」、「社交工程郵件測試服務」、「行動應用 App 檢測」及「應用程式原始碼安全檢測」等服務。

2.2.2.6 網路管理

網路管理指監控機關內部網路活動，包含路由器、交換集線器、防火牆管理與網路流量分析及網路蠕蟲與病毒攻擊防護等服務，並提供問題診斷與產生各類網路活動統計資料，以協助機關之網路管理者維持網路正常運作。

2.2.2.7 資料處理

資料處理指協助電腦系統線上作業與批次作業之運作，機關將需要以電腦處理之工作，全部或一部分委由委外廠商以其自有設備，代為規劃、設計及處理，或委由委外廠商派員前來操作機關之設備，按一定程序與程式處理產出資料者。

2.2.2.8 資料登錄

資料登錄指將機關之書面或微縮影片等原始文件，資訊委外以人工作業方式輸入、校對、彙整及轉換，產出電腦可處理之電子媒體檔案者。

2.2.2.9 整體委外

整體委外是指將全部或部分資訊系統之整體運作，包含人員、環境設備、機器設施、作業程序、管理制度及其他相關或延伸之資訊委外管理。系統管理服務之方式可以是機關自備設備，由委外廠商派提供管理服務；或設備與管理服務皆由委外廠商提供，機關擁有使用權等不同之方式。工作內容包含整體資訊管理制度規劃與建置，擬定資訊系統運作方式與執行，由機關訂定服務水準指標，以做為執行之要求與改善依據等工作。

2.2.2.10 人力支援

人力支援指依機關所需技術能力採人力派遣或業務承攬方式供機關使用。

2.2.3 顧問訓練類

2.2.3.1 顧問輔導

顧問諮詢是指在特定主題範圍內，進行民眾需求調查、相關資訊法規制度研擬、新技術導入可行性、資訊技術服務及訂定專案相關採購案件之規格研擬等，如資訊安全管理系統(ISMS)導入。

2.2.3.2 稽核審查

稽核審查是指機關為驗證管理程序或資通系統符合特定規範或標準而進行之專案，例如政府機關資訊安全管理系統(ISMS)第三方驗證。

2.2.3.3 系統稽核

系統稽核是為確保資訊單位內部作業安全控制，能有效建立並長期維持一定品質，協助評估並稽核資訊單位安全作業管制標準。

2.2.3.4 軟體驗證

軟體驗證是透過一連串具稽核功能之特殊程式，驗證資訊系統運用與功能是否正確與符合原始需求，通常由公正第三方執行。

2.2.3.5 教育訓練

教育訓練是協助機關於業務資訊化過程中，有關各階層人員常態性或專案性資訊教育訓練之規劃與執行。訓練範圍可包含電腦軟、硬體技術、資訊管理技術、行政管理技術及資安等專業領域技術等。

2.2.3.6 整體規劃

整體規劃是指在政府整體業務、跨機關業務或機關業務範圍內，進行政府

整體、跨機關業務或機關整體資訊服務需求彙整、網路與資訊技術架構規劃、訂定相關系統間資訊交換規格及相關配套措施之規劃等。

2.2.4 雲端服務類

政府機關辦理雲端委外服務應參考行政院 101 年 4 月 20 日院臺經字第 1010129213 號函訂定「行政院及所屬各機關採購雲端服務參考要項」辦理。

- 雲端服務之 3 種模式
  - 軟體即服務(Cloud Software as a Service, SaaS)

    透過網際網路提供軟體服務模式之一，供應商將應用軟體統一部署在雲端伺服器上，客戶可透過瀏覽器使用供應商提供之應用軟體服務，使用者不用再購買軟體，且無須對軟體進行更新維護，供應商會全權管理與維護軟體，如 Google DOCS、Microsoft Office 365、Facebook、Saleforce 及中華電信雲端 ERP 等。部分政府機關或企業使用 Google Gmail 即為 SaaS 之一種服務模式。

  - 平台即服務(Platform as a Service, PaaS)

    廠商透過網際網路將雲端服務平台，例如：儲存設備、資料庫等開放給使用者，使用者可以自行部署應用程序，自行使用編程語言使用服務平台，但無須管理或控制雲端設備，包含網路設備、伺服器，如 Google App Engine、Windows Azure 及 AMAZON AWS：S3(Simple Storage Service)等。

  - 基礎設施即服務(Infrastructure as a Service, IaaS)

    廠商透過網際網路，以虛擬主機方式提供完整之作業系統、資料庫存取，如 Flexiscale、AWS(Amazon Web Services)及中華電信 hicloud

CaaS 雲運算等。

2.3 資訊委外資安策略

2.3.1 政府資訊業務委外原則

●遵循「資通安全管理法」第 9 條

機關委外辦理資通系統之建置、維運或資通服務之提供，應考量廠商之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之廠商，並監督其資通安全維護情形(相關做法詳見「3.1 計畫作業階段」)。

●遵循「資通安全管理法施行細則」第 4 條第 1 項

– 委外廠商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(相關做法詳見「3.1.3.1 建立資訊委外資安策略」)。

– 委外廠商應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員(相關做法詳見「3.1.3.1 建立資訊委外資安策略」)。

– 委外廠商辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施(相關做法詳見「3.1.3.1 建立資訊委外資安策略」)。

– 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境(相關做法詳見「3.1.3.2 識別委外廠商之限制」)。

– 受託業務包含客製化資通系統開發者，委外廠商應提供該資通系統之安全性檢測證明；該資通系統屬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，機關應自行或另行委託第三方進行安全性檢

測；涉及利用非委外廠商自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明(相關做法詳見「3.2.3.2 建議書徵求文件」)。

– 委外廠商執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知機關及採行之補救措施(相關做法詳見「3.4.2.7 資訊委外資通安全事件管理」)。

– 委託關係終止或解除時，應確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料(相關做法詳見「3.4.2.2.3 僱用終止或變更」)。

– 委外廠商應採取之其他資通安全相關維護措施(相關做法詳見「3.4.2 外關係管理與監督」)。

– 委託機關應定期或於知悉委外廠商發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形(相關做法詳見「3.4.2.5.5 委外廠商服務交付管理」)。

●遵循「資通安全管理法施行細則」第 4 條第 2 項

– 委託機關辦理「資通安全管理法施行細則」第 4 條第 1 項第 4 款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項(相關做法詳見「3.1.3.2 識別委外廠商之限制」)：

➢曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

➢曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

➢曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事

不利國家安全或重大利益情事。

➢其他與國家機密保護相關之具體項目。

●遵循「資通安全管理法施行細則」第 4 條第 3 項

– 第 1 項第 4 款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。

●其他遵循事項

– 為協助公務機關及特定非公務機關於資通安全管理法適用範圍內委外辦理相關作業，補充說明委託機關依資通安全管理法施行細則第 4 條規定選任或監督受託者之相關行政流程及應注意事項，訂定「資通系統籌獲各階段資安強化措施」，詳細內容請參閱數位發展部資通安全署(以下簡稱資安署)網站[5]「資安法規專區」→「相關作業規定及指引」連結中之「資通系統籌獲各階段資安強化措施」。

– 為推動資通安全管理法第 4 條第 1 項第 3 款所定資通安全產業之發展及「資安產業發展行動計畫(107-114 年)」提高國內自主率等事宜，並鼓勵中央與地方機關(構)、公立學校、公營事業及行政法人依政府採購法採用資通安全自主產品，進而帶動資通安全產業發展及強化國家資通安全防護能量，訂定「資通安全自主產品採購原則」，詳細內容請參閱資安署網站「資安法規專區」→「相關作業規定及指引」連結中之「資通安全自主產品採購原則」。

– 遵循「資通安全管理法施行細則」第 6 條第 1 項第 11 款，於資通安全維護計畫中陳述資通系統或服務委外辦理之管理措施。

– 具敏感性或國安(含資安)疑慮之業務範疇，於招標文件載明不允許經濟部投資審議委員會(以下簡稱投審會)公告之陸資資訊服務業者參與。

– 政府資訊業務委外應建立「事前規劃、事中招標及事後執行維運」機

制，並妥善規劃服務移轉事宜，納入契約進行，確保服務之延續。

– 重要資訊專案得視需要以顧問導入，考量資安需求，並經由顧問標、規劃標、建置標及監督審驗標等程序辦理。

– 為擴大委外經濟規模效益，各機關得整合其他相關需求一次委外，朝最適合之標案規模辦理。

– 為達到委外作業透明與公平公開，重要資訊專案委外案件於正式公告招標前，應透過「公開徵求資訊文件(Request For Information, RFI)」或「徵求修正意見文件(Request For Comments, RFC)」等方式，廣納各界意見，據以訂定合宜之資安需求規格。

– 為提升資通安全服務品質，應用軟體宜與硬體分開招標，並先行辦理應用軟體招標建置，如需合併於同一標案辦理，應由各機關視個案性質訂定應用軟體與硬體經費比例上下限，列入計價，本項計價各機關得於招標過程中，納入評選計分，遴選出能提供最佳整體解決方案之廠商。

– 各機關應將應用軟體品質保證計畫列為委外必要工作項目，並要求委外廠商依照主管機關訂定之標準或規範發展系統，以確保軟體品質與政府資訊之流通互用。

– 委外廠商或團隊人員通過軟體相關資格評鑑或管理能力認證者，得列入評選加分項目。

– 為確保委外服務績效，各機關應落實監督、稽核及管控服務水準，協助廠商溝通協調事宜，以確保服務績效。

– 委外開發涉及共通性應用程式介面開發或整合者，應依國家發展委員會訂定之「共通性應用程式介面規範」辦理。

2.3.2 政府資訊委外資安策略

●從自行建構、採購硬體或訂製軟體轉為購買資訊服務。

●從開立軟硬體規格轉為設定「服務水準(Service Level)」。

●從短期與一次性購買關係轉為中長期夥伴關係。

●從重視價格轉為重視價值。

●從解決個別問題轉為購買整體解決方案。

2.3.3 訂定機關資訊委外資安策略

依據委外服務策略，各機關得據以規劃機關本身之委外服務資安策略，此外，下列各點亦請機關參酌：

●委外廠商執行受託業務，違反資安相關法令或知悉資安事件時，應立即通知委託機關及採行補救措施。

●考量資訊廠商專業領域之差異，各機關得視委外個案性質決定，將資通安全需求所需費用列入成本分析計價項目。例如 Web 應用程式開發案，鑑於網路攻擊無所不在，問題層出不窮，為避免日後因系統漏洞產生資安攻擊事件或個資外洩等問題，建議機關將資安檢測另列預算，並將資通安全服務成本納入考量。

●各機關並宜於招標遴選委外廠商過程中，將資通安全需求納入評選計分，藉以提高委外廠商重視，除一般功能滿足外，遴選出能提供最佳資安解決方案之廠商，以保障機關之資通安全。

●機關應於「計畫作業」階段，將機關資安規範對委外廠商要求納入契約書或 RFP，必要時將資通安全計畫需求納入 RFP，列為委外工作項目，以便日後「履約管理」階段，要求委外廠商遵循主管機關訂定之標準或規範執行，並提供可行建議方案，以確保資訊委外資通安全。

個資法之施行，委外廠商增加多項義務與賠償責任，經濟部商業司推動臺

灣個人資料保護與管理制度(Taiwan Personal Information Protection and Administration System, TPIPAS)，將提供委外廠商個資保護標章之認證與個資保護直接或間接相關之國際或國家標準，如 BS 10012、ISO/CNS 27001、CNS/ISO 27701、CNS/ISO 29151、CNS/ISO 29134、CNS 29001-1、CNS 29001-2 及 PCI DSS 等，建議未來將委外廠商是否取得個資保護認證納入評比項目。另個資保護可能涉及日後賠償之保險問題，亦會增加委外廠商營運成本，建議機關於估算成本時應一併考量。另歐盟個人資料保護規則(General Data Protection Regulation, GDPR)自 107 年 5 月 25 日開始實施，GDPR 規範重點包含：

●擴大適用範圍：及於歐盟境外，並明文涵蓋網路識別碼。

●加重企業相關責任：要求資料保護並要求設置資料保護長。

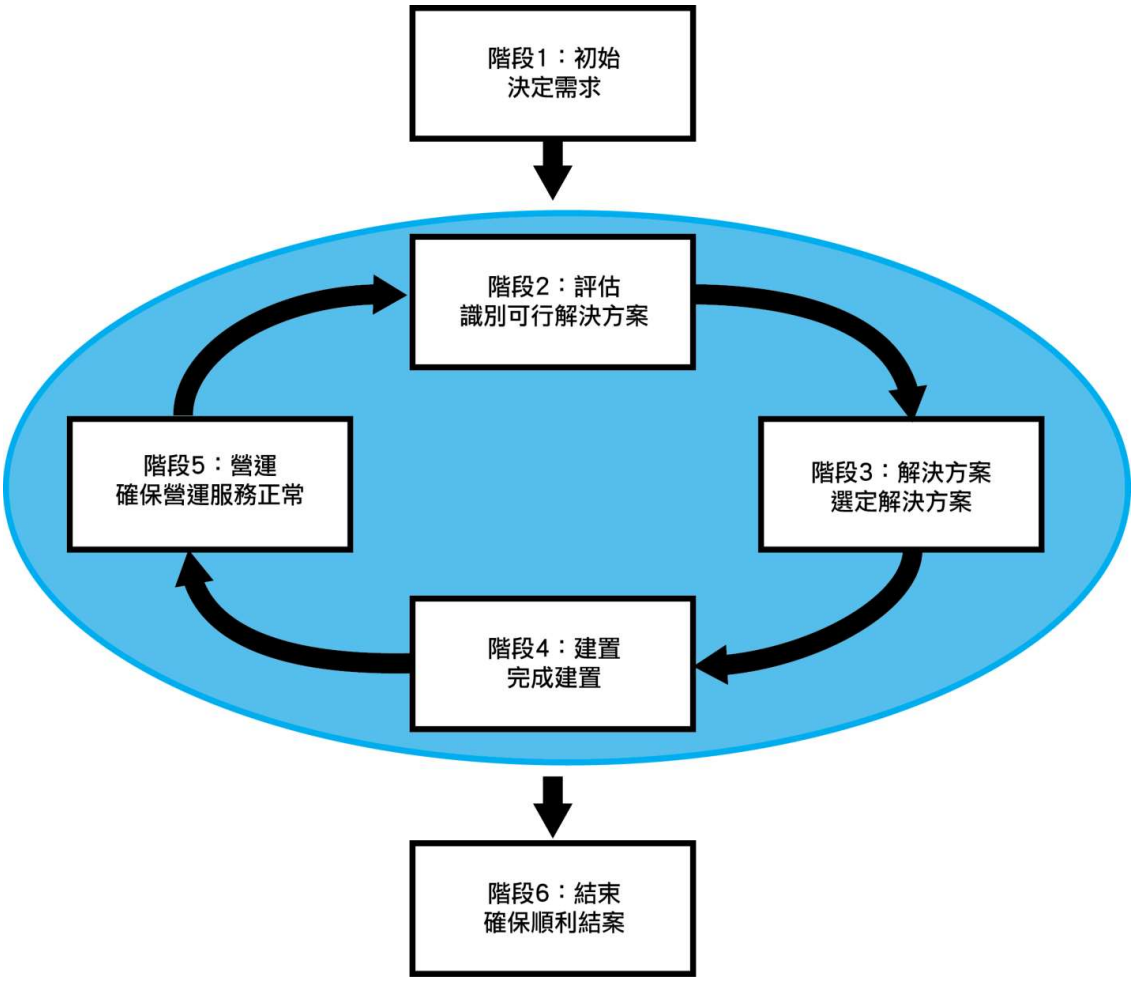
●賦予個資當事人更完整權利。

●個資境外傳輸採「原則禁止，例外允許」。

因此政府機關如果服務交易涉及歐盟境內個人資料取得，應遵循 GDPR 要求，相關內容請參閱國發會歐盟一般資料保護規則專區網站。國發會已於 107 年 7 月 4 日成立「個人資料保護專案辦公室」， 以加強跨部會因應 GDPR 事宜之協調整合，並負責統籌各部會向歐盟申請適足性認定事宜。

2.4 資訊技術安全服務生命週期

參考美國國家標準技術研究所 NIST SP 800-35 資訊技術安全服務參考指引(Guide to Information Technology Security Services)，資訊技術安全服務(IT Security Service Life Cycle)可分為 6 個階段，詳見圖 1 所示。



資料來源：本計畫整理

圖1　資訊技術安全服務生命週期

2.4.1 階段 1：初始(Initiation)

資訊技術安全服務生命週期於初始階段，由組織識別出資通安全之需求。此階段對應第 3 章資訊委外各階段資安要求之計畫作業階段，將委外常見之一般性策略、管理、需求、契約及廠商等面向之資安風險納入考量。

2.4.2 階段 2：評估(Assessment)

於選商前，先審慎分析資訊作業環境現況與期望達成目標差異，識別出可行解決方案之選項，並能定義適當之有效評估指標。此階段對應第 3 章資

訊委外各階段資安要求為仍屬計畫作業階段，規劃可行之資通安全解決方案。

2.4.3 階段 3：解決方案(Solution)

依階段 2 分析結果由決策者選出適當之解決方案。此階段對應第 3 章資訊委外各階段資安要求之決標階段，選出委外廠商，並完成契約、相關保密協議簽訂及配套資通安全解決方案之執行辦法等事項。

2.4.4 階段 4：建置(Implementation)

依階段 3 產出結果要求委外廠商依需求完成契約。此階段對應第 3 章資訊委外各階段資安要求屬履約管理階段，於完成決標後，成立專案組織，督導服務廠商遵循 RFP 與契約，如期如質完成委外服務。

2.4.5 階段 5：營運(Operations)

服務進入營運狀態，需持續量測服務水準是否持續滿足原規劃需求?如服務需求因應組織策略方向改變或業務需求增加，則必須回到階段 2 進行再評估。至此，階段 2 至階段 5 形成一個生命週期持續循環改進，直到環境變化，變革性需求出現，則需重新定義初始需求。此階段對應第 3 章資訊委外各階段資安要求之保固作業階段，針對服務水準及安全事項進行監控與管理，並檢討是否須因服務需求改變組織策略方向或增加業務需求，或考量現有委外服務無法滿足組織需求而終止。

2.4.6 階段 6：結束(Closeout)

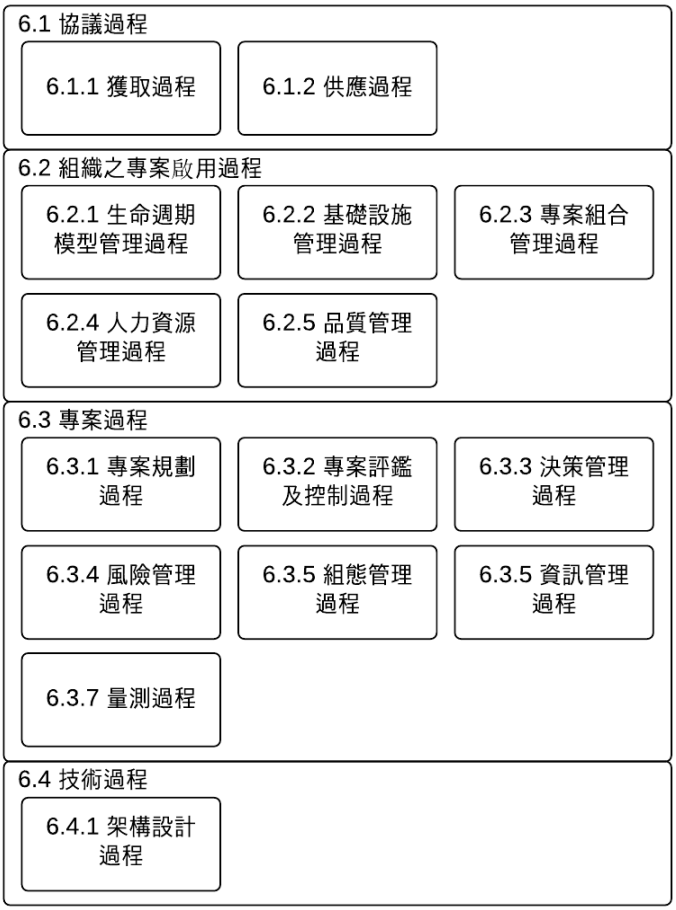
當環境變更，原資安服務解決方案之基礎架構無法透過改善達成環境變更後需求，通常會在原服務後期即開始依循此 6 階段開始新一代生命週期，並規劃新舊資安服務解決方案轉移。

2.5 資訊委外關係管理資安要求

政府機關於有資訊委外需求時，即應著手規劃委外廠商管理事宜，最直觀易懂方式之一即參考 CNS 27036-2:2018，以具有時序之生命週期各階段切入，定義、實作、運作、監視、審查、維護及改進各階段中委外關係之資安要求事項。

2.5.1 以系統生命週期為架構之資訊委外關係管理資安要求

圖 2 以系統生命週期為架構，說明 4 個時期之資安要求事項，做為普遍適用於資訊委外關係管理之方案。



資料來源：CNS 27036-2:2018

圖2　以系統生命週期為架構之資安要求事項

2.5.1.1 協議過程

機關應與委外廠商就獲取與供應過程，於委外關係中雙方之資安角色與責任取得共識。

●獲取過程

機關應建立、定義、實作、維護及改善委外關係策略，包含資安風險管理框架、委外廠商評選準則框架、移轉計畫、資安變更管理計畫、資安事件管理計畫及委外終止計畫等。委外關係存在期間，機關亦應指派專人負責上述管理策略之相關過程，並至少每年或遇重大變更時審查之。

●供應過程

如同政府機關考量「獲取過程」中對委外關係管理之資安要求，相對於「供應過程」中，委外廠商應以同樣之資安要求，評估與機關之關係。

2.5.1.2 組織之專案啟用過程

委外專案啟動期間，機關應考量下列 5 個面向：

●生命週期模型管理過程

在管理委外關係之資安時，機關與委外廠商應建立生命週期管理過程，以確保各階段定義與使用之各項政策與程序之可用性。

●基礎設施管理過程

機關應定義、實作、維護及改進委外關係中得以支援其資安管理之基礎設施能力，包含實體與邏輯存取、應變計畫等。

– 專案組合管理過程

機關與委外廠商應於專案進行過程，考量該專案所涉及資安與整體營運目標所隱含之要求事項與相依性，包含共享資訊之敏感性、績效評

估之方法等。

– 人力資源管理過程

機關與委外廠商應於委外關係中，指派適任之人力資源。該些人員應對委外關係中之資安要求事項有完整訓練與認知，而對於其資格部分，針對承擔關鍵職務人員，在法律允許下，應執行詳細刑事與背景調查。

– 品質管理過程

機關與委外廠商應於委外關係中，建立品質管理過程，以確保委外標的符合品質目標且達到顧客滿意。

2.5.1.3 專案過程

委外專案期間，機關應考量下列 7 個面向：

●專案規劃過程

於規劃專案時，考量雙方協議之資安要求事項對專案成本、計畫及時程之影響，將相關資安考量整合至專案之角色、責任、可歸責性及權限中，並保護專案可能涉及之資訊資產。

●專案評鑑及控制過程

於管理委外關係之資通安全時，機關與委外廠商應建立專案評鑑與控制機制，確保專案得依其規劃之預算與期程進行，並滿足技術目標。

●決策管理過程

於管理委外關係之資通安全時，機關與委外廠商應建立決策管理機制，以利於有替代方案時，能選擇最有利之專案行動方向。

●風險管理過程

於管理委外關係之資通安全與整個委外生命週期中，機關與委外廠商建立資安風險管理框架，定期且持續檢視委外所伴隨之資安風險。

●組態管理過程

於管理委外關係之資通安全時，機關與委外廠商應建立組態管理機制，以識別委外關係管理中所分享之資料完整性。

●資訊管理過程

於管理委外關係之資通安全時，機關與委外廠商應考量委外關係期間所交換資訊之敏感性，並建立資訊管理機制，以利雙方皆能適時地提供或取得相關、完整、有效及機密之資訊。

●量測過程

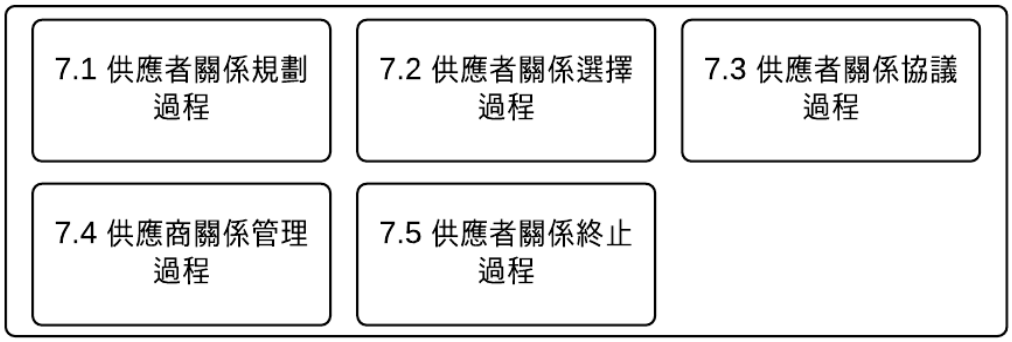
機關與委外廠商應共同定義、實作、維護及改進資通安全量測框架，以展示委外關係中雙方之資安成熟度。資通安全量測框架應含有量測對象、量測報告方式、報告頻率及未達量測標準之處置對策等。

2.5.1.4 技術過程

委外廠商應考量委外關係中所協議之要求事項，將之轉變或整合至其所提供之產品或服務，並確保能持續提供與維持品質。

2.5.2 以建立與維護時序架構之資訊委外關係管理資安要求

於 CNS 27036-2:2018 中亦依機關與委外廠商建立與維護關係之時序，提出各階段之資安要求事項，詳見圖 3。



資料來源：CNS 27036-2:2018

圖3　以建立與維護為架構之資安要求事項

2.5.2.1 供應者關係規劃過程

於初始階段中，機關應依資訊委外關係策略中之資安風險管理框架，識別與評鑑委外所伴隨之風險，並建立相關風險管理計畫。而於風險評鑑過程中必不可少之活動則為審查機關管轄權之法律與法規要求事項，以及可能約束委外廠商之法律與法規領域。此外，亦應依循資訊委外關係策略，建立委外關係計畫，記錄管理階層對於啟動委外所採取之決策，識別委外範圍、受眾、型式及本質，規劃依資產特性與機敏程度之資安控制措施，指派資安角色與責任。

2.5.2.2 供應者關係選擇過程

本階段之目標在於選擇適宜之委外廠商，在選商過程中，機關應依上述階段所建立之委外關係策略與委外關係計畫，定義與實作委外廠商選擇準則。同時，機關應備妥保密協議書，以保護選商期間所分享之資訊資產；備妥招標文件，確保招標文件依委外關係計畫產生，充分包含所識別之資安要求事項。最終，蒐集來自可能之委外廠商所提交之服務建議書，進行評估，以選擇最符合機關期待之廠商。

2.5.2.3 供應者關係協議過程

接續於選定委外廠商後，機關與委外廠商應議定於產品或服務提供期間之

管理活動，包含資安角色與責任、資安要求事項、先前非由該委外廠商所提供產品或服務之移轉程序、資安變更管理、資安事件管理、遵循性監視與實施及委外終止計畫等。

2.5.2.4 供應者關係管理過程

當委外關係存在期間，機關與委外廠商應遵循前階段所共同簽署之委外關係協議，維持雙方之資通安全。除持續訓練所有涉入委外關係之人員外，亦應監視與審查對資安條款之遵循性，並於必要時，審查與更新委外關係協議。

2.5.2.5 供應者關係終止過程

委外關係終止期間，為避免於終止通知後之所有資通安全、法律及法規衝擊，機關與委外廠商應於取得管理階層決策後，指派專人執行委外終止計畫。對於因委外關係終止而受衝擊之內部人員與第三方，應定義與實作溝通計畫，並於委外終止達成後，留存終止計畫執行報告備查。

2.6 資訊委外風險說明與風險處理原則

2.6.1 常見委外風險評估面向

大部分資訊委外風險來自於未將自身之資安需求與規範完整地納入契約，如未定義委外廠商所能處理之個人資料範圍，蒐集、處理、利用及銷毀之權利與義務，導致廠商歇業或破產時，無法取回委外處理資訊；即便已將相關事項納入契約，實務上經常疏忽未確認廠商是否完全遵守契約所訂定內容。以下就 5 個面向說明一般常見委外風險：

- 策略面(Strategy)

  政府機關之資訊委外管理對於整個營運活動中有相當重要之影響力，特別是對於資訊委外內容之型態、範圍及管理方式等策略是否妥適，會直接或間接影響機關資通安全。

如資訊委外範圍，包含關鍵性或具高度機敏性工作，若未由政府機關有效管理，將大幅增加資安風險；另應避免過度倚賴特定或少數廠商，在專業分工與防止廠商於資通安全壟斷面向都需要考量，對於廠商所在地理位置所適用之法律也必須考慮，特別是海外廠商或與契約相關之雲端服務，都會增加法律面向風險。

●管理面(Governance)

契約關係生命週期中對廠商缺乏管理，為資訊委外資安之主要風險。政府機關與廠商間未定義適當之管理模式，可能增加資訊作業失誤與遵循性風險。與管理面有關條款也包含在契約生命週期中，如缺乏有效之契約變更管理程序，將增加執行作業風險與財務風險。

●需求面(Requirements)

不適當之需求規劃或描述，可能對廠商執行服務之合理性產生衝擊。政府機關常以軟硬體設備規格取代實質需求，尤其是系統建置完成後之日常維運與資通安全需求，經常未納入委外服務需求範圍，長期可能導致政府機關在營運(無法提供服務)、財務(因無法提供服務所產生之損失)、法律(與廠商產生之爭議)及聲望(無事實根據之謠言、無法對民眾提供服務)等問題，應於計畫階段即考量資通安全需求，並納入需求規劃。

●契約面(Contract development)

未能完整涵蓋契約需要被管理之各種關係，即為不完整之契約，是整個契約關係中最大風險。例如：忽視款項支付細節或定價機制是主要財務風險，相對於財務風險，要求廠商不適當或不切實際之服務水準，則可能導致營運相關風險，並可能造成過度設計之解決方案、高價格、未能充分有效利用資源，或喪失其他可能機會。其他營運風險包含缺乏契約終止規範或對廠商訂定不適當之溝通需求。另外，缺乏細部權益或任何

智慧財產權、個人資料及資料安全等契約規範，包含使用、處置及散布軟體與資料等，則可能出現法律或遵循性風險。

●廠商面(Vendor selection)

未選擇合適之廠商將使政府機關暴露於財務風險中，包含因取得契約廠商無法達成服務水準，導致解約而替換廠商需額外付出預算、潛在施政績效喪失及及無法有效地要求賠償。在營運風險上，可能包含無法達成政府機關預期目標或取得所需資源，導致資通安全防護作業出現空窗期；另外也可能造成政府形象受損或出現勞資、法律等爭議。

鑑於未適當選擇廠商，可能出現履約期間廠商無法確實履行義務之風險，在簽訂契約前應採取適當之廠商盡責調查(Due Diligence)措施，如檢視廠商近三年財務報表、查詢過去有無違反採購法或未能及時履約等紀錄，以降低類似風險，使廠商能有較佳之長期履約能力與穩定性。

政府機關較常見委外相關風險為：

– 機關內因跨專案間之統合協調不佳，導致單一專案執行成效不彰。

– 委外廠商因自身資通安全管理疏失，發生資安事件，連帶影響委外機關資通安全。

– 委外機關需求無法確定或頻於修改，影響專案執行進度與驗收期程。

2.6.2 降低資訊委外風險原則

依據前述常見委外風險，說明降低委外風險之主要原則，執行這些原則可以有效降低可能之風險與衝擊，然而風險依然存在，因此階段性滾動風險評估有其必要性，重點說明詳見表 3。

2.6.2.1 多樣化來源策略，以避免過度倚賴或鎖定特定廠商

●對應風險：策略面。

●說明：過度倚賴特定廠商可能使政府機關暴露在受限特定廠商提供特定產品、服務及缺乏議定商業條款空間風險。當一個專案中有太多關鍵工作都只能由特定廠商執行時，代表機關有極可能沒有任何足夠資源與能力來完成這個專案，於採取委外作業時，應思考多樣化執行方式，避免倚賴或鎖定特定廠商。

2.6.2.2 建立委外廠商管理程序

●對應風險：管理面。

●說明：建立標準程序可以幫助樹立可靠之委外廠商關係，並在客觀基礎上做出決定，例如：機關可思考建立委外廠商之選取標準與評估程序。

2.6.2.3 建立委外廠商之管理模式

●對應風險：管理面。

●說明：於契約中建立一個正式委外管理模式，以適用於整個契約生命週期至關重要。委外管理模式應定義利害關係人之角色與責任、變更程序、報告方式與頻率、管理主體等。這個模式必須能夠管理營運、技術及策略等不同層次之契約關係。政府機關應利用委外管理模式，與委外廠商建立良好之合作與互信，並注意委外利害關係分工與風險溝通，避免機關內因跨專案間之統合協調不佳，導致單一專案執行成效不彰。

2.6.2.4 建立委外廠商管理組織

●對應風險：管理面。

●說明：對於政府機關而言，必要時可考慮建立專屬之委外廠商管理組織(Vendor Management Office)，尤其是具有許多高度複雜之契約或少數高度策略性委外關係，如依據採購法第 76 條之規定，行政院採購暨公共工程委員會、直轄市或縣(市)政府設有採購申訴審議委員會，負責廠商申訴

與履約爭議之調處事項。另外亦可考慮建立委外廠商關係人(Vendor Relationship Manager)，用以管理眾多委外廠商，包含接受契約雙方投訴、抱怨。這些組織與角色可附屬於資訊、採購或企劃部門。惟就目前政府機關實際執行情形而言，對於廠商多以臨時性與以事件為導向之方式管理，如發生履約爭議時，由資訊、採購、法規或企劃承辦人員組成臨時性組織，針對特定事件進行審查。此種方式除難以延續廠商管理政策一貫性，亦缺乏第三方以客觀角度處理雙方爭議，對於長期合作關係與履約糾紛亦無相當助益。這些組織或角色應具備之能力說明如下：

– 對於履約相關事項與政府機關運作應有相當之知識與經驗。

– 足以促進所有參與者共同合作技巧。

– 衡量廠商履約表現與是否遵循契約能力。

– 以大方向策略觀點與高層次角度了解某些合作關係之重要性。

– 解決問題與發現根本原因之分析性思考能力。

– 了解契約用語與各項情境之基本法律常識。

– 談判技巧。

– 實踐廠商管理相關知識。

2.6.2.5 預先規劃廠商之技術與能力需求

●對應風險：契約面。

●說明：契約中應規定委外廠商人員具備相關驗證與經驗，例如：接受相關教育訓練、驗證或工作年資、經驗等。另外也應確保廠商人員能夠接受政府機關之內部管理規範與行為，如廠商人員必須簽訂某些保密條款或通過安全查核作業。

2.6.2.6 使用標準文件與範例

- 對應風險：契約面。
- 說明：政府機關應建立適宜之契約標準文件與範例，以確保委外廠商在契約生命週期中，能完整對應政府機關之政策與目標，因為使用廠商提供之契約文件與範例，有可能因在法律遵循、各方法律權益規範不完整，造成契約內容不利於政府機關。

2.6.2.7 制定明確之需求

- 對應風險：需求面。
- 說明：契約中之需求內容為委外廠商投標基礎，應明確表達政府機關對委外廠商履約表現、交付事項、服務品質及成本之要求。不當之需求內容在後續談判與履約時可能會造成混淆與爭議，且機關委外需求無法確定或頻於修改，亦影響專案執行進度與驗收期程。因此對專案管理人、資訊、法務或其他利害關係人而言，應於進行委外作業之每個步驟前，對契約需求都能有一定了解。於招標公告前，應能夠確保下列事項：
  - 契約內容與工作事項必須清楚，定義契約範圍與解釋政府機關之目標，有助於廠商了解政府機關作業環境。
  - 需求必須明確被定義且經利害關係人確認。
  - 如有必要時，可將程序納入以釐清需求。
  - 針對複雜大型專案，建議機關於確定公告契約需求前，能辦理意見徵求 (Request for Comments，RFC)，以確保契約規定符合市場能量。
  - 著作權歸屬應明確訂定，以利機關後續利用與開放。
  - 必須給予廠商足夠之時間提出規劃。

– 獎勵標準與決策過程應被清楚定義，這些標準可以傳達給參與廠商，但應避免於評估過程中過度強調，過於詳細之評估標準可能影響廠商企劃內容。

以下類型需求應被包含於契約內：

– 經由營運標的本身定義需求，說明執行營運所需之產品或服務型式。

– 法律與規範需求。

– 人力需求，說明相關工作人員狀態、行為準則及內部規定。

– 於契約草擬過程中涵蓋所有生命週期相關項目。

2.6.2.8 適當之選擇委外廠商

●對應風險：委外廠商面。

●說明：選擇委外廠商有效方式之一為確認有無做到委外廠商盡責調查(Due Intelligence)，包含審查以往客戶給予之評價、檢視財務狀況、評估委外廠商於市場之定位，以及參考委外廠商之控制與遵循性報告。委外廠商財務狀況應特別關注，若委外廠商財務狀況長期不佳時，做為長期合作對象風險相對較高，在未完成應有服務水準時，也無足夠資金支付契約所訂定之罰金；另外，建立正式選擇委外廠商標準亦是良好實務做法之一。

2.6.2.9 契約草擬過程中應涵蓋生命週期所有相關項目

●對應風險：契約面。

●說明：概述契約草擬過程注意重點如下：

– 付款條件應詳細說明並納入契約條款，以降低混淆與爭議。

– 契約內應包含軟體使用與散布條款，包含取得特定軟體之合法授權，

使用非法軟體可能帶來法律之問題。

– 考量周詳之契約可讓委外廠商於問題發生時，提供快速解決與修正方案。當然，損害無法完全避免，責任義務問題亦可能浮現，此為雙方之責任義務應於契約中明述之因。

– 契約中應訂定賠償條款，以保護政府機關權益。通常於賠償條款中亦提及免責規定，以免不可抗力發生。

– 契約生命週期中，某些狀況可能改變或影響產品或服務履行。因此變更條款應納入契約內容，且任何重要變更都應經由雙方協商同意後實施。變更條款考量重點如下：

➢如何實施變更?

➢什麼可以變更?

➢何時可以變更?

➢誰有權可以提出與確認變更?

➢變更次數之限制。

2.6.2.10 決定適當安全與控制措施

●對應風險：管理面、契約面。

●說明：契約應說明資料、資訊、軟體、手冊及其他文件等智慧財產權之歸屬。在整個契約生命週期中，資料擁有者應被訂定於契約內，以避免契約結束時產生爭議。例如：委外廠商可能依照契約服務提供所需之商業授權軟體，而政府機關資料可能儲存於這些軟體中。當契約結束時，這些資料、紀錄檔及報告等最終處置方式應律訂於契約內。若政府機關未於契約內說明擁有者，在要求委外廠商返還資料時可能會被要求額外費用。如使用開源軟體，應依該開源軟體之授權範圍，授權機關利用，

並以執行檔及原始碼共同提供之方式交付予機關使用，委外廠商並應交付開源軟體清單（包含但不限於：開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文）。履約期間，委外廠商可能存取機敏資料，為確保資料之隱私、安全性、完整性及機密性，應強制委外廠商遵守政府機關相關政策與程序。委外廠商存取應被限制於履約所必要之資料即可，例如委外廠商存取資料庫時，應只能存取服務所需之部分資料欄位，而非任意存取整個資料庫。實際訂定契約時，應注意下列事項：

– 誰可以存取資料?

– 資料儲存於何處?

– 備份程序。

– 資料保存政策。

– 能否支援電子蒐證(e-discovery)?

2.6.2.11 建立服務水準協議(Service Level Agreement, SLA)

●對應風險：契約面。

●說明：服務水準是委外廠商提供給政府機關所能量測之最低要求標準，應包含量測標準與報告，服務水準清楚提供政府機關與委外廠商對於服務之責任，執行績效直接影響委外廠商績效，政府機關可據此獎勵或罰款，訂定服務水準時應注意下列事項：

– 明確定義服務項目與相關條款內容。

– 包含績效水準、績效量測、品質水準、錯誤率、服務限制、重新議價及服務調整規則。

– 可以主契約之附件方式附加，做為主契約參考。

– 明定服務水準有效期間，於何種情況可中止或變更，要如何進行中止或變更。

– 設定服務水準高低以符合政府機關需求與可支付預算標準，但要求過高之服務水準相對會付出更高成本。

2.6.2.12 建立執行水準協議(Operating Level Agreement, OLAs)與支持契約(Underpinning Contract)

●對應風險：契約面。

●說明：前一節服務水準是政府機關與委外廠商之間服務遞送協議，委外廠商提供之服務，可能需要與政府機關內部單位或其他外部委外廠商協同合作，才能滿足服務水準。執行水準協議目的是明確規定委外廠商之相互依賴關係，以確保委外廠商與這些政府機關內部單位或再委外之第三方委外廠商，可以支持主契約委外廠商對政府機關之服務水準。如政府機關允許主契約委外廠商將服務之一部分外包給第三方委外廠商，為確保第三方委外廠商可達成執行水準協議，可於服務水準中再附加支持契約。

2.6.2.13 建立適當之委外廠商績效或服務水準監控與報告機制

●對應風險：契約面、管理面。

●說明：當訂定報告需求與服務水準時，政府機關應考慮某些報告之規格，例如負責指標、蒐集資訊及撰擬績效報告之對象，而且雙方都必須確認報告內之需求與服務水準，必須公正以做為評估服務之基礎。此外，應詳細地說明這些資訊如何蒐集與處理，使雙方對報告內容之正確性有信心。

2.6.2.14 建立委外廠商獎懲模式

●對應風險：契約面。

●說明：建立明確之懲罰與獎勵模式，如採用逾期履約違約金、品質不符時減價驗收或可獎勵經常性超越服務水準獎勵金等。

2.6.2.15 於契約生命週期中建立適當之委外廠商關係管理

●對應風險：管理面。

●說明：從契約初始之雙方互動到關係結束，於契約生命週期中提供透明度是合作成功之關鍵因素。於報價階段，委外廠商應提供報價透明度，政府機關則應提供包含服務指標與評估結果等透明度。

2.6.2.16 檢視契約與服務水準

●對應風險：管理面。

●說明：應階段性檢視契約與服務水準，以確定履約情形是否符合契約與服務水準。任何服務模式、價格、風險或是法律需求之改變，都應重新檢視履約情形，並納入契約或服務水準。較佳實務作法是於契約內制定變更條款，以避免雙方日後面臨困難與不愉快之協商過程。

2.6.2.17 要求委外廠商風險管理

●對應風險：管理面。

●說明：可以契約或協議要求委外廠商實施風險管理。前述所提到之委外廠商盡責，應是政府機關要求委外廠商實施風險管理之重要管理活動與確證。政府機關應發展詳細風險管理，以識別所有由委外作業所產生之潛在風險，避免委外廠商因自身資通安全管理疏失，發生資安事件，連帶影響委外機關資通安全，其類別至少應包含財務、營運、聲譽及法規遵循性等。在發展風險管理之後是建立風險監控機制；監控委外廠商之績效至少應包含評估與追蹤有關委外廠商被投訴紀錄，這些投訴紀錄是

檢視委外廠商執行成果與相關議題之良好指標；另外，風險評估也應基於風險監控結果進行階段性更新。

2.6.2.18 以政府機關政策檢視委外廠商法規遵循性

●對應風險：管理面。

●說明：於履約階段，政府機關之政策與規範應與委外廠商分享，以建立對於內部控制環境與法規遵循性需求之共識。政府機關重要政策與規範文件如下：

– 政府機關策略。

– 資通安全政策。

– 實體環境安全策略。

– 存取控制策略。

– 相關法規列表。

2.6.2.19 實施委外廠商內部控制評估

●對應風險：管理面。

●說明：於研擬契約時應決定政府機關是否有稽核委外廠商內部控制之權利，或是由委外廠商或第三方獨立評估者提出委外廠商內部控制評估報告，這些都應事先訂定於契約內。一般而言，擁有眾多客戶之委外廠商通常會事先準備好第三方獨立評估報告，提供客戶以確認其內部控制措施無誤。

2.6.2.20 規劃與管理契約關係結束

●對應風險：契約面、管理面。

●說明：一般契約對於關係結束階段很少著墨，這個階段委外廠商應逐漸

退出服務，並可能將服務之知識與經驗轉移到新委外廠商。有時這種轉移作業難以訂出確認時間，較佳之做法可訂定一個目標，讓政府機關內部足以熟悉整個服務運作方式；另外，必要時亦可訂定服務轉移時間，例如新委外廠商接手時，由舊委外廠商支援重疊一段時間。

2.6.2.21 訂定軟硬體處置規定

- 對應風險：契約面、管理面。
- 說明：於契約生命週期中，可能會有資料或硬體設備交由委外廠商使用，契約中應清楚定義這些軟硬體之處置方式，是應交回政府機關或於契約結束時銷毀。若資料中包含個資或其他重要資料時，契約應清楚要求委外廠商確保這些資料在委外廠商系統中被永久消除。

表3 降低資訊委外風險原則之重點說明

原則序號	降低資訊委外風險原則	對應風險	重點說明
1	多樣化來源策略	策略面	為確保產品、服務及商業條款的彈性與議定空間，應避免過度倚賴或鎖定特定廠商
2	建立委外廠商管理程序	管理面	樹立可靠之委外關係，並雙方可在客觀之基礎上做出決定
3	建立委外廠商之管理模式	管理面	著重於委外利害關係分工與風險溝通，建立良好合作與互信關係，以避免機關內因跨專案間之統合協調不佳進而影響各別專案
4	建立委外廠商管理組織	管理面	機關可考量建立專屬之委外廠商管理組織(VMO)或委外廠商關係人(VRM)，以處理雙方之爭議
5	預先規劃廠商之技	契約面	依專案特性，於契約中規定委外廠

原則序號	降低資訊委外風險原則	對應風險	重點說明
	術與能力需求		商人員應具備相關驗證與經驗
6	使用標準文件與範例	契約面	用以確保委外廠商在契約生命週期中，能完整對應政府機關之政策與目標
7	制定明確之需求	需求面	為避免後續談判或履約時可能會造成之混淆與爭議，應明確表達機關對委外廠商履約表現、交付事項、服務品質及成本之要求
8	適當之選擇委外廠商	委外廠商面	建立正式之選商標準，並進行完整之委外廠商盡責調查(Due Intelligence)
9	契約草擬過程中應涵蓋生命週期所有相關項目	契約面	契約草擬中應考量專案之生命週期，納入必要且詳細之條款。特別應著重在爭議處置之描述
10	決定適當安全與控制措施	管理面、契約面	依專案特性，對可能產生資安風險處進行識別並建立安全控制措施
11	建立服務水準協議	契約面	以服務水準協議規範委外廠商應達成之最低服務標準
12	建立執行水準協議(OLA)與支持契約(Underpinning Contract)	契約面	明確規定委外廠商之相互依賴關係，以確保委外廠商與機關內部單位或再委外之第三方委外廠商，可以支持主契約委外廠商對政府機關之服務水準
13	建立適當之委外廠商績效或服務水準監控與報告機制	契約面、管理面	為確保有公正評估服務之基礎，機關應建立適用之委外廠商績效或服務水準監控與報告機制
14	建立委外廠商獎懲	契約面	建立明確之懲罰與獎勵模式，以嚇

原則序號	降低資訊委外風險原則	對應風險	重點說明
	模式		阻任何未符預期之行為
15	於契約生命週期中建立適當之委外廠商關係管理	管理面	從契約初始之雙方互動到關係結束，於契約生命週期中提供透明度是合作成功之關鍵因素
16	檢視契約與服務水準	管理面	應階段性檢視契約與服務水準，以確定履約情形是否符合契約與服務水準
17	要求委外廠商風險管理	管理面	政府機關應發展詳細風險管理，以識別所有由委外作業產生之潛在風險，避免委外廠商因自身資通安全管理疏失，影響機關資通安全
18	以政府機關政策檢視委外廠商法規遵循性	管理面	於履約階段，政府機關之政策與規範應與委外廠商分享，以建立對於內部控制環境與法規遵循性需求之共識
19	實施委外廠商內部控制評估	管理面	機關於研擬契約時，可考量納入稽核權，或由委外廠商或第三方獨立評估者提出委外廠商內部控制評估報告
20	規劃與管理契約關係結束	契約面、管理面	機關應對服務之知識與經驗轉移制訂目標與計畫
21	訂定軟硬體處置規定	契約面、管理面	機關應於契約中明確定義交由委外廠商使用之軟硬體之舒置方式

資料來源：本計畫整理

2.6.3 個人資料委外管理風險與注意事項

不論政府機關或企業，隨著服務專業分工或限於組織人力與資源限制，將

個人資料管理委託第三方廠商處理趨勢日益增加。個人資料雖然委外處理，但在執行個人資料保護之實務作業與法律責任強度，並未減弱。我國個人資料保護法第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關」，明確說明委外廠商受政府機關委託處理個人資料時，在個人資料保護之規範下與政府機關並無二致，政府機關不能因為將個人資料處理委外而免除應盡監督義務與法律責任。另委託處理個人資料若屬特種個人資料，則除符合我國個資法中所列之特定情形外，不得蒐集、處理或利用。政府個人資料委外主要類型可分下列：

●內部業務委外

政府機關在個人資料仍僅限於以政府機關實體範圍進行管理，但實質由委外廠商執行，如將官方網站、系統開發、網路管理、資料庫建置管理、資通安全監控或薪資計算與發放等委外進行建置及維運，個資當事人難以察覺個人資料有委外處理。

●以第三方提供服務

政府機關將個人資料定期由內部向委外廠商傳送進行資料處理作業，如稅務單位稅單、聯合考試或學力測驗成績單委託列印封裝廠商進行列印與寄送等。

●以受託廠商名義提供服務

政府機關透過專業服務公司進行個人資料蒐集、處理及利用，如委外進行電話訪問、民意調查或辦理各項宣傳、抽獎活動等，個資當事人可明確得知或被告知是由委外廠商受政府機關委託執行個人資料管理。

●將個人資料委外處理

在個人資料生命週期資料流之範圍、管理及法規遵循責任，由政府機關

延伸至委外廠商，相對在違法使用與外洩風險皆會提高。政府機關主要控管風險手段為監督與進行稽核，主要風險為：

– 委外廠商缺乏對個人資料保護法與資通安全認知

委外廠商專注於提供政府機關服務，不了解個人資料保護法對受委託廠商要求等同於委託公務機關或非公務機關，對資通安全防護之意識薄弱，或不願投資額外成本強化資通安全管理與防護機制。

– 既有契約未到期，不願配合個人資料保護修訂契約條款

政府機關與委外廠商簽訂中長期個人資料處理委外契約，持續沿用舊契約，於契約尚未到期前不願因應個人資料保護法遵循，增加符合個人資料蒐集、處理、利用規範及保護條款，使政府機關監督管理委外處理個人資料廠商有困難。

– 委外廠商監督與查核不易落實

政府機關個人資料委外業務承辦人公務繁忙，無法落實定期監督，確認委外廠商是否依法執行個人資料蒐集、處理及利用。

●綜合以上個人資料委外風險，主要解決方法還是來自於明確於契約規範。委外廠商個人資料保護要求與監督並促使其自律，雙方義務就個人資料保護法施行細則[6]第 7 條(規範受委託機關遵從委託機關個人資料保護規定)與第 8 條(委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督)已有明定。政府機關監督委外廠商注意事項至少包含如下，實際執行時，並可參考國家資通安全研究院(以下簡稱資安院)發布之個人資料保護參考指引[7]，於契約內訂定相關規範：

– 委外廠商預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

– 委外廠商就下列事項採取之措施

➢配置管理之人員與相當資源。

➢界定個人資料之範圍。

➢個人資料之風險評估與管理機制。

➢事件之預防、通報及應變機制。

➢個人資料蒐集、處理及利用之內部管理程序。

➢資料安全管理與人員管理。

➢認知宣導與教育訓練。

➢設備安全管理。

➢資料安全稽核機制。

➢使用紀錄、軌跡資料及證據保存。

➢個人資料安全維護之整體持續改善。

– 委外廠商有複委託者，其約定之受託者。

– 委外廠商或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項與採行之補救措施。

– 委託機關如對受託者有保留指示者，其保留指示之事項。

– 委託關係終止或解除時，個人資料載體之返還，與委外廠商履行委託契約以儲存方式而持有之個人資料之刪除。

– 為減低對委外廠商監督與稽核時花費人力與時間，可於選商時，將廠商是否通過第三方個人資料保護或資通安全管理國內外認證列入評選項目。評估廠商是否有自主管理能力，可於履約與保固期間以委外廠

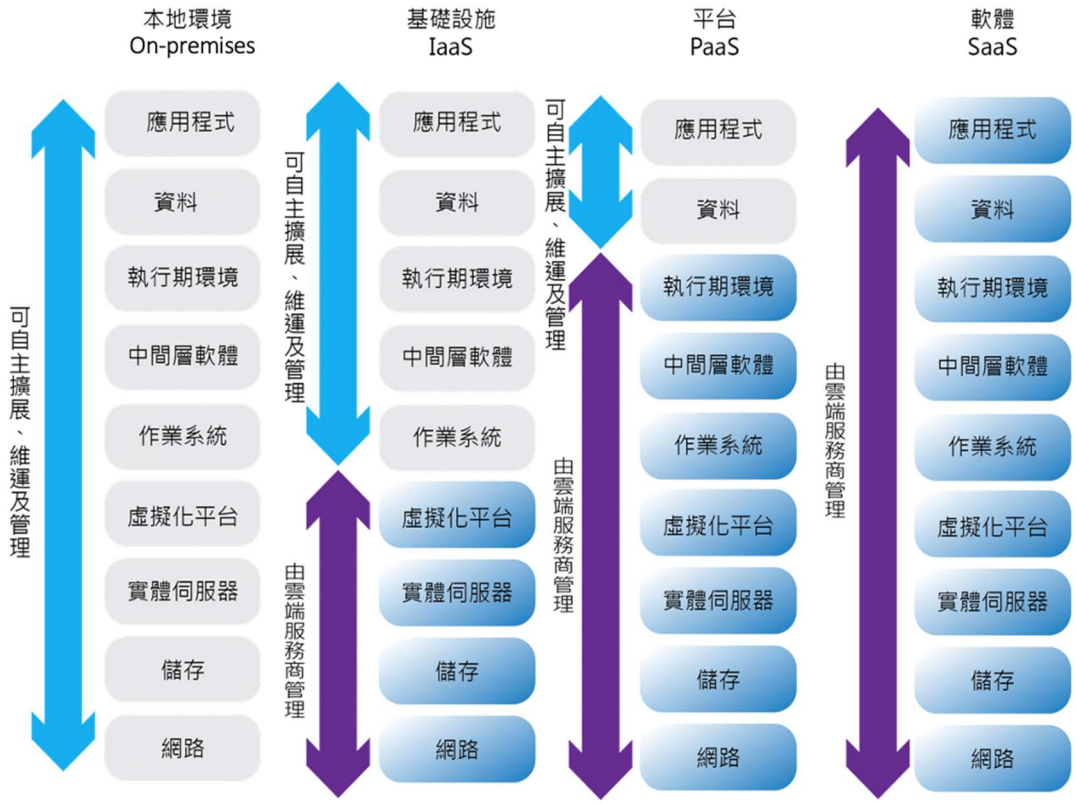
商第三方驗證單位外部稽核報告，取代部分實地稽核所花費之人力與時間。

– 如委外廠商並無第三方驗證單位對其實施定期稽核，亦可考慮以符合個人資料保護法、施行細則及政府機關對個人資料管理之要求，委託第三方稽核人員實施獨立委外稽核，惟須注意第三方稽核人員是否有相關專業資格與實務經驗。

- 機關可要求委外廠商在個人資料處理時，將個人資料採匿名或去連結性納入考量，以降低各個資項目機密性之風險等級，甚至可採去識別化，使個資無法直接或間接識別。
- 機關可要求委外廠商在個人資料利用時，以採經資料分析後之結果為用，以免直接利用。

2.6.4 雲端委外風險與注意事項

依 NIST 定義軟體即服務(Software as a Service, SaaS)、平台即服務(Platform as a Service, PaaS)及基礎設施即服務(Infrastructure as a Service, IaaS)等 3 種服務模式，就雲端委外服務控制權之觀點(詳見圖 4)。以完全自行建置本地環境(on-premises)之各項 IT 環境元件，如網路、儲存、實體伺服器、虛擬化平台、作業系統、中間層軟體、執行期環境、資料及應用程式等服務元件之控制權比較雲端 3 種服務模式，愈往基礎設施即服務時，在作業系統以上用戶仍保有可自主擴展、維運及管理控制權。在平台即服務只剩資料與應用程式，軟體即服務即全由雲端服務商管理服務，亦即在機關擁有之控制權而言，IaaS > PaaS > SaaS。



資料來源：本計畫整理

圖4　雲端服務控制權比較

對 IT 環境控制權多寡，意味對雲端服務廠商契約、服務水準及價格議定空間有多少，對於資通安全需求水準，僅能參考雲端服務廠商所提供之方案來選擇。

就雲端服務部署方式，常見雲端服務風險參考歐洲網路與資通安全局(European Network and Information Security Agency, ENISA)，以雲端服務風險分析，針對政策與組織風險、法規風險及技術風險 3 個面向歸納如下：

●政策與組織風險

– 供應商綁定(Provider Lock-in)。

– 喪失管理(Loss of Governance)。

– 遵循與合規上之挑戰(Compliance Challenges)。

– 組織名譽損失源於其他用戶行為(Loss of Business Reputation Due to Co-tenant Activities)。

– 雲端服務之中止與失效(Cloud Service Termination or Failure)。

– 雲端供應商之收購(Cloud Provider Acquisition)。

– 供應鏈失效(Supply Chain Failure)。

●法規風險

– 傳票與電子蒐證(Subpoena and E-discovery)。

– 管轄權變更之風險(Risk from Changes of Jurisdiction)。

– 資料保護風險(Data Protection Risks)。

– 授權之風險(Licensing Risks)。

●技術風險

– 資源匱乏風險(Resource Exhaustion)。

– 隔離失效(Isolation Failure)。

– 惡意內部人員(Cloud Provider Malicious Insiders)。

– 管理介面被破解(Management Interface Compromise)。

– 傳輸資料攔截風險(Intercepting Data in Transit)。

– 資料傳輸時之外洩風險(Data Leakage on Up/download)。

– 不安全或無效之資料移除(Insecure or Ineffective Deletion of Data)。

– 分散式阻斷服務攻擊風險(DDoS)。

– 加密金鑰遺失與外洩(Loss of Encryption Keys)。

– 服務引擎弱點攻擊(Compromise Service Engine)。

– 用戶嚴謹之程序與雲端環境衝突(Conflict Between Customer Hardening Requirement and Cloud Environment)。

將 IT 服務轉換至雲端服務廠商，視選用雲端服務模式與部署方式不同，有不同程度之 IT 環境已不再由政府機關本地端維護與管理，資通安全管理責任也由政府機關與雲端服務廠商共同分擔責任，於資通安全政策與管理程序是否具備透通性?於雲端服務平台仍能維持與機關內部相同資料安全服務水準?依據上述有關政策與組織及法規面向風險之因應，主要需透過委外契約，此部分已於第 2.5.2 章節討論。

因應雲端服務風險除依機關之資通安全需求外，建議可參考我國與國際資通安全標準如 CNS 19086-1(資訊技術－雲端運算－服務水準協議(SLA)框架－第 1 部：概觀與概念)、CNS19086-3(資訊技術－雲端運算－服務水準協議(SLA)框架－第 3 部：核心一致性)標準、雲端安全聯盟(CSA)雲端控制矩陣(Cloud Control Matrix, CCM)、ISO 27000 系列，以及美國 NIST SP800-144 等建議控制措施，選擇機關必要項目列入 RFP，要求雲端服務廠商執行。

2.7 資訊委外利害關係人分工與風險溝通

2.7.1 資訊委外利害關係人角色與責任

資訊委外多數係透過專案過程進入日常維運，專案成功主要關鍵因素之一即在於利害關係人管理，惟有識別所有利害關係人並滿足其需求與期望，方有提升專案成功之可能。政府機關資訊委外專案可能涉及之資安利害關係人角色與責任說明如下，實際執行時必須依據現況適時調整，避免疏漏。

● 資訊長(Chief Information Officer, CIO)

我國對於資訊長之規定，依行政院數位國家創新經濟推動小組設置要點第 8 點之規定，為統籌協調、推動數位政府，行政院及中央二級機關置資訊長，其設置方式及運作機制如下：

– 行政院置資訊長一人，由「行政院數位國家創新經濟推動小組」總召集人指派副總召集人之一兼任，負責督導數位政府發展，提高政府機關行政效率與便民服務及網路普及應用等事宜。

– 各中央二級機關置資訊長一人，由機關首長指定副首長或主任秘書兼任，負責協調業務及資訊資源，統籌推動業務流程改造、法規鬆綁，應用資訊科技提升行政效能及創新便民服務等事項。

– 各中央二級機關資訊長幕僚作業由所屬資訊單位辦理，協助推動各機關及所屬資通安全管理、數位政府策略規劃、業務流程改造、資訊計畫審定及資源分配等事項。

● 資通安全長(Chief Information Seurity Officer, CISO)

依資安管理法第 11 條之規定，公務機關應由其首長指派副首長或適當人員擔任資通安全長(以下簡稱資安長)，負責推動及監督機關內資通安全相關事務。

● 採購人員(Contracting Officer)

一般為政府採購單位承辦人，負責專案契約之發包、管理及終止等採購相關執行事項。

● 採購人員技術協辦(Contracting Officer’s Technical Representative, COTR)

由採購人員指定之技術人員，負責專案契約技術相關之協助工作，就政府機關而言，可能為資訊或資安單位承辦人員。

●計畫審查小組(IT Investment Board)

由政府機關內部包含企劃、主計、採購或其他技術與需求相關單位組成，採購金額較大之計畫多由資訊長或資安長召集，並於計畫階段針對計畫之目標、預算來源、用途及預期效益等合理性進行審查。

●資安管理負責人(IT Secuity Program Manager)

負責政府機關資安政策與規範之規劃及管理人員，如發展合理、結構化之方法論，以識別、評估及降低資安風險，並提出適當解決方案來幫助機關面對真實世界威脅，同時協助資安長等高階人員確保資安管理工作符合機關資安目標。

●資安技術人員(IT System Security Officer)

在技術方面確保資訊系統於生命週期中安全無虞之技術人員。

●計畫管理人/需求提出者(Program Manager/Acquistion Initator)

計畫管理人/需求提出者在資安方面扮演重要角色，因為他們不僅在資安服務規劃之起始階段就被納入，並且要確認服務功能需求。

●個人資料保護專人/隱私官(Privacy Officer)

確保服務與其規劃於資料保護、散播(資訊分享與交換)及解密時，符合現行個資保護政策。依個人資料保護法第 18 條規定，我國政府機關應指定專人辦理個資安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏；另依該法施行細則第 25 條，所稱專人指具有管理與維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。

●其他參與者(Other Participants)

除上述角色外，為識別所有利害關係人，必須根據資訊服務類型、範

圍、整體規劃及組織大小，並納入決策、執行及管理過程中，包含規劃、招標、決標、驗收及履約各階段所有參與者，對一個龐大政府組織而言，甚至必須考量外部組織之資安需求，如政府友軍或合作供應商等。

2.7.2 資訊委外風險溝通

2.7.2.1 利害關係人分析

於整個資訊服務生命週期中，識別並分析利害關係人是持續進行過程之一，為解決專案各階段利害關係人之競爭與衝突，並符合其需求與期望，必須識別並蒐集所有利害關係人之相關資訊，了解其影響或支持程度，並做適當分類，以做為日後發展解決策略方案之依據，於實際執行分析時，可依據下列重點製作關係人登錄表，範例詳見表 4：

- 基本資料：單位、姓名、職務、專案角色及聯繫方式。
- 評估資料：需求、期望及影響，屬於專案生命週期哪一階段。
- 利害關係人分類：內部/外部與支持者/中立者/反對者等。

表4　利害關係人登錄表範例

編號	單位	姓名	職務	專案角色	聯繫方式	需求與期望	影響	利益關切階段	內/外部
S01	副首長室	李 OO	副首長	資安長	OO	需求：資安政策 期望：成功專案	高	各階段	
	(略)								

資料來源：本計畫整理

2.7.2.2 風險溝通

風險溝通係於整個風險評估與管理過程中與利害相關人互相交換有關風險、風險相關因素及風險認知之資訊與意見，其中包含解釋風險評估結果與建立風險管理決策基礎。

良好之風險溝通必須是雙向互動、資安管理負責人必須蒐集各利害關係人對資通安全之期望，充分了解對資安風險之認知與觀點，進行溝通規劃，並善用正式與非正式溝通方式及訊息管理等，消除重大歧見。

利害關係人所產生主要風險，通常是發生在缺乏良好溝通情況下，風險溝通牽涉到訊息發送與接受者責任、溝通方式、溝通規劃及訊息發布：

●訊息發送與接受者責任

– 訊息發送者：發送之訊息須完整、清楚及明確，確認訊息接收者明白訊息內容。

– 訊息接收者：確認完整接收並了解訊息內容，並向訊息發送者確認。

●溝通方式

– 正式：如計畫書、履約文件、各式函文、專案執行各階段會議所產出之研討資料、分辦表、管制表及會議紀錄等。

– 非正式：如電子郵件、筆記及備忘錄、或對話與聊天等口頭溝通方式。

●溝通規劃

就政府機關而言，專案溝通管理規劃除可納入契約規範，要求廠商定期召開工作進度報告會議，並提交工作報告外，亦可採取非正式方式，由雙方於契約規範外，自行依需求進行溝通，專案溝通管理內容重點如下：

– 專案利害關係人之溝通需求。

– 資訊發布之需求，如資訊格式與內容或詳細程度。

– 負責發布與接受資訊之成員。

– 溝通與資訊發布之頻率。

– 資訊處理層級規劃，如當低階專案成員無法處理某些問題時，應於多長時間內向上通報。

– 更新與變更專案溝通管理方式之方法。

– 專案中所使用共同詞彙或專案術語。

●訊息發布

溝通主要目的即在有效並正確地交換資訊，確保正確對象適時、適地取得適當資訊。為達成有效溝通目的，負責專案管理者應確實發布專案訊息，除讓利害關係人了解並掌握專案執行狀況，一般而言，可採取下列

方式達成訊息發布目標：

– 資訊蒐集與檢索

資訊可以不同形式存在與傳遞，專案團隊可依據實際運作需求，選擇最適當之資訊蒐集與檢索工具，例如將檔案儲存於共用資料庫或檔案伺服器等，以利專案成員能透過檢索、搜尋方式取得所需資料。

– 資訊發布

資訊發布是適時並及時將資訊蒐集、分享及發布給專案利害關係人，資訊發布工作分布於整個專案生命週期。資訊發布方式各異，如專案會議、紙本檔案、共用檔案資料庫、電子郵件及網路會議或專案管理軟體等。

– 專案過程文件之保存與更新

- 經驗學習文件：如將任何問題發生原因、解決方法、參與人員及結果詳盡記錄，並存入資料庫。
- 專案紀錄：包含各項專案規範、專案管理計畫、專案文件、備忘錄等，均須以適當方式加以記錄與保存。
- 利害關係人回饋：利害關係人於接收到訊息後，會根據實際狀況提出意見，專案管理者會根據利害關係人之回饋，對專案管理做出適當修正，相關回饋與修正結果應予以記錄保存。

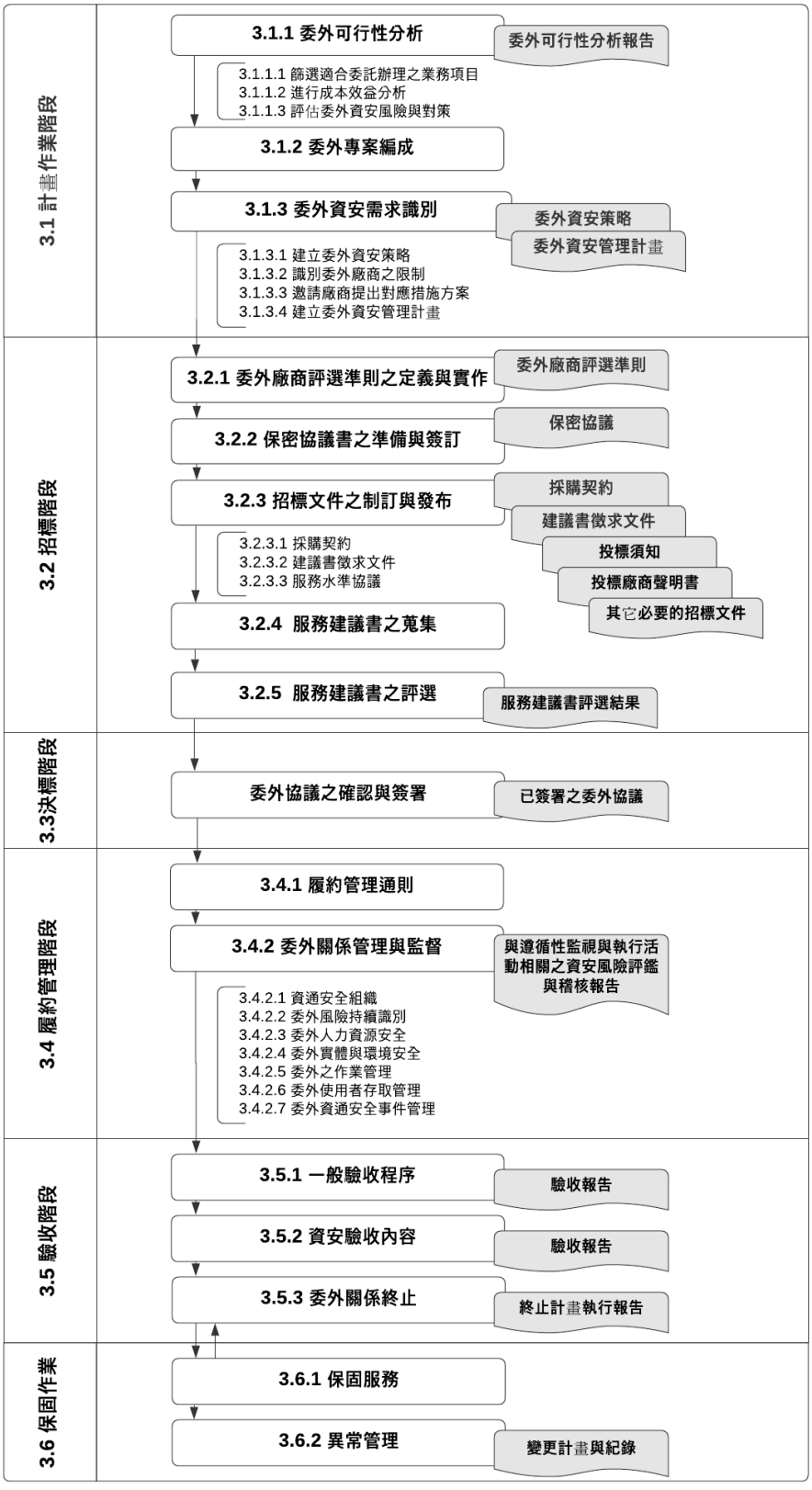
3. 資訊委外各階段資安要求

本章依一般通用採購流程，以「計畫作業」、「招標」、「決標」、「履約管理」、「驗收」及「保固作業」等為架構，以遵循「政府採購法」[8]、參照政府頒訂之各項資安相關法規命令及導入 CNS 27036 等，提出各階段應有之資安控管建議，以確保資訊委外之資通安全。

為確保未來所有資訊委外作業達到政府機關之資安管理水平，且能良善管理委外廠商與其可能帶來之資安風險，機關於平日營運就應具備基礎資安管理意識、認知及控管措施，其資安控管措施應至少包含下列項目：

- 了解資訊委外所應遵循之法律、法規、命令、相關標準及指引等。
- 具備依 CNS 27001 或其相似標準所制定之資通安全政策。
- 具備依 CNS 27001 或其相似標準所制定之相關資安規範與程序，以便機關於進行資訊委外資安需求識別時，有穩固參考基礎，並將必要之資安控管納入契約與 RFP 中。此外，明確且具體化資安控制措施，可讓雙方工作團隊有統一遵循基準，據以進行各項資訊業務發展與運作。
- 具備依 CNS 27001 或其相似標準中對資訊資產分類分級之規範，依不同分類設定不同資安等級與可接受使用準則。

當機關已具備基礎之資安能量，未來在考量進行任何類型之資訊委外時，若能再依循本章所建議之資安控管措拖，勢必能降低因資訊委外而帶來之資安風險。本章陳述結構將依據採購作業流程進行說明，詳見圖 5。



資料來源：本計畫整理

圖5　資訊委外資安管理架構

3.1 計畫作業階段

計畫作業階段涉及大量資訊蒐集與分析，評估個案之委外可行性與委外風險，以確認是否進行委外。當確認辦理委外時，機關應識別所有相關資安要求事項，而此部分將是委外作業中相對重要且複雜之環節。故為強化機關對資訊委外中之資安管理作業，本節將引入 CNS 27036-1 與 CNS 27036-2 供應者關係資通安全與 CNS 27002 中所規範之供應者關係管理概念，藉由從高階資安需求辨識至詳細委外資安管理計畫編寫，了解該委外個案之資安控管全貌，並依此製作契約、RFP 及 SLA 等。

當機關確認辦理委外但於進行規劃活動前，宜優先確認工程會政府電子採購網中與資訊作業有關之採購項目，與數位發展部數位產業署(以下簡稱產業署)資訊服務採購網中與資安服務有關之採購項目。若無合適者，可參考其共同供應契約自行依需求辦理招標作業。

此外，為強化機關資訊服務採購需求明確、合理編列費用及減少履約爭議，工程會訂定「政府資訊服務採購作業指引」(詳見附件 8)，從採購全生命週期提醒機關辦理資訊服務採購應注意事項，作為辦理資訊服務採購之作業指引。

3.1.1 資訊委外可行性分析

機關於考量是否辦理資訊委外時，應將資訊委外工作範圍與期望達成之功能、效果及目的等委外工作需求，用文字與圖表方式表達，以提供內部討論形成共識。其次則應評估專案於財務、技術、組織、經濟、法律及風險因素等之可行性，該可行性分析除可自行辦理外，也可委請專業顧問機構參與協助規劃，以利後續委外招標作業程序之執行。

資訊委外可依委外作業型態不同、委外規模大小及專案機敏特性，參考下列步驟進行分析：

3.1.1.1 篩選適合委託辦理之業務項目

為確定委外作業符合實務，委託機關應先調查潛在委託對象，積極探詢可受委託辦理民間團體之參與意願，以了解潛在受託者之概況，並加強與潛在受託者溝通協調，以確定該項業務委外之資通安全可行性無虞。

3.1.1.2 進行成本效益分析

政府機關於決定業務委託民間辦理前，除一般成本分析外，宜將資通安全列入成本進行效益分析，以期確實有效執行，分析內容應包含以下「量化指標」與「非量化指標」。

3.1.1.2.1 量化指標

在量化指標方面，應考量人力、時間、資產維護及資安防護等，說明如下：

- 專案自行開發之人事成本(包含薪資、保險及退休等費用)。
- 專案自行開發之時間成本(包含業務需求時程與機關自行開發時程)。
- 委外專案資訊服務之人事成本(包含僱用、薪資、保險及退休等費用)。
- 委外專案資訊設施之資產成本(如設備、用地、建築等購置及維持成本)。
- 因資安所增加之費用(如委託第三方資安弱點掃描，交付軟體資安驗證等成本)。
- 大型(複雜)系統增加之監督人事成本(如委託第三方定期與不定期督導委外業務執行成本與委外業務成效評估成本)。
- 機關如進行案件複雜度較高者，可聘請資通安全、財務及法律等專業顧問或專業機構依工程會所頒相關作業手冊協助辦理，其辦理程序應依採購法與評選及計費辦法等相關規定辦理。

3.1.1.2.2 非量化指標

在非量化指標方面，應考量受服務者滿意度與信賴度。

●考量對機關外部客戶之可用性提升，評估其可行性。

●考量對機關外部客戶之安全信賴度提升，評估社會成本效益。

3.1.1.3 評估資訊委外資安風險與對策

在一般專案可行性分析中，分析風險因素與對策內容涉及甚廣，故回歸本指引主題，本小節僅針對委外資安風險因素之可行性評估進行說明。首先，機關應確認委外資安風險評估之範圍，包含可能受影響之資訊資產、流程及作業環境，或對機關之特殊威脅，威脅性質包含法律法規(如個人資料保護相關法律)、國際協議與限制、營運與資安策略、財務、科技與資訊環境、資訊設備、資料存取與運用、智慧財產及其他潛在之任何因素等。機關可參考「2.6 資訊委外風險說明與風險處理原則」以獲得更多委外風險熱點之細節；而針對委外風險評估之執行方法與程序，則可參考「資通系統風險評鑑參考指引」[9]。由於本步驟屬於初期風險評估，在有限資訊與資源下，機關可採用「資通系統風險評鑑參考指引」中之高階風險評鑑，以得出風險值，並制定降低風險之對策，但當所識別之資安風險無法降低至可接受風險等級時，則不宜取得此項產品或服務。

經由風險評估過程，機關得以較準確地將有限之成本與時間聚焦於風險熱點，對各階段應具備之防護措施亦有初步了解。而該風險評估與處置對策可做為委外契約協議輸入之一。惟由於高階風險評鑑本質，其風險評估結果存有不精確之可能性。若有必要，如風險值較高時，機關宜在締結委外契約前，進行「資通系統風險評鑑參考指引」中之詳細風險評鑑，以確保更精確之風險得以被辨識。

3.1.2 資訊委外專案編成

當確定進行委外後，機關首要任務則為指派適任之專案負責人。此人應對資訊委外專案性質或內容有充分了解之能力，並能對資訊委外專案所衍生之風險有控制與處置權力，故其位階不宜過低。在專案規劃期間，專案負責人除應了解委外產品與服務本質外，可視委外性質與規模諮詢與邀請採購(總務)、法務、會(主)計、業務、資訊及政風等單位人員，參與在資通安全、資訊技術、法規遵循、服務水準、專案細項預算及選商需求分析等工作。

機關如因員工工作負荷過重或技術能力不足，宜遴聘外部顧問予以輔助。如因系統複雜或技術層次較高，則宜採取兩階段方式作業，即先委外進行系統規劃工作，再進行系統發展與建置工作。

3.1.3 資訊委外資安需求識別

當機關選派適當專案負責人後，下一步則需了解與分析該資訊委外專案應有之資安要求事項。此分析完善程度將深遠影響該資訊委外專案之成敗，機關不得不嚴謹視之。本段落將引入 CNS 27036 中，資訊委外關係規劃時對識別與建立資安管理之概念，由高階資安需求識別至詳細資訊委外資安管理計畫，以循序漸進方式協助機關識別所有資訊委外資安需求事項。

3.1.3.1 建立資訊委外資安策略

機關應針對資訊委外個案，建立其資訊委外資安策略，其內容應考量(但不限於)下列項目：

- 識別欲取得之產品與服務，包含其涉及範圍、使用對象、利害關係人、類型及本質。
- 上級機關與機關管理階層對資訊委外產品或服務之動機、需要及期望。
- 機關管理階層對配置必要資源之承諾。

●持續因應資通安全風險之管理程序

機關應於資訊委外關係存在期間，持續因應並處置資通安全風險。而已導入 CNS 27001 之機關，可將此程序納入既有之風險管理機制中，即將因資訊委外專案而產生之資訊資產納入 ISMS 資產清冊中，進行定期或不定期(視需求)之風險評鑑。

●將採用之資安管理架構

機關應確認使用何種資安管理架構，並將此架構套用於資訊委外資安管理。已導入 CNS 27001 之機關，即可使用 ISMS 資安管理架構做為對委外廠商進行資安管理之參考基準。

●委外廠商評選準則項目

機關應綜合委外產品或服務之特性，建立委外廠商評選準則項目，以利於招標階段，機關能在充分考量資通安全前提下，成功選擇合適之委外廠商。其評選準則應包含(但不限於)下列項目：

– 評選委外廠商是否具備資安能量之方法

  ➢可考量該委外廠商過往資安執行績效、積極管理資安之證據(例如通過 CNS 27001 驗證)或有營運持續性計畫之書面證據等。

  ➢委外廠商是否配置充足且經適當訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

– 評鑑委外廠商對遵循機關所要求資安事項而提出證據之方法。

– 評鑑委外廠商接受下列項目之方法

  ➢評鑑委外廠商對遵循性監視與執行服務承諾之方法。

  ➢評鑑委外廠商對機關已採購產品或服務之移轉支援。

➢評鑑委外廠商對產品或服務終止之支援方法。

– 對委外廠商之特定要求事項，應依機關所預期之營運、法律、法規、架構、政策及契約等面向而定義，例如委外廠商之財力、委外廠商之位置、由何處提供產品或服務及其複委託廠商之相關限制，尤其是降低法律與法規漏洞之風險。

●用以定義下列項目時之高階資通安全要求事項

– 移轉所採購產品或服務至不同資訊委外廠商之移轉計畫。

– 資安變更管理程序。

– 資安事件管理程序。

– 遵循性監視與執行計畫。

– 終止產品或服務獲取之終止計畫。

機關應視資訊委外專案時程，定期審查資訊委外資安策略，或於發生重大營運、法律、法規、架構、政策及契約變更時審查之，並確保資訊委外資安策略以適當方式讓相關人員知曉與了解。必要時，應包含委外廠商相關人員。

3.1.3.2 識別委外廠商之限制

在為個別資訊委外專案建立資訊委外資安策略後，在此階段機關亦需視資訊委外產品或服務之本質，考量委外產品與服務是否涉及國家機密、影響國家安全或受世界貿易組織(WTO)政府採購協定之規範，以限制投標廠商或其人員之資格。

●涉及國家機密之執行人員限制

當資訊委外產品或服務涉及國家機密者，機關應於 RFP 中敘明所有參與

此資訊委外專案之第三方人員應接受適任性查核，並依「國家機密保護法」之規定，管制其出境。適任性查核項目如下：

– 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。

– 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。

– 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

– 其他與國家機密保護相關之具體項目。

●涉及國家安全之採購限制

當機關辦理涉及國家安全之採購時，應遵循下列事項：

– 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

當機關辦理涉及國家安全採購時，得於招標文件中載明對我國或外國投標廠商與其分包廠商之資格限制，詳細內容可參考工程會網站[10]中「政府採購」→「政府採購條法規」→「修訂草案」連結中之「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」。此外，機關應依據「各機關對危害國家資通安全產品限制使用原則」，避免採購或使用危害國家資通安全之軟體、硬體及服務等產品。

– 具敏感性或國安(含資安)疑慮之業務範疇

茲因兩岸尚未締結與政府採購法第 17 條第 1 項有關之條約或協定，機關辦理採購，得依個案特性及實際需要於招標文件中限制大陸地區之財物或勞務參與。故當機關辦理資訊服務採購，如認委外廠商所供應之財物或勞務之原產地為大陸地區，有影響國安(含資安)或機敏資訊外

洩之疑慮者，可於招標文件中明定委外廠商所提供之財物或勞務之原產地不得為大陸地區。機關應參考經濟部投資審議委員會(下稱投審會)公告之陸資資訊「具敏感性或國安(含資安)疑慮之業務範疇」，應於招標文件中載明不允許投審會公告之陸資資訊服務業者參與，以限制大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商之參與。

●WTO 政府採購協定

世界貿易組織(WTO)政府採購協定(Agreement on Government Procurement, GPA)係於 1993 年關稅暨貿易總協定(GATT)烏拉圭回合談判中議定，目的為促成世界貿易更高度之自由與擴展，並改善世界貿易行為之國際架構。因此協議我國政府機關於採購產品或服務時，不得以保護國內產品或服務或國內供應商之理由，對國外產品或服務或國外供應商有所歧視，以增加透明度並建立磋商、監督及爭端解決機制。故政府機關於辦理資訊委外業務時，若涉及對國外產品或服務之採購事宜，宜遵循 WTO 政府採購協定，相關訊息請參閱工程會網站「政府採購」連結下之「政府採購條約協定」。

3.1.3.3 邀請廠商提出對應措施方案

機關辦理資訊委外作業時，可針對各項資通安全需求，於規劃時徵詢委外廠商提供相對應之建議措施，以符合我方最大利益，並經由 RFI 或 RFC 等方式，廣納各界意見，據以訂定實際可行之 RFP；另為達到資訊委外透明與公平公開，重要資訊專案委外於正式公告招標前，亦可綜合 RFI 或 RFC 文件所蒐集之資料，研判各家廠商於資通安全防護做法與概略之經費需求。

3.1.3.4 建立資訊委外資安管理計畫

機關應依據資訊委外資安策略與來自廠商之回饋內容，對委外個案應具備

之資安需求項目進行詳細分析，並將之具體化為資訊委外資安管理計畫，以提供擬訂委外契約書、RFP 及 SLA 之依據，確保資安要求之全面與一致性。資訊委外資安管理計畫應包含(但不限於)下列項目：

- 所規劃取得產品或服務之規格，包含其範疇、使用對象、利害關係人、類型及本質。
- 於委外專案期間需存取之資訊資產(如伺服器、資料庫、應用系統、網路基礎設施等)與其擁有者。
- 委外廠商之資訊資產分類分級與資通系統防護需求分級等相關資安控制措施，至少應採取與機關資安管理水平相同之方法。管理水平相同並非指相同之管理措施，而是在可控之風險等級下，施行管理強度一致之控管機制。例如當機關提供機密等級資訊予委外廠商時，委外廠商對此資訊之保護等級至少須等同機關保護機密等級資訊之控管相同，包含該資訊之存取、傳輸及複製限制等管控。
- 委外專案之生命週期各階段應有之角色與責任，機關可視需要成立跨部門資安小組，以推動下列事項：
  - 跨部門資通安全事項權責分工之協調。
  - 應採用資通安全技術、方法及程序之協調研議。
  - 整體資通安全措施之協調研議。
  - 資通安全管理計畫之協調研議。
  - 其他重要資通安全事項之協調研議。
- 依委外產品或服務之本質，確認過往同質委外專案資安事件之矯正預防措施，以做為本次委外資安強化之參考依據。
- 機關所屬管轄權內之法律法規要求事項，以及於選任委外廠商期間，應

審查可能約束委外廠商之法律法規，例如：

– 於「3.1.3.2 識別委外廠商之限制」所識別之限制。

– 出口管制。

– 個人資料保護法與勞動相關法規。

– 資通安全管理法施行細則第 4 條。

– 第三方智慧財產權。

– 其他法律與法規之要求事項，諸如稅法、產品責任或調查權。

●為可能取得之產品或服務指派特定資安角色與責任。

●針對可能取得之產品或服務，機關能與潛在廠商分享之資訊。

3.2 招標階段

本階段旨在遴選適宜之委外廠商，其資安管理熱點著重在 RFP 撰寫之完整度、評選準則中之資安要求符合度及在選商期間雙方資訊交換之安全性。本階段將導入 CNS 27036 中招標階段之最佳實務，以招標過程之時序為架構，敘述各作業應注意之資安事項，過程包含定義委外廠商評估準則、備妥保密協議書、備妥招標文件、蒐集廠商投標文件及評選服務建議書等作業。

3.2.1 委外廠商評選準則之定義與實作

招標階段之首要作業即需依「3.1.3.1 建立資訊委外資安策略」所定義之委外廠商評選準則項目與「3.1.3.4 建立資訊委外資安管理計畫」內容，定義並實作委外廠商評選準則，其應包含(但不限於)下列各項：

●委外廠商對招標文件定義之資安要求事項接受度。

- 委外廠商之資安能量。
- 委外廠商允許機關或經授權之第三方稽核，以確認所定義資安要求事項之遵循性。
- 先前由機關或不同委外廠商運作或製造之可能採購產品或服務之移轉計畫完整度。
- 於委外關係終止時，終止計畫之完整度。
- 委外廠商對其產品或服務之容量管理機制。
- 委外廠商之財務優勢。
- 委外廠商位置與提供產品或服務之位置，機關應特別考量此因素，以利識別機關與委外廠商間法律法規差異所造成之所有潛在法律法規風險，並確保適用於委外廠商之法律法規義務，在資安方面不致對委外關係協議有不利衝擊。此外，亦可評估諸如當地犯罪率或地理議題等環境威脅。

3.2.2 保密協議書準備與簽訂

當選商過程中存在資訊資產移交(如資訊交換)，機關應備妥保密協議書，並於交換任何可能與採購產品或服務相關之資訊前簽署。若前述情況不允許，機關應定義得以交換之資訊類別或內容，並取得資訊擁有者同意，以避免過多或不必要機密資訊被揭露。

3.2.3 招標文件之制定與發布

招標文件包含項目眾多，機關在制定相關文件時，可參考工程會網站中「政府採購」→「招標相關文件及表格」連結下之相關文件與表格，包含「投標廠商聲明書範本」(詳見附件 9)與「投標須知範本」(詳見附件 10)等。而下列僅提出與資安相關內容之建議，包含契約條款、RFP 及 SLA

等之撰寫注意事項。

3.2.3.1 採購契約

資訊委外之契約書為機關與委外廠商執行委外作業之法定文件，內容可參考工程會網站中「政府採購」→「政府採購條法規」→「子法」→「正式通過子法」連結中之「採購契約要項」。

契約書係機關與委外廠商間就資訊委外契約所為之詳細規定。機關在借重廠商之專業資源處理自身資訊業務時，除要求廠商遵守相關法律法規(如個資法)外，更須明示廠商義務與責任，以降低機關須負擔之風險。機關於制定契約時，應衡量其公平性，並尋求機關內法務單位或具備資訊與法律專業之顧問協助，以免於契約履行出現紛爭時與廠商陷入僵局，甚至產生對己不利之狀況。

針對資訊服務採購，機關可參考工程會所提供之「資訊服務採購契約範本」(詳見附件 11)，或於工程會網站中「政府採購」→「招標相關文件及表格」連結中下載最新版本，並依所識別之資安需求與限制，酌予修改。另外，工程會於民國 112 年 9 月 25 日函頒「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」(詳見附件 12) ，將其納為「資訊服務採購契約範本」之附件，由機關視個案特性將所列資安事項納入契約辦理，該表之資料或系統類型屬普級部分之資安要求訂於 113 年 3 月 1 日正式施行，中、高等級則訂於 113 年 8 月 1 日正式施行。

3.2.3.2 建議書徵求文件(RFP)

RFP 為廠商執行資訊委外之需求依據，其中應明定委外廠商之責任與義務，而針對資安管理部分，機關應特別謹慎訂定相關規範要求，或要求投標廠商於投標之服務建議書中提出相對應做法。在此建議機關可依下列項目進行(詳見表 5)，以研擬妥適之 RFP。

表5　撰寫 RFP 主要工作項目

項次	工作項目
1	確認專案目標
2	界定專案範圍
3	掌握業務與資通系統現況
4	蒐集現行資訊軟硬體作業環境
5	釐訂需求內容
6	制定服務水準指標
7	規範交付項目與內容
8	訂定專案管理需求
9	訂定評選標準與方式
10	參考機關契約條文、資訊服務採購相關手冊與指引
11	RFP 撰寫大綱

資料來源：政府機關資訊通報第 325 期

●確認專案目標

專案成立旨在達成機關之政策方向與專案目標，故專案負責人應先向主管與業務單位確認專案目標，以確保 RFP 內容、後續廠商所提之建議方案及資訊服務成果符合專案目標。

●界定專案範圍

專案範圍主要受限於採購經費與專案預定完成時間，機關應通盤考量專案所涵蓋單位、涉及業務及專案本質(即不同之委外類型)。

●掌握業務與資通系統現況

專案負責人應確實掌握機關現行業務狀況，包含作業流程、各作業項目內容與相關人員、資料量及作業量等資訊，並能在 RFP 內清楚描述，以利廠商能精準評估專案服務內容。

●蒐集現行資訊軟硬體作業環境

專案負責人應確實掌握機關現行資訊環境，如整體網路與硬體配置架構圖、伺服器作業系統概述及資料庫系統概述等，以利於撰寫 RFP 時，能依此提出適切且具整合性之技術建議。

●釐訂需求內容

此為 RFP 之核心工作，除與需求單位充分通溝與討論以得出具體、明確及可行之需求規格外，本指引旨在協助機關識別必要之資安控制措施，務必使該資訊委外專案之資安風險可控並降至最低，故機關應根據「3.1.3.4 建立資訊委外資安管理計畫」，仔細考量必要之資安要求事項，使委外廠商能準備其計畫書與理由闡述，本節後續篇幅將提供相關資安要求以供參考。

●制定服務水準指標

機關應制定服務水準，以監督廠商之服務品質，機關可參考「3.2.3.3 服務水準協議(SLA)」內容。

●規範交付項目與內容

機關應依專案類型規範各交付項目之具體內容，如交付各類計畫、報告、手冊及系統文件等，並應清楚敘明內容大綱與各分項之簡要說明，以避免廠商交付項目內容與預期成果不符。

●訂定專案管理需求

為增進專案品質，機關應要求廠商敘明專案組織與人力、人員角色與責

任、工作流程與查核點、專案工作細部期程、交付項目與時程、定期工作審查會議、風險與變更管理、品質管理、驗收計畫及資安管理等方法與內容，以做為履約監控依據。

●訂定評選標準與方式

依專案類型與需求制定評選項目、評選子項、配分及評分重點等內容，並就評選程序、評選方式、計分標準等進行規劃，更進一步之資訊可參考工程會所制定之「資訊服務評選項目及配分權重範例」[11]。

●參考機關契約條文、資訊服務採購相關手冊與指引

RFP 品質是影響資訊委外作業成敗之重要因素，因此機關可善加參考權責主管機關所訂定法規、各類參考手冊及範例文件，例如工程會所制定之「機關委託資訊服務廠商評選及計費辦法」、「資訊服務評選項目及配分權重範例」及「資訊服務採購契約範本」，以及相關採購手冊及範例[12]等。

●RFP 撰寫大綱

機關撰寫 RFP 時，可參考表 6 所列之建議大綱撰寫，再依據專案性質與預算額度進行裁適。

表6　RFP 內容大綱撰寫建議

章	節	小型	中型	中大型	大型	巨型
		<1 百萬	>=1 百萬	>=5 百萬	>=1 千萬	>=2 千萬
		標註項目 –V：必要，O：視需要				
壹、專案	一、專案名稱	V	V	V	V	V

章	節	小型	中型	中大型	大型	巨型
		<1 百萬	>=1 百萬	>=5 百萬	>=1 千萬	>=2 千萬
		標註項目 –V：必要，O：視需要				
概述	二、專案機關與專案使用者	V	V	V	V	V
	三、專案背景	O	O	O	V	V
	四、專案目標	V	V	V	V	V
	五、專案範圍	V	V	V	V	V
	六、專案期程	V	V	V	V	V
	七、專案預算	V	V	V	V	V
貳、現況與問題說明	一、現況說明	O	O	V	V	V
	二、問題說明	O	O	V	V	V
參、專案工作需求	一、專案整體需求	V	V	V	V	V
	二、資訊系統應用需求	O	V	V	V	V
	三、介面系統應用需求	O	O	O	V	V
	四、IT 環境需求	O	O	O	V	V
	五、系統測試與系統上線	O	O	V	V	V
	六、新舊系統轉移管控	O	O	O	V	V
	七、服務管理需求	O	V	V	V	V
	八、資通安全需求	O	O	V	V	V
肆、專案	一、專案期程	V	V	V	V	V

章	節	小型	中型	中大型	大型	巨型
		<1 百萬	>=1 百萬	>=5 百萬	>=1 千萬	>=2 千萬
		標註項目 –V：必要，O：視需要				
管理需求	二、專案管理	V	V	V	V	V
	三、專案組織與人力	V	V	V	V	V
	四、專案費用	V	V	V	V	V
	五、交付項目與規範	V	V	V	V	V
	六、履約規範與罰責	V	V	V	V	V
	七、推廣宣導	O	O	V	V	V
	八、教育訓練	V	V	V	V	V
伍、驗收與付款	一、驗收	V	V	V	V	V
	二、付款	V	V	V	V	V
陸、建議書製作規定	一、製作原則與內容	O	O	V	V	V
	二、裝訂格式	V	V	V	V	V
	三、建議書交付事宜	V	V	V	V	V
柒、評選作業	一、評選作業流程	O	O	V	V	V
	二、評選項目與評分	O	V	V	V	V
	三、優勝廠商評定方式	O	V	V	V	V
附件		O	O	O	O	O

資料來源：政府機關資訊通報第 325 期

機關在依據上述大綱撰寫 RFP 時，應力求內容清楚、嚴謹及具體，避免有模稜兩可或彈性之解釋空間，以減少履約爭議。此外，RFP 宜儘可能

僅包含公開或解密資訊，並僅包含允許委外廠商可合理回應之必要資訊。故在任何情況下，RFP 不宜包含機敏性資訊。

以下篇幅將著重於機關於制定 RFP 時，應注意下列資安環節：

●投標廠商背景資格限制

根據政府採購法第 36 條所述，機關辦理採購，得依實際需要，規定投標廠商之基本資格。特殊或巨額採購，須由具有相當經驗、實績、人力、財力及設備等之廠商始能擔任者，得另規定投標廠商之特定資格。外國廠商投標資格與應提出之資格文件，得就實際需要另行規定，必須提供經公證或認證之中文譯本，並於招標文件中訂明。上述所提及之基本資格、特定資格及特殊或巨額採購之範圍及認定標準，由主管機關定之。

機關應參考「3.1.3.2 識別委外廠商之限制」，將所識別之限制載明於 RFP 中。機關亦可要求廠商於「服務建議書」之「廠商能力與經驗」中補充說明，以便於進行廠商之過濾工作。內容可包含主要資金來源、委外工作位置、參與專案之人員及專案分包廠商等。

●投標廠商專案人員之背景調查

當機關對於委外廠商專案人員有背景調查需求時，亦應載明於 RFP 中，取得施行之共識。機關應考量下列情況，確認背景調查之需求：

– 如「3.1.3.2 識別委外廠商之限制」小節中之「涉及國家機密之執行人員限制」所述，受託業務若涉及國家機密，則執行廠商之相關人員應接受適任性查核。如經適任性查核認為不適於繼續執行專案者，廠商應將其調離專案團隊。

– 廠商執行專案時，機關如認為其參與人員或分包商人員，必須接觸到機密性或敏感性資料者，應要求其接受素行調查，如經素行調查認為不適於繼續執行專案者，委外廠商應將其調離專案團隊。

– 廠商派遣人員或指定之分包委外廠商人員，應於開始投入專案執行前，取得上述人員個人之書面同意，允許機關對上述人員進行素行調查，並提供必要之合作。素行調查，包含有無犯罪紀錄、財務與信用狀況及進出入國境等調查，上述做法如執行有窒礙時，建議可由廠商主動提供相關資訊予機關進行審驗。

●委外工作地區限制

為確保委外產品或服務之安全性，機關可考量於 RFP 中規定，不得將其一部分或全部之工作移至對大陸地區或其指定排除之國家進行，亦可要求廠商提出「同意不將專案移至境外執行聲明書」。

●排除外國人參與專案

為確保委外產品或服務之安全性，機關可考量於 RFP 中規定，禁止將其一部分或全部之工作交予非具備中華民國國籍員工執行，亦可要求廠商應提出「同意不將專案交予外國人執行聲明書」。

●投標廠商專案人員之專業資格限制

針對委外廠商將承接該委外產品或服務之人員，各機關可依委外作業型態、委外規模大小及專案機敏特性，訂定其專長、能力、資格及專業證照等相關條件限制。下列為常見之限制條件，但不以此為限：

– 委外廠商是否通過 ISMS 驗證，或擁有相關驗證，例如 CMMI。

– 相關規劃或顧問諮詢之業績案例。

– 委外廠商專案成員擁有之資安專業證照；各機關可依委外作業型態、委外規模大小、專案機敏特性及預算資源考量選擇，但不以下列為限：

➢資安專業相關證照，如 CISA、CISM、CRISC、ISSAP、ISSMP、

CNS 27001 LA、ISO 27701 LA、CEH 及 CSSLP 等。

- 若為滲透測試委外服務，宜擁有 CEH、CPENT、CompTIA PenTest+、CPSA、OSCP 等其他資安相關專業證照。
- 若為 ISMS 輔導顧問諮詢服務，宜擁有 CISA、CISM 或 CNS 27001 LA 等同質性資安證照。
- 若為系統發展類之軟體開發，顧問訓練類之系統稽核與軟體驗證(原始碼檢測)，宜擁有 CMMI 或曾接受「撰寫安全程式碼」相關訓練，或取得 CSSLP 資安證照。
- 若為維運管理類之整體委外、網路及資安服務等，宜擁有 ISSAP、ISSMP、CISSP 或 CNS 27001 LA 等同質性資安證照。
- 若為雲端服務類，宜擁有 CCSP(Certified Cloud Security Professional)、CSA(雲端安全聯盟)或英國標準協會(BSI)所推出之 STAR 等相關認證。

更多相關的資通安全證照清單，可參考行政院國家資通安全會報所制定之「資通安全專業證照清單」。

●專案組織與人力安全需求

– 要求委外廠商依專案特性，成立專案組織並指定專案管理人員，負責推動、協調及督導資通安全管理事項。

– 要求委外廠商對組織成員明訂其專案職掌與業務分工，敏感性作業需對成員適當性進行篩選，包含人員角色、人員責任及人員背景，並對成員施行適當之資安認知教育訓練。

●委外廠商適任優勢列舉

機關於訂定 RFP 時，可要求廠商於服務建議書中說明自身條件與資格，

並斟酌納入評選標準表內。其列舉內容依委外類型之不同而不同，可能包含事項如下：

– 對於產業知識之掌握與了解。

– 同類產品或服務之經驗。

– 客戶多寡與市場占有率。

– 企業規模與財務穩定性。

– 廠商之聲譽與口碑。

– 與客戶法律訴訟情形與歷史紀錄。

– 產品性能、品質及可靠度。

– 軟硬體技術能力。

– 資通安全技術能力。

– 廠商服務與支持能力。

– 專案管理能力。

– 專案人員數量、資歷、專長及學經歷。

– 專案管理之資安作為，例如適切人員資安認知、教育及訓練、存取權限管理、懲處準則、專案終止或變更之條款及資產歸還等。

– 委外廠商企業社會責任施行之成熟度。機關可於 RFP 中請廠商於服務建議書中提出其對企業社會責任報告書或宣示，列入招標評審加分項目。

●採購產品或服務之資安要求事項

RFP 中詳細陳述對欲採購產品或服務本身資安要求，故機關應根據

「3.1.3 委外資安需求識別」所得結果，在此將其內容具體化為詳細、合適及與成本相對稱之資安要求事項。於撰寫資安要求事項時，至少應包含下列項目：

– 識別委外標的應遵循之相關法規命令，以確保其資訊作業本身之資安控管。例如對於委外辦理資通系統建置、維運或資通服務之提供，在選任與監督廠商時，應遵循「資通安全管理法施行細則」第 4 條內容；對於契約內各項資通系統，機關可要求投標廠商，依「資通安全責任等級分級辦法」採行適當安全控制措施，以確保資訊系統達到應具備之資安防護水準。

– 於委外專案各階段，對委外廠商人員與其將接觸之資訊資產，應有必要之資安管理要求。故機關可於 RFP 中要求廠商提出資安管理計畫，並確保其資安管理強度應至少等同於機關，其內容可能包含(但不限於)下列項目：

  - 專案期間將接觸之資訊資產範圍。
  - 資訊資產分類分級、資通系統防護需求分級及其生命週期各階段之可接受使用原則。
  - 資訊資產所有權與智慧財產權之歸屬原則。
  - 專案人員籌組、資安角色與職責及異動時之規劃。
  - 專案人員於專案期間，維持資安認知與持續接受資安管理訓練之規劃。
  - 對專案期間所接觸之資訊保密作為。
  - 於機關所屬場所內工作時將施行之資安作為。
  - 依資訊資產特性，防範異常或未經授權存取之措施，如系統開發時

防範資安漏洞、購入雲端服務時防範後門程式等。

- 資通安全事件之管理機制。
- 專案終止之資安措施。

然而不同資訊委外類型，有各別應注意之資安重點。針對常見之委外作業，本指引將於「4.1 常見機關資訊委外類型資安注意事項」提供應注意之資安重點與提供可參考之來源依據。

- 保固服務

機關應考量委外專案之性質，與廠商約定保固服務，即當系統異常造成全部或部分作業無法正常運作時，若可歸責於廠商，廠商有義務依契約規定，進行異常之排除。故機關可於 RFP 中要求廠商提出保固計畫，以說明廠商對於異常作業處理程序與做法。計畫中應考量事項可包含(但不限於)下列事項：

– 重大變更之識別與紀錄。

– 規劃與測試變更內容。

– 評鑑此類變更之潛在衝擊，包含資安衝擊。

– 申請變更之正式核准程序。

– 向所有相關人員通報變更細節。

– 變更之復原程序，包含不成功變更與預期外事件之中止與復原程序與責任。

- 常見資訊委外專案 RFP 範例：

– 附件 3「Web 網站建置與個人資料管理維運」RFP 資安需求範例。

– 附件 4「Infrastructure 基礎設施建置與維運管理」RFP 資安需求範例。

– 附件 5「雲端服務商提供資訊系統部署、託管及維運服務」RFP 資安需求範例。

– 附件 6「政府機關資訊安全管理系統(ISMS)顧問輔導」RFP 資安需求範例。

– 附件 7「政府機關資訊安全管理系統(ISMS)公正第三方驗證」RFP 資安需求範例。

3.2.3.3 服務水準協議(SLA)

在資訊委外作業中，「委外服務水準之管控」被視為委外服務成敗重要因素之一，於管控作業上，藉由明確服務項目與水準指標，建立清楚管理制度，確保服務水準，建立考核與輔助措施，有效掌控問題發生與處理過程結果，所有使用者在選擇服務水準上，享有符合服務水準規範一致服務。

對於資訊委外作業而言，服務水準管控可以系統之可用率、作業效能、安全性及作業稽核等 4 大類指標，為服務水準協議規範之主要指標，其中作業效能與系統安全較無關連，宜由各機關自行訂定，故不述，其餘如系統可用率、安全性及作業稽核各項相關說明如下：

●系統可用率

系統可用率常被簡單地描述成系統在整個時段中，必須維持正常作業之特定時間，或者是可定量控管系統當機時間。對於使用者而言，系統可用率，常是影響他們對服務水準評量最重要因素，而系統可用率高低好壞，直接影響到使用者生產力與政府機關整體資訊管理作業。基於系統安全考量，可訂定系統可用率指標，以確保系統維持一定服務水準。

●安全性

安全性管理是為有效控制來自於未被授權或錯誤使用方法去取用資料，修改資料而造成政府機關作業風險與巨大傷害，然而資通安全防護有效性，實務上是無法百分之百達成，為確保發生資安意外事件時可警示與正確處理，資通安全意外管制與通報處理程序皆為必備基本工作，完善處理程序可將發生損失與傷害降到最低程度。

資訊管理作業，常藉由系統安全、通信安全、人員管制及作業管制等方式達成安全性目標，透過這些方式整合，確保資訊系統(包含軟體、硬體、防火牆、資料庫及電信通訊等)之機密性與可用性，同時也可做為評斷政府機關現行作業整體安全性指標。

●稽核作業

於服務水準協議中，提升績效並符合需求，必須持續不斷改善管理各項相關作業，因此稽核作業被視為是重要管理工具。如發現不符合事項時，訂定矯正或預防措施完成時限，以利追蹤稽核作業服務水準。

3.2.4 服務建議書之蒐集

蒐集由可能之委外廠商所提交回應招標文件之服務建議書，並依委外廠商評選準則評選之。而對於非客製化服務之取得(例如 ASP 服務)，機關應驗核委外廠商所提供之資安管理、控制措施、實作及服務等級皆符合委外廠商評選準則。

3.2.5 服務建議書之評選

招標之最後一步即對委外廠商所提出之服務建議書進行評選。但在評選服務建議書前，機關應選擇合格適任之評選委員，其中應考量其學經歷、相關領域實務經驗及利益迴避等條件，並向其強調有關遵守保密原則之事宜，詳細內容請參考 107 年 8 月 8 日工程會工程企字第 10700240070 號令修正發布「採購評選委員會組織準則」第 6 條相關規定。具備適當評選人

員後，評選內容分為 2 個重點，其一為投標廠商資格，另一個則為整體產品或服務之內容。

●投標廠商資格

機關應對投標廠商之背景資格限制進行嚴格審核。必要時，審核欲採購產品或服務所涉及之供應鏈廠商背景資料。對於投標廠商背景資格審核方式，可採用下列機制：

– 由投標廠商自行聲明陳述；可參考工程會所提供之「投標廠商聲明書範本」(詳見附件 9)。

– 為利機關查詢投標廠商是否為陸資廠商，可至工程會「政府電子採購網」查詢投審會網站公告之「陸資投資事業名錄」、「具敏感性或國安(含資安)疑慮之業務範疇」及「陸資投資資訊服務業清冊 」3 項資料表。

●整體產品或服務內容

機關應考量整體產品或服務供應鏈中有較佳透明度，且保證符合機關於招標文件中所定義之資安要求事項者，服務建議書評分表範例詳見表 7。

表7　服務建議書評分表範例

章節	說明	評分比重	備註
壹、投標廠商能力與經驗	一、投標廠商組織與資本額 二、投標廠商對於專案之能力與經驗 三、最近 3 年類似專案營業額	20%	
貳、專案技術能力	一、整體系統架構建議 二、專案提供設備建議 三、專案軟體技術建議 四、專案資安技術建議	40%	

章節	說明	評分比重	備註
	五、其他		
參、專案管理能力	一、專案組織 二、專案時程 三、專案執行方式 四、專案維運方式或保固服務 五、投入專案人數、技術能力及資歷	20%	
肆、專案成本分析	一、專案人力成本 二、專案系統軟硬體成本 三、專案資安成本 四、專案維運成本 五、其他成本(例如：保險)	20%	
註：專案技術能力、管理能力及專案成本等係評分內容，請依專案特性自行調整			

資料來源：本計畫整理

3.3 決標階段

決標階段之重點即與得標廠商進行簽約作業，即機關與委外廠商雙方依據招標文件與廠商回應之服務建議書進行最終協議，並於達成協議後，雙方啟動委外專案，機關則進入委外關係管理階段(即履約管理階段)。前者所提及之協議包含(但不限於)下列項目：

- 符合機關之招標文件與符合委外廠商之服務建議書，尤其指委外廠商應遵循之資安要求事項、產品或服務交付期間及服務水準指標等。
- 於委外作業範圍內，載明機關與委外廠商雙方之資安角色與責任。
- 闡明委外廠商分包計畫(若有)對委外標的可能產生之資安風險。

- 闡明先前由機關或由不同委外廠商所提供產品或服務之移轉計畫與其資安要求事項，以確保其持續性。
- 闡明資安變更或資安事件之處置程序。
- 敘明機關將監視與執行委外廠商所定義資安要求事項遵循性，包含監視活動型式(如資安風險分析或稽核)、矯正措施管理與追查機制等。
- 闡明委外產品或服務之智慧財產權。
- 闡明機關或委外廠商擁有於其執行期間終止該協議權利之情況，例如當委外廠商無能力履行所協議之資安要求事項。
- 闡明於未遵循協議所要求資安事項，加諸於機關或委外廠商之罰則。
- 闡明當委外過程中出現爭議時，可選擇之處置方式，例如：向採購申訴審議委員會申請調解或向仲裁機構提付仲裁等。若雙方對於問題標準界定上有所爭議時，可蒐集發生之事證與相關資訊，尋求具公信力第三者、學者專家、法院或調解委員會(如工程會)等，進行問題釐清與相關問題調解。
- 定義資安義務與有關委外關係終止執行之服務持續性要求事項，即定義終止計畫，其應包含(但不限於)下列項目：
  - 若決定將產品或服務由原委外廠商移轉回機關或至另一個廠商時，原委外廠商與機關雙方應遵循之資安要求事項。
  - 承上，明列實施交接期間之相關訓練。
  - 明列使用於委外專案中所涉及之資訊資產，以利於專案終止時得以完整歸還於雙方、轉交予另一個廠商或確保其銷毀。
  - 承上，明列歸還、轉交或銷毀之程序，必要時要求其落實之證明文件。

– 當委外關係終止後，保密承諾之持續性。

– 終止程序執行之時限。

於雙方協議並確定契約內容後，即進行簽約作業。簽約程序中應確認廠商是否完成保密切結與完成專案編組等事宜。例如：得標廠商於簽約前須依據招標文件規定，提出各項保密切結，並就機關需求規劃資通安全管理措施，廠商專案組織人員之遴選與質量需考量重新調整，並賦予適當職掌，以利承辦單位依據契約執行各項查核，並做成紀錄，相關文件要求如下：

●得標廠商與其專案工作成員應簽訂保密約定至少一式三份，並於指定期限內送交甲方一份備查。

●得標廠商應就專案建置過程中之文件資料與人員管控訂定保密安全規範，並應於契約生效日起一定期間(如兩週)內送交甲方，其後如有不足，並應適時修正之。

為扶植國內廠家，依採購法第 43 條第 2 款與該法施行細則第 46 條規定，機關於決標時可採行下列做法：

●機關辦理採購，除我國締結之條約或協定另有禁止規定者外，若外國廠商為最低標，且其標價符合第 52 條規定之決標原則者，得以該標價優先決標予國內廠商，並應載明於招標文件中。

●機關依採購法第 43 條第 2 款優先決標予國內廠商者，應依各該廠商標價排序，自最低標價起，依次洽減一次，以最先減至外國廠商標價以下者決標。

●前項國內廠商標價有二家以上相同者，應同時洽減一次，優先決標予減至外國廠商標價以下之最低標。

以最有利標辦理之委外業務，應依招標文件所規定之評審標準，就廠商投

標之技術、品質、功能、商業條款及價格等項目，作序位或計數之綜合評選，評定最有利標，於此階段應將資安要求納入評定項目，藉以實際反應委外廠商資安作業能量。另廠商若於建議書中增列說明其企業社會責任，則提醒評選委員納入加分項目。

3.4 履約管理階段

3.4.1 履約管理通則

當雙方確認契約內容並簽署後，委外專案將正式啟動，機關則應依據契約內容進行委外關係管理。其主要活動可能包含(但不限於)下列項目：

- 確保委外廠商收到最終協議，並完全了解其中包含之資安要求事項。
- 於專案期間，當未預期事件發生時，依議定之移轉計畫進行產品或服務移轉，並及時通知另一方。
- 依議定程序管理資安變更與處置資通安全事件。
- 對可能參與終止計畫執行之人員進行定期訓練。
- 於委外廠商通知時，管理未涵蓋於資安變更管理程序中，但可能影響委外專案之其他變更，例如：
  - 組織營運、使命或環境之變更。
  - 相關於組織財力之變更。
  - 組織所有權變更，或建立合資公司。
  - 委外產品或服務之獲取或供應之來源地點之變更。
  - 組織資安等級之變更，例如 CNS 27001 驗證之取得或失效。
  - 支援所要求營運持續能量之能力之變更。

– 適用於組織之法律、管理及契約要求事項之變更。

而機關應對上述之相關變更進行風險評估與管理，以確保變更所產生之資安風險於可接受之等級。

●與委外廠商議定協議之變更，並核准更新之。

●進行遵循性監視與專案執行活動符合度確認，並確保不符合事項矯正處置之執行或使用違約罰則條款。在此，機關應規劃監視之範圍、執行頻率及執行方式等。

3.4.2 委外關係管理與監督

以下就機關進行委外關係管理期間可能適用之資安控管項目進行詳細說明，機關應就委外專案之性質，參考適用之事項。

3.4.2.1 資通安全組織

3.4.2.1.1 內部組織

●機關與委外廠商皆應指定專案負責人員，負責推動、協調及督導下列資通安全管理事項：

– 資通安全責任之分配與協調。

– 資訊資產保護事項之監督。

– 資通安全事件之檢討與監督。

●委外專案宜視需要成立跨部門資通安全推行小組，推動下列事項：

– 跨部門資通安全事項權責分工之協調。

– 應採用之資通安全技術、方法及程序之協調研議。

– 整體資通安全措施之協調研議。

– 資通安全計畫之協調研議。

– 其他重要資通安全事項之協調研議。

3.4.2.1.2 行動裝置與遠距工作

●委外廠商專案人員所攜帶之行動裝置原則上禁止串接機關內部網路。當有業務需求時，應由機關專案負責人協助申請，經權責主管核准後始得執行。

●當委外廠商專案人員有遠距工作之需求時，應由機關專案負責人協助申請，經權責主管核准後始得執行。

●當有委外人員使用 VPN 連線至機關內部網路時，機關宜採用下列措施：

– 至少採用雙因子認證登入。

– 設置中間跳板機，避免直接連結內部資通系統。

– 安裝連線側錄軟體，記錄人員所有之操作行為。

●對於委外人員進行遠距工作之電腦設備或場所，機關亦應有相關資安規範。例如：用於進行遠距工作之筆記型電腦應安裝防毒軟體並於連線前更新病毒碼、該筆記型電腦登入帳號應具備一定複雜度之密碼組合等。

3.4.2.2 資訊委外風險持續識別

機關經由委外作業過程產生對機關資訊與資訊處理設施之風險，宜於核准委外廠商存取內部設施之前加以識別，並作適當之控制措施；若需要允許委外廠商存取機關之資訊處理設施或資訊，宜執行風險評鑑以識別特定控制措施之要求。

有關委外廠商存取風險之識別，宜考慮下列事項：

●委外廠商攜帶存取資訊處理設備與儲存媒體

– 處理設備，例如手機與電腦等。

– 儲存媒體，例如磁片、磁碟、光碟、隨身碟及報表等。

●委外廠商對資訊與資訊處理設施存取之型式

– 實體存取，例如辦公室、機房及檔案櫃。

– 邏輯存取，例如機關資料庫與資訊系統之連結與存取。

– 機關與委外廠商網路連接方式，例如固定連接或遠端存取。

– 存取發生於現場(On-Site)或場外(Off-Site)。

– 所涉及資訊價值與敏感性及其對營運之關鍵性。

– 保護禁止委外廠商存取資訊所必要之各項控制措施。

– 如何識別被授權存取之委外廠商或人員，如何查證該授權與多久需再確認一次。

– 與委外廠商於儲存、處理、通信、分享及交換資訊時，所採用之各種不同方法與控制措施。

– 當委外廠商需存取而無法存取時，以及因登錄或收到不精確或誤導資訊時之衝擊。

●有關委外廠商人員異動風險之識別，宜考慮於委外廠商專案成員人員調整與異動時，限期調整其權限。

3.4.2.3 資訊委外人力資源安全

為確保委外作業員工與委外廠商了解其責任，並勝任其所被認定之角色，以降低竊盜、詐欺或設施誤用風險，於資訊作業委以適當工作職掌，並依契約條款與條件闡明委外廠商應負之安全責任，進行充分適當篩選，尤其

是敏感性工作。

3.4.2.3.1 人員僱用前

●委外人員安全角色與責任

資訊委外時應對機關相關業務人員、委外廠商及分包與轉包商之安全角色與責任，依照機關資通安全政策加以界定與文件化，安全角色與責任包含下列要求：

– 依據機關之資通安全政策實作與行動。

– 保護資產不受未授權之存取、揭露、修改、銷毀及干擾。

– 執行特定之各項資安過程與活動。

– 確保已指派責任給採取行動之個人。

– 向機關通報資安事件、潛在事件或其他資安風險。

– 安全角色與責任定義時機。

– 安全角色與責任宜於資訊委外作業人員僱用前事先定義，且明確地傳達給受僱用者，工作描述能用以書面佐證其安全角色與責任。

●篩選

資訊委外作業人員之背景查證檢核

宜依照相關法律、法規及倫理，並兼顧機關營運要求之相稱性、存取資訊之保密類別與察覺之風險，由機關或委外廠商對所有資訊委外作業人員(含分包與轉包廠商)之背景進行查證檢核(Verification Check)，查證檢核時宜考量所有相關之隱私權與個人資料保護等相關法令。若允許時，宜包含以下控制措施：

➢是否有合格之品格推薦信或可資詢問者。

➢進用者之學經歷檢核。

➢確認應徵者所宣稱之學歷與專業資格。

➢獨立之身分檢核(護照或類似文件)。

➢更詳細之核對，如信用核對或犯罪紀錄檢核。

– 定義查證檢核之準則與限制程序

宜定義查證檢核之準則與限制程序，例如何人有資格篩選人員，如何、何時及為何執行查證檢核。

●僱用條款與條件

– 保密切結書

為保障委外作業安全，宜針對參與委外廠商之作業員工，經由個人同意並簽署其僱用同意書，該同意書陳述其與機關對資通安全之責任。

– 同意書宜反映機關之安全政策，並澄清與陳述：

➢被賦予敏感資訊存取權之資訊委外作業人員，宜於被允許存取資訊處理設施之前，簽署機密性或保密協議。

➢資訊委外作業人員之法定責任與權利，例如：關於著作權法或個資法規定。

➢資訊委外作業人員所處置資訊系統與服務相關之資訊分類和機關資產管理之責任。

➢資訊委外作業人員處理所收到來自其他公司或外部團體資訊之責任。

➢延伸至機關以外與正常工作時間以外(例如：在家工作)之責任。

➢資訊委外作業人員違反機關資安要求時所採取之行動。

– 機關宜確保資訊委外作業人員同意關於機關資通安全條款與條件，及其將會取得機關之資訊系統與服務存取權限之範圍與限制。

3.4.2.3.2 僱用期間

為確保資訊委外作業人員認知資通安全之威脅、關切事項、基本責任及強制責任，並有能力於日常工作中支持機關安全政策與降低人為錯誤之風險，宜界定機關與委外廠商管理階層之責任，以確保安全性施行。

另對參與資訊委外作業人員，宜提供妥適等級之資安程序與資訊處理設施之正確使用認知教育及訓練，以將可能之資安風險降至最低，並制定正式懲處程序，以處置資安危害。

●管理階層責任

– 機關組織內管理階層應要求資訊委外作業人員，依照機關已制定之政策與程序施行資安事宜，其責任包含：

➢確保資訊委外作業人員於被核准存取敏感之資訊或資訊系統前，正確地向其簡要說明資通安全角色與責任。

➢提供指導綱要給予資訊委外作業人員，述明機關內對其角色之資安期望。

➢激勵資訊委外作業人員符合機關之資安政策。

➢激勵資訊委外作業人員達到其在機關內所扮演角色與責任之資安認知等級。

➢激勵資訊委外作業人員符合僱用條款與條件，包含符合機關資安政

策與適切之工作方法。

➢激勵資訊委外作業人員持續擁有適切之技能與資格。

– 激勵工作之重要

若資訊委外作業人員未認知其資安責任，可能導致對機關巨大損害。受激勵之人員較少引起資通安全事件，而拙劣之管理可能令委外人員感覺被輕視，導致對機關資通安全之負面衝擊。

●資通安全認知、教育及訓練

– 機關宜對委外相關承包者與作業人員，使其接受與工作職務相關之認知與訓練作業，且定期更新機關政策與程序內容之適切性，並於核准存取資訊或服務之前進行認知訓練，內容以介紹機關之資安政策與期望。

– 持續不斷之訓練宜包含資通安全要求、法律責任及營運控制措施，以及資訊處理設施之正確使用訓練，例如登入程序、軟體套件之使用、安全程式之設計及懲處過程資訊。

– 有關資安認知、教育及訓練活動宜適切且相關於該人員之角色、責任及技術，並包含已知威脅資訊、更進一步建議聯絡人與通報資通安全事件之適當管道。

●懲處作業程序

– 資訊委外作業人員如有違反資通安全，宜有正式懲處過程，對於未查證資安違例已發生前，不宜執行懲處作業程序。

– 正式懲處過程宜確保涉嫌違反資安政策之員工得到正確與公平之處理。正式之懲處過程宜考量諸如違例之性質與嚴重性、其對營運衝擊、是否為初犯或累犯、違反者是否經過適當訓練、相關法律、營運

契約等因素及所需之其他因素，採取累進處罰。

– 於嚴重不當行為狀況下，宜允許立即停止其職務、存取權限及特權，必要時立即將其護送出該場域，懲處過程應適當以預防資訊委外作業人員違反機關資安政策與程序及其他安全違例。另有關委外廠商因違反契約，機關採取罰款之懲處方式如不符合委外案件承作金額之比例原則，可由委外廠商自行至工程會請求仲裁。

3.4.2.3.3 僱用終止或變更

為確保資訊委外作業人員以程序方式離開機關或變更僱用條件，確保資訊委外作業人員於離開機關時受到管理，並完成資訊業務之移轉交接、歸還設備及移除所有存取權限。

●終止責任

委外專案終止責任宜包含持續之資安要求、法律責任及機密性協議內之責任，以及於結束委外作業後持續一段界定期間之僱用條款與條件。

●資產歸還

機關於委外作業完成、契約或協議終止時，應歸還其保管所有機關資產。包含歸還所有先前分發軟體、機關文件及設備。其他如存取卡、軟體、手冊及儲存於電子媒體等資訊也需一併歸還，並保留執行紀錄，有關歸還方式建議如下：

– 若委外作業由委外廠商提供或使用設備時，宜將所有相關資訊移轉回機關並安全地自設備上清除。

– 若委外廠商擁有對進行中作業運作之重要知識，宜將該資訊文件化並移轉回機關。

●存取權限移除

資訊委外作業人員對資訊與資訊處理設施之存取權限，於其僱用契約、協議終止或因變更而調整時，宜重新考量資訊系統與服務相關之資產之存取權限。

應注意若為由管理階層發起之僱用終止，情緒不悅員工可能蓄意毀損資訊或破壞資訊處理設施；若為員工自行請辭，他們可能企圖為將來用途而蒐集資訊。

3.4.2.4 資訊委外實體與環境安全

為防止機關場所內資訊因委外作業而遭未經授權之實體存取、損害及干擾，關鍵或敏感之資訊處理設施宜置放於安全區域，經由適當之安全屏障與進出控制措施加以保護，確保這些設施免受未經授權之存取、損害及干擾。

3.4.2.4.1 安全區域

機關宜使用安全周界(如牆、卡控入口閘門或人員駐守之接待櫃檯等屏障)，以區隔委外作業與內部資訊處理設施之區域。

安全區域可為有門禁管制之辦公室，或有連續實體安全屏障之空間。在安全周界內不同之安全要求，可能需要額外之周界以控制資訊委外作業人員進出。

3.4.2.4.2 設備安全

- 應考量機關內因委外作業所需存取或資訊委外作業人員攜入之資訊設備，包含個人電腦、行動裝置、行動電話、可攜式儲存媒體、智慧卡及所有形式等，並注意設備攜出與攜入機關辦公環境之各種風險。
- 所有涉及委外作業設備，應確保其設備上軟體與韌體更新作業，並依資安政策設定合適帳號密碼，禁止使用原廠預設密碼。

●不管設備所有權屬誰，於機關場所內使用任何資訊處理設備均宜經過主管或/及安全事件管理階層之授權。

3.4.2.5 資訊委外管理

3.4.2.5.1 文件化作業程序

機關內操作程序宜加以文件化與維持，並讓資訊委外人員依其被指派工作項目，可隨時或經要求取得資訊處理與通信設施相關系統活動之文件化程序，如電腦開機與關機程序、備份、設備維護、媒體處置、電腦機房及郵件處置管理等，以供資訊委外作業人員遵循使用。

3.4.2.5.2 變更管理

因委外作業所產生之資訊處理設施與系統變更宜受控制，對於運作中之系統與應用軟體之變更，應嚴格管理控制並特別考量下列事項：

●重大變更之識別與紀錄。

●規劃與測試變更。

●評鑑此類變更之潛在衝擊，如安全衝擊。

●對所提議變更之正式核准程序。

●向所有相關人員通報變更細節。

●復原程序，包含不成功變更作業與意外事件中止與復原之程序與責任。

另機關宜有正式管理責任與程序，以確保對設備、軟體或程序之所有變更符合控制要求，變更完成後，宜保留一份內含所有相關資訊之稽核日誌。

3.4.2.5.3 職務區隔

職務區隔是降低意外或蓄意系統誤用風險方法之一，對於委外職務與責任

領域宜加以區隔，以降低機關資產遭未經授權或非意圖之修改或誤用產生，並注意無任何人員可未經授權或未受偵測之存取、修改或使用資產。

規模較小之機關或委外專案可能認為職務區隔難以達成，但建議儘可能實施此一原則。當職務難以區隔時，宜考慮其他控制措施，如活動監視、稽核存底及管理監督等。

3.4.2.5.4 委外開發、測試及運作

委外廠商廠宜分隔開發、測試及運作之設施，以降低對運作系統未經授權存取或變更之風險，並識別出於運作、測試及開發環境間可能產生之資安問題，採取適當之控制措施，並考慮下列事項：

- 於軟體開發階段導入安全程式開發，製作一套資安測試與評估計畫，實作此計畫，並將結果文件化。
- 將軟體由開發移轉到運作狀態之規則，宜加以定義與文件化。
- 開發與運作之軟體宜在不同系統或電腦處理器上運轉，且位於不同網域或目錄。
- 不能由現行運作之系統，存取編譯器(Compiler)、編輯器(Editor)及其他開發工具或系統公用程式。
- 委外測試系統環境宜儘可能逼真地模擬運作之系統環境。
- 對運作測試系統，宜使用不同使用者測試帳號，功能選單宜顯示適切之識別訊息以降低錯誤風險。
- 敏感資料不宜複製至測試系統環境

為使委外開發或維護資訊系統失效風險最小化，應預先規劃與準備，以確保有足夠容量與資源可達成所要求之系統效能，並對未來容量要求預作規劃，以降低系統超載風險，新系統驗收與使用之前，宜建立、記錄

及測試其操作要求，並採行下列審查措施：

– 要求提供授權文件、程式碼所有權及智慧財產權。

– 要求執行品質驗證與功能執行之準確性。

– 要求提供移交清冊，預防受委託者因故無法執行之託管協助。

– 工作完成時，提供稽核品質與正確性所需之存取權限。

– 要求依契約提供良好之程式碼品質。

– 應自行或交由第三方於安裝前進行測試，檢查是否有惡意程式、特洛伊木馬程式、隱密通道(Covert Channel)及 SQL Injection 等，並交付測試報告。

●系統需求評估

委外開發產製新系統被認可與納入正式作業之標準與執行要項如下：

– 評估系統作業效能與電腦容量是否滿足機關之需求。

– 檢查發生錯誤後之回復作業、系統重新啟動程序準備作業及資通安全事件之緊急應變作業是否已經完備。

– 進行新系統正式納入例行作業程序之準備與測試。

– 宜選定經評估過之安全控制措施。

– 有效之手動作業程序。

– 持續營運之管理要求。

– 評估新系統建置是否影響現有系統作業效能，尤其是現行系統於尖峰作業時段之影響。

– 宜考量新系統對機關整體安全造成之影響。

– 辦理新系統作業與使用者教育訓練。

– 宜考量是否容易使用，不影響使用者工作或提供客戶諮詢服務管道，並避免產生錯誤。

●適當之測試作業

於開發新系統時，應確定系統功能與效能可滿足機關需求，故在系統開發的每一階段，皆應充分諮詢相關人員之意見。於新系統上線作業前，應執行適當且全面之測試作業與資安檢測，以驗證系統功能符合既定之標準與資安需求。測試作業應依系統之特性進行規劃，可包含單元測試、整合測試、系統測試、壓力測試及使用者接受度測試等等。機關應保存所有之測試規劃、腳本及執行紀錄。

●第三者執行查核與驗證

如係委由第三者執行查核與驗證事宜，則應舉行專案聯席會議，確定專案進行程序與相關作業紀錄表單等，以確保專案能夠順利進行。

3.4.2.5.5 委外廠商服務交付管理

委外廠商服務交付管理旨在確保資通安全與服務交付與委外廠商所議定之協議一致，包含對委外廠商服務之監視與審查，與管理委外廠商服務之變更。

●委外廠商服務之監視與審查

機關宜定期監視與審查由委外廠商提供之服務，以確保委外廠商遵守協議中資通安全條款與條件，且資通安全事件與問題均受到妥適管理。機關應先依專案之性質與資安防護等級評估該資訊委外專案，依委外專案之重大性施行與其相稱之監視與審查活動，在有限資源下獲得最高之監視與審查效益。一般資訊委外案，委外廠商應遵循機關採購文件內載明

之資安相關要求。當委外專案風險較低時，機關可採用書面審查，而隨著委外風險升高，實地審查、自動化工具審查或其不同審查機制就視需要搭配進行。以下就依重大等級區分委外專案，並提供可使用之監視與審查機制供機關參考。

– 第一級為通案要求

所有資訊委外案，委外廠商皆應依循機關採購文件內載明之資安相關要求事項辦理，並需於資安要求事項變更時，重新評估風險。專案若超過 1 年者，建議機關應進行年度評估，以確認其風險並無改變。

– 第二級為書面審查

若經機關評估該資訊委外案風險較低，建議可採書面審查方式進行，其範圍可包含取得委外廠商之第三方審查報告(或驗證文件)、取得委外廠商內部稽核報告(僅與專案範圍相關)、要求委外廠商提供以自動化工具進行掃描後所產生之報告、要求委外廠商提出資安控管之相關執行紀錄、要求委外廠商填寫自我評估報告(或機關可提供問卷)。而執行頻率應依議定內容進行，或於發生異常或事件時進行。機關於進行上述之書面審查活動時，可視需要邀請機關之稽核單位、業務單位或 IT 單位等人員參與。

– 第三級為實地審查

若經機關評估該資訊委外案風險較高，建議可採實地審查方式進行，實地審查用意在於機關能深入了解委外廠商對所議定資安要求之落實度，機關可召集適切之稽核人員至委外廠商地點進行稽核。實地審查方式顧名思義即是至委外廠商執行委外活動之處所對相關人員進行訪談，確認所進行資安事項之執行證據。在預算及資源限制下，訪談進行亦可採用電話或視訊會議。若必要，此等級之委外專案亦可同時要

求進行書面審查。機關可參考附件 14「委外廠商查核項目表」，依委外類型進行調整。

然而，對於委外產品或服務最有效與及時之審查方式，即是要求委外廠商定期產出服務報告，並安排定期進度會議，以即時反映與管理相關議題。

委外廠商服務變更管理

對於委外廠商所提供服務之變更，包含維持與改進現有資通安全政策、程序及控制措施，應加以管理，並考量所涉及之營運系統與過程，並重新評鑑風險，實施委外廠商服務變更管理需考量：

– 網路變更與加強。

– 新技術使用。

– 新產品或較新版本發行採用。

– 新開發工具與環境。

– 服務設施實體位置之變更。

3.4.2.5.6 防範惡意程式與行動碼

機關於委外作業需要採取預防措施，防止與偵測惡意程式與未經授權行動碼之植入，以保護軟體與資訊完整性，管理者宜適時導入與實作控制措施，防止、偵測及移除惡意程式與控制行動碼。

3.4.2.5.7 資訊委外媒體處置

為防止資產被未經授權揭露、修改、移除或破壞而導致營運活動中斷，與委外作業有關之媒體宜加以控制與實體保護，並建立適切操作程序，以防止文件、電腦媒體(如磁帶與磁碟)、輸入、輸出資料及系統文件被未經授

權揭露、修改、移除及破壞。

委外作業過程中之資料(含書面與磁性媒體)，應進行妥善控管與處理，避免機敏資訊外洩，造成重大損害與賠償事件發生。

3.4.2.5.8 可攜式媒體管理

可攜式媒體包含磁帶、磁碟、快閃磁碟、外接式硬碟、光碟(CD)、隨身碟、數位視訊影碟(DVD)、手機、數位相機及印出等媒體，機關宜採取適當程序以管理資訊委外作業人員使用之可攜式媒體，以避免資訊外洩或惡意程式入侵，管理可攜式媒體宜考量下列原則(有關可攜式媒體管制詳細做法可參考電子資料保護參考指引)[13]：

若不再需要，任何從機關移除之可再利用媒體內容，宜使其無法復原(如備份之磁帶與可覆寫光碟片)。

若需要與實際可行時，從機關移除媒體應需授權，並保存該筆移除紀錄，以維持稽核存底。

委外廠商攜入可攜式媒體進機關應受程序管制或限制。

宜明確以書面記載所有程序與授權等級。

3.4.2.5.9 系統文件安全

機關提供或經委外作業產製之系統文件（如機關組織架構表、網路架構圖及系統程式碼等）宜加以保護，免遭未經授權之存取，並採行下列管控措施：

- 應於相關文件規定資通安全控制措施，以利使用者與電腦支援人員了解電腦系統內建之安控系統功能。
- 系統文件於每次完成變更作業後，應立即更新，舊版之系統文件亦應妥善保管與處理。

- 確保操作文件與使用者程序根據需要作適切變更。如資料庫與資料檔案、系統文件、使用者手冊、訓練教材、作業性與支援程序、營運持續管理計畫及預備作業計畫等。
- 要求資訊委外作業人員辦公桌面淨空政策，以減少文件與儲存媒體等在正常辦公時間之外，遭未被授權人員取用、遺失或是被破壞之機會。
- 應有正式資訊委外作業人員離職程序，顯示其已繳回機關資產，包含所發給軟體、文件及設備，如行動式電腦設備、憑證、手冊及其他必須繳回之電子媒體，並保留執行紀錄。
- 電腦與網路之日常管理作業，如開關機程序、資料備援、設備維護及電腦機房之安全管理之作業程序，應視為正式文件，作業程序變更必須經權責單位核准。
- 保護委外作業系統文件宜考慮下列項目：
  - 系統文件宜安全地存放並執行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
  - 系統文件存取清單宜保持最簡短並經應用系統擁有者授權。
  - 放在公眾網路上或透過公眾網路提供之系統文件宜加以妥善保護。
  - 系統文件可包含一系列之敏感資訊，如對應用過程、程序、資料結構及授權過程等之說明。

3.4.2.6 資訊委外使用者存取管理

為確保未經授權資訊委外作業人員對資訊系統存取，機關宜有正式程序，以控制資訊系統與服務存取權限配置作業，這些程序應從開始登記使用註冊，到最終不再需要存取資訊系統與服務註銷。宜特別注意特權存取權限之配置是否有控制必要，使用者註冊與註銷之存取控制程序宜包含：

- 檢核資訊委外作業人員是否經過系統擁有者授權使用資訊系統或服務；由管理階層另行個別核准存取權限也是適當方法。
- 檢核所授予存取權限等級是否符合營運目的，以及是否與機關安全政策一致，例如不會違反職務區隔。
- 給予資訊委外作業人員存取權限之書面聲明。
- 要求資訊委外作業人員簽署聲明，表示了解其存取限制。
- 確保服務提供者於完成授權程序前不會提供存取。
- 維持一份含所有註冊使用該服務之正式使用者紀錄。
- 機關可透過帳號、識別證及卡片等機制來管理資訊委外作業人員帳號，使每一位資訊委外作業人員具有「唯一」識別符，並可依識別驗證每一位使用者身分。
- 資訊委外作業人員因變更角色、調職或離職後，應立即移除或封鎖其存取權限。

3.4.2.7 資訊委外資通安全事件管理

為確保與委外作業相關之資通安全事件與弱點，能夠被採取及時矯正措施之方式傳達，委外機關宜備妥正式之事件通報與提報程序供委外廠商配合並施予合宜訓練，委外廠商宜認知可能對機關資產安全造成衝擊不同型式事件與弱點之通報程序，並要求所有人員儘快向指定聯絡點通報任何資通安全事件與弱點，通報程序應包含：

- 適當記錄資安事件之作業處理程序，以確保資安事件回報處理或撰寫資安事件檢討(或結果)報告。
- 資通安全事件報告格式可支援回報行為，並幫助回報人員記錄在資通安全事件所有必要之行為狀況。

●發生資通安全事件狀況後之正確行動

– 記錄所有重要細節(例如螢幕上出現錯誤訊息與奇怪現象)。

– 除規定之處理程序外(例如中毒時，應先行拔掉網路線以防止擴散)，應儘速通知相關人員前來處理，不要自己隨意執行任何動作。

●資通安全弱點之反映

– 資訊委外作業人員，應隨時注意資訊系統或資訊服務設施內部之資安弱點與可能面臨之威脅，並迅速向機關業務承辦人或主管報告。

– 系統安全上之弱點，應由專業人員處理，不應任由系統使用者自行修改。

●軟體功能不正常之反映

資訊委外作業人員發現軟體功能有異常時，應迅速向機關業務承辦人或主管報告，並要求權責資訊單位支援。

3.5 驗收階段

3.5.1 一般驗收程序

機關於執行「驗收階段」係依據契約文件與「履約管理」階段執行成果辦理，依採購法施行細則[14]第 90 條之 1 說明「勞務驗收，得以書面或召開審查會方式辦理；其書面驗收文件或審查會紀錄，得視為驗收紀錄」。一般資訊委外驗收不外乎上述兩種方式，機關為有效順遂驗收階段執行，可依下述建議要求委外廠商專案驗收內容與進度：

●委外廠商於簽約後一定時間(例如 15 個日曆天)內提交「專案工作計畫書」，以確認委外專案進行方式、專案組織、相關時程及資通安全要求事項等。

- 委外廠商須定期召開工作進度報告會議，並提交工作報告，內容應包含已執行之應完成重要工作項目、已完成工作項目、預計工作項目及問題與建議等。
- 於資訊委外作業執行過程中，依 3.4 履約管理階段應配合各階段需求，規劃並實施充足之教育訓練，並提供訓練教材，俾利資通安全管理制度建置工作順利推動，並提升資訊委外作業人員資安知識與技能。
- 完成 3.4 履約管理階段之 3.4.2.5.5 委外廠商服務交付管理，依機關要求格式，交付契約內要求之各項文件。
- 除上述專案文件外，委外廠商應衡酌各工作項目之性質與內容，詳述擬交付之文件或資料，並負責製作專案進行過程中每次會議之紀錄，交由機關確認。
- 製作結算驗收證明書，驗收完畢後規定時間(例如 15 個日曆天)內填具(採購法施行細則第 101 條)。
- 進行功能檢測，包含系統(網路)架構、人機介面及系統介面；非功能檢測，包含效能檢測、承載力檢測及資安檢測。除資安檢測將於下面章節詳述外，其他各項檢測需求，非屬資安範圍，請各機關依需求自行規劃。

3.5.2 資安驗收內容

於履約管理階段，機關隨著專案時間推移，監視與審查委外廠商是否遵循資安要求事項，而於驗收階段(若必要，可設定多個驗收點)，機關應為驗收範圍內產品或服務本身之資安要求進行嚴謹之把關。故在驗收階段，各資訊委外專案應特別注意下列事項：

- 顧問訓練類

顧問訓練類服務為純粹提供管理與技術服務，在完成顧問服務時即可得知是否符合機關要求。對於某些需由顧問使用軟體輔助才可完成專案之情況，應確認委外廠商是否使用最適之檢測工具與版本；而大多數本類之專案驗收可以滿意度訪問與調查來確認其執行成效。

●系統發展類

系統發展類服務通常除功能與效能測試外，應要求委外廠商提供該資通系統之安全性檢測證明，其中可包含確認無程式後門、進行程式原始碼檢測、弱點掃描或滲透測試等，避免日後因系統漏洞造成傷害。此外，當資通系統使用非委外廠商自行開發之元件時，宜要求委外廠商揭露第三方程式元件之來源與授權證明，以確保其元件非來自大陸地區或其他限制地區。

●維運管理類

維運管理類與顧問訓練類之服務類似，若維運過程有新發現程式漏洞，需進行程式修補者或定期進行程式弱點掃描外，一般狀況是每年定期執行系統弱點掃描。

●雲端服務類

雲端服務類與系統發展類相似，除確認功能與效能外，對於產品或服務之資安保證大多來自於委外廠商所提供之證明。機關應確認與評估雲端服務供應商宣稱之證認範圍，包含控制與評估涵蓋功能及服務。

3.5.2.1 委外關係終止

當專案如預期順利結束後，機關應立即停止委外廠商所涉及之實體與邏輯存取權限，並回收或請委外廠商銷毀屬於機關之資訊資產，必要時可要求委外廠商出具銷毀證明。若因該委外專案具有保固期，而無法執行上述項目時，機關應詳細審查委外廠商所擁有之存取權限適當性，以及委外廠商

所持有屬於機關之資訊資產必要性。

然而，若專案因未預期之情況，由契約其中一方決定終止，在驗收階段除依上述之驗收流程確認已完成之專案活動外，對於未預期終止之情況應至少執行下列事項：

- 釐清機關決定終止專案決策背後之資安動機。若有，機關應識別與評鑑與該資安動機相關之風險，並定義與實作其相對應之處置選項。
- 確認產品或服務之移轉程序。
- 定義與實作溝通計畫，以通知因委外專案終止而受衝擊之內部人員與第三方。
- 指派專人依終止計畫處理委外專案之終止。
- 確保委外專案過程中所涉及之所有資訊資產，並更新於資產清冊中。
- 確認使用於委外專案中所涉及之資訊資產之歸還、轉交予另一個委外廠商或銷毀。
- 確認委外廠商專案期間所取得之實體與邏輯存取權限之及時移除。

3.6 保固作業階段

3.6.1 保固服務

軟硬體系統完成驗收程序後進入保固期，期間不論軟硬體資產，應以維持驗收完成時之狀態為主要目的。各機關如因後續維護預算(經常門)編列有困難，而將部分系統維護工作整併於系統發展類之系統整合或軟體開發工作項目中，其所列方式應比照系統發展類之軟體維護或維運管理類服務方式處理，不宜與保固服務混為一談；例如其後續資安檢測作為，可比照列為維運管理類服務方式執行，不宜列為保固服務範圍。

3.6.2 異常管理

保固期間對於運作中之資訊處理設施和應用軟體系統，均應受到嚴格之變更管理控制，如系統有重大資安顧慮或瑕疵，經與委外廠商協調後，如屬委外廠商責任，需由委外廠商另提變更計畫，該計畫中宜特別考量事項如下：

- 重大變更之識別與紀錄。
- 規劃與測試變更內容。
- 評鑑此類變更潛在衝擊，包含安全衝擊。
- 申請變更之正式核准程序。
- 向所有相關人員通報變更細節。
- 委外廠商應先提供變更後新系統之復原程序，包含不成功變更作業與意外事件中止與復原之程序與責任。

保固期間系統如有委外廠商派駐人員協助者，發生異常事件時，應由派駐人員負責將問題反映至資訊業務承辦人員，再循正常程序陳報，否則仍應由資訊業務承辦人員循序陳報。

另機關宜有正式管理責任與程序，以確保對設備、軟體或程序之所有變更，符合控制要求。變更完成後，宜保留一份內含所有相關資訊之稽核日誌。

4. 資訊委外資安注意事項

本章分 2 部分，首先因應機關常見之 6 種資訊委外類型，彙整其應注意之資安事項，強化機關辦理該類委外專案時之資安風險管控。第 2 部分則跳脫條文式之敘述，以一資通系統委外維護案為例，第 3 章內容為基礎，依委外專案辦理時序，提供完整參考情境，加強機關對指引內容之理解，進而實現完善之資訊委外資安控管。

4.1 常見機關資訊委外類型資安注意事項

第 3 章以一般通用採購流程為架構，說明各階段之主要活動(詳見圖 6)與其應注意之資安事項，其中多數為通用概念，但仍有依資訊委外類型不同而應特別注意者，且該些注意事項極為重要，故本小節將特別針對 6 種機關常見資訊委外類型之資安注意事項進行說明。機關應了解下列所列舉事項並非窮舉，機關仍應依實際執行情況。

4.1.1 系統發展類－系統開發

機關於規劃資通系統開發專案時，應特別注意下列資訊委外資安注意事項與稽核重點：

- 資通系統安全防護基準

  於規劃系統開發類專案時，機關應先參考「資通安全責任等級分級辦法」附表 9 所訂之資通系統防護需求分級原則，以資通系統之機密性、完整性、可用性及法律遵循性等 4 大構面，評估該資通系統之防護需求等級。接續機關應依「資通安全責任等級分級辦法」附表 10 所訂資通系統防護基準列示之控制措施，識別應落實之資安相關事項，並載明於 RFP。

- 資通系統開發程序安全

– 針對資通系統開發程序，機關可參考資安院網站上之共通規範「安全軟體發展流程指引」、「安全軟體設計參考指引」及「安全軟體測試參考指引」。

– 若為 Web 應用程式，可再參考「Web 應用程式安全參考指引」。

– 若為行動 App 開發，可再參考產業署頒布之「行動應用 App 安全開發指引」。系統開發完成後，應要求委外廠商依產業署頒布之「行動應用 App 基本資安檢測基準」，委託第三方機構針對行動應用程式，進行資通安全檢測。機關可至網站 https://www.mas.org.tw/download/app 參考行動應用 App 相關資安規範。

– 若為雲端服務開發，可參考產業署軟體採購辦公室共同供應契約採購雲端服務之檢測規範(詳見附件 13)。

– 若為物聯網系統，可參考產業署所發布之 IoT 資安相關標準，例如：影像監控系統資安標準。機關可至網站 https://www.mas.org.tw/download/iot 確認 IoT 相關資安標準。

– 為確保委外開發資通系統原始程式碼之完整性與可用性，機關應要求委外廠商施行程式碼版控機制，例如使用 Git。並考量在必要之專案檢核點後，將程式碼版控軟體上之所有重要資訊進行備份，並留存相關稽核軌跡。

– 屬高度防護等級之資通系統，機關應加強資通系統原始程式碼之存取安全，宜考量採用類似 Virtual Desktop Infrastructure (VDI)之機制，使程式碼於開發與測試，甚至於維護階段，皆能在機關可控管之區域內撰寫與測試，以降低原始碼被惡意或非惡意外洩之風險。

●個人資料保護

若該資通系統涉及蒐集、處理及利用個人資料時，機關應將「個人資料

保護法」及其施行細則之要求納入資通系統開發需求中。

- 資通系統安全性檢測

  – 為確保資通系統之整體性安全，機關應遵循「資通安全管理法施行細則」第 4 條第 1 項第 5 款之要求，要求委外廠商提供該資通系統之安全性檢測證明。而舉凡與戶役政、健保、財稅資料庫相關之資通系統，以及與台灣地形、地物、氣象相關資料庫之資通系統開發與維護，皆應設有技術審查機制，以協助政府單位與委外單位於計畫執行上技術層面與程式碼之檢測。

  – 若該資通系統屬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，委外廠商於開發系統時，使用大陸地區或其他限制地區提供之軟體與硬體元件，應確認委外廠商使用之檢測工具與版本是否適當。

- 資通系統透明度之確保

  為持續確保系統安全性，機關應取得系統開發專案所有資訊，除最核心程式碼外，從開發初始階段之需求與設計文件，一直到測試、除錯及系統上線程序等。此外，當資通系統使用非委外廠商自行開發之元件時，宜要求委外廠商對第三方程式元件之揭露。

4.1.2 系統發展類－系統維護

系統維護案應注意之資安事項與「4.1.1 系統發展類－系統開發」大致相同，包含依系統防護需求等級識別應實作之資安控制措拖、持續遵循資通系統開發程序進行系統維護、持續注意個人資料保護、進行資通系統安全性檢測及留存資通系統相關變更文件與紀錄，確保資通系統之透明度等。而在系統維護專案中，機關應特別注意，當系統維護廠商與開發廠商不同時，應確保維護廠商務必在明瞭維護範圍所涉及之資安管控下，進行系統

維護或變更，以避免資安控管之失效、矛盾或斷層，詳見表 8。

表8　系統發展類應注意之資安事項與採購階段對應表

採購階段	應注意之資安事項	遵循依據
計畫作業階段	▪系統防護需求等級確認，識別應落實之資安相關事項，載明於 RFP，機關應遵循「資通安全管理法施行細則」第 4 條第 1 項第 5 款之要求，若該資通系統屬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，機關應自行或委託第三方進行安全性檢測 ▪系統開發程序應參考相關資通系統開發安全指引 ▪系統涉及蒐集、處理及利用個人資料時，機關應將「個人資料保護法」及其施行細則之要求納入資通系統開發需求中	▪資通安全管理法施行細則第 4 條第 1 項第 5 款 ▪資通系統開發安全指引 ▪個人資料保護法及其施行細則
履約管理階段	▪機關應遵循「資通安全管理法施行細則」第 4 條第 1 項第 5 款之要求，要求委外廠商提供資通系統之安全性檢測證明 ▪當系統維護廠商與開發廠商不同時，應確保維護廠商務必在明瞭維護範圍所涉及之資安管控下，進行系統維護或變更，以避免資安控管之失效、矛盾或斷層	資通安全管理法施行細則第 4 條第 1 項第 5 款
驗收階段	機關應取得系統開發專案所有資訊，除最核心程式碼外，從開發初始階段之需求與設計文件，一直到測試、除錯及系統上線程序等	CNS 27036-2

資料來源：本計畫整理

4.1.3 維運管理類 - 網路與資安服務(系統檢測)

●機關應辦理之項目

各級機關應依「資通安全責任等級分級辦法」附表 1、3 及 5 之要求，辦理安全性檢測與資通安全健診作業。安全性檢測包含網站資安弱點檢測與系統滲透測試；資通安全健診包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視等，辦理頻率依機關之不同級別而有不同。

●資訊委外資安注意事項與稽核重點

若機關欲將上述或其他維運管理類作業委外，除應於 RFP 中詳細說明委外作業本身之執行活動外，對於因該類委外作業而產生之資安風險，亦應在 RFP 中載明其資安控管要求。由於本類作業委外之本質大多是讓委外廠商操作或存取機關之資訊資產，故在此情況下，其資安控管重點如下：

– 委外人員：機關應要求委外廠商對於其人員，實施至少等同於機關管理內部人員之資安強度。

– 資通系統：機關應參考「資通安全責任等級分級辦法」之附表 9 與附表 10，依系統防護需求等級識別應實作之資安控制措施。

4.1.4 維運管理類 - 網路與資安服務(系統監控)

●機關應辦理之項目

各級機關應依「資通安全責任等級分級辦法」附表 1、3 及 5 之要求辦理建置資安威脅偵測管理機制，並持續維運與依主管機關指定之方式提交監控管理資料。

●監控範圍與有效性

建議將資通安全責任等級分級辦法內之資通安全防護項目，如防毒軟體、網路防火牆、電子郵件過濾機制、入侵偵測及防禦機制、核心資通系統之應用程式防火牆、進階持續性威脅攻擊防禦措施、端點偵測及應變機制等納入監控範圍考量。監控之有效性包含回傳能力、監控偵測能力及資安監控情資品質。回傳能力之評估指標包含資安監控情資格式與回傳頻率驗證與資安防護項目回傳率，監控偵測能力之評估指標包含網路攻防演練驗證、技服中心資安警訊驗證及機關資安事件通報驗證，資安監控情資品質之評估指標則包含資安監控情資品質分析與資安監控情資回饋能量。

●資訊委外資安注意事項與稽核重點

當機關欲將系統監控作業委外時，即當 A 與 B 級機關依「資通安全責任等級分級辦法」附表 1 及 3 建立資通安全威脅偵測管理機制時，應參考「資通安全責任等級分級辦法」之附表 9 與附表 10，依資通系統防護需求等級實作資通系統監控要求。於發現不尋常或未授權之活動時，應對該事件進行分析。對於資通事件評判標準、通報及應變措施之規定，機關應遵循「資通安全事件通報及應變辦法」所要求之事項，對資通安全事件採取適當行動。此外，亦需規劃並定期辦理資通安全演練作業。最終依主管機關指定之方式提交監控管理資料，而於提交關於資通安全情資時，機關應參考「資通安全情資分享辦法」，研判適當之揭示內容與範圍，針對資通安全情資之訊息接收，亦應採取必要研判與合宜處置措施。故當機關將系統監控作業委外時，對專案任務之設定應包含上述相關內容。維運管理類應注意之資安事項內容，詳見表 9。

表9　維運管理類應注意之資安事項與採購階段對應表

採購階段	應注意之資安事項	遵循依據
計畫作業階段	▪機關應要求委外廠商對於其人員，實施至少等同於機關管理內部人員之資安強度 ▪建議將資通安全責任等級分級辦法內之資通安全防護項目，如防毒軟體、網路防火牆、電子郵件過濾機制、入侵偵測及防禦機制、核心資通系統備應用程式防火牆、進階持續性威脅攻擊防禦措施納入監控範圍考量 ▪監控之有效性包含回傳能力、監控偵測能力及資安監控情資品質也應納入評估選擇委外廠商之考量	▪CNS 27036-2 ▪資通安全責任等級分級辦法
履約管理階段	▪遵循「資通安全事件通報及應變辦法」所要求之事項，對資通安全事件採取適當行動 ▪提交關於資通安全情資時，機關應參考「資通安全情資分享辦法」，研判適當之揭示內容與範圍	▪資通安全事件通報及應變辦法 ▪資通安全情資分享辦法
驗收階段	停止委外廠商所涉及之實體與邏輯存取權限，並回收或請委外廠商銷毀屬於機關之資訊資產，必要時可要求委外廠商出具銷毀證明	CNS 27036-2

資料來源：本計畫整理

4.1.5 顧問訓練類－顧問輔導

●機關應辦理之項目

A、B 及 C 級機關依「資通安全責任等級分級辦法」附表 1、3 及 5 所定

義之資安管理事宜辦理，如資訊安全管理系統(ISMS)導入、業務持續運作演練等。

●資訊委外資安注意事項與稽核重點

當機關決定委外作業時，委外專案之資安熱點不在服務本身，而在於委外廠商對機關資訊資產實體與邏輯之存取。以 ISMS 導入案為例，顧問團隊於專案期間可能因進入機關辦公區域或電腦機房而看到機敏文件、為傳送檔案將可攜式儲存媒體連結至機關承辦人員之電腦、因執行資安風險管理而知曉機關管理弱點、因協助資產管理而得知關鍵資通系統型號版本，甚至是未修補漏洞等，故此等委外專案必須實施嚴謹之顧問團隊管理機制，並提升機關專案團隊本身之資安管理認知。

由此引出本類委外專案之資安關注與稽核重點如下：

– 委外廠商所提出資安管理計畫之完整度，其內容可參考「3.2.3.2 建議書徵求文件(RFP)」一節中「採購產品或服務之資安要求事項」下第 2 點之內容，做為控管委外風險之基礎。

– 確保顧問團隊能確實遵循其資安管理計畫，並進行必要調整。

– 機關專案團隊之資安認知程度。若可能，可將該專案涉及範圍之所有人員納入，確認該些人員具備基礎之資安認知，例如當人員需離開辦公桌一段時間(如開會)或下班時，應將機敏資料收至可上鎖之區域(如上鎖櫃)。

4.1.6 顧問訓練類－稽核審查

●機關應辦理之項目

A、B 及 C 級機關應依「資通安全責任等級分級辦法」附表 1、3 及 5 所定義之資安管理事宜與執行頻率辦理，例如 A 級機關每年應辦理二次內

部資通安全稽核，以及取得資訊安全管理系統(ISMS)之公正第三方驗證，並持續維持其驗證有效性。

●資訊委外資安注意事項與稽核重點

稽核審查類與顧問輔導類在委外作業中其資安注意事項大致相同，皆著重在專案過程中，委外廠商對機關資訊資產實體與邏輯之存取。本類委外專案之資安關注重點如下：

– 機關應了解委外廠商所提出之資安管理計畫，確認相關資安控管是否至少等同於機關之管理水平。

– 對於稽核人員，機關宜事先審查其身分是否適宜，而當稽核人員到場後，則應確認其身分。

– 對於稽核審查範圍內之所有人員，應加強其資安認知，如提醒相關涉及人員僅提供必要資訊，原則上不宜提供文件或檔案，若有必要，務必遮蔽相關機敏資訊，並經由權責人員核准。

– 控管稽核人員所攜入之電子設備，如筆記型電腦或智慧型手機等，視情況限制電子設備之使用。在極端情況下，機關可禁止稽核人員攜入所有電子設備，僅以紙筆進行稽核審查。

顧問訓練類應注意之資安事項內容，詳見表 10。

表10 顧問訓練類應注意之資安事項與採購階段對應表

採購階段	應注意之資安事項	遵循依據
計畫作業階段	A、B 及 C 級公務機關應依「資通安全責任等級分級辦法」附表 1、3 及 5 所定義之資安管理事宜與執行頻率辦理，例如 A 級公務機關每年應辦理二次內部資通安全稽核，以及取得資訊安全管理系	資通安全責任等級分級辦法」附表 1、3 及 5

採購階段	應注意之資安事項	遵循依據
	統(ISMS)之第三方驗證，並持續維持其驗證有效性	
履約管理階段	▪廠商/稽核人員對機關資訊資產之存取控管，實施嚴謹之顧問團隊管理機制，並提升機關專案團隊本身之資安管理認知 ▪對於稽核人員，機關宜事先審查其身分是否適宜，而當稽核人員到場後，則應確認其身分 ▪控管稽核人員所攜入之電子設備	CNS 27036-2
驗收階段	回收或請委外廠商銷毀屬於機關之資訊資產，必要時可要求委外廠商出具銷毀證明	CNS 27036-2

資料來源：本計畫整理

4.2 資訊委外情境探討－以維運管理類為例

本小節將以一家已導入 ISMS 之 B 級機關，欲將郵件伺服器委外由資訊服務廠商維運管理為例，提供委外作業過程之參考情境，加強機關對指引內容之理解。

4.2.1 計畫作業階段

●資訊委外可行性分析

該 B 級機關執行成本效益分析內容截錄如下：

– 有鑑於內部資安人力與時間之限制，委外進行郵件伺服器除能解決目前局內資安資源短缺外，由更具資通系統維運專業之委外廠商進行系統管理，更具經濟與時間上之效益。

– 考量郵件伺服器之重要性與委外期間委外廠商將對系統進行存取而產生之相關資安風險，機關將於招標階段要求委外廠商提出專案資安管理計畫，做為控管委外風險之基礎。

●資訊委外專案編成

機關於評量後將推派資訊單位主管擔任專案負責人。於專案規劃期間，由該專案負責人諮詢與邀請採購(總務)、法務、會(主)計、資訊及政風等單位人員編成專案工作小組，參與在資通安全、資訊技術、法規遵循、服務水準、專案細項預算及選商需求分析等工作。

●資訊委外資安需求識別

– 建立資訊委外資安策略

專案負責人與專案工作小組商討後，依據「3.1.3.1 建立資訊委外資安策略」擬訂本專案委外資安策略，內容僅截錄部分如下：

➢本專案標的為機關之郵件伺服器，涉及對象為系統所有使用者。

➢委外執行方式預計由委外廠商指派專責人員，進行郵件伺服器之日常維運與管理。

➢為降低郵件伺服器運行過程或由其衍生出之資安風險，本專案目標除確保郵件伺服器正常運作外，對於因電子郵件而衍生之風險，如網路釣魚郵件、惡意網址及已知惡意程式等社交工程議題，委外廠商亦應於維運期間協助強化局內人員之資安意識、建立有效之資安控管及合宜之資安技術支援等，機關之資訊作業暨安全審議會已決議提供必要預算，包含維運或因強化資安而產生之相關採購。

➢為確保委外專案執行期間相關資安風險得以被識別與處置，機關將依內部既有之 ISMS 風險評鑑管理機制，管理委外期間之資安風險。

– 邀請潛在廠商提出對應措施方案

於諮詢上級機關與其他平級機關之建議後，機關聯絡 2 家郵件伺服器維運廠商，邀請廠商至機關辦公地點提供相對應之建議措施。

– 建立資訊委外資安管理計畫

根據上級機關、其他平級機關及委外廠商回饋內容，專案負責人依「3.1.3.4 建立資訊委外資安管理計畫」擬訂本專案之資訊委外資安管理計畫，對本專案應具備之資安需求項目進行詳細分析，內容僅截錄部分如下：

➢本專案為郵件伺服器之委外維運與管理，涉及對象包含所有郵件伺服器之管理者與使用者。

➢委外廠商主要於機關資訊單位辦公地點進行郵件伺服器維運作業，但於特殊情況並獲核准時，得使用遠端連線進行管理。

➢帳號權限管理

◆每位資訊委外管理人員將獲得一組郵件伺服器之日常維運帳號，該帳號僅擁有必要之管理權限，禁止擁有安裝軟體、新增或變更使用者帳號與權限及刪除資訊等權限。

◆當有使用最高權限需求時(如進行系統更新)，應於專案負責人全程監督下使用，遠距工作時亦同。

➢遠距工作管理

若有遠距工作之情況，委外廠商與委外管理人員應遵循機關內部之遠距工作管理規範，降低其 VPN 帳號密碼被濫用之風險。機關資訊單位亦需因應此遠距工作可能帶來之資安風險，採取必要之資安控管，其措施應包含(但不限於)下列措施：

◆採用雙因子認證登入。

◆設置中間跳板機，避免直接連結郵件伺服器。

◆安裝連線側錄軟體，記錄該委外管理人員所有操作行為。

➢異常監控與通報

於維運期間，機關與委外管理人員應建立一套系統監控與通報機制，以證明所有管理作業皆在被允許之維運操作範圍內。當發現存取異常時，應有通報與遏止之流程。此異常監控範圍至少包含：

◆每當最高權限帳號被使用完畢後，應最晚於隔日下班前審核其所有活動紀錄，以確認其操作皆合宜。

◆每週產出一份 VPN 活動稽核報告，以分析遠距工作內容之適切性。

➢委外廠商服務之監視與審查

依專案性質與重大程度來看，單一郵件伺服器之維運委外作業單純且具侷限性，故將採用定期書面審查方式，確認委外廠商之服務遵循度。此書面審查包含取得委外廠商之第三方驗證證明文件、取得委外廠商內部稽核報告(僅與專案範圍相關)、要求委外廠商提出資安控管之相關執行紀錄及要求委外廠商填寫自我評估報告等。

➢有關於郵件伺服器作業系統或軟體更新與可攜式媒體管理等規範，應依機關既有之資安管理規範與程序辦理。

4.2.1.1 招標階段

●委外廠商評選準則之定義與實作

機關依服務委外之特性，建立委外廠商評選準則，內容截錄部分如下：

– 投標廠商應完全遵循招標文件所要求之資安事項，若有窒礙難行之處，應採取相同效果之資安控管。

– 投標廠商不得為大陸地區廠商或第三地區含陸資成分廠商，並不得有分包廠商。

– 投標廠商本身應通過 ISMS 驗證，並於專案期間持續有效。

– 投標廠商所安排之管理人員應具備 CISA、CISM、CISSP 或 CEH 等資安相關證照。

●保密協議書準備與簽訂

根據經驗，投標廠商為求精確地規劃專案執行方式、專案投入人力與時間及其他必要費用，若要求機關提供專案範圍內之相關資訊時，專案負責人應使用機關制式保密協議書，會同法務單位，依本委外專案之特性進行調整，俟得標廠商有此需求時使用。

●招標文件之制定與發布

招標文件包含下列項目：

– 投標廠商聲明書：使用本指引附件 9 為範本進行調整。

– 投標須知：使用本指引附件 10 為範本進行調整。

– 標價清單：使用工程會網站中「政府採購」→「招標相關文件及表格」連結下之投標標價清單範本進行調整。

– 建議書徵求文件：參考本指引「3.2.3.2 建議書徵求文件(RFP)」一節。

– 契約書(樣本)：使用本指引附件 11 為範本進行調整。

– 退還押標金申請單。

– 投標專用信封。

●服務建議書之蒐集

機關蒐集 2 家郵件伺服器維運公司所提交之服務建議書，分別為甲公司與乙公司。

●服務建議書之評選

機關依「採購評選委員會組織準則」選擇 5 位合格適任之評選委員，進行服務建議書之評選作業。

– 投標廠商資格

於確認「投標廠商聲明書」所載內容，並進一步至工程會「政府電子採購網」查詢投審會網站公告之「陸資投資事業名錄」、「具敏感性或國安(含資安)疑慮之業務範疇」及「陸資投資資訊服務業清冊 」3 項資料表後，確認 2 家投標廠商皆非陸資企業，並皆符合機關所訂之資格。

– 整體產品或服務內容

機關邀集 5 位專家學者組成評選委員會，除對 2 家投標廠商之建議書進行書面審查外，於書面審查後一週內召開評選會議。由投標廠商提出 15 分鐘對建議書之簡報，其後接受評選委員之詢問。簡報與答詢結束後，各評選委員參考 RFP 內之評選項目表進行評分。2 家投標廠商之分數皆大於 70 分合格門檻，惟甲公司之經驗略勝乙公司，甲公司所安排之管理人員之資歷、專長及學經歷亦優於乙公司，故甲公司以總分高出乙公司 10 分之差距成為優勝廠商。

4.2.1.2 決標階段

●委外協議之確認與簽署

以本指引附件 11 為範本，依招標文件與委外廠商之服務建議書內容進行調整，並於契約中載明雙方之資安角色與責任，明訂不得分包與專案期間機關所擁有之管理權利等。經過雙方主責單位與法務單位之確認後，與甲公司進行簽約作業，並確保甲公司各專案成員皆簽訂保密約定。

簽約作業結束後，專案負責人與甲公司確認專案啟動事宜。

4.2.1.3 履約管理階段

當專案啟動後，機關依與委外廠商約定之管理事項進行管理，包含但不限於以下項目：

- 每兩週審核委外廠商所提交之服務報告，並對維運方式進行適當調整。
- 當郵件伺服器之最高權限被使用完畢後，至少於隔天下班前審核該最高權限所有活動紀錄，以確認無異常行為。
- 每週審核 VPN 活動稽核報告，以分析遠距工作內容之適切性。
- 每半年對委外廠商進行書面審查，以確保委外廠商持續維持其資安能量，其書面審查包含：
  - 委外廠商 ISMS 證照持續有效之證明。
  - 取得委外廠商內部稽核報告(僅與專案範圍相關)。
  - 要求委外廠商填寫由機關提供之自我評估報告。
- 當有異常行為或不適當操作情況發生時
  - 要求委外廠商執行矯正預防機制。
  - 遵循機關既有之資安事件應變機制，進行通報、處置及檢討。

4.2.1.4 驗收階段

該專案為一年一簽，於年度驗收時，專案負責人邀請雙方專案團隊召開專案結束會議，彙整年度之服務報告與書面審查資訊為總驗收資料，確認專案目標與成效之達成情況。專案結束會議後，專案負責人召開總驗收會議。由專案負責人邀請 3 位資訊單位代表與 1 位採購單位代表，審查總驗收資料。

5. 結論

政府資訊委外牽涉到之問題較為複雜，除採購法與相關行政命令外，還涉及國家、機關資安政策及相關法規之規定，故本指引係以資通安全管理法、CNS 27036 及 CNS 27001 為體，採購程序為用，依採購案流程，分別敘述各階段在資通安全方面應注意事項。

在計畫作業、招標、決標、履約管理、驗收及保固作業各階段，已分別說明應注意之資安重點。其中於「計畫作業」階段機關應準備之作業，如：風險評估、預算規劃及內部之委外資安政策等較容易被忽略；此外，內部規定之文件化部分亦常被忽略，容易造成委外廠商執行時誤觸地雷或無所適從。計畫作業階段之準備作業如較周詳，後續履約管理階段執行將相對容易，亦不易產生爭議，委外才能順利完成。

額外需提醒各機關在遇到一般系統開發案之保固時，常因與維護案之維護作業定義混淆，將兩者混為一談，容易造成系統開發類採購案之爭議。各機關如考量後續維護經費編列困難，於辦理開發案委外時，建議應另依維護案方式規劃維護需求，再併入採購案中執行。

建議使用者依欲辦理之資訊委外類型，參閱本指引所提供該類資訊委外之資安重點。於執行資訊委外作業時佐以檢核表應用，對於採購資訊委外資通安全方能有所幫助，亦是本指引修訂之主要目的。

6. 參考文獻

[1]V Grover, MJ Cheon & JTC Teng (1996). The Effect of Service Quality and Partnership on the Outsourcing of Information Systems Functions. Journal of Management Information Systems, Volume 12, 1996 - Issue 4.

[2]JN Lee, YG Kim (1999). Effect of partnership quality on IS outsourcing success: conceptual framework and empirical validation. Journal of Management Information Systems, Volume 15, 1999 - Issue 4.

[3]Kishore, R., Rao, H. R., Nam, K., Rajagopalan, S. and Chaudhury, A. (2003) A Relationship Perspective on IT Outsourcing, Communications of The Association for Computing Machinery, 46(12): 87–92.

[4]行政院公共工程委員會(106 年 9 月)，機關委託資訊服務廠商評選及計費辦法，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030077

[5]數位發展部資通安全署全球資訊網，https://moda.gov.tw/ACS/

[6]法務部(105 年 3 月)，個人資料保護法施行細則，https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022

[7]國家資通安全研究院，個人資料保護參考指引，https://www.nics.nat.gov.tw/CommonSpecification.htm?lang=zh

[8]行政院公共工程委員會(108 年 5 月)，政府採購法，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030057

[9]國家資通安全研究院，資通系統風險評鑑參考指引，https://www.nics.nat.gov.tw/CommonSpecification.htm?lang=zh

[10]行政院公共工程委員會全球資訊網，https://www.pcc.gov.tw

[11]行政院公共工程委員會，資訊服務評選項目及配分權重範例，
https://www.pcc.gov.tw/cp.aspx?n=33DE8745316D5A90

[12]行政院公共工程委員會之相關採購手冊及範例，
https://www.pcc.gov.tw/cp.aspx?n=10CA9F72C981FC4C

[13]國家資通安全研究院，電子資料保護參考指引，
https://www.nics.nat.gov.tw/CommonSpecification.htm?lang=zh

[14]行政院公共工程委員會 (107 年 3 月)，政府採購法施行細則，
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030058

7. 附件

附件 1 政府資訊委外資安注意事項或常見缺失

附件 2 政府資訊委外資安檢核表

附件 3「Web 網站建置與個人資料管理維運」RFP 資安需求範例

附件 4「Infrastructure 基礎設施建置與維運管理」RFP 資安需求範例

附件 5「雲端服務供應商提供資訊系統部署、託管及維運服務」RFP 資安需求範例

附件 6「政府機關資訊安全管理系統(ISMS)顧問輔導」RFP 資安需求範例

附件 7「政府機關資訊安全管理系統(ISMS)公正第三方驗證」RFP 資安需求範例

附件 8 行政院公共工程委員會「政府資訊服務採購作業指引(1120925)」

附件 9 行政院公共工程委員會「投標廠商聲明書範本(1110502)」

附件 10 行政院公共工程委員會「投標須知範本(1120630)」

附件 11 行政院公共工程委員會「資訊服務採購契約範本(1121123)」

附件 12 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)

附件 13 112 年第六次電腦軟體共同供應契約採購-雲端服務產品公開徵求-雲端服務檢測規範

附件 14 委外廠商查核項目表

附件 15 專有名詞英中對照表