政府資訊作業委外安全管理

行政院國家資通安全會報技術服務中心

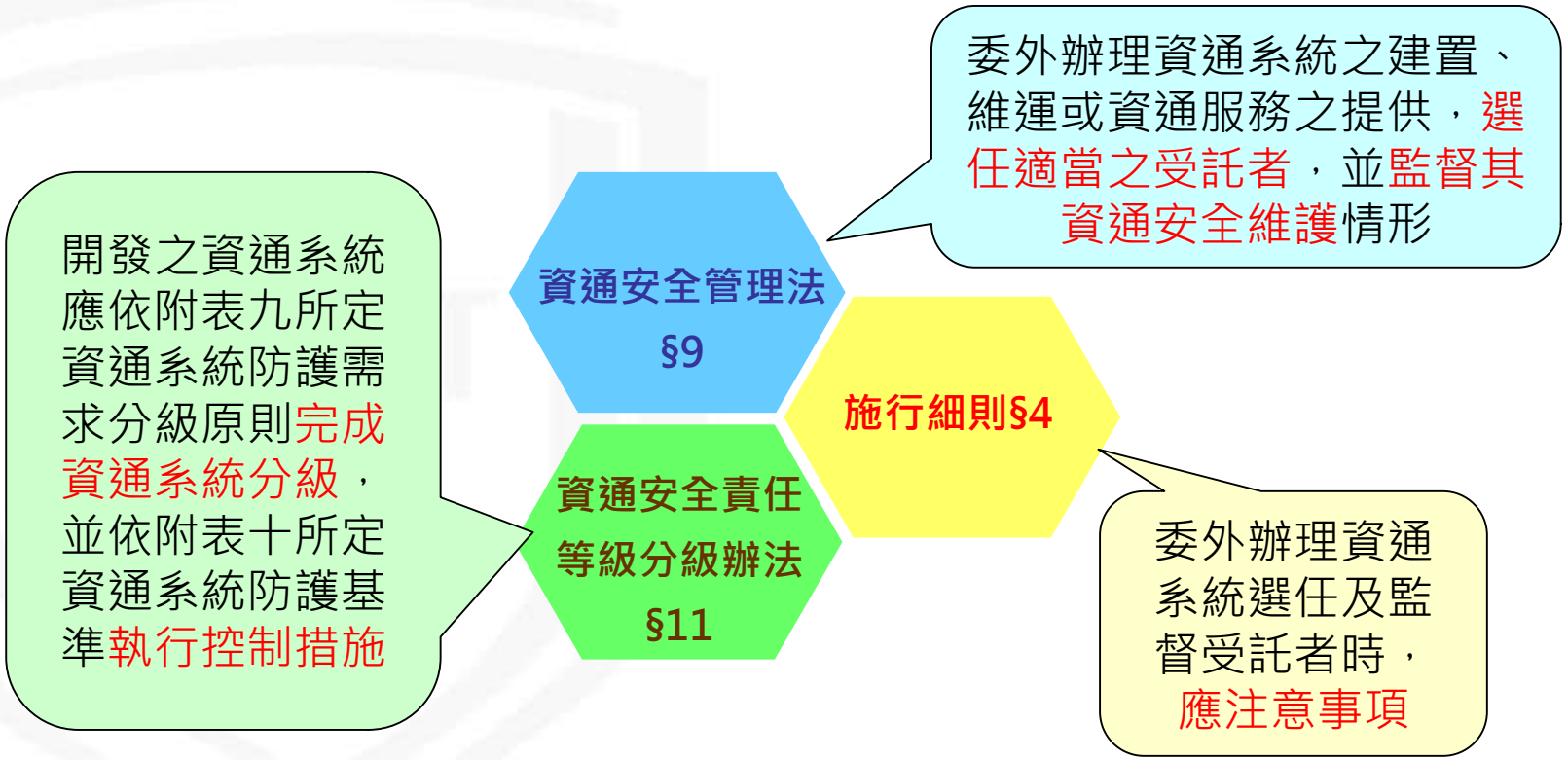
108年5月

大綱

- 前言
- 資訊作業委外安全管理
- 資訊作業委外安全參考資訊
- 結論與建議

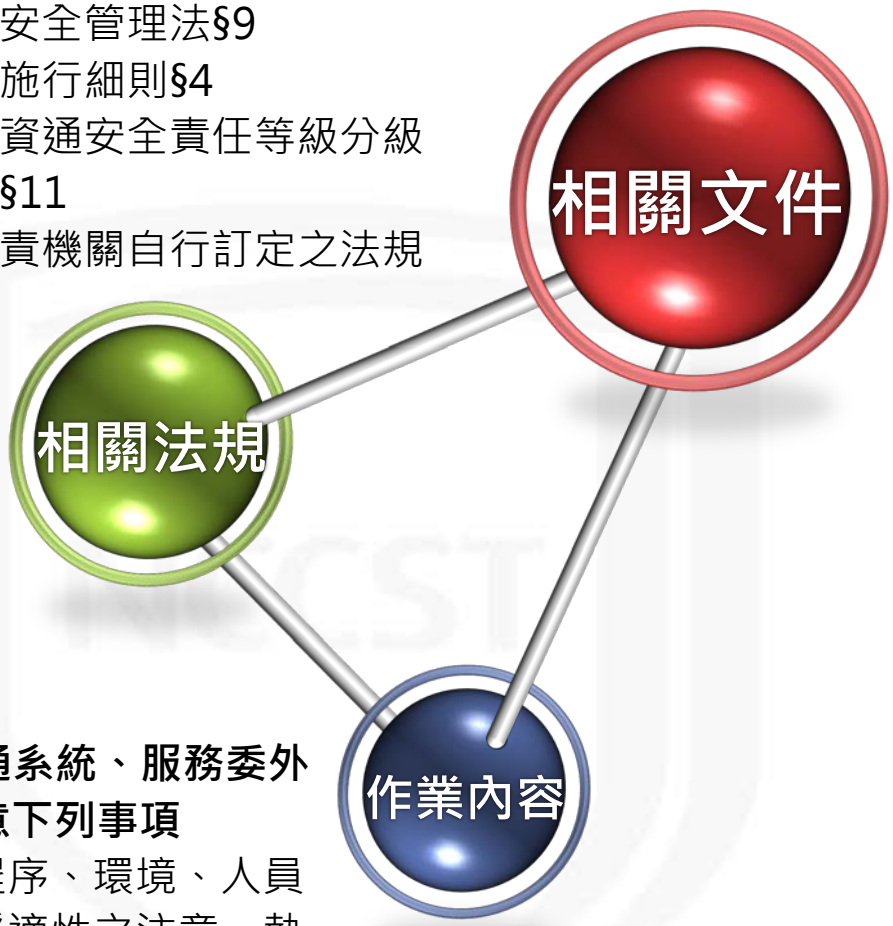
前言

- 資通安全管理法於107年5月11日立法院三讀通過，同年6月6日總統令公布，相關子法行政院於同年11月21日發布，並自108年1月1日開始施行



資訊作業委外安全法規與文件

- 資通安全管理法§9
- 本法施行細則§4
- 本法資通安全責任等級分級辦法§11
- 各權責機關自行訂定之法規



- **資通系統、服務委外注意下列事項**
  - 程序、環境、人員妥適性之注意、執行內容之查核、資料之移轉、刪除

各機關適用

- **參考指引**
  - 政府資訊作業委外安全參考指引
  - 資通系統風險評鑑參考指引
- **RFP**
  - 資通系統委外開發資安需求RFP
  - 資安健診服務RFP
  - 資安監控服務RFP
  - 弱點掃描服務RFP
  - 滲透測試服務RFP
  - 社交工程郵件測試服務RFP
  - 政府機關資訊安全管理系統(ISMS) RFP
  - 政府機關資訊安全管理系統(ISMS)第三方驗證RFP
- **表單與文件**
  - 委外廠商人員保密切結書
  - 委外廠商查核項目表

大綱

- 前言
- 資訊作業委外安全管理
- 資訊作業委外安全參考資訊
- 結論與建議

資訊作業委外安全管理

- 資訊作業委外定義
- 資訊作業委外型態
- 資訊作業委外安全原則
- 資訊作業委外資安策略
- 資訊作業委外資安重點
- 資訊作業委外常見風險
- 資訊作業委外注意事項與常見缺失

資訊作業委外定義

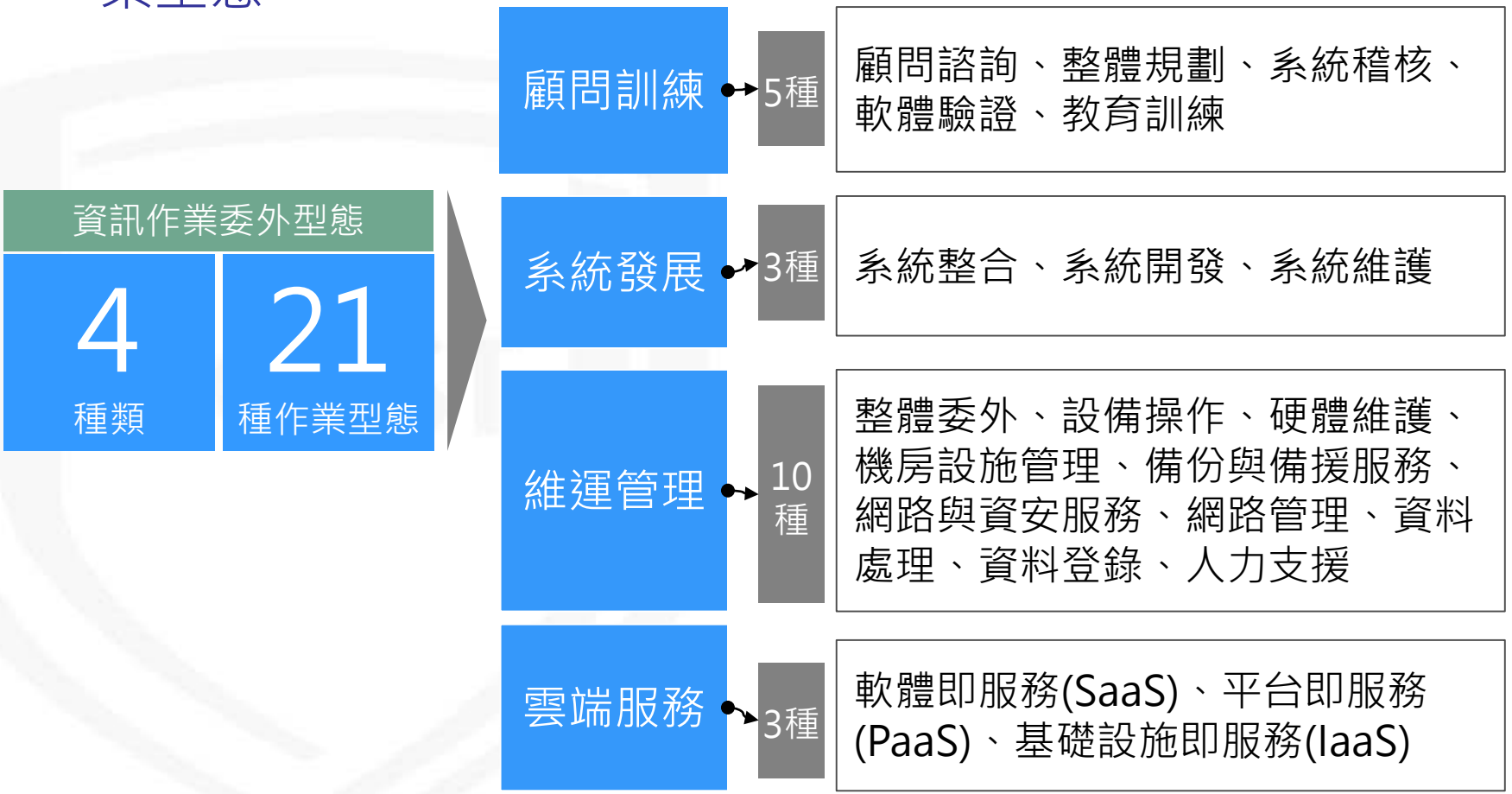
資訊作業委外定義

- 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、系統規畫及應用系統軟體採購等(Grover, Cheon & Teng-1996)
- 將組織中資訊相關活動，部分或全部由組織外的資訊服務提供者來完成(Lee & Kim-1999)
- 將資訊系統之功能以合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(Kishore et al.-2003)

將政府機關之資訊服務所有相關活動，部分或全部委由機關外之資訊服務提供者完成

資訊作業委外型態

- 為方便承辦人辦理委外作業，將委外作業區分為：顧問訓練、系統發展、維運管理及雲端服務等 4 類，共 21 種作業型態



資訊作業委外安全原則(1/3)

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訊安全需求，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

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

依據：施行細則§4

資訊作業委外安全原則(2/3)

受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明

資通系統屬委託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，委託機關應自行或另行委託第三方安全性檢測證明

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

依據：施行細則§4

資訊作業委外安全原則(3/3)

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訊安全維護措施

受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行補救措施

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

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訊服務業者參與

依據：施行細則§4

資訊作業委外資安策略(1/2)

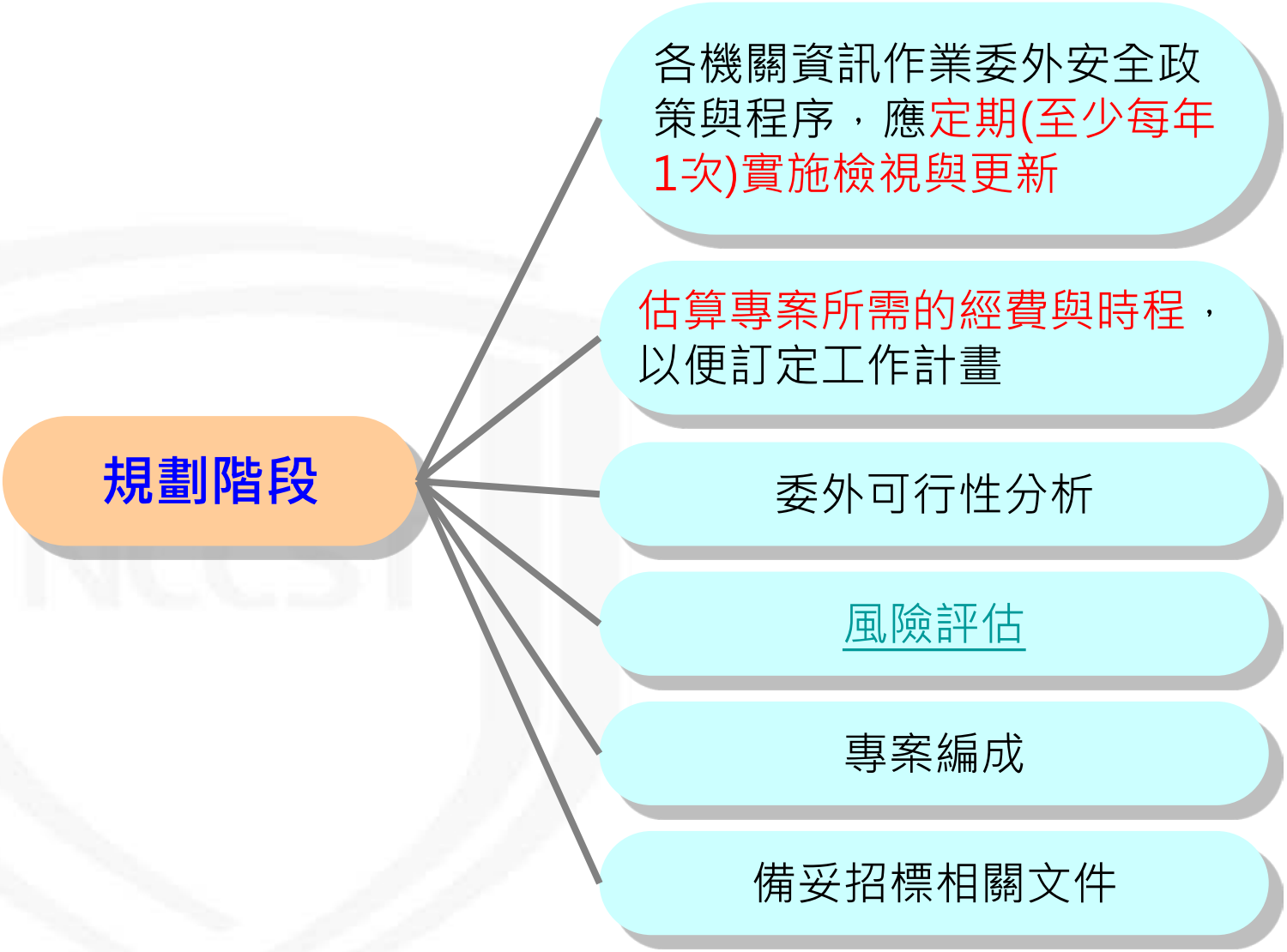
- 規劃階段
  - 將機關之安全規範與對廠商資安要求納入【契約書或RFP】
  - 將資通安全檢測需求所需費用列入成本分析計價項目，如Web資安檢測服務與報告等
  - 將資通安全需求納入RFP中，列為委外需求與評比必要項目
  - 委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形
- 執行階段
  - 要求廠商遵循主管機關訂定之標準或規範執行，並提供可行建議方案，確保委外作業安全

資訊作業委外資安策略(2/2)

- 因應【個資法/施行細則】之施行
  - 委託機關必須負起「監督」職責
  - 廠商(被委託單位)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
- 因應歐盟隱私保護法(General Data Protection Regulation, GDPR)
  - 機關如果服務之交易涉及歐盟境內個人之資料取得，應遵循GDPR之要求

行動應用App的開發與運作日益普及，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“相關要求

資訊作業委外資安重點-1



建議書徵求文件(RFP)

- 建議書徵求文件(RFP)為廠商執行委外作業之需求依據，為資通安全要求之重點，需謹慎訂定相關要求，或可要求投標廠商於投標建議書中提出相對應作法。相關執行重點如下
  - 基礎環境需求
  - 系統功能需求
  - 介面需求
  - 績效需求
  - 安全需求
  - 專案管理需求
  - 其他需求

專案管理需求參考內容

項次	計畫項目	顧問訓練	系統發展	維運服務	雲端服務
1	與機關資安相關之協調作業	O	O	O	O
2	作業人員職務的區隔		O	O	O
3	開發、測試及作業程序規劃		O		
4	系統運作程序與方式			O	O
5	由第三者執行查核與驗證相關之配合作業		O	O	O
6	系統存取控制之安全			O	O
7	作業變更管理		O	O	O
8	服務交付方式	O	O	O	O
9	資料被查詢與異動之軌跡紀錄		O	O	O
10	交付之軟體與硬體元件來源不得為大陸地區		O		O
11	防範惡意碼與安全漏洞措施		O	O	O
12	後門程式清理		O	O	O
13	保固期間發現系統或程式弱點之修復方式		O		
14	系統維運期間之定期系統弱點掃描服務措施			O	O
15	委外媒體的處置措施	O	O	O	
16	服務驗收或稽核服務之管理程序	O	O	O	O

項次	計畫項目	顧問訓練	系統發展	維運服務	雲端服務
17	專案人員應參與機關之資安管理規範與個資法等之教育訓練	○	○	○	○
18	專案人員籌組與異動時之規劃	○	○	○	○
19	訂定驗證項目，以鑑定資安服務水準	○	○	○	○
20	駐點人員之管理計畫			○	
21	新應用程式與系統的開發建置應有之規劃		○		
22	資訊安全事故管理			○	○
23	資訊安全事件之檢討與監督			○	○
24	服務終止之措施	○	○	○	○
25	所有權與智慧財產之保障	○	○	○	○
26	遵循適法性做法	○	○	○	○

資訊作業委外資安重點-2

執行階段

管理重點	
資通安全組織	委外人力資源安全
委外相關風險識別	委外實體與環境安全
與廠商協議中之安全說明	委外作業管理
委外使用者存取管理	委外資通安全事件管理

遵循適法性要求

資訊作業委外資安重點-3

驗收階段

- 請廠商提交「專案工作計畫書」
- 定期召開工作進度報告會議，並提交工作報告
- 依機關要求格式，交付契約內要求之各項文件
- 進行功能檢測，包括系統(網路)架構、人機介面及系統介面等，規劃並實施充足教育訓練
- 進行非功能檢測，包括效能檢測、承載力檢測及資安檢測等
- 保固作業與異常管理

資訊作業委外常見風險

策略面

對於整個營運活動中有相當重要的影響力，特別是對於資訊作業委外服務內容之型態、範圍及管理方式等策略是否妥適，會直接或間接影響到機關資通安全

治理面

在合約關係生命週期中，對廠商缺乏管理，可說是資訊委外安全的主要風險。政府機關與廠商之間沒有定義適當的管理模式，可能增加資訊作業失誤、遵循性風險、作業風險及財務風險

需求面

不適當的需求規劃或描述可能對廠商合理的執行服務產生衝擊，長期可能導致政府機關在營運、財務、法律及聲望上的問題，應該在計畫階段就必須考量資通安全需求，並納入需求規劃

合約面

未能完整涵蓋合約需要被管理的各種關係，即不完整的合約是整個合約關係中最大的風險。例如忽視款項支付細節、要求廠商不切實際的服務水準、缺乏合約終止規範與任何智慧財產權、個資等規範

廠商面

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的風險，在簽訂合約前應採取適當的廠商盡責調查措施，以降低各類風險，使廠商能有更好的長期的履約能力與穩定性

參考CNS 27014資安治理標準，
獲得更多對治理面概念

資訊作業委外注意事項或常見缺失(1/2)

1	專案編成：專案編組不恰當或專業人力不足
2	資訊風險評估：未確實評估潛在風險或虛應故事
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
4	建立委外安全管理制度：常以抄襲代替建立符合機關實況之資通安全管理制度

資訊作業委外注意事項或常見缺失(2/2)

5	軟體委外開發稽核：軟體委外開發稽核能力不足，或未執行第二方稽核
6	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
7	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
8	資安事件之反應與處理：發生資安事件時隱匿不報

大綱

- 前言
- 資訊作業委外安全管理
- 資訊作業委外安全參考資訊
- 結論與建議

資訊作業委外安全參考資訊

- 勞務採購契約範本及相關文件
- 資訊服務採購契約範本
- 資訊作業委外RFP範本

勞務採購契約範本及相關文件(1/3)

- 公共工程委員會所提供諸如投標須知範本、勞務採購契約範本等招標、投標及契約範本(https://www.pcc.gov.tw/cp.aspx?n=99E24DAAC84279E4)及相關法規、說明等文件，均適用於資訊委外作業
- 契約書與資安相關部分

招標方式

- 為避免產生資安困擾，針對外國廠商、大陸地區、第三地區含陸資成分廠商或在臺陸資廠商，建議依採購法第20條與第22條採「限制性招標」或「選擇性招標」方式辦理
- 要求投標廠商應詳列資金來源，禁止有來自大陸地區、第三地區含陸資成分廠商或在臺陸資廠商，得標廠商之專案成員中，不得有來自大陸地區者，其分包廠商亦同
- 不適用我國締結之條約或協定之外國廠商，前述三類採購對象均建議勾選「不可參與投標」

勞務採購契約範本及相關文件(2/3)

履約管理

- 涉及須保密事項者，廠商未經機關書面同意，不得將契約內容洩漏予與履約無關之第三人
- 廠商擬分包之項目與分包廠商，機關得予審查。廠商對於分包廠商履約之部分，仍應負完全責任。「具敏感性或國安(含資安)疑慮之業務範疇」，廠商不得以投審會網站公告之陸資資訊服務業者為分包廠商
- 履約管理內容已包含個資法對機關與非機關之個資保護不當之損害賠償責任

勞務採購契約範本及相關文件(3/3)

契約經依規定或因可歸責於廠商之事由致終止或解除者，機關得依其所認定之適當方式，自行或洽其他廠商完成被終止或解除之契約；其所增加之費用及損失，由廠商負擔

因應個資法之規定，若機關業務致生個資損害，即可能面臨賠償責任，建議增列保險需求，以分散風險

專案如係由第三方協助驗收或稽核服務，建議增加「本案委託第三方協助驗收或稽核服務，其相關之職掌與作業程序等，依RFP之規定辦理

資訊服務採購契約範本(1/2)

- 資訊安全責任

廠商應遵守行政院所頒訂之各項資訊安全規範及標準，並遵守機關資訊安全管理及保密相關規定。此外機關保有對廠商執行稽核的權利

廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號

契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄

資訊服務採購契約範本(2/2)

廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存

廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理

廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合機關對系統品質及資訊安全的要求

資訊作業委外RFP範本

- 網站建置RFP資安需求範例(系統發展類)
- 資通系統委外開發RFP資安需求範本(系統發展類)
- 網路架構委外建置與維運RFP資安需求範例(維運管理類)
- 資通系統雲端服務管理RFP資安需求範例(雲端服務類)

共通性RFP資安需求範例(1/2)

- 基礎環境需求

投標廠商背景資格限制
• 廠商不得為大陸地區廠商或第三地區含陸資成分廠商 • 分包廠商亦不得為大陸地區廠商或第三地區含陸資成分廠商 • 不得將開發工作移至本國以外地區或其指定排除之國家 • 本專案廠商宜通過專業之認證，如CMMI、ISO 27001及CNS 27001等

實體與環境安全管理需求
• 設備安全：委外所需存取或委外作業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、智慧卡及所有形式的儲存設備等，於機關場所內使用任何資訊處理設備均應受管理 • 門禁管理：委外作業人員進出本機關均應配帶臨時員工證件，非經許可不得至工作場所以外地區活動

共通性RFP資安需求範例(2/2)

專案管理	• 得標廠商應於決標後○日曆天(如15日曆天)內提交專案工作計畫書，作為工作交付項目並為執行專案之依據
作業安全項目	• 作業人員職務的區隔 • 作業變更管理 • 專案人員應參與機關之資安管理規範與個資法等之教育訓練
資安稽核需求	• 本機關基於法令及合約需求，得要求實施定期或不定期稽查，以監督專案內各項安全管理執行情形
所有權與智慧財產之歸屬	• 廠商因履行契約所完成之著作，其著作財產權之全部於著作完成之同時讓與機關 • 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

網站建置RFP資安需求範例

- 資安技術功能需求
  - 本專案系統經鑑別屬「○」安全等級，投標廠商應依資通安全管理法及相關子法規定採行適當安全控制措施，以確保資通系統達到應具備之安全防護水準。廠商應於評選階段提出自我說明報告或由第三方公正單位提出驗證報告，以確認執行情形；另資安技術需求檢測內容，應依附件3之附錄1「政府Web網站委外安全注意事項與安全檢核表」辦理

- 安全服務需求
  - 漏洞修補更新需求
  - 資通安全改善建議
  - 安全傳輸需求
  - 行動App開發安全

Web 應用程式安全檢核表						
控制措施	類別	實作項目	適用分級			是否符合
			普	中	高	
存取控制	帳號管理	使用者的會談階段，設定該帳號在合理的時間(至多 30 分鐘)內未活動即自動失效	◎	◎	◎	
		使用者的會談階段在登出後失效	◎	◎	◎	
		管理者介面限制存取來源或不允許遠端存取	◎	◎	◎	
	最小權限	對使用者/角色，僅賦予所需要的最低權限		◎	◎	
		軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限		◎	◎	
	遠端存取	採用伺服端的集中過濾機制檢查使用者授權	◎	◎	◎	

資通系統委外開發RFP資安需求範本(1/2)

本範本內容係依據「資通安全責任等級分級辦法」之附表10「資通系統防護基準」安全控制措施，進行資安需求項目分級(普、中、高)與內容訂定

共計41項技術面及13項管理面資安需求項目(資通系統資安需求項目查檢表)

另22項資通系統防護基準之控制措施，因其性質屬於日常維運工作，較不適合交由委外開發廠商(乙方)代為履行，建議整合至機關(甲方)內部之管理流程(機關日常維運管理需求項目查檢表)

政府機關可依據資通系統防護需求等級，選取適用之資安需求項目列入RFP

資通系統委外開發RFP資安需求範本(2/2)

3.2.1.3 識別與鑑別

3.2.1.3.1 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。

適用分級：普、中、高。

說明：資通系統應具備唯一識別及鑑別機關使用者之功能，如禁內部使用者建立個別帳號，以強化系統之可歸責性(Accountability)。若多人共用同一個帳號登入系統，則難以從稽核紀錄識別確切的使用者身分。

3.2.1.3.2 對帳號之網路或本機存取採取多重認證技術。

適用分級：高。

說明：系統身分驗證或重要交易行為，可採用多重因素身分驗證以強化安全性。多重因素身分驗證係指具備兩種以上驗證類型，驗證類型一般區分為所知之事(Something you know)、所持之物(Something you have)及所具之形(Something you are)。所知之事類型如密碼、特定問題之答案等；所持之物類型如晶片卡、憑證等；所具之形類型常採用生物特徵，如指紋、虹膜辨識等。

技術面資安需求					
分類	安全需求項目	適用分級			評量結果(是/否/不適用)
		普	中	高	
識別與鑑別	3.2.1.3.1 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	V	V	V	
	3.2.1.3.2 對帳號之網路或本機存取採取多重認證技術。			V	

網路架構委外建置與維運RFP資安需求範例(1/2)

遠端存取服務

投標廠商應依本專案需求提供安全的遠端存取服務，以利遠端使用者透過公眾網路安全的連接本機關公務網路，並應說明其配置、規劃、運作及管理方式，同時符合相關工業或網路安全標準

網路安全防護需求

投標廠商應規劃、配置及提供網路安全服務，以利本機關於履約期間各種實體與邏輯設備能安全的連接公共網路，包括網路防火牆、應用程式防火牆、入侵偵測系統及其他相關資安防護設備

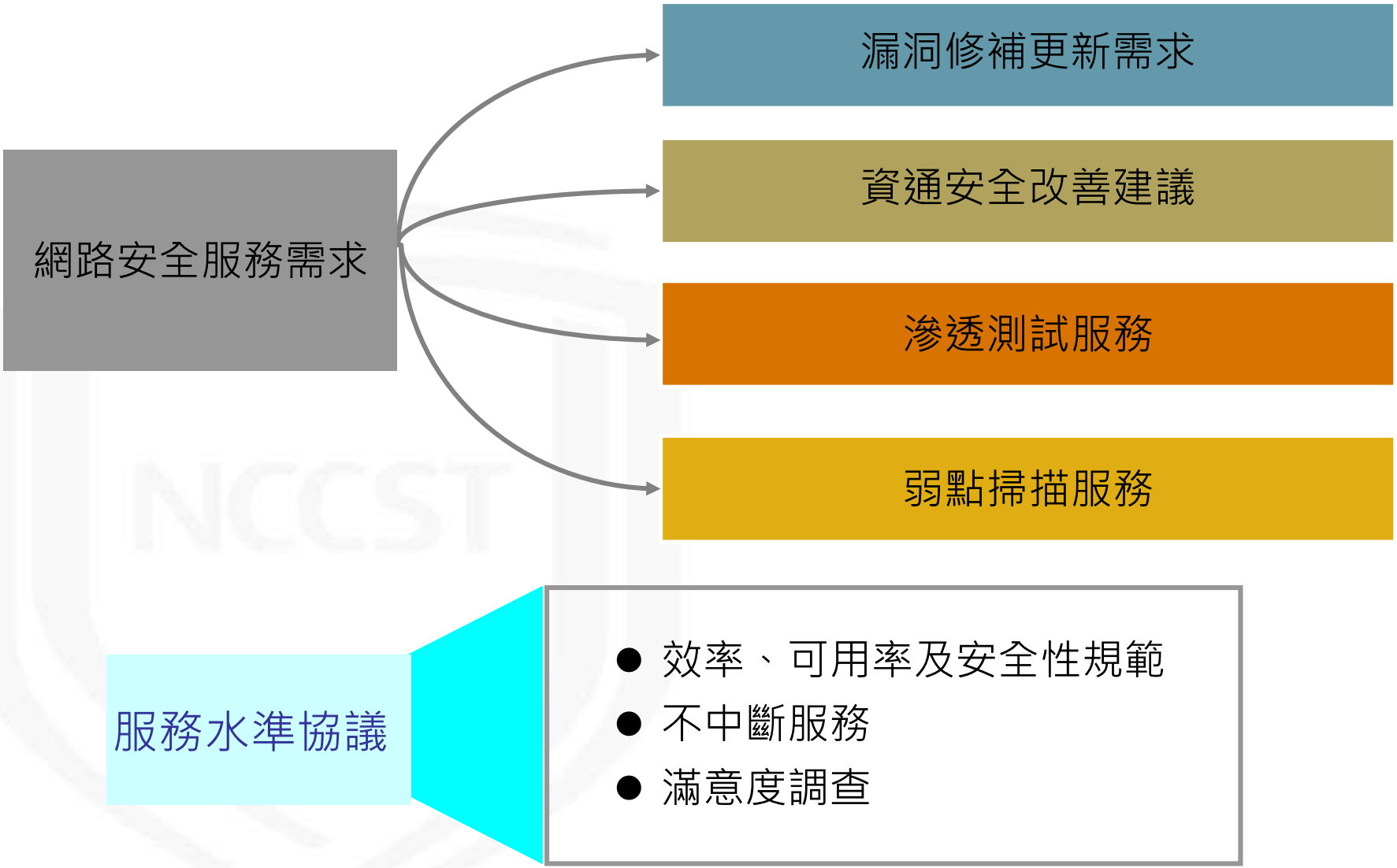
事件緊急應變處理與鑑識需求

投標廠商應根據日常監控與狀況，主動分析是否屬安全事件，並依照行政院國家資通安全會報相關通報應變標準啟動對應之處理程序，協助本機關執行相關處理程序

資安攻防演練服務

廠商應針對本機關對外提供服務之網路或資訊系統，每年至少辦理資安攻防演練1次，演練期間應提供滲透測試服務至少1次，測試時間與標的由本機關指定，並於測試前30天通知廠商，廠商提出攻防演練計畫後經本機關同意後施行，廠商於攻防演練辦理完畢後，應提出書面報告，除說明現有系統弱點及安全狀況，並提供本機關整體資安改善方法與建議

網路架構委外建置與維運RFP資安需求範例(2/2)



資通系統雲端服務管理RFP資安需求範例(1/2)

- 網路及系統安全需求
  - 網路安全需求
  - 持續性監控
  - 事件緊急應變處理與鑑識需求
  - 安全認證機制
- 隱私安全需求
  - 符合個人資料保護法及相關法規
  - 隱私衝擊分析
  - **資料儲存**

資通系統雲端服務管理RFP資安需求範例(2/2)

- 雲端電子紀錄蒐集與保護管理

廠商應針對專案資料內容及政府需求於專案期間內提供電子蒐證機制

在蒐集的過程，應遵守相關法規及標準程序進行，確保日後相關證據可被法庭採納

廠商應保留雲端資訊系統紀錄檔，另應依機關需求定期備份稽核紀錄到機關指定之系統外安全處所

運用加密機制，以保護稽核資訊之完整性

大綱

- 前言
- 資訊作業委外安全管理
- 資訊作業委外安全參考資訊
- 結論與建議

結論與建議

- 政府機關資訊作業大多採委外方式辦理，應依資通安全管理法與相關子法加強委外安全管理
- 依據資通安全需求與機關ISMS相關規定，建立委外安全管控制度與資安計畫，並納入契約與RFP中加以規範
- 確實評估潛在風險，以明確資通安全需求
- 依據委外安全管控需求，確實執行第二方稽核與監督改善措施

報告完畢
敬請指教

適任性查核

- 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(應記載於招標公告、招標文件及契約)
- 辦理適任性查核前，並應經當事人書面同意

委外風險評估

評估風險範圍包含資訊委外內容所可能影響之資產、流程及作業環境，或對機關之特殊威脅性質，並於專案執行前審慎評估可能的潛在安全風險，以強化委外安全

- 威脅性質包括財務、法令、策略、科技、資訊設備、資料運用、智慧財產及可能影響機關環境之結果
- 委外範疇如為資通系統，其風險評估作法可參考「資通系統風險評鑑參考指引」

政府機關於辦理委外作業時，常伴隨受託業務涉及國家機密、資訊科技引用、設備採購或向第三地(如大陸與印度等地區)協同開發等狀況發生，使資安管控條件趨於複雜，機關應了解下列考量

- 受託業務涉及國家機密
- 大陸地區廠商或在台陸資企業之規範
- 資訊科技保護考量
- WTO議題

相關資料請參閱經濟部投資審議委員會與行政院公共工程委員會公告