教育部國民及學前教育署
111 年度校園資通安全專責人員知能研習

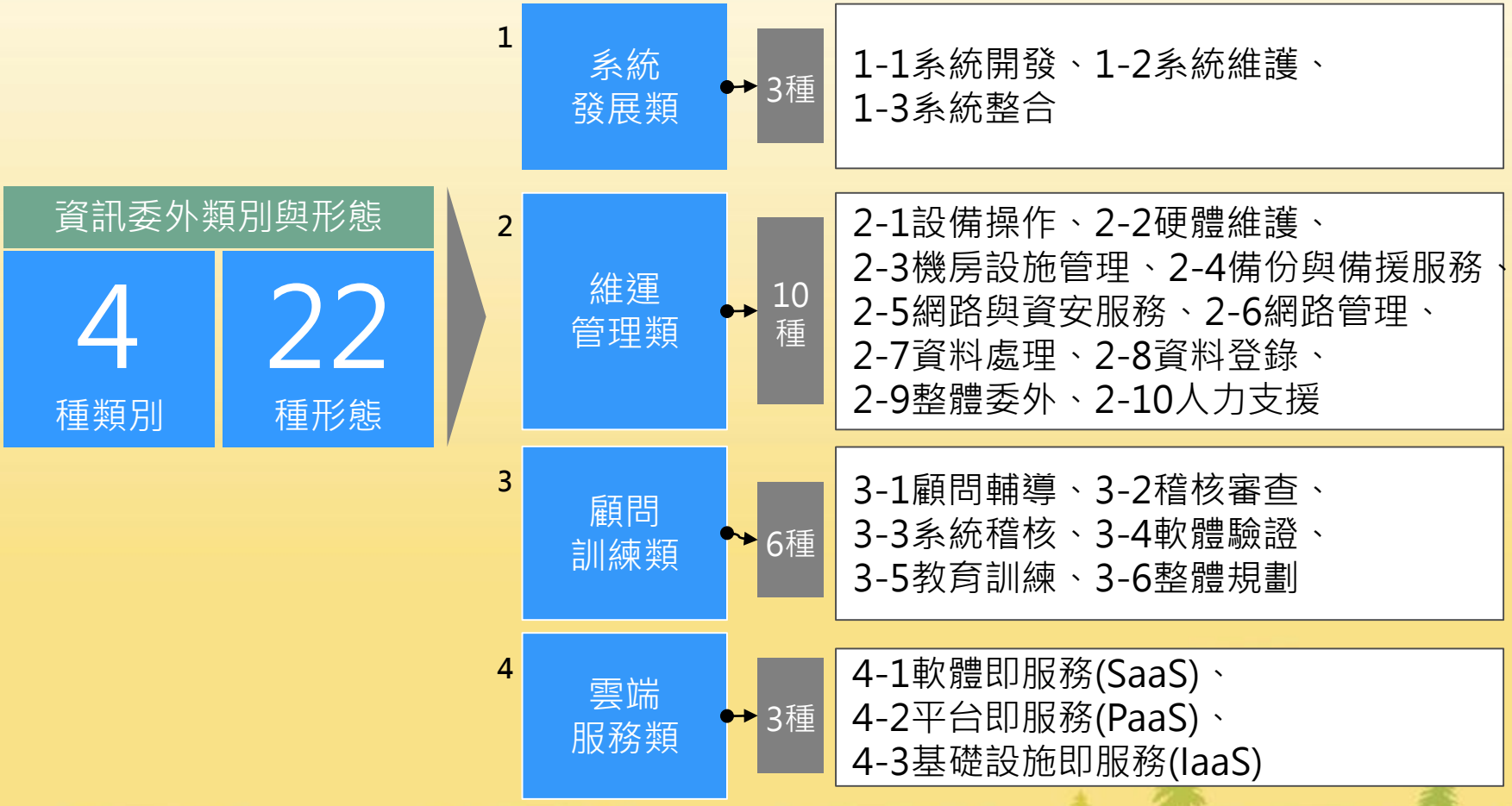
委外合約的訂定與管理

大綱

- **資訊委外類別與形態**
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- 注意事項與常見缺失
- 政府資訊委外資安檢核表
- Q&A

資訊委外類別與形態

委外作業區分為：系統發展類、維運管理類、顧問訓練類及雲端服務類等 4 類，共 22 種作業形態。



系統發展類

1-1 系統開發

- 依機關規格需求，開發一套應用系統程式，並於開發完成後，進行測試、訓練、製作技術文件及上線之專案
- 其作業範圍包括新系統開發設計、舊系統汰舊換新、舊系統架構更改、系統移轉訓練及系統保固等工作

1-2 系統維護

- 應用軟體之維護服務與功能增修，包括軟體版本更新、應用程式錯誤與漏洞之排除及更正性服務等

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)或套裝軟體，及新資通系統教育訓練等項目

維運管理類(1/5)

2-1 設備操作

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報告

2-2 硬體維護

- 在設備保固期滿後，為維持原硬體功能與正常運作，提供定期維護合約工作，統稱為硬體維護
- 購買硬體設備(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，應由原供應廠商依購買時契約約定，提供各項售後服務，非屬硬體維護範圍
- 惟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，保固期限由1年延長3~5年不等

維運管理類(2/5)

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

2-4 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
- 資訊委外之備援服務可有效降低機關資通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

維運管理類(3/5)

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

2-6 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

維運管理類(4/5)

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

2-8 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

維運管理類(5/5)

2-9 整體委外

- 將全部或部分資通系統之整體運作，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，擬定資通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

2-10 人力支援

- 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

顧問訓練類(1/2)

3-1 顧問輔導

- 在特定主題範圍內，進行需求調查、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ISMS導入

3-2 稽核審查

- 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，如政府機關資訊安全管理系統(ISMS)第三方驗證

3-3 系統稽核

- 為確保資訊單位內部作業資安控制，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資安作業管制標準

顧問訓練類(2/2)

3-4 軟體驗證

- 透過一連串具稽核功能之特殊程式，驗證資通系統運用與功能是否正確與符合原始需求，常由公正第三方執行

3-5 教育訓練

- 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

3-6 整體規劃

- 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通服務需求彙整、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

雲端服務類

4-1 軟體即服務(Cloud Software as a Service, SaaS)

- 透過網際網路提供軟體的一種服務模式，廠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廠商提供的應用軟體服務，使用者不用再購買軟體，且無須對軟體進行更新維護，服務提供商會全權管理和維護軟體，例如：Google DOCS、Microsoft Office Live、Facebook及Saleforce等。部分政府機關或企業使用Google Gmail即為SaaS的一種服務模式

4-2 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式，自行使用程式語言使用服務平台，但無須管理或控制雲端設備，包含網路設備、伺服器，例如：Google App Engine、Windows Azure及AMAZON AWS:S3 (Simple Storage Service)等

4-3 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的作業系統、資料庫存取，如Flexiscale、AWS (Amazon Web Services)等

大綱

- 資訊委外類別與形態
- **資訊委外資安策略**
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- 注意事項與常見缺失

- Q&A

資訊委外原則(1/5)

- 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
- 涉及國家機密業務不宜委外，惟若經評估仍須委外辦理，則執行廠商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
- 限制使用危害國家資通安全產品
- 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
- 委外廠商應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

資通安全專業證照請參閱數位發展部資通安全署官網之資通安全專業證照清單
https://moda.gov.tw/ACS/laws/certificates/676

資訊委外原則(2/5)

- 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
- 若得複委託，機關應要求委外廠商對複委託廠商進行管理，包含設定一致的資安與個資保護目標、執行風險評鑑以達成該資安與個資保護之目標。機關甚至可與委外廠商協商，由委外廠商提出該些複委託廠商的監控管理報告
- 受託業務包括客製化資通系統開發者，委外廠商應提供該資通系統之第三方安全性檢測證明
- 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

資訊委外原則(3/5)

- 委託關係終止或解除時，應確認委外廠商返還、移交、刪除或銷毀履行委託契約而持有之資料(含委外廠商交付複委託之資料)
- 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安事件時，以稽核或其他適當方式確認受託業務之執行情形
- 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投審會公告之陸資資通服務業者參與
- 應建立資安管理之事前規劃、事中招標及事後執行維運機制

資訊委外原則(4/5)

- 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
- 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
- 重要資訊專案得視需要區分顧問標、規劃標、建置標及監督審驗標辦理
- 應透過RFI或RFC等方式，廣納各界意見，據以訂定合宜的資安需求(RFP)規格：
  - 公開徵求資訊(Request For Information，RFI)
  - 徵求修正意見(Request For Comments，RFC)
  - 徵求建議書文件(Request For Proposal，RFP)

資訊委外原則(5/5)

- 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，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，並要求廠商依照主管機關訂定之標準或規範發展系統，確保軟體品質與政府資訊的流通互用
- 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，確保服務績效

資訊委外策略(1/2)

- 以政府機關採購招標觀點而言
  - 自行建構、採購硬體或訂製軟體轉為購買資通服務
  - 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

資訊委外策略(2/2)

- 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資安檢測服務與報告

- 規劃過程
  - 將機關的資安規範與對廠商(含複委託廠商)資安要求納入【契約書或RFP】
  - 將【資通安全需求】納入RFP中，列為委外需求與評比必要工作項目
- 執行過程

  要求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，確保委外作業安全
- 因應【個資法/施行細則】之施行
  - 廠商(被委託機關)增加多項義務與賠償責任，建議機關在估算成本時應一併考量
  - 委託機關必須負起「監督」職責

最近行動應用App的開發與運作越趨興盛，規劃委外安全時也可以考慮加入”工業局行動應用App基本資安自主檢測 “的相關要求。

大綱

- 資訊委外類別與形態
- 資訊委外資安策略
- **資訊委外風險說明與風險處理原則**
- 資訊委外各階段資安要求
- 注意事項與常見缺失

- Q&A

機關常見的資訊委外風險

- 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
- 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

常見資訊委外風險處理原則

以下為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的風險與衝擊，然而風險依然存在，階段滾動進行風險評估仍然是必要的

- 多樣化來源策略，以避免過度倚賴或鎖定特定廠商
- 建立委外廠商管理程序
- 建立委外廠商的管理模式
- 建立委外廠商管理組織
- 預先規劃廠商的技術與能力需求
- 使用標準文件與範例
- 制定明確的需求
- 適當的選擇廠商
- 在合約草擬過程中涵蓋生命週期中所有相關項目
- 決定適當的資安控制措施
- 建立服務水準(SLAs)
- 建立執行水準協議(Operating Level Agreement, OLAs)及支撐合約(Underpinning contract)
- 建立適當的廠商績效或服務水準監控與報告機制
- 建立廠商獎懲模式
- 在合約生命週期中建立適當的廠商關係管理
- 檢視合約與服務水準
- 要求廠商風險管理
- 以政府機關政策檢視廠商法規遵循性
- 實施廠商內部控制評估
- 規劃與管理合約關係結束
- 訂定軟硬體處置規定

大綱

- 資訊委外類別與形態
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- **資訊委外各階段資安要求**
- 注意事項與常見缺失

- Q&A

計畫作業階段(1/8)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 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
- 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，與經濟部工業局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

計畫作業階段執行作業有3大重點：

- **資訊委外可行性分析**
- **資訊委外專案編成**
- **資訊委外資安需求識別**

計畫作業階段(2/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1.資訊委外可行性分析(1/3)

資訊委外可依「委外之作業形態不同、規模大小及專案機敏特性」參考下列步驟進行分析：

- 篩選適合委託辦理之業務項目

  就各預定委外業務項目檢討分析具資安作業能量之民間辦理部分，積極探詢可受委託辦理民間團體之參與意願，以確定該項業務委託民間辦理之資通安全可行性無虞

- 進行成本效益分析

  政府機關在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「量化指標」與「非量化指標」

計畫作業階段(3/8)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

1.資訊委外可行性分析(2/3)

- 量化指標
  - ➢ 應考量：人力、時間、資產維護及資安保護等
    - ◆專案自行開發之人事成本(包括薪資、保險及退休等費用)
    - ◆專案自行開發之時間成本(包括業務需求時程與機關自行開發時程)
    - ◆委外專案資訊設施資產成本(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)系統增加的監督人事成本(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)
    - ◆如進行案件複雜度較高者，可聘請資安、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

計畫作業階段(4/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1.資訊委外可行性分析(3/3)

– 非量化指標

➢ 應考量：受服務者滿意度與信賴度

◆對機關外部客戶之可用性提升，評估其可行性

◆對機關外部客戶之安全信賴度提升，評估社會成本效益

- 評估資訊委外資安風險與對策

  機關應確認委外資安風險評估之範圍，經由風險評估過程，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。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

計畫作業階段(5/8)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

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
- 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

計畫作業階段(6/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3. 資訊委外資安需求識別(1/3)

當機關選派適當之專案負責人後，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。此分析之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

- 建立資訊委外資安策略

  應針對資訊委外個案，建立其資訊委外資安策略，包含：

  - 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、類型及本質評估資安負責人的專業能力
  - 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
  - 將採用之資安管理架構
  - 委外廠商評選準則項目
  - 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

計畫作業階段(7/8)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

3.資訊委外資安需求識別(2/3)

- 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，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

- 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

計畫作業階段(8/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3.資訊委外資安需求識別(3/3)

- 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，應包含(但不限於)下列項目：

  - 所規劃取得產品或服務之規格
  - 於委外專案期間需存取之資訊資產
  - 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
  - 各階段應有之角色與責任
  - 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
  - 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

招標階段(1/8)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 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，本階段以招標過程之時序為架構，敘述各作業應注意之資安事項

招標階段執行作業有5大重點：

- **委外廠商評選準則之定義與實作**
- **保密協議書準備與簽訂**
- **招標文件之制定與發布**
- **服務建議書之蒐集**
- **服務建議書之評選**

招標階段(2/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1. 委外廠商評選準則之定義與實作

- 招標階段之首要作業，需依資訊委外資安策略所定義之委外廠商評選準則項目與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

招標階段(3/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

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

招標階段(4/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3. 招標文件之制定與發布(1/3)

- 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」與「投標須知範本」等。而下列僅提出與資安相關內容之建議，包含採購契約、RFP及SLA等之撰寫注意事項
  - 採購契約
    - 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
    - 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
    - 針對資訊委外，機關可參考工程會網站中「政府採購」→「招標相關文件及表格」連結下載最新版本，並依所識別之資安需求與限制，酌予修改

招標階段(5/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3. 招標文件之制定與發布(2/3)

- 建議書徵求文件(RFP)
  - 徵求建議書文件(RFP)為廠商執行委外作業之需求依據，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，以研擬妥適之RFP
    - ◆ 確認專案目標
    - ◆ 界定專案範圍
    - ◆ 掌握業務與資通系統現況
    - ◆ 蒐集現行資訊軟硬體作業環境
    - ◆ 釐訂需求內容
    - ◆ 制定服務水準指標
    - ◆ 規範交付項目與內容
    - ◆ 訂定專案管理需求
    - ◆ 訂定評選標準與方式
    - ◆ 參考機關契約條文、資訊服務採購相關手冊與指引

招標階段(6/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3. 招標文件之制定與發布(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之一致服務
  - 對於資訊委外作業而言，資安相關之服務水準管控以系統可用率、安全性及稽核作業為3大指標：
    - 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。基於系統資安考量，可訂定系統可用率指標，以確保系統維持一定服務水準
    - 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，確保資通系統(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
    - 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

招標階段(7/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

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

招標階段(8/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

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，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
  - 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

決標階段(1/2)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 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
- 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：廠商在簽約前須依據招標文件之規定，提出各項保密切結，並依據規定訂定資通安全防護計畫，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，以利承辦單位依據合約執行各項查核，並做成紀錄
- 相關文件要求：
  - 得標廠商與其專案工作成員應簽訂保密約定至少1式3份，並於指定期限內送交甲方1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(例如：2週)內送交甲方，其後如有不足，並應適時修正之

決標階段(2/2)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 最有利標之注意事項
  - 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，藉以實際反映廠商資安作業能量

履約管理階段(1/23)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 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，應對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

履約管理階段(2/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

下列為進行委外關係管理期間可能適用之資安控管項目，機關應就委外專案之性質，參考適用之事項

管理重點	
資通安全組織	資訊委外風險持續識別
資訊委外人力資源安全	資訊委外實體與環境安全
資訊委外管理	資訊委外使用者存取管理
資訊委外資通安全事件管理	

履約管理階段(3/23)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

資通安全組織

- 機關與委外廠商皆應指定專案管理人員，負責推動、協調及督導下列資通安全管理事項
  - 資通安全責任分配與協調
  - 資訊資產保護事項監督
  - 資通安全事件檢討與監督
- 委外專案視需要成立跨部門資通安全推動小組，推動下列事項
  - 協調跨部門資通安全事項權責分工
  - 協調研議應採用之資通安全技術、方法及程序
  - 協調研議整體資通安全控制措施
  - 協調研議資通安全計畫
  - 協調研議其他重要資通安全事項

履約管理階段(4/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外風險持續識別(1/2)

- 經由委外作業過程中產生之風險，在核准廠商存取內部設施前加以識別，並作適當的控制措施
- 若允許委外廠商存取機關資訊處理設備或資訊時，執行風險評鑑識別特定控制措施的要求
- 委外廠商存取風險之識別，應考慮下列事項
  - 委外廠商攜帶存取的資訊處理設備與儲存媒體
    - 處理設備：手機與電腦
    - 儲存媒體：磁片、磁碟、光碟、隨身碟及報表
  - 委外廠商對資訊與資訊處理設備之存取形式
    - 實體存取：辦公室、機房及檔案櫃
    - 邏輯存取：機關的資料庫與資通系統的連結與存取
    - 機關與委外廠商的網路連接：固定連接或遠端存取
    - 存取發生於現場(On-Site)或場外(Off-Site)
    - 涉及資訊的價值與敏感性及對營運的關鍵性
    - 保護不打算被廠商存取的資訊，必要的各項控制措施

履約管理階段(5/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外風險持續識別(2/2)

- 委外廠商對資訊與資訊處理設備之存取型式(續)
  - 如何識別被授權存取的委外廠商或人員，如何查證授權與多久需再確認一次
  - 與廠商在儲存、處理、通信、分享及交換資訊時，所採用的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，及因登錄或收到不精確或誤導資訊時的衝擊
- 委外廠商人員異動風險
  - 考慮廠商專案成員調整與異動時，限期調整其權限

履約管理階段(6/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(1/9)

- 為確保委外員工與廠商能勝任其角色，以降低竊盜、詐欺或設施誤用的風險，應於委外前，依契約條款闡明廠商應負之安全責任(尤其是敏感性工作)，並進行適當篩選，例如：人員背景查證審核、簽訂保密切結書及完成適當教育訓練

人員僱用前	僱用期間
● 角色與責任 – 篩選 – 僱用條款與條件	● 管理階層責任 ● 資通安全認知、教育及訓練 ● 懲處作業程序 ● 僱用終止或變更 ● 終止責任 ● 資產歸還 ● 存取權限移除

履約管理階段(7/23)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

資訊委外人力資源安全(2/9)

- 人員僱用前-委外人員資安角色與責任(1/3)
  - 資訊作業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資安角色與責任，依照資通安全政策加以界定與文件化，並包含下列要求
    - 依據機關資通安全政策實作與行動
    - 保護資產不受未授權存取、揭露、修改、銷毀及干擾
    - 執行特定的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
    - 資安角色與責任定義時機
    - 資安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資安角色與責任

履約管理階段(8/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(3/9)

- 人員僱用前-委外人員資安角色與責任(2/3)
  - 篩選
    - ➢ 委外人員背景查證檢核

      查證檢核時考量所有隱私權與個人資料保護等相關法令，參酌下列控制措施：

      - ◆是否有合格的品格推薦信或可諮詢的人員
      - ◆進用人員的學經歷檢核
      - ◆確認應徵人員學歷與專業資格
      - ◆獨立身分檢核，例如：護照或類似文件
      - ◆更詳細的核對，例如：信用核對或犯罪紀錄檢核
    - ➢ 定義查證檢核準則與限制程序
      - ◆宜定義查證檢核準則與限制程序，例如：誰有資格篩選人員，如何、何時及為何執行查證檢核

履約管理階段(9/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(4/9)

- 人員僱用前-委外人員資安角色與責任(3/3)
  - 僱用條款與條件
    - ➢ 保密切結書

      為保障委外作業安全，宜針對參與廠商之作業員工，經由個人同意並簽署僱用同意書。該同意書陳述其與機關對資通安全的責任
    - ➢ 僱用同意書，反映機關資安政策
      - ◆ 被賦予敏感資訊存取權之委外人員，在被允許存取資訊處理設備前，簽署機密性或保密協議
      - ◆ 委外人員法定責任與權利，例如：著作權法或個資法規定
      - ◆ 委外人員所處置資通系統與服務相關資訊分類及機關資產管理之責任
      - ◆ 委外人員處理來自其他公司或外部團體資訊之責任
      - ◆ 延伸至機關外與正常工作時間外之責任，例如：在家工作
      - ◆ 委外人員違犯機關資安要求時，所採取之行動
    - ➢ 確保委外人員同意機關資通安全條款與條件，及其將會取得資通系統與服務之存取權限範圍與限制

履約管理階段(10/23)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

資訊委外人力資源安全(5/9)

- 僱用期間-管理階層責任
  - 管理階層應要求委外人員，依照機關制定的政策與程序施行資安事宜
    - 確保委外人員在被核准存取敏感資訊或系統前，正確地說明資通安全角色與責任
    - 提供指導綱要予委外人員，述明對其角色的安全期望
    - 激勵委外人員符合機關資安政策
    - 激勵委外人員達到所扮演角色與責任的資安認知等級
    - 激勵委外人員符合僱用條款與條件，包括符合資安政策與適切的工作方法
    - 激勵委外人員持續擁有技能與資格
  - 激勵工作之重要

    若委外人員未認知資安責任，可能導致對機關巨大損害。受激勵的人員較少引起資通安全事件，而拙劣管理可能令委外人員感覺被輕視，導致負面衝擊

履約管理階段(11/23)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

資訊委外人力資源安全(6/9)

- 僱用期間-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

履約管理階段(12/23)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

資訊委外人力資源安全(7/9)

- 僱用期間-懲處作業程序
  - 委外人員如有違反資通安全，宜有正式的懲處過程，對於未查證資安違例已發生前，不宜執行懲處作業程序
  - 懲處過程宜確保涉嫌違反資安政策員工，得到正確與公平之處理，並考量違例之性質與嚴重性、對營運衝擊、是否為初犯或累犯、是否經過適當訓練、相關法律、營運契約及其他因素等，採取累進處罰
  - 在嚴重的不當行為狀況下，宜允許立即停止其職務、存取權限及特權，必要時立即護送離開場域，懲處過程應適當，以預防委外人員違反資安政策、程序及其他資安違例
  - 有關廠商因違反契約，機關採取罰款之懲處方式，如不符合委外案件承作金額比例原則，可由廠商自行至工程會請求仲裁

履約管理階段(13/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(8/9)

- 僱用期間-僱用終止或變更

  為確保委外人員依程序離開機關或變更僱用條件，確保離開時受到管理，並完成資訊業務移轉交接、歸還設備及移除所有存取權限

- 僱用期間-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

履約管理階段(14/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(9/9)

- 僱用期間-資產歸還

  委外作業完成、契約或協議終止時，應歸還所有機關資產，包括歸還所有軟體、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的資訊等，也需一併歸還，並保留執行紀錄

  – 若委外作業由廠商提供或使用設備時，將所有相關資訊移轉回機關，並安全地從設備上清除
  – 若廠商擁有進行中之運作重要的知識，將該資訊文件化，並移轉回機關

- 僱用期間-存取權限移除
  – 委外人員對資訊與資訊處理設備之存取權限，在契約、協議終止或因變更而調整時，宜重新考量資通系統與服務相關之資產存取權限
  – 應注意若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備；若為員工自行請辭，可能企圖為將來用途而蒐集資訊

履約管理階段(15/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

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備，宜置放於安全區域，經由適當的資安屏障與進出控制措施加以保護，確保設備免受未經授權之存取、損害及干擾

安全區域

使用安全周界，例如：牆、卡控入口閘門或有人員駐守的接待櫃檯等屏障，以區隔委外作業與內部資訊處理設備的區域

設備安全

委外設備安全，應考量機關內因委外所需存取或委外人員攜入之資訊設備，包括個人電腦、個人數位助理、行動電話、智慧卡及其他形式，並注意由機關工作地點攜出與機關外攜入的各項風險

履約管理階段(16/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(1/6)

- 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

- 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
  - 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

- 職務的區隔

  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

履約管理階段(17/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(2/6)

- 委外開發、測試及運作

  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

  - 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
  - 系統需求評估
  - 適當之測試作業
  - 第三者執行查核與驗證

履約管理階段(18/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(3/6)

- 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
    - 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
    - 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

履約管理階段(19/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(4/6)

- 防範惡意碼與行動碼

  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

- 委外媒體的處置
  - 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

履約管理階段(20/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(5/6)

- 委外媒體的處置(續)
  - ➢ 可攜式媒體的管理
    - ◆ 可攜式媒體包括磁帶、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、數位相機及印出的媒體，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，應考量下列原則
      - ■ 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

履約管理階段(21/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(6/6)

- 委外媒體的處置(續)
  - ➢ 系統文件的安全
    - ◆ 經委外產製的系統文件宜加以保護，免遭未經授權存取，並採行下列管控措施：
      - ■ 文件化相關資通安全控制措施
      - ■ 更新系統文件，並妥善保管與處理舊版文件
      - ■ 確保操作文件與使用者程序根據需要作適切變更。例如：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
      - ■ 辦公桌面的淨空政策
      - ■ 正式委外人員離職程序，確保繳回機關資產，並保留執行紀錄
      - ■ 電腦與網路之日常管理作業，應有正式文件，變更應經權責單位核准
      - ■ 保全委外作業系統文件應考慮：安全存放、版本控管、存取控制

履約管理階段(22/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

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通系統存取，機關宜有正式程序，以控制資通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通系統與服務註銷
- 宜特別注意特權存取權限配置是否有控制必要，使用者註冊與註銷之存取控制程序包括：
  - 檢核是否經過系統擁有者授權，或由管理階層另行個別核准存取權限
  - 檢核所授予的存取權限等級，是否符合營運目的，是否與機關資安政策一致，例如：不違反職務區隔
  - 給予委外人員存取權限的書面聲明
  - 要求委外人員簽署聲明
  - 確保服務提供者在完成授權程序前，不會提供存取
  - 維持一份含所有註冊使用服務之使用者的正式紀錄
  - 機關可透過帳號、識別證及卡片等機制，管理委外人員帳號，使每一位委外人員具有「唯一」識別，並可依識別驗證使用者身分
  - 委外人員因變更角色、調職或離職後，應立即移除或封鎖其存取權限

履約管理階段(23/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

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：
  - 適當記錄資安事件的作業處理程序，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的行為狀況
  - 發生資通安全事件後的正確行動
    - 記錄所有重要細節
    - 應儘速通知相關人員處理，不隨意執行任何動作
  - 反映資通安全弱點
  - 反映軟體功能不正常

驗收階段(1/4)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 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，並得以書面或召開審查會議方式辦理
- 依下列建議，要求廠商專案驗收內容與進度：
  - 廠商於簽約後一定時間內提交「專案工作計畫書」
  - 廠商須定期召開工作進度報告會議，並提交工作報告
  - 於資訊委外作業執行過程中，配合各階段需求，規劃並實施充足教育訓練
  - 完成履約管理階段之廠商服務交付管理，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，廠商應衡酌各工作項目性質與內容，詳述擬交付的文件或資料，並負責製作專案進行過程中每次會議紀錄，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，包括：系統(網路)架構、人機介面及系統介面
  - 進行非功能檢測，包括：效能檢測、承載力檢測及資安檢測
  - 除資安檢測外，其他各項檢測需求，非資安範圍，請機關依需求自行規劃

驗收階段(2/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 資安驗收內容(1/2)
  - 顧問訓練類
    - 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測
  - 系統發展類
    - 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

驗收階段(3/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 資安驗收內容(2/2)
  - 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
    - 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

驗收階段(4/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 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
  - 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

保固作業(1/2)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 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

保固作業(2/2)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 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
- 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
- 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

大綱

- 資訊委外類別與形態
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- **注意事項與常見缺失**
- Q&A

計畫作業階段注意事項(1/5)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

1	專案編成：專案編組不恰當或專業人力不足

- 解決方案
  - 適時向資安主管反應，以明確律定各單位權責
    - 尤其是資訊委外之個資清查與風險評鑑，通常需要各業務單位的全力協助
  - 儘量爭取經費以安排適當之教育訓練課程，提升資安專業能力，或外聘顧問解決資安專業人力不足問題

計畫作業階段注意事項(2/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

2 資訊風險評估：未確實評估潛在風險或虛應故事

- 解決方案
  - 參閱「資通系統風險評鑑參考指引」，根據時間與資源限制，選擇合適風險評鑑方式，評估資訊委外資安風險
    - ➢ 高階風險評鑑
    - ➢ 詳細風險評鑑

計畫作業階段注意事項(3/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

3	廠商提出對應措施方案：無法有效評鑑廠商提出對應措施建議方案是否符合需要

- 解決方案
  - 對於複雜或大型資訊專案，解決方法是遵循RFI、RFC及RFP之作業程序，配合廠商相互競爭實況，提升方案適用性與有效性
  - 對於簡單或小型資訊專案，則外聘顧問協助審查

計畫作業階段注意事項(4/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

4	建立委外資安管理制度：常以抄襲代替建立符合單位實況之資訊安全管理制度

- 解決方案

  依據機關屬性、規模及資源，確實建立符合機關實際需求之「資訊委外資安政策」與相對應程序與表單

計畫作業階段注意事項(5/5)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

5	資通安全服務水準定義：資通安全服務水準定義不當或不明確
6	委外服務契約項目規劃：委外服務契約項目規劃不當或不明確

- 解決方案

  依時間與資源，適當評估資訊委外資安風險，並遵循RFI、RFC及RFP之作業程序辦理

履約管理階段注意事項(1/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

1	執行契約規範項目：未能依據合約與RFP要求，確實執行契約規範項目
2	採行控制措施：未能依據合約與RFP要求，確實執行契約規範項目

- 解決方案

  依時間與資源，適當評估資訊委外資安風險，並遵循RFI、RFC及RFP之作業程序辦理

履約管理階段注意事項(2/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

3 新系統上線作業審查措施：未能確實執行新系統上線作業審查，並依相關作業程序辦理

- 解決方案

  確實要求執行新系統上線審查，如有專業或人力不足時，應及早請求協助，或委請第三方協助解決專業與人力不足問題

履約管理階段注意事項(3/5)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

4	資安事件之反應與處理：發生資安事件時隱匿不報

- 解決方案
  - 在資通安全管理政策、規範或程序中，訂定適當獎懲措施，以建立資安作業紀律
  - 定期或不定期實施抽查與演練

履約管理階段注意事項(4/5)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

5	營運持續管理：營運持續管理計畫未依據實際狀況修訂，或事件發生時無法有效執行

- 解決方案

  定期或不定期實施演練，並檢討實際執行與計畫間差距，適時修訂營運持續管理計畫，做為後續矯正預防參考

履約管理階段注意事項(5/5)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

6 緊急應變計畫檢查缺失的改善：未能確實追蹤管制缺失改善情形

- 解決方案

  建立追蹤機制，並納入定期會議中檢討改善

驗收階段注意事項(1/4)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

1	定期評估與稽核廠商資安控管績效：未能確實執行定期評估與稽核廠商資安控管績效

- 解決方案

  將評估與稽核廠商資安相關工作，納入工作要項與機關工作行事曆

驗收階段注意事項(2/4)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

2	會議與文件資料：會議與文件資料建立不確實或不完整

- 解決方案

  委請第三方協助解決專業與人力不足問題

驗收階段注意事項(3/4)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

3	軟體委外開發稽核：軟體委外開發稽核能力不足

- 解決方案

  委請第三方協助解決專業與人力不足問題

驗收階段注意事項(4/4)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

4	異動稽核措施是否符合預期效能：未能確實執行異動稽核措施

- 解決方案

  確實執行異動稽核措施，如有專業或人力不足時，應及早請求協助，或委請第三方協助解決專業與人力不足問題

其他注意事項

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

1	廠商資格審查是否依RFP與契約書規定辦理(含外國或大陸地區廠商)
2	遴選評選委員時，是否考量其學經歷、相關領域實務經驗及利益迴避等條件
1	評選廠商投標建議書時，評選委員是否將資安列入評選項目
1	廠商是否定期召開工作進度報告會議，並提交工作報告
2	配合各階段需求，規劃並實施充足之教育訓練，推動並提昇委外人員資安知識與技能
3	是否完成程式源碼檢測，執行程式弱點掃描
4	是否定期執行系統弱點掃描
5	發現資安弱點與可能面臨的威脅，是否請原設計廠商提供變更計畫
6	執行中之資通系統發生異常或系統漏洞時，機關對是否詳細評估廠商所提之變更計畫對系統的影響並獲得批准

稽核資訊服務委外常見缺失-1

- 委外資訊服務應在選商、訂定契約相關文件與執行時注意：
  - 應符合資安法施行細則第四條之受託者(委外廠商)應具備與應提供事項，如資安專業人員、資安管理措施或第三方驗證、系統上線之安全檢測證明。
  - 應與廠商約定委外系統適用之防護基準。
  - 應與廠商約定維護水準，如保證系統的完修時間，符合資安維護計畫中的最大容忍中斷時間。
  - 應依資安維護計畫，落實委外廠商與人員簽署保密協議。

稽核資訊服務委外常見缺失-2

- 委外資訊服務應在選商、訂定契約相關文件與執行時注意：
  - 應對受委託廠商履約督導管理，如受託者服務範圍之資安管理措施的有效性、系統適用防護基準之檢核。
  - 應將軟體開發生命週期之各階段安全要求納入合約。
  - 應將委外關係結束後之資料返還、刪除與保密責任列入合約要求中。
  - 應約定受委託廠商，知悉資安事件的通報與應變處理責任。

相關範本

- 資通系統籌獲各階段資安強化措施(資安署)
  https://moda.gov.tw/ACS/laws/guide/rules-guidelines/1355
- 政府資訊作業委外資安參考指引
  https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh
- 辦理受託業務-受託者之選任及監督
  https://moda.gov.tw/ACS/laws/faq/06/642
- 資訊服務採購契約範本
  https://www.pcc.gov.tw/cp.aspx?n=99E24DAAC84279E4

Thanks for your Attention

Thanks for your Attention

Thanks for your Attention

Thanks for your Attention

Q & A