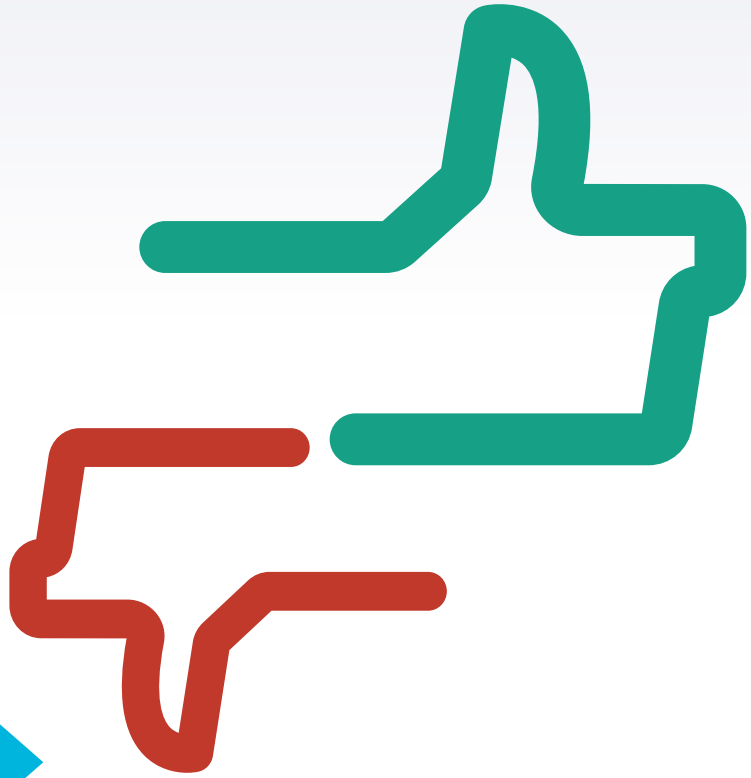
資通安全管理

資安做得比較好的產業來自三大驅動力



- **主管機關或法規要求**（公務機關、關鍵基礎設施產業）
- **客戶要求**，像是大型跨國企業台灣供應鏈資訊安全的強力要求。
- **自身要求**，先行法令高度自我要求的企業組織，擁有目光前瞻的特質，獲得更好安全性的同時，也擴大與同業的競爭力差距。

從ESG角度著手企業資安管理已是全球共識

- **未來政府勢必將有更多作為**，帶動整體產業、跟上時代的腳步。(如:上市上櫃公司資通安全管控指引)
- **道瓊永續發展指數（DJSI）及明晟永續指數（MSCI）等國際永續指標**將資安管理納入永續企業評比項目，資訊安全將是 CXO 層級需要更加正視的課題與挑戰。

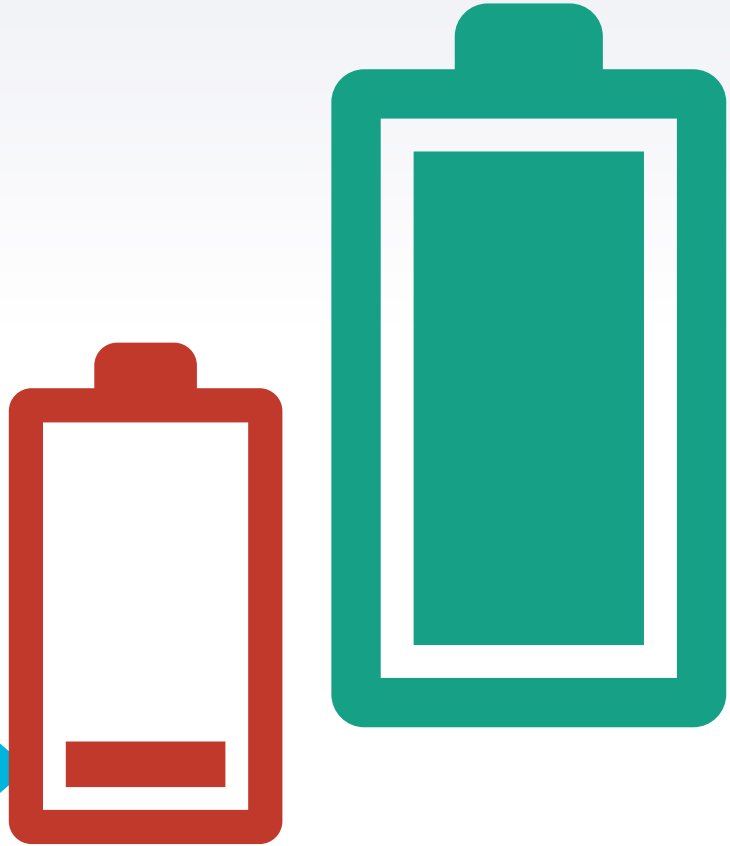
資安管理 v.s. 聯合國永續發展目標SDGs

- SDG 9 產業、創新與基礎設施，投資基礎建設，提高基礎建設的運作效率，**建立具有韌性的基礎建設**。
- SDG 8 尊嚴就業與經濟成長，**加強職業培訓和技能提升**，提高勞動力市場競爭力和就業機會。
- 資安韌性是永續營運的關鍵能力，鞏固企業永續發展的基石。

SDGs一次看懂：聯合國17項永續發展目標內涵是什麼？如何實踐？

ESG治理與數位轉型 — 永續發展於資訊安全風險管理之策略方向

資安政策面、管理面、技術面 全面執行



- **<u>企業永續是目標，而韌性是過程</u>**，「營運不中斷」以及「建立信任」是企業永續與企業韌性的交集。
- 營運服務中斷造成客戶的服務不周，也可能影響到獲利，甚至有可能因為未即時發現的資安漏洞受攻擊蒙受智財權遭竊、個資外洩的風險，是公司治理的隱憂，應提升全員資安意識。

關鍵資安：企業展現韌性是追求永續的必要布局 安碁吳乙南總經理

老闆要轉念 資安才能落實

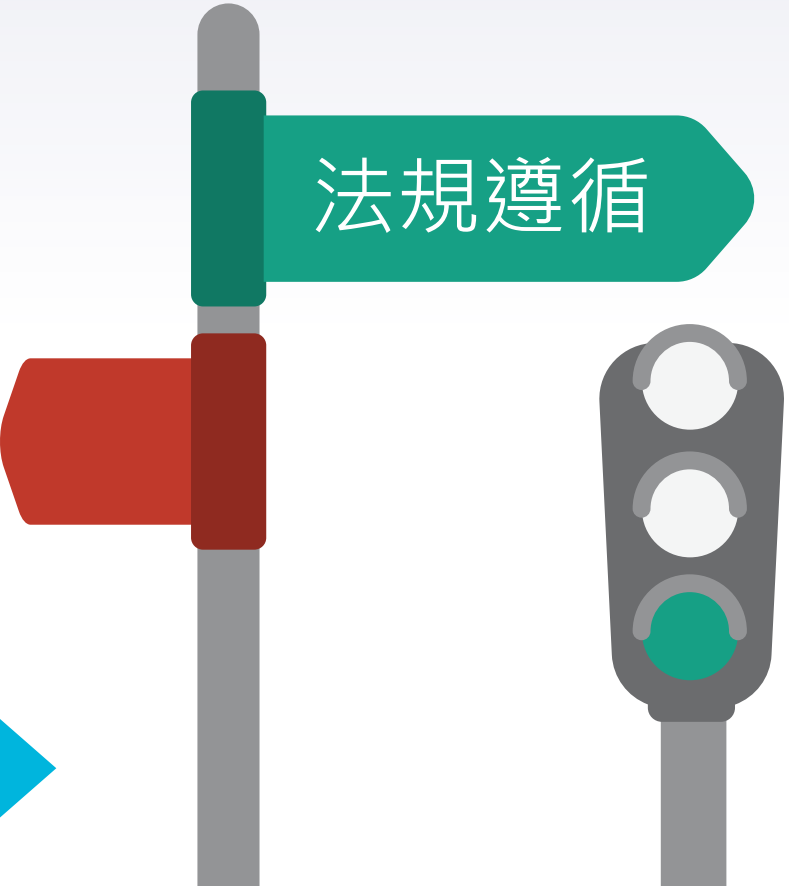
- **資安常面臨「看不到執行效益」的困境**。但是，資安問題只要一發生，對企業造成聲譽、營運、業績的衝擊絕對不輕，資安超前佈署落實與落實，老闆轉念才是關鍵。
- **資安策略的擬定**，(1)建立資安策略的高度、(2)訂定一系列管理制度、(3)投入資源在技術面的提升。

資安政策面、管理面、技術面 全面執行

- 企業談到資訊安全管理，主要著重在**技術面資安基礎建設**，例如建置網路防火牆、防毒軟體及入侵偵測系統等，希望藉由資訊安全軟硬體設備來強化資通安全。
- 但是要有效解決各種資訊安全問題的發生，也必須考量到人員與作業流程，從**政策面、管理面及執行面**全面執行。

上市櫃公司資通安全管控指引發布， 產業該如何因應　安華聯網

資通安全管理法及相關子法、常見問題



資通安全管理法

資通安全管理法施行細則

資通安全責任等級分級辦法

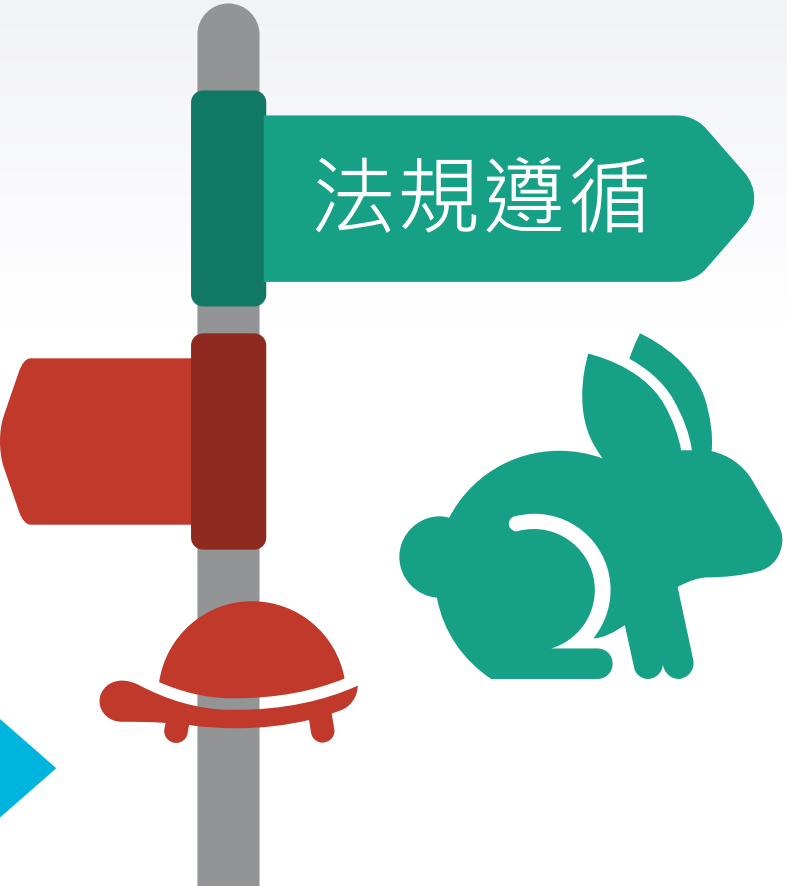
資通安全管理法常見問題

各機關對危害國家資通安全產品限制使用原則

行政院及所屬各機關行動化服務發展作業原則

資通安全事件通報及應變辦法

教育機構資安驗證中心(中興大學)參考資源



[資安法及相關法規重點心智圖]

[資通系統籌獲各階段資安強化措施宣導海報]

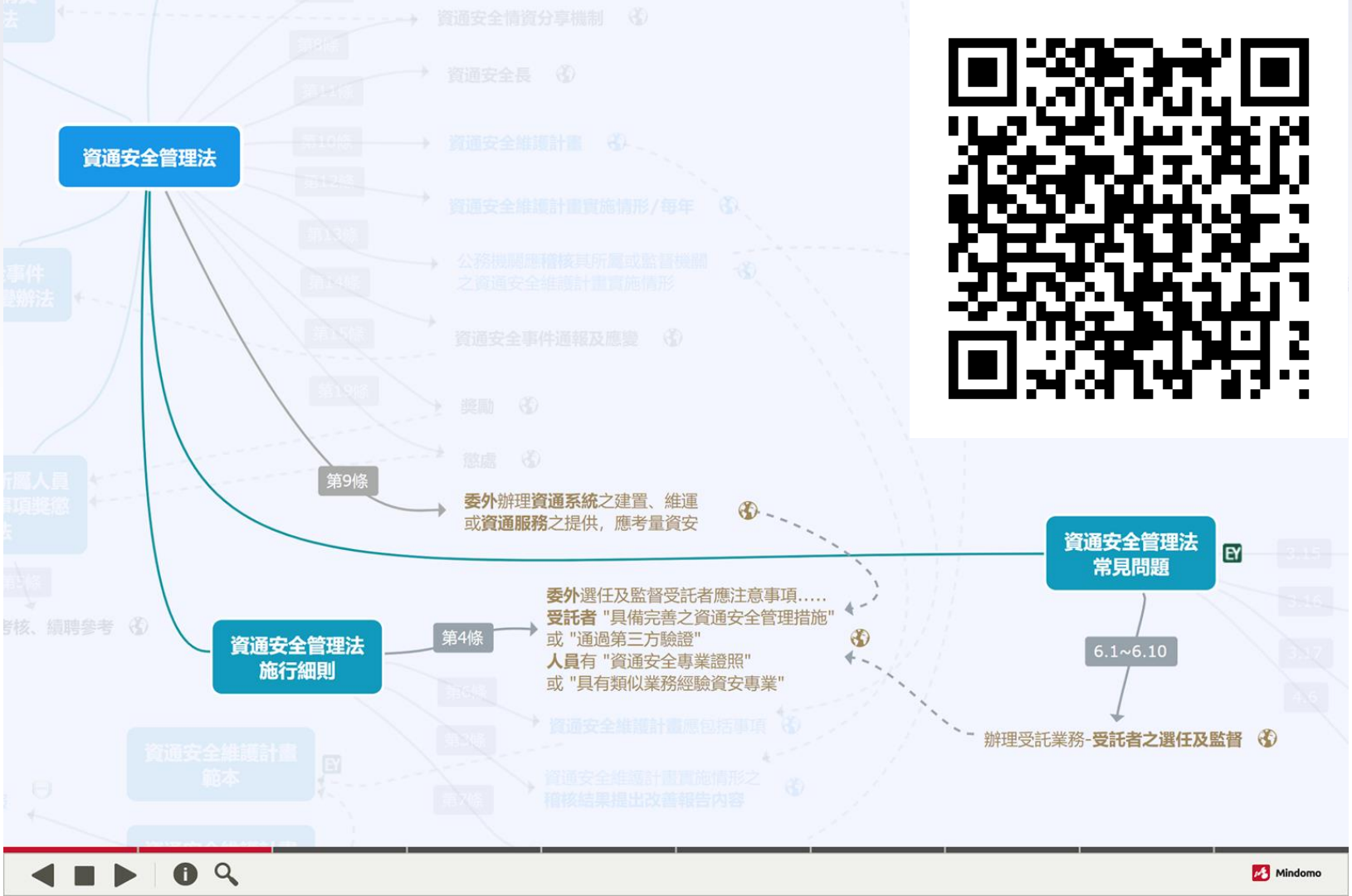
[ISMS優先落實執行策略]

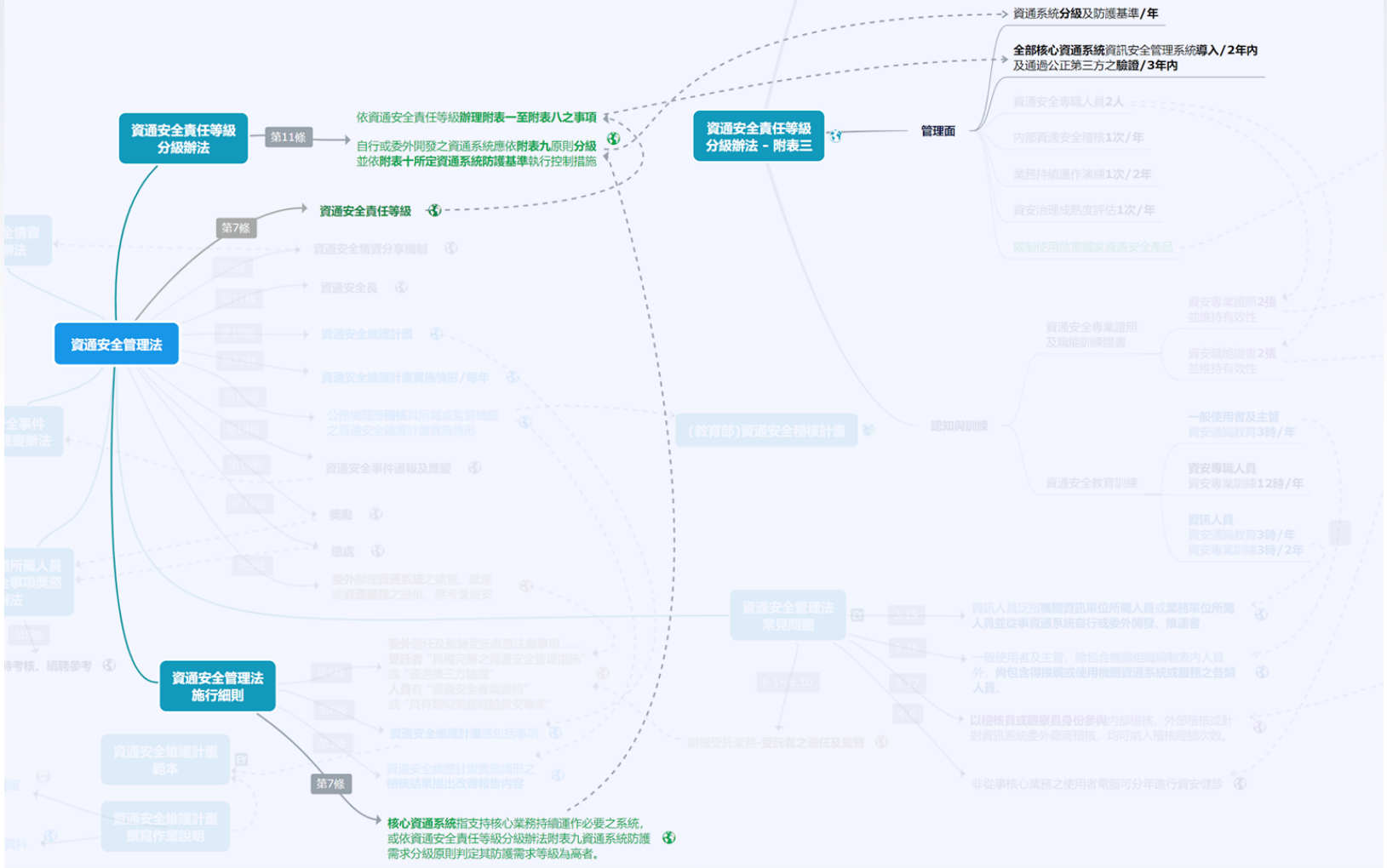
[安全系統發展生命週期SSDLC]

[資通系統高階風險評鑑]

[資訊資產詳細風險評鑑]

[中興大學資安管理更多做法]


資通安全管理法
第9條
委外辦理資通系統之建置、維運
或資通服務之提供，應考量資安
資通安全管理法
常見問題
EY
委外選任及監督受託者應注意事項.....
受託者 "具備完善之資通安全管理措施"
或 "通過第三方驗證"
人員有 "資通安全專業證照"
或 "具有類似業務經驗資安專業"
資通安全管理法
施行細則
第4條
6.1~6.10
辦理受託業務-受託者之選任及監督
Mindomo

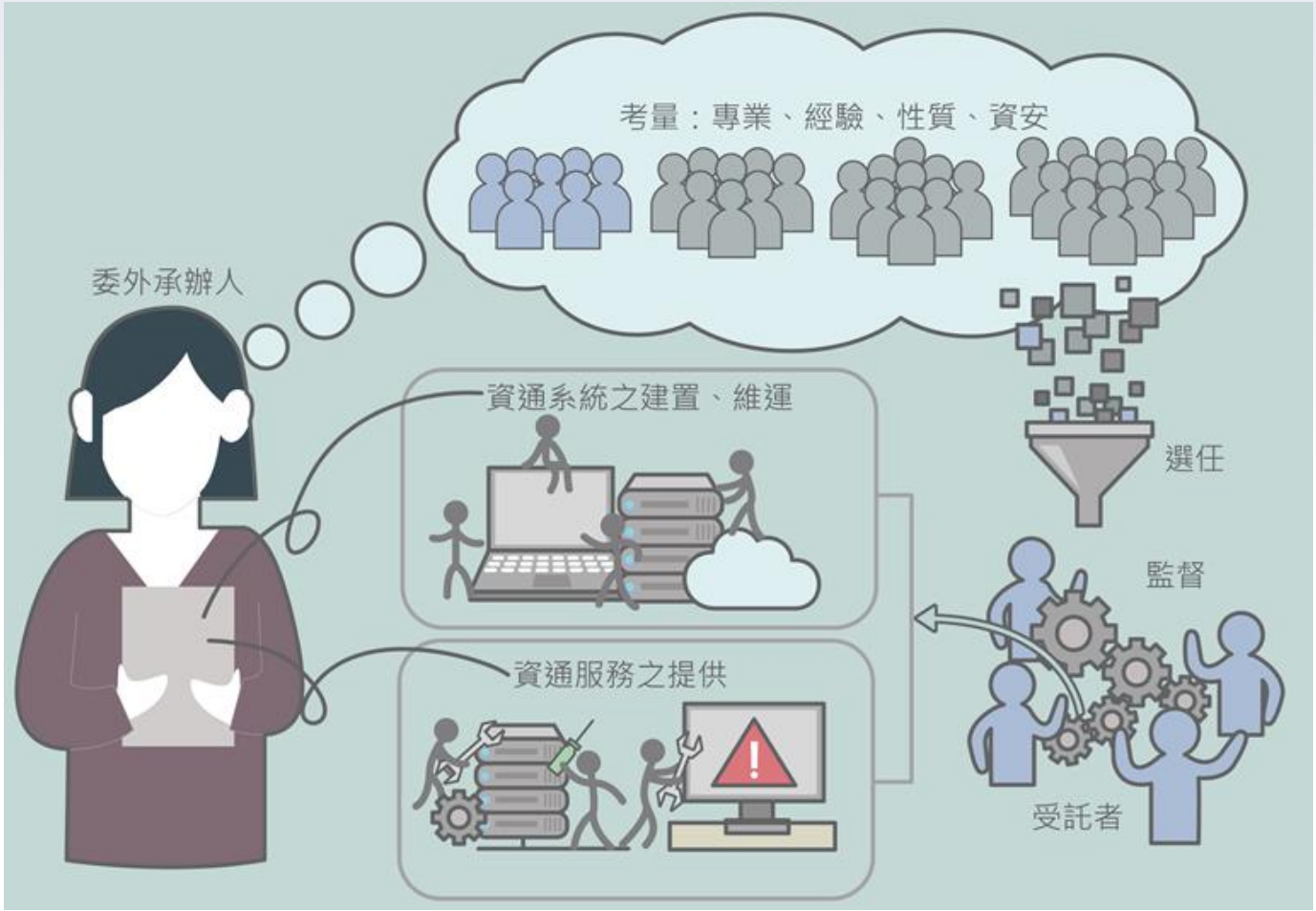

資通安全管理法
資通安全責任等級分級辦法
第11條
依資通安全責任等級辦理附表一至附表八之事項
自行或委外開發之資通系統應依附表九原則分級
並依附表十所定資通系統防護基準執行控制措施
第7條
資通安全責任等級
資通安全情資分享機制
資通安全長
資通安全維護計畫
資通安全維護計畫實施情形/每年
公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形
資通安全事件通報及應變
獎勵
懲處
委外辦理資通系統之建置、維運或資通服務之提供，應考量資安
資通安全管理法施行細則
委外選任及監督受託者應注意事項……受託者「具備完善之資通安全管理措施」或「通過第三方驗證」
人員有「資通安全專業證照」或「具有類似業務經驗資安專業」
資通安全維護計畫應包括事項
資通安全維護計畫實施情形之稽核結果提出改善報告內容
第7條
核心資通系統指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則判定其防護需求等級為高者。
資通安全維護計畫範本
資通安全維護計畫撰寫作業說明
資通安全責任等級分級辦法－附表三
管理面
資通系統分級及防護基準/年
全部核心資通系統資訊安全管理系統導入/2年內及通過公正第三方之驗證/3年內
資通安全專職人員2人
內部資通安全稽核1次/年
業務持續運作演練1次/2年
資安治理成熟度評估1次/年
限制使用危害國家資通安全產品
(教育部)資通安全稽核計畫
認知與訓練
資通安全專業證照及職能訓練證書
資安專業證照2張並維持有效性
資安職能證書2張並維持有效性
資通安全教育訓練
一般使用者及主管 資安通識教育3時/年
資安專職人員 資安專業訓練12時/年
資訊人員 資安通識教育3時/年 資安專業訓練3時/2年
資通安全管理法常見問題
資訊人員泛指機關資訊單位所屬人員或業務單位所屬人員並從事資通系統自行或委外開發、維運者
一般使用者及主管，除包含機關組織編制表內人員外，尚包含得接觸或使用機關資通系統或服務之各類人員。
以稽核員或觀察員身份參與內部稽核、外部稽核或針對資訊系統委外廠商稽核，均可納入稽核經驗次數。
非從事核心業務之使用者電腦可分年進行資安健診
辦理受託業務-受託者之選任及監督

2023.4.7 行政院院授數資安字第1124000032號函
修正「資通安全實地稽核項目檢核表」

資通安全實地稽核檢核項目第五大類

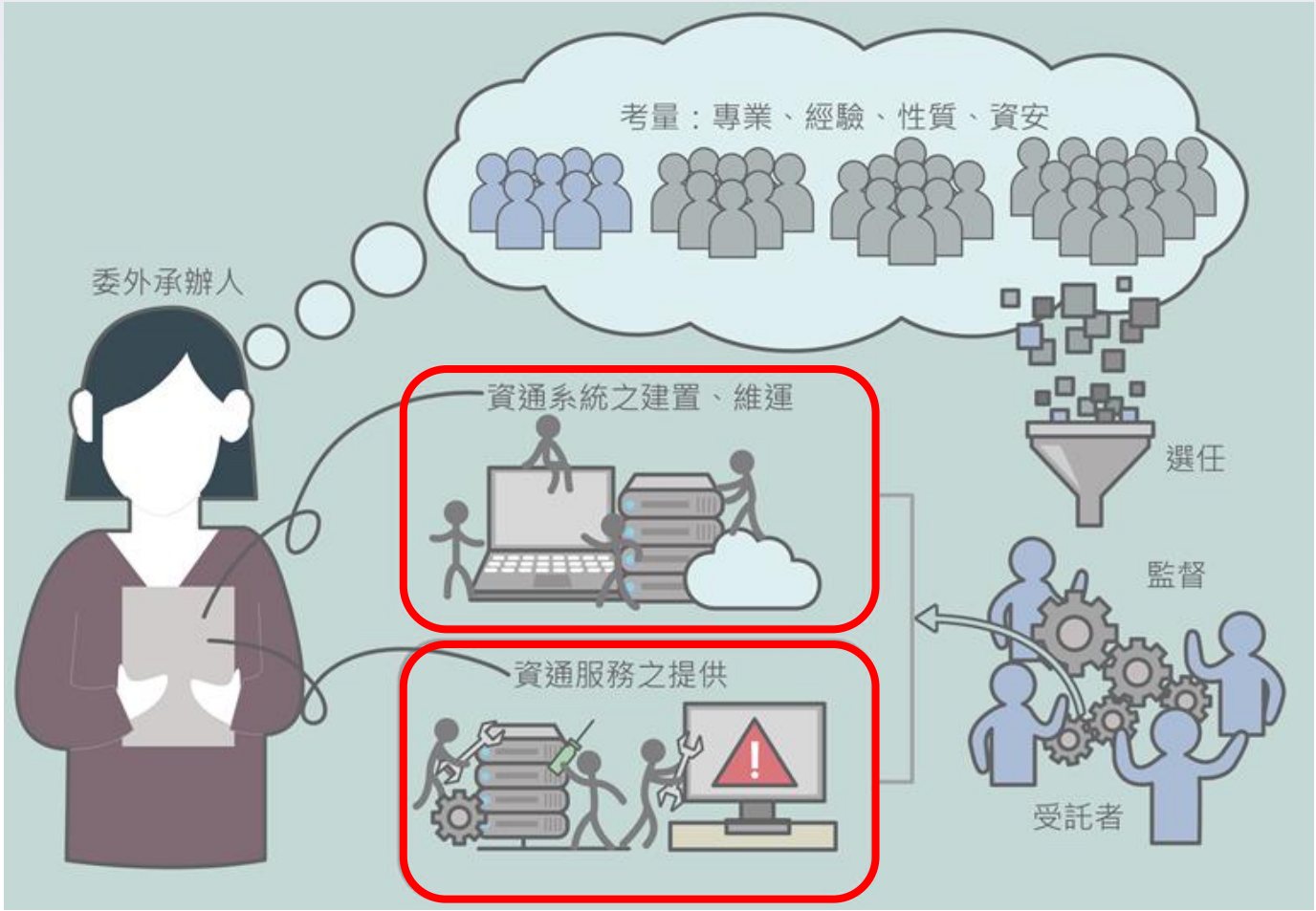
(系統委外開發)

「**資通安全管理法**」第9條：「公務機關或特定非公務機關，於本法適用範圍內，**委外**辦理**資通系統之建置、維運**或**資通服務之提供**，應**考量**受託者之專業能力與經驗、委外項目之性質及資通安全需求，**選任**適當之受託者，並**監督**其資通安全維護情形。」



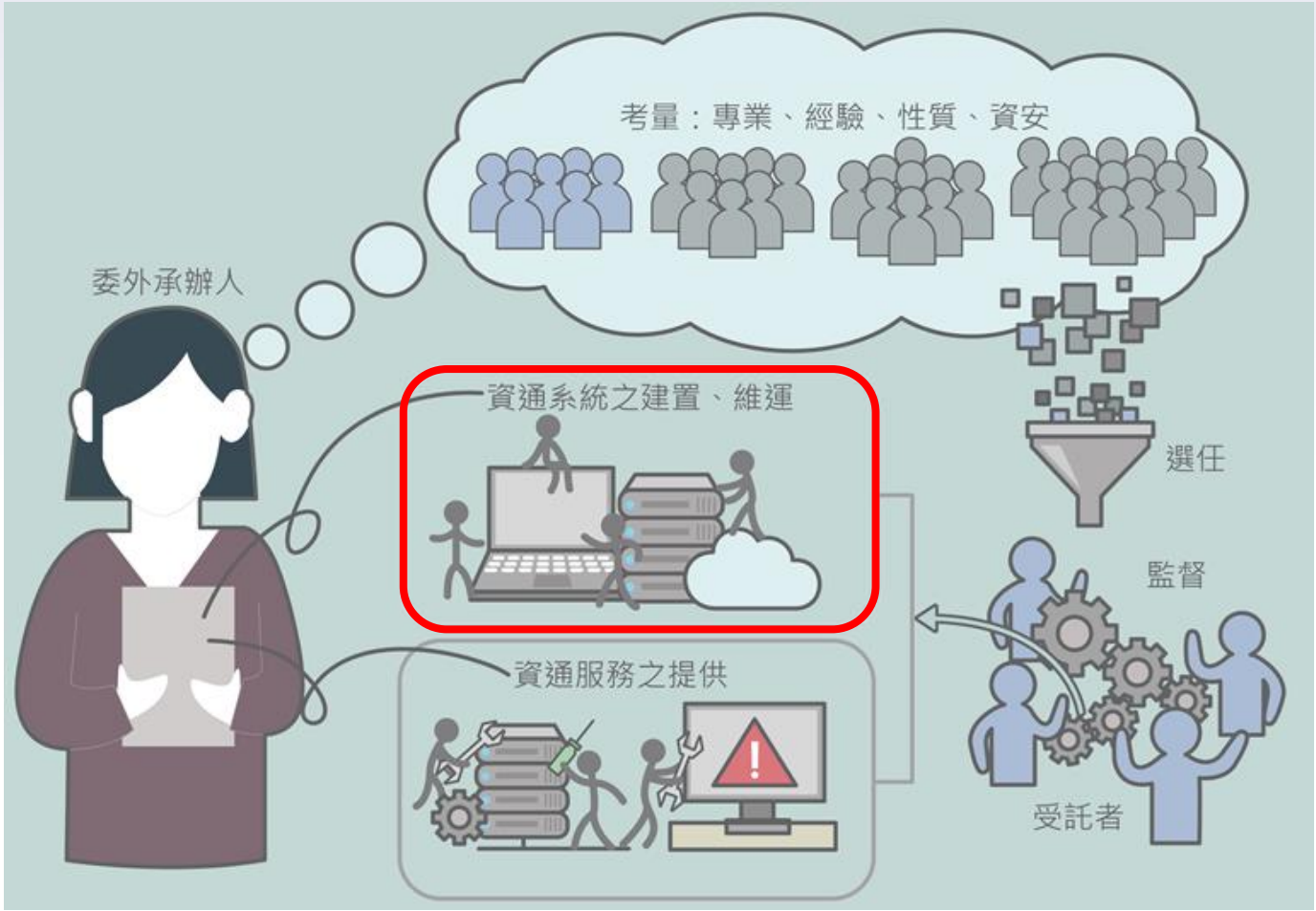
「資通安全管理法」第3條：「一、**資通系統**：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、**資通服務**：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。」



「資通安全管理法常見問題」4.18：如**套裝軟體**僅有低度客製化，是否仍屬於自行或委外開發之資通系統？

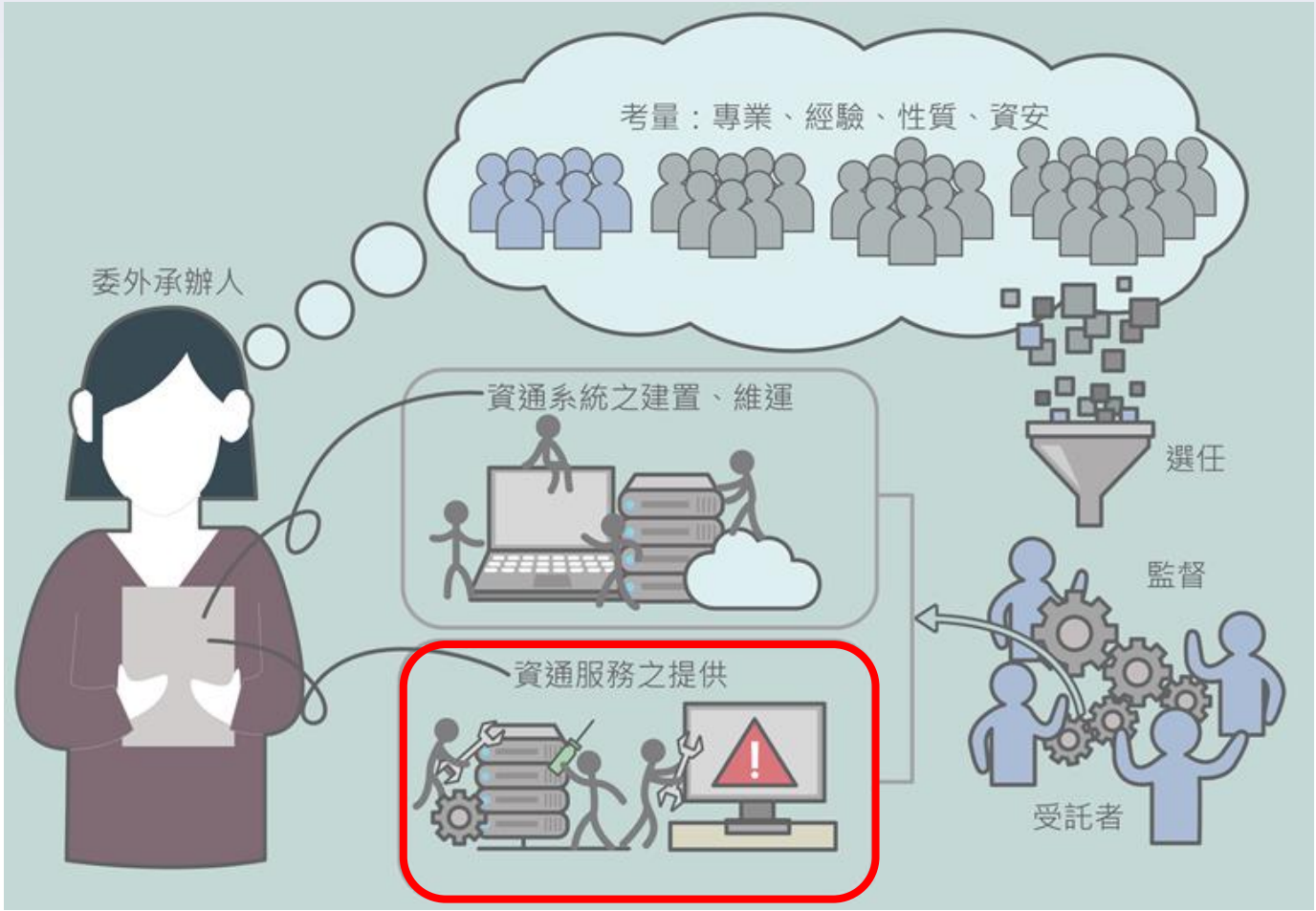
資通系統**如包含客製化的部分，即屬**自行或委外開發之資通系統，須依分級辦法第11條規定，完成資通系統防護需求分級，並依系統防護基準執行相關控制措施。



「資通安全管理法常見問題」8.3：資通服務提供的定義為何？PC維護案是否屬之？須不須第三方驗證？

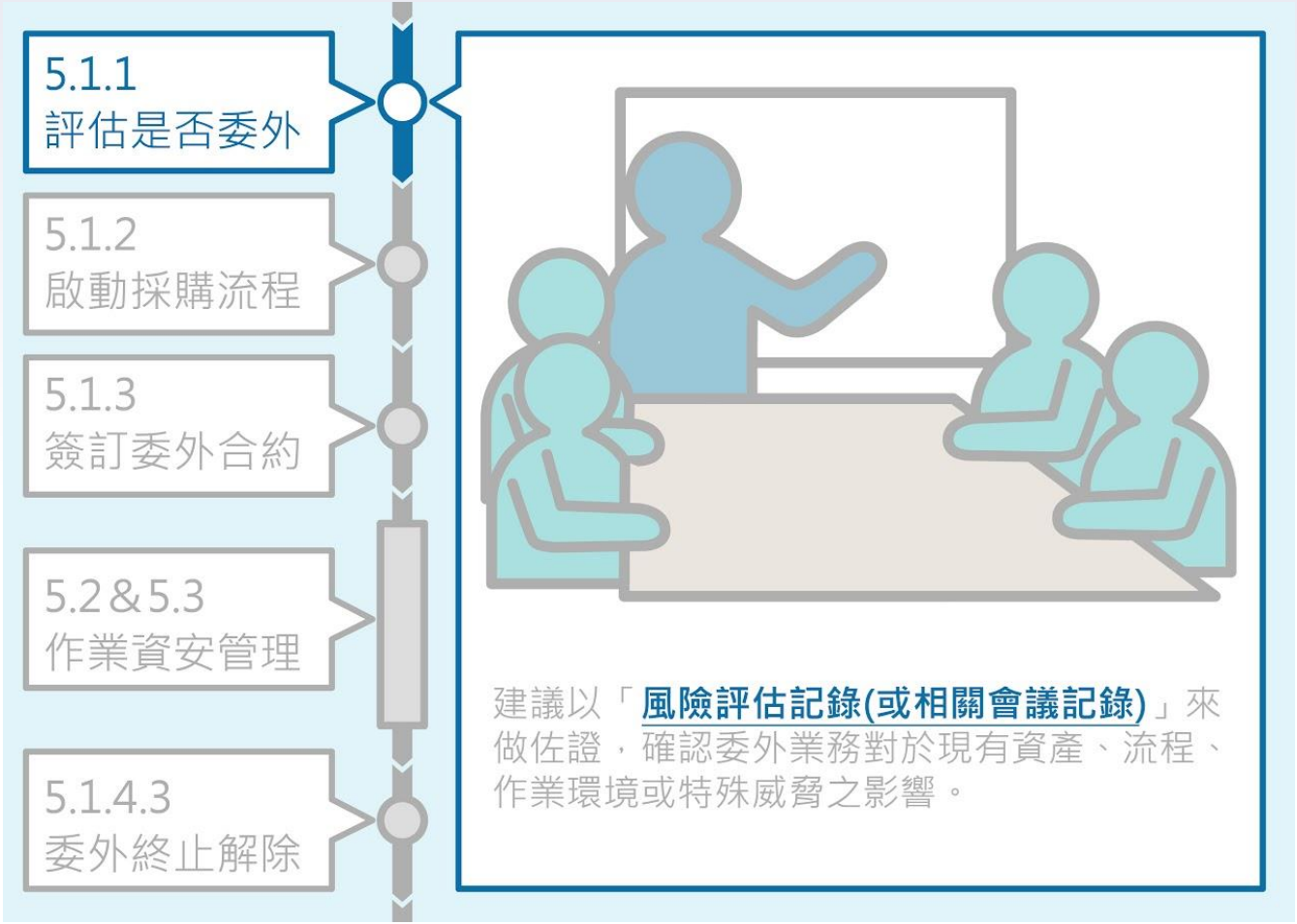
一、資通服務之定義依母法第3條規定，指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。**是以PC維護屬資通服務之一種**。

二、施行細則第4條要求應注意受託者「具備完備資通安全管理措施」或「通過第三方驗證」通過第三方驗證並不是必要項。



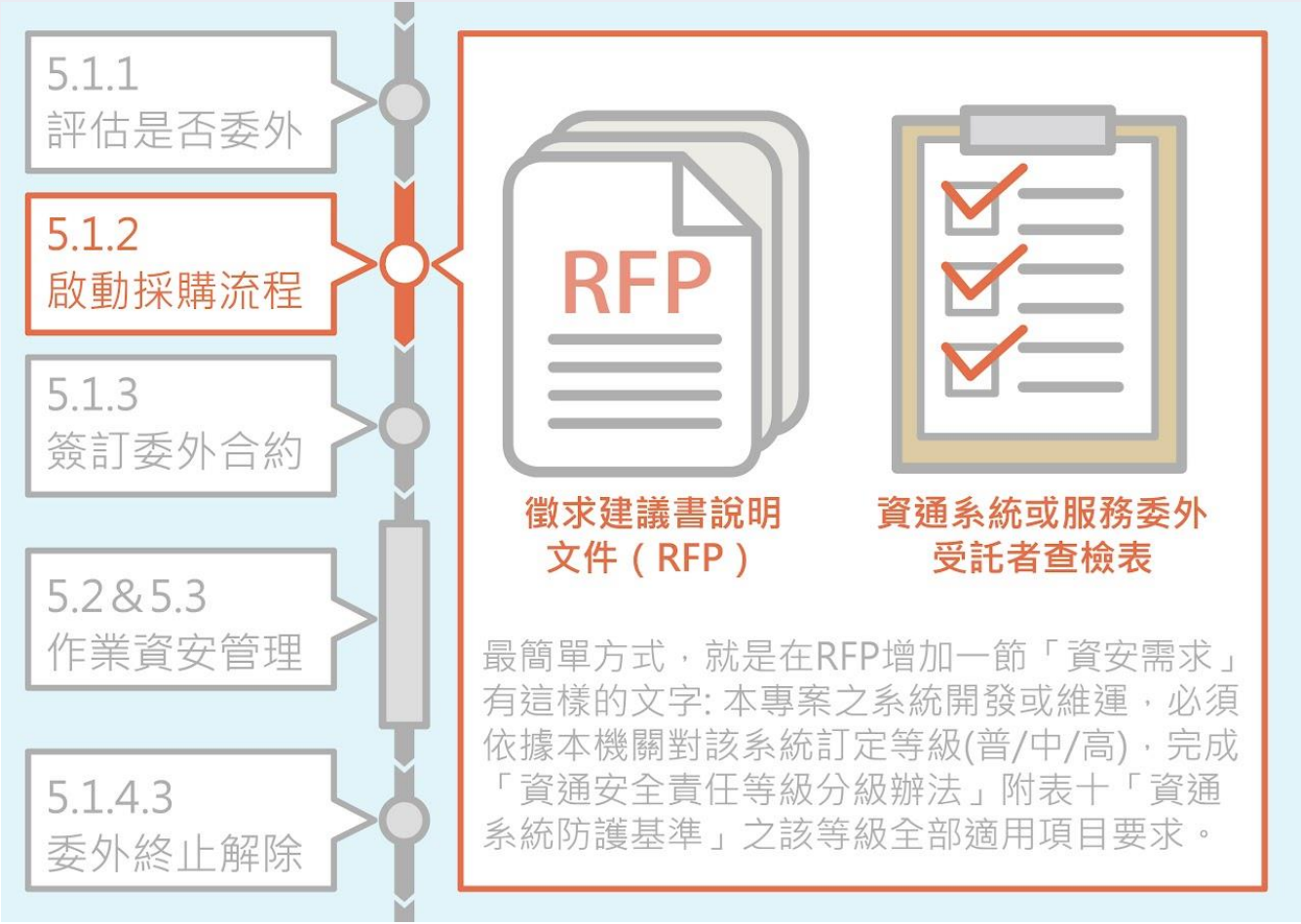
基於「**資通安全管理法**」第9條：「應**考量**受託者之專業能力與經驗、**委外項目之性質及資通安全需求**」

資通安全稽核檢核項目5.1：「是否**針對委外業務項目進行風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？」

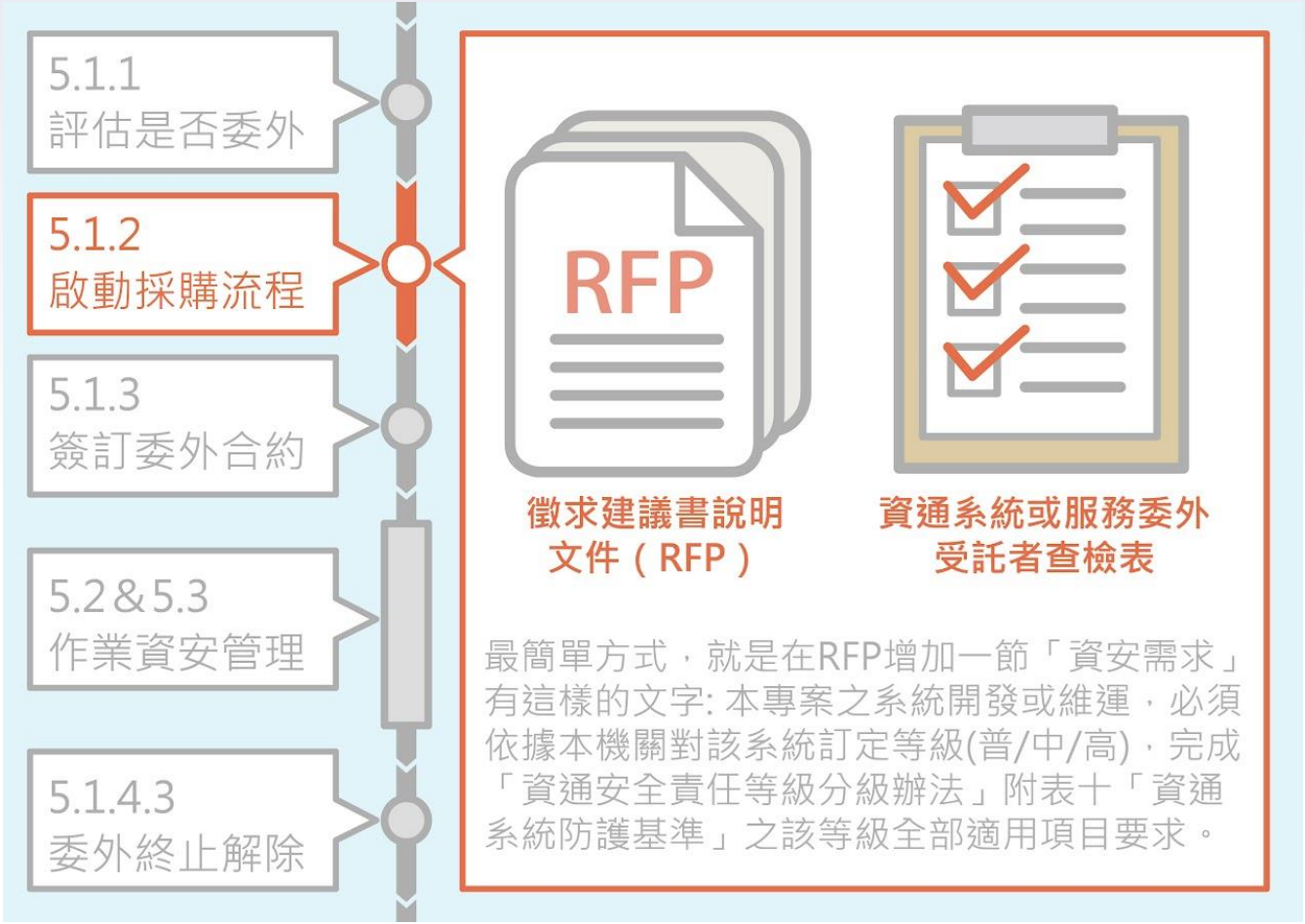


對於委外項目之性質及資通安全需求已經做過考量而決定委外了，那就應該會擬定徵求建議書(RFP)。

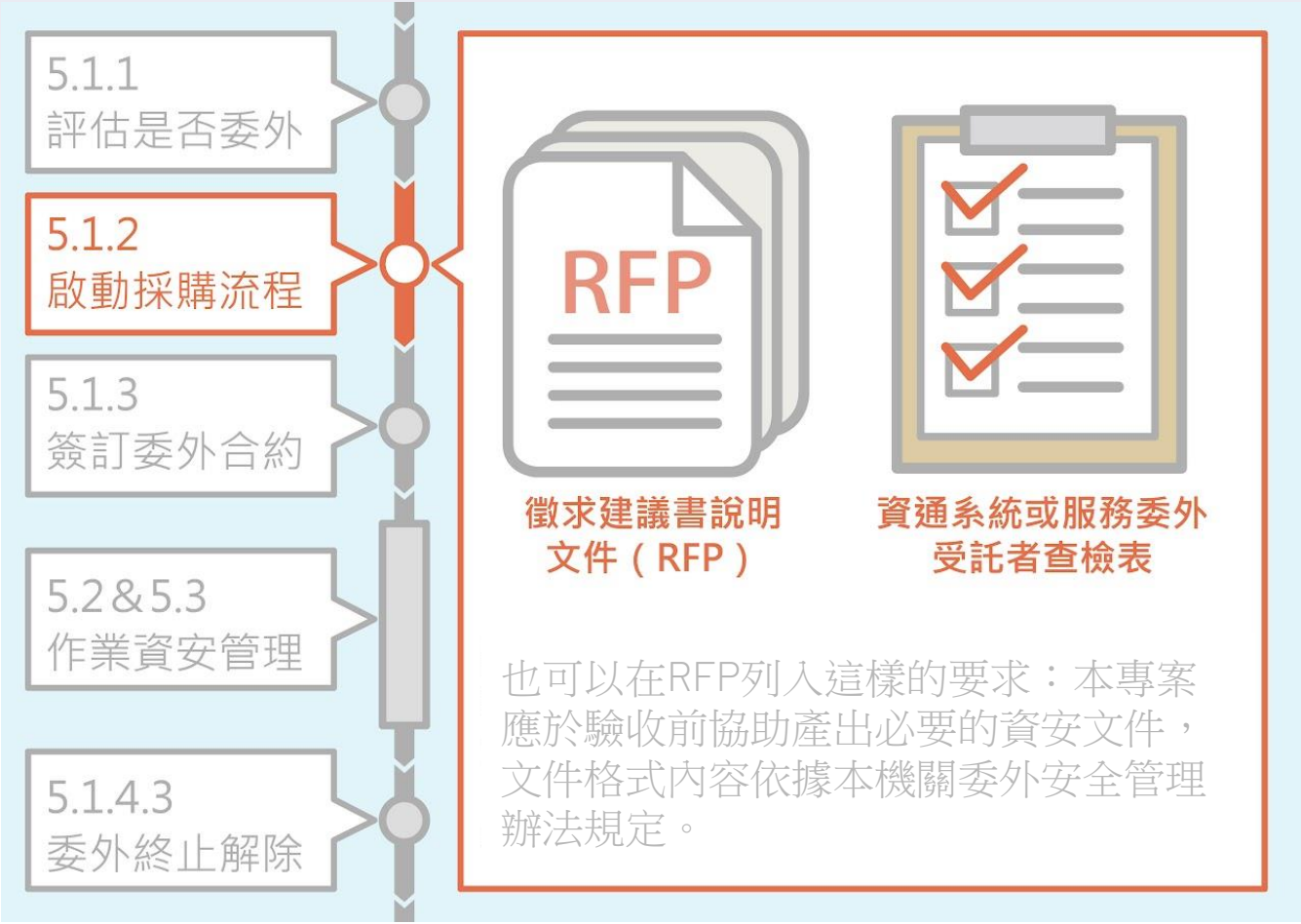
資通安全稽核檢核項目5.2：「依資通系統分級，於徵求建議書文件(**RFP**)相關採購文件中明確規範**防護基準需求**？」



對於「**資通系統**」委外建置或維運，更是要在RFP中明確規範防護基準需求，法源依據「**資通安全責任等級分級辦法**」第11條第2項：「各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定**資通系統防護基準執行控制措施**。」

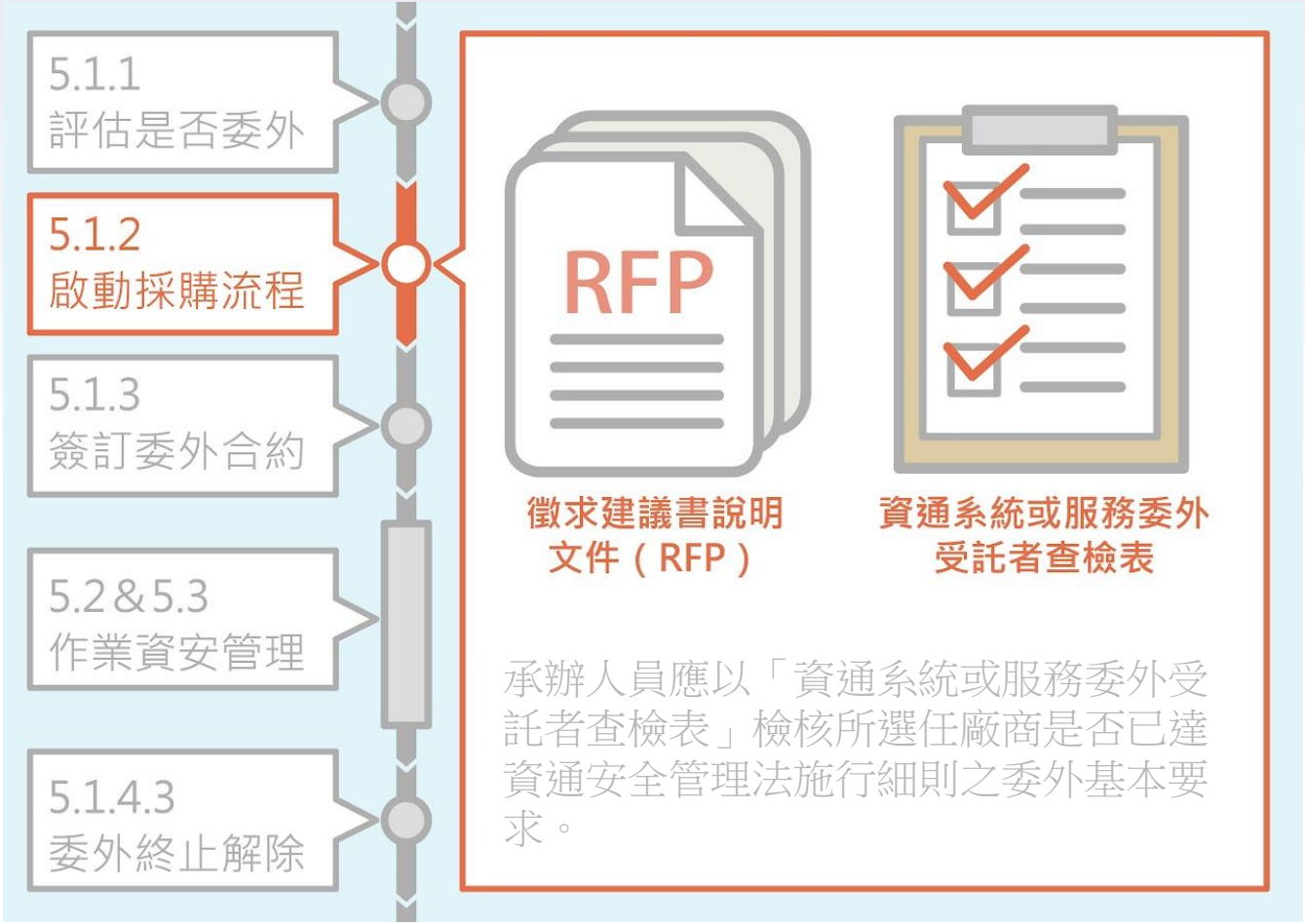


另外建議RFP可列出**委外廠商應協助產出的資安管理文件**(例如資通系統安全等級評估表、弱點處理報告單、SSDLC文件等)，以減輕委外承辦人員或後續接手系統管理人員的負擔。



基於「**資通安全管理法**」第9條：「應**考量受託者之專業能力與經驗**、委外項目之性質及資通安全需求」

增加一份「**資通系統或服務委外受託者查檢表**」是比較理想的



關於**選任**適當受託者，「**資通安全管理法常見問題**」有幾項補充說明6.1、6.3、6.4、6.5、6.6、6.9。

6.1	**委外注意事項何時要納入？** 資安法施行細則第4條訂有委外前受託者之**選任**及委外後受託者之**監督**等事項，建議機關於**辦理委外案前**，即應了解法規事項，並**透過契約規範及專案管理**落實本法規定。
6.3	**受託者是否必須通過第三方驗證，第三方驗證之範圍？** 機關委外辦理資通業務時，應要求受託者具備完善的資通安全管理措施，或通過第三方驗證，故機關可評估委託規模、內容及委託標的之防護需求等級等因素，綜整考量後適當**擇一要求**受託方應具備之資安管控措施或要求通過第三方驗證。(詳參施行細則第4條第1項第1款)。另第三方驗證之範圍，係指受託者辦理業務之相關程序、人員、設備及環境。

關於**選任**適當受託者，「**資通安全管理法常見問題**」有幾項補充說明6.1、6.3、6.4、6.5、6.6、6.9。

6.4	**何謂完善的資通安全管理措施？** 除遵行機關自定之**資通安全防護及控制措施**所要求之項目外，機關得依委託之項目個案判斷，並可於採購、**委外招標時，納入相關需求並列為評分項目**。例如： 1.應用系統委外開發：可考慮廠商的開發環境是否安全，程式的測試資料是否合宜等。 2.SOC監控委外：可考量蒐集的資料是否做好相當之管理及防護。
6.5	**如何判斷廠商之資通安全管理措施是否"完善"？由誰來判斷(是採購單位、業務單位、資訊單位或稽核單位)？** 建議**可參考**資訊安全管理系統國家標準**CNS27001或ISO27001**之管理要求及相關資安法規之要求據以審視之；至於機關內部之單位權責分工議題，原則尊重各機關之內部行政作業與文化而定，但考量本項工作仍需仰賴資安專業，建議機關之**資訊單位及資安專職人力**應統籌扮演跨單位**統籌及規劃**之角色。

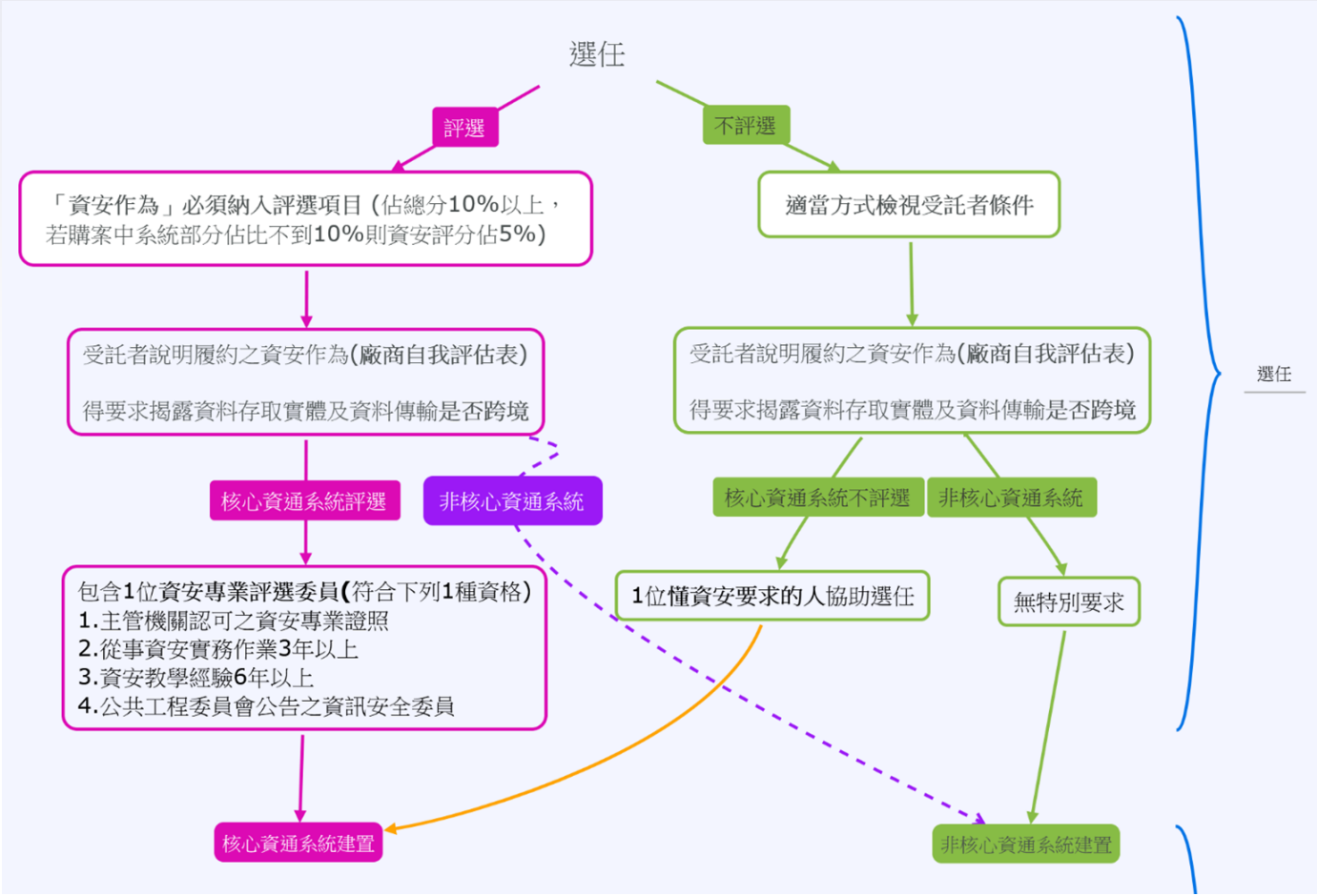
關於**選任**適當受託者，「**資通安全管理法常見問題**」有幾項補充說明6.1、6.3、6.4、6.5、6.6、6.9。

6.9	**若單純採購套裝軟體或硬體，採購、安裝都依機關所訂程序，且安裝僅於機關環境，是否就無須要求廠商要具備完善之資通安全管理措施或通過第三方驗證？** 一、如受託者辦理受託業務之**相關程序及環境都在機關內**，廠商應**無**第4條第1款須具備完善之資通安全管理措施或通過第三方驗證的議題。 二、機關及委託執行業務廠商應檢視並評估相關產品供應程序有無潛在風險，進而採取**必要之防護機制**。
6.6	**若廠商通過第三方驗證，如何判斷辦理受託業務之相關程序及環境有無含括在驗證範圍？** 建議**先查明**廠商通過之**第三方驗證範圍**(包含人員、資安管理作業程序、資通系統、實體環境)是否已**涵蓋貴機關委外之業務**，另外以稽核方式確認受託業務之執行情形，確認前述第三方驗證通過及維運狀況。另外建議委託機關應先於招標文件敘明委託業務須通過第三方驗證及接受查核之要求，避免履約爭議。

關於**選任**適當受託者，「**資通系統籌獲各階段資安強化措施**」對於廠商資安作為評選做法有這四項。

一	資通系統籌獲，以採**最有利標**，不訂底價為原則，並以評選方式選任受託者，將委託案之相關**資安作為納入評選項目**，配分至少占總分之百分之十；如籌獲案中之資通系統或服務占比低於百分之十，配分至少占總分之百分之五。評選時應要求投標廠商說明履約之資安作為。
二	**無須辦理評選/評審**之採購或採其他執行方式者，應**以適當方式檢視**受託者之資安作為。
三	獲涉及委託機關之**核心**資通系統，且採用評選方式選任受託者時，**評選委員**應包含至少一位資安專業人員。
四	如**不採用評選方式**選任受託者時，委託機關辦理資通系統籌獲案之團隊應至少包含一位**資安專業人員**，協助受託者辦理選任相關作業。(註：這裡說的資安專業人員並非指定是機關的資安專職人員，可以理解為要有一位懂資安要求的人協助選任。)

關於**選任**適當受託者，「**資通系統籌獲各階段資安強化措施**」對於廠商資安作為評選做法要求，這部分的流程圖如右所示。

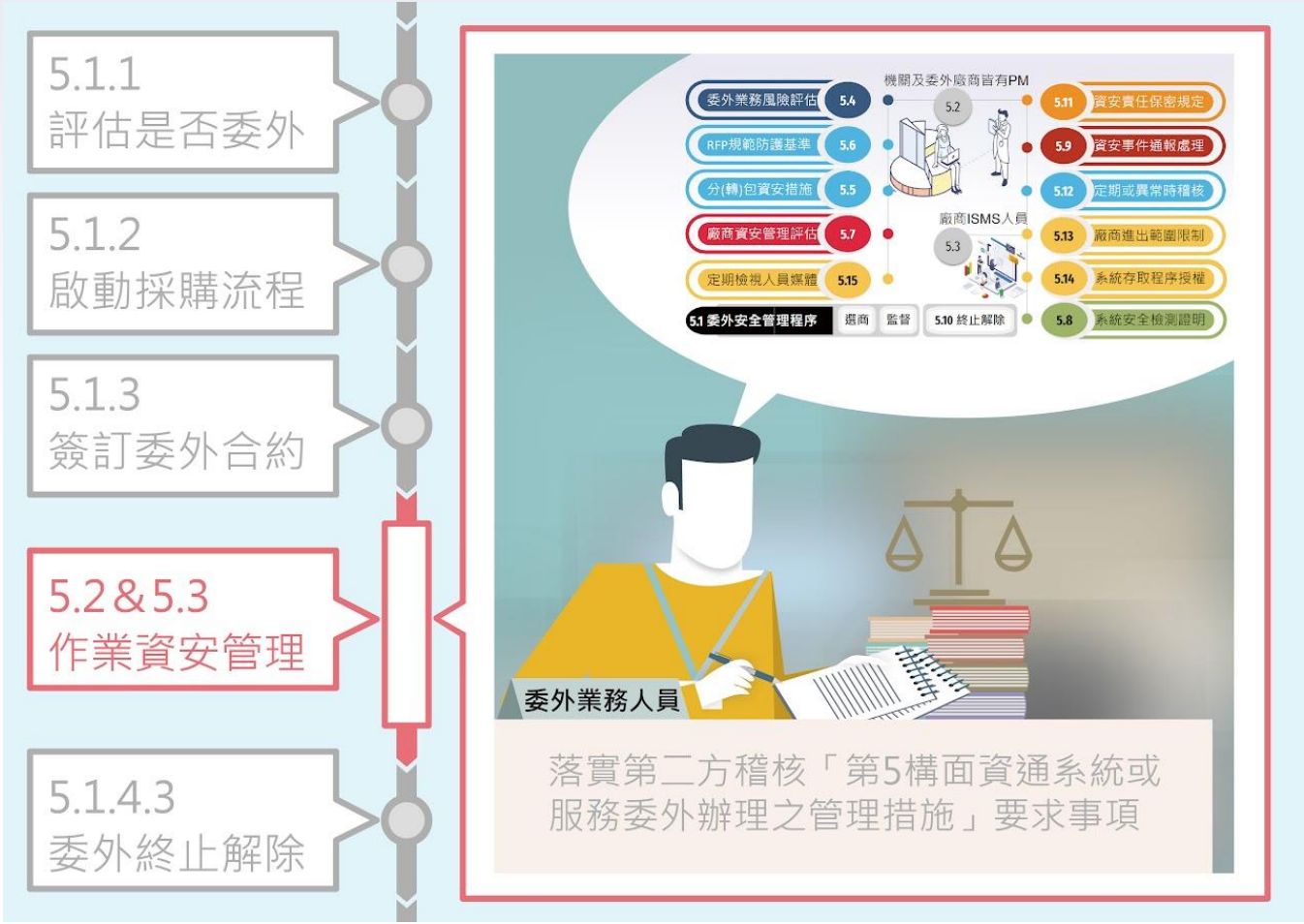


關於**選任**適當受託者，「**資通系統籌獲各階段資安強化措施**」說明評選應要求投標廠商說明履約之資安作為，以及無須辦理評選/評審之採購或採其他執行方式者應以適當方式檢視受託者之資安作為。我們建議使用「**資通安全維護計畫範本**」附件6「**委外廠商查核項目表**」要求廠商自評。

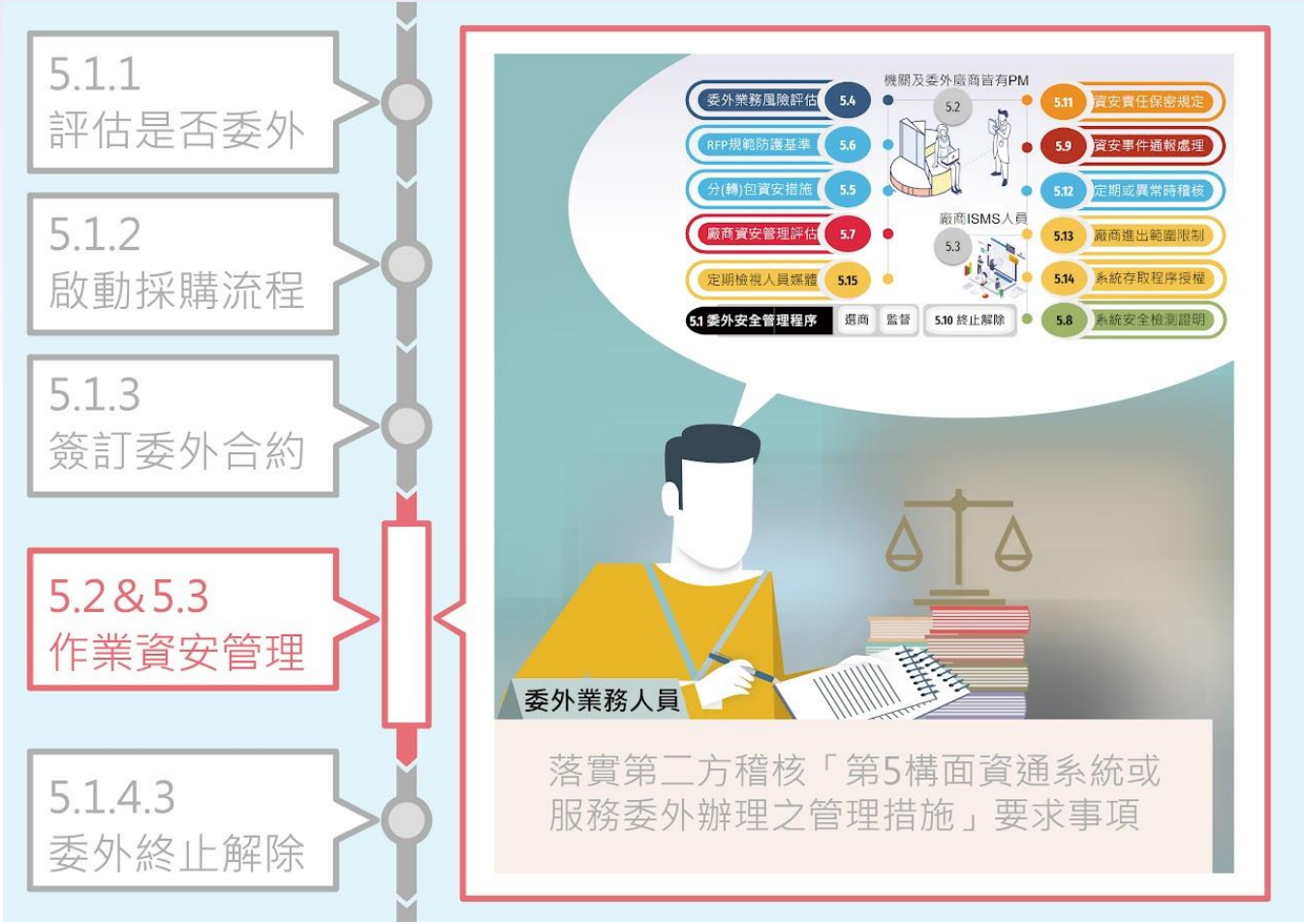
委外廠商查核項目	ISO 27001控制項
資通安全政策之推動及目標訂定	A.5 資訊安全政策訂定與評估
設置資通安全推動組織	A.6 資訊安全組織
配置適當之資通安全專業人員及適當之資源	A.7 人力資源安全
資訊及資通系統之盤點及風險評估	A.8 資產管理
資通安全管理措施之實施情況	A.9 存取控制 A.10 密碼學(加密控制) A.11 實體及環境安全 A.12 運作安全 A.13 通訊安全 A.14 系統獲取、開發及維護
訂定資通安全事件通報及應變之程序及機制	A.16 資訊安全事故管理
定期辦理資通安全認知宣導及教育訓練	A.7 人力資源安全
資通安全維護計畫實施情形之精進改善機制	A.18 遵循性
資通安全維護計畫及實施情形之績效管考機制	

基於「**資通安全管理法**」第9條：「選任適當之受託者，並**監督**其資通安全維護情形。」

「**資通安全管理法施行細則**」第4條第1項「各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供，選任及**監督**受託者時，應注意下列事項....」(註:第五至九款)



「**資通安全管理法施行細則**」[第4條](#)第1項第五至九款為監督受託者之注意事項，所以在資通安全稽核檢核項目也都有對應的5.8、5.9、5.10、5.12，稽核時可以據此要求委外承辦人提出佐證。



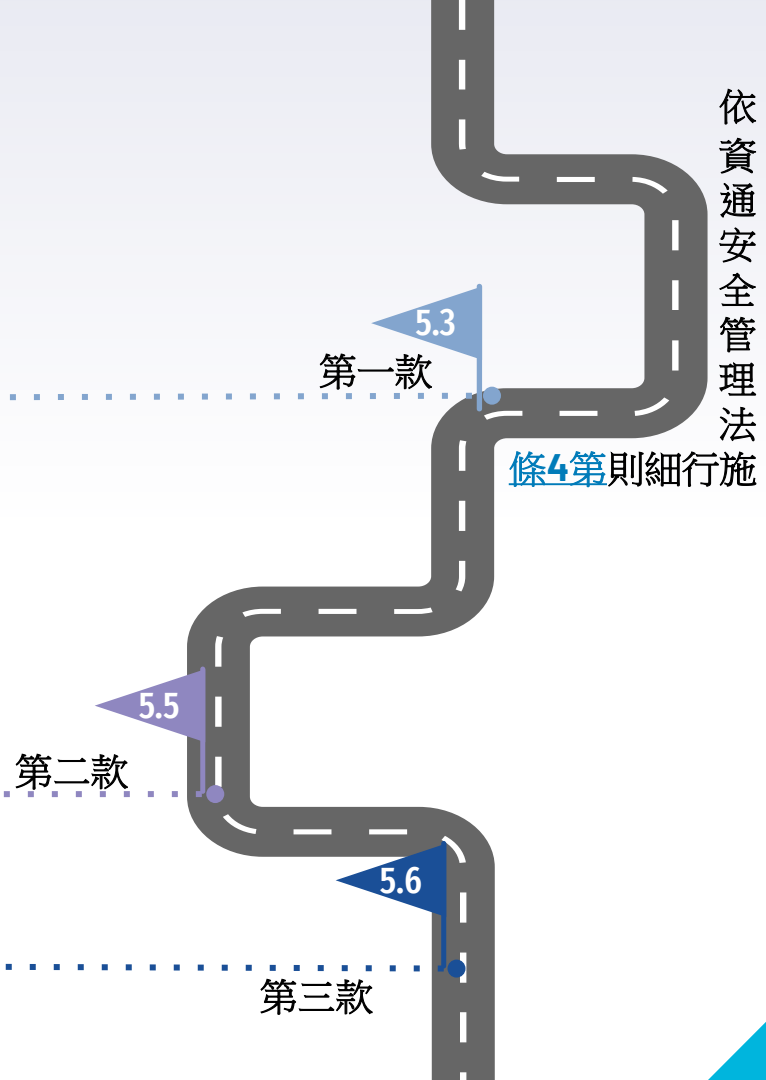
5.1 針對委外業務項目進行風險評估，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？

5.3 訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保廠商執行委外作業時具備**完善資通安全管理措施**或**通過第三方驗證**？

5.4 機關及委外廠商皆指定專案管理人員，負責推動協調及督導委外作業之資通安全管理事項？負責督導的委外作業資通安全管理事項有哪些？

5.5 要求委外廠商配置充足且經適當資格訓練、擁有**資通安全專業證照**或具有**類似業務經驗**資通安全專業人員？其**要求標準**為？

5.6 委外業務如允許分包，對**分包廠商**資通安全維護措施要求為？如何確認其落實辦理？



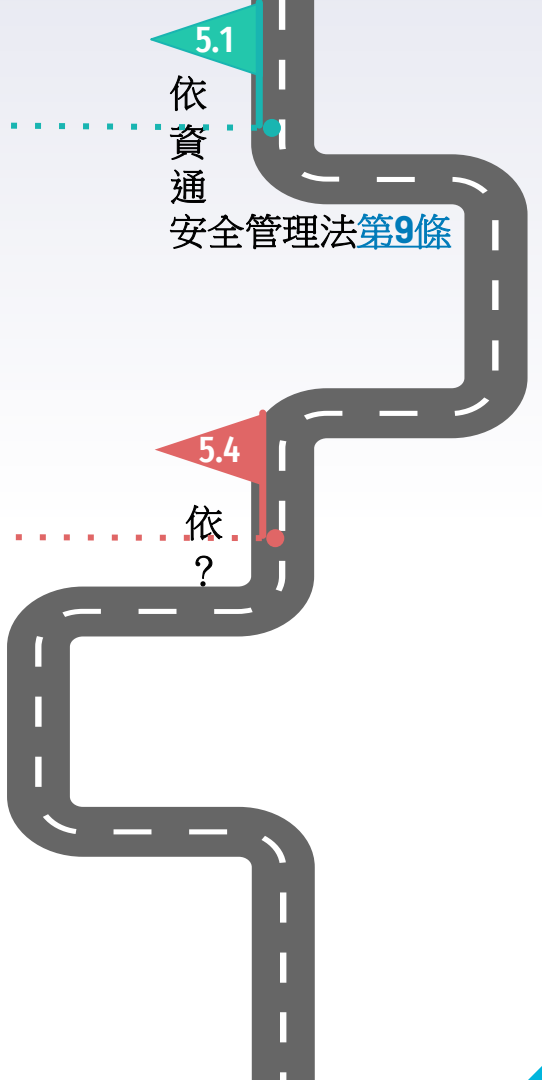
5.1 針對**委外業務**項目進行**風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？

5.3 訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保廠商執行委外作業時具備完善資通安全管理措施或通過第三方驗證？

5.4 **機關**及**委外廠商**皆指定**專案管理人員**，負責推動協調及督導委外作業之資通安全管理事項？負責督導的委外作業資通安全管理事項有哪些？

5.5 要求委外廠商配置充足且經適當資格訓練、擁有資通安全專業證照或具有類似業務經驗資通安全專業人員？其要求標準為？

5.6 委外業務如允許分包，對分包廠商資通安全維護措施要求為？如何確認其落實辦理？



5.1 針對**委外業務**項目進行**風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？

5.1

依資通

全管理法第9條

4

- ✓ 基於「資通安全管理法」第9條提到「委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求」
- ✓ 在稽核時可以據此要求委外承辦人提出佐證，該「資通系統」或「資通服務」**是否有評估過適合委外嗎**？
- ✓ 譬如系統需要與校務資訊整合，校務系統需要配合委外系統的資料交換方式是否有考量過？資安面的管控方式如何呢？例如某個系統的歷史資料需要補建，評估過資料敏感度合適委外處理嗎？

資通安全專業證照或具有類似業務經驗資通安全專業人員？其要求標準為？

5.6 委外業務如允許分包，對分包廠商資通安全維護措施要求為？如何確認其落實辦理？

E1

5.1 針對**委外業務**項目進行**風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？

5.1

依資通

全管理法第9條

4

- ✓ 基於「資通安全管理法」第9條提到「委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求」
- ✓ 在稽核時可以據此要求委外承辦人提出佐證，該「資通系統」或「資通服務」**是否有評估過適合委外嗎**？
- ✓ 譬如系統需要與校務資訊整合，校務系統需要配合委外系統的資料交換方式是否有考量過？資安面的管控方式如何呢？例如某個系統的歷史資料需要補建，評估過資料敏感度合適委外處理嗎？

資通安全法常見問題

8.7 政府機關於建置或使用雲端服務時，請參考國家資通安全研究院網站之共通規範專區所公布「政府機關雲端服務應用資安參考指引」，其內容包括共通資安管理規劃、IaaS、PaaS、 SaaS以及自建雲端服務等資安控制措施。

E2

✓ 委外廠商執行專案有個專案經理是常態，不需要法規要求也必然會有安排。

✓ 機關的專案管理人員難道就是資安專職人員嗎？若機關所有委外案僅由一位資安專職人員擔任聯繫窗口，在每個專案進行過程的資安相關事務也由這位人員負責，必然無法負荷。

全管理法第9條

5.4

5.4 **機關**及**委外廠商**皆指定**專案管理人員**，負責推動協調及督導委外作業之資通安全管理事項？負責督導的委外作業資通安全管理事項有哪些？

依？

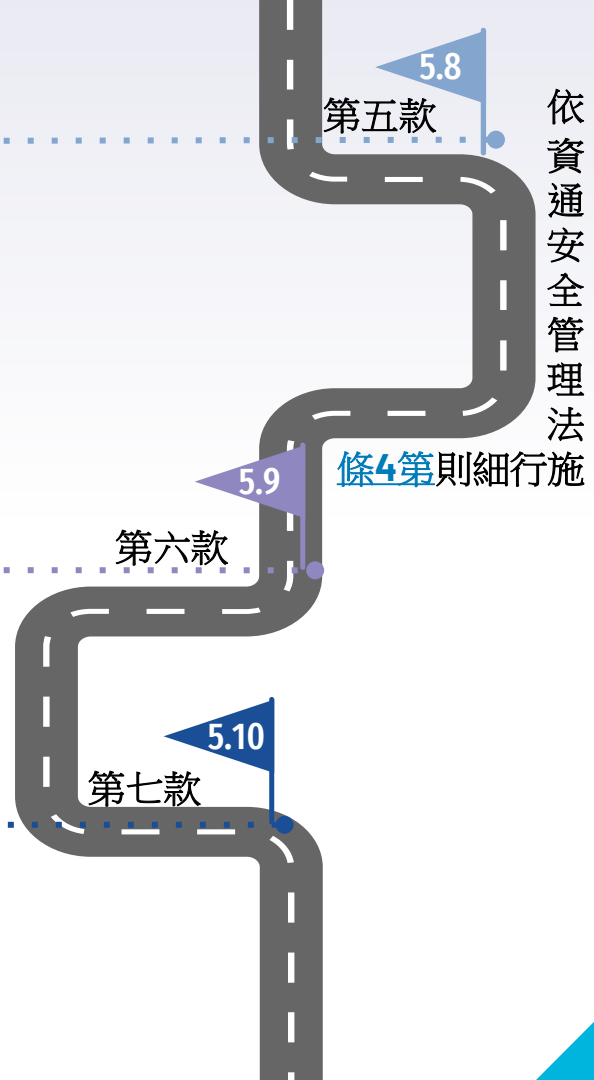
✓ 「資通安全管理法常見問題」3.18定義資訊人員是較為廣義的，擴大認定包含負責**資通系統委外**開發/設置/維運的**業務單位人員**(也就是指委外案的主要承辦人員)也是「資通安全專責人員以外之**資訊人員**」，既然將委外承辦人員視為資訊人員，就應該具資安專業認知能承擔委外案監督受託者之責任，當然也就應該賦予教育訓練足以擔任其負責委外案的資安聯繫窗口。

E5

5.8 委外客製化資通系統開發者，要求委外廠商提供資通系統之**安全性檢測證明**，並請其針對**非自行開發**之系統或資源，**標示內容與來源及提供授權證明？**若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，自行或另行委託第三方進行安全性檢測之複測？

5.9 訂定委外廠商對於機關委外業務之**資安事件通報**及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，立即通知機關並採行補救措施？

5.10 委外關係**終止或解除**時，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？



5.8 委外客製化資通系統開發者，要求委外廠商提供資通系統之**安全性檢測證明**，並請其針對**非自行開發**之系統或資源，**標示內容與來源及提供授權證明？**若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，自行或另行委託第三方進行安全性檢測之複測？

- ✓ 依據「資通安全責任等級分級辦法」附表十資通系統防護基準的「系統與服務獲得」之系統發展生命週期開發階段、測試階段的要求 (所以此項檢核僅針對108年資安法實施後的委外開發系統)
- ✓ 分級為「高」之系統才需要執行源碼掃描、滲透測試
- ✓ 「中」級以下系統僅要求執行弱點掃描
- ✓ 通常資通系統不全然都是廠商自行開發的，開發過程可能引用了一些框架、套件、外掛程式等，若在交付系統沒列出這些非自行開發的來源，就可能忽略存在的安全風險及版權合法性，後續在系統維運時也就不會關注必要的漏洞修補及版本更新。

5.8 第五款 依資通安全管理法

5.9 條4第則細行施

10

E6

5.8 委外客製化資通系統開發者，要求委外廠商提供資通系統之**安全性檢測證明**，並請其針對**非自行開發**之系統或資源，**標示內容與來源及提供授權證明？**若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，自行或另行委託第三方進行安全性檢測之複測？

5.9 訂定委外廠商對於機關委外業務之**資安事件通報**及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，立即通知機關並採行補救措施？

- ✓ 「訂定資安事件通報及相關處理規範」，這部分通常是資訊中心及資安專職人員負責，而且機關的程序必須符合「資通安全事件通報及應變辦法」之相關要求。
- ✓ 重點概念要加強教育訓練讓委外承辦人員知悉，而委外承辦人員就是要了解程序並告知廠商依程序配合。

E7

5.11 訂定委外廠商之**資通安全責任及保密**規定，且落實執行？

5.12 對委外廠商執行受託業務之**資安**行為進行**檢視**？其**時機及做法**為何？針對查核發現，建立**後續追蹤及管理**機制？

5.11 訂定委外廠商之資通安全責任及保密規定，且落實執行？

5.11 第八款

依資通安全管理法第4條第1項第八款：「受託者應採取之其他資通安全相關維護措施」

- ✓ 基於「資通安全管理法施行細則」第4條第1項第八款：「受託者應採取之其他資通安全相關維護措施」，委外廠商應承諾「資通安全責任及保密規定」是最基本的，也才能進一步要求做好各項資通安全維護措施。
- ✓ 再加上「資通安全管理法常見問題」6.4對完善的資通安全管理措施要求：「除遵行機關自定之資通安全防護及控制措施所要求之項目外，機關得依委託之項目個案判斷，並可於採購、委外招標時，納入相關需求並列為評分項目。」，所以委外承辦人應了解機關資安程序書相關規定並要求廠商落實資通安全維護措施。
- ✓ 回到程序書規定來看，可以檢視委外程序書有無訂定委外廠商作業資訊安全要求、.委外服務交付管理等相關條文(以符合ISO 27001:2022 A.5.19供應者關係中之資訊安全及A.5.20於供應者協議中闡明資訊安全)，以供委外承辦人員及廠商有所依循。

E8

- ✓ 對「資安行為進行檢視」受託業務之執行情形，宜**列入RFP**聲明具權利可對受託者進行資安稽核，如此就可以用來佐證。
- ✓ 具有權利以「資安行為進行檢視」受託業務之執行情形，**不一定**就代表每個委外案都要在進行過程中對廠商進行**稽核**。至於「時機及做法」可以自訂，譬如知悉委外廠商發生可能影響委外作業之資通安全事件時，才是真正需要對廠商進行稽核的必要時機。
- ✓ 拿到**相關的報告**、紀錄由專業人員進行安全檢視也是找出問題的可行做法，不一定就是要大張旗鼓對廠商進行稽核。

5.11 第八款

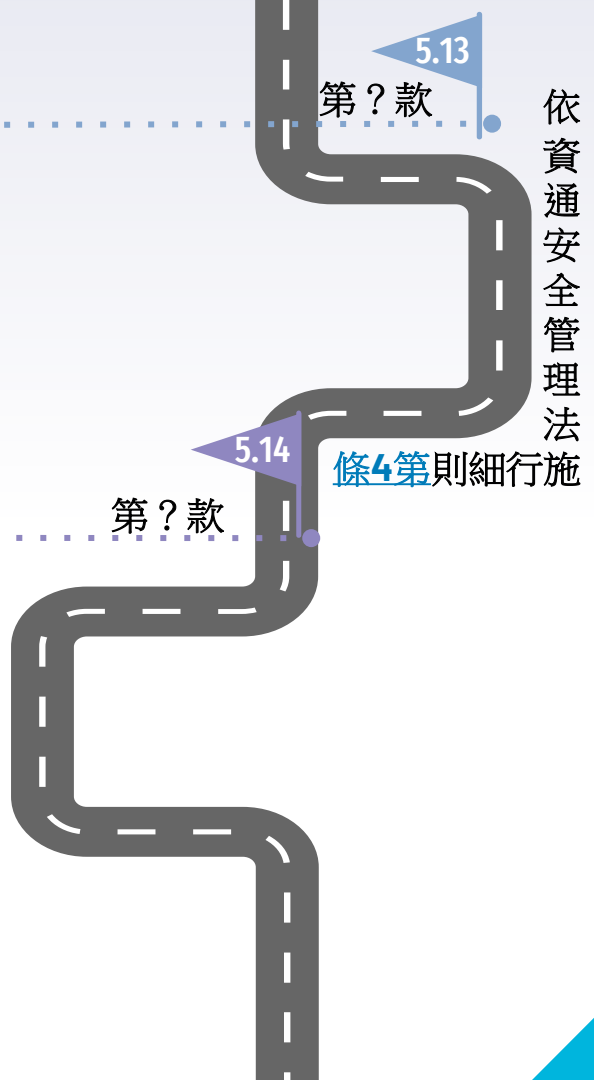
依資通安全管理法第4條細則施行

5.12 對委外廠商執行受託業務之**資安**行為進行**檢視**？其**時機及做法**為何？針對查核發現，建立**後續追蹤及管理**機制？

5.12 第九款

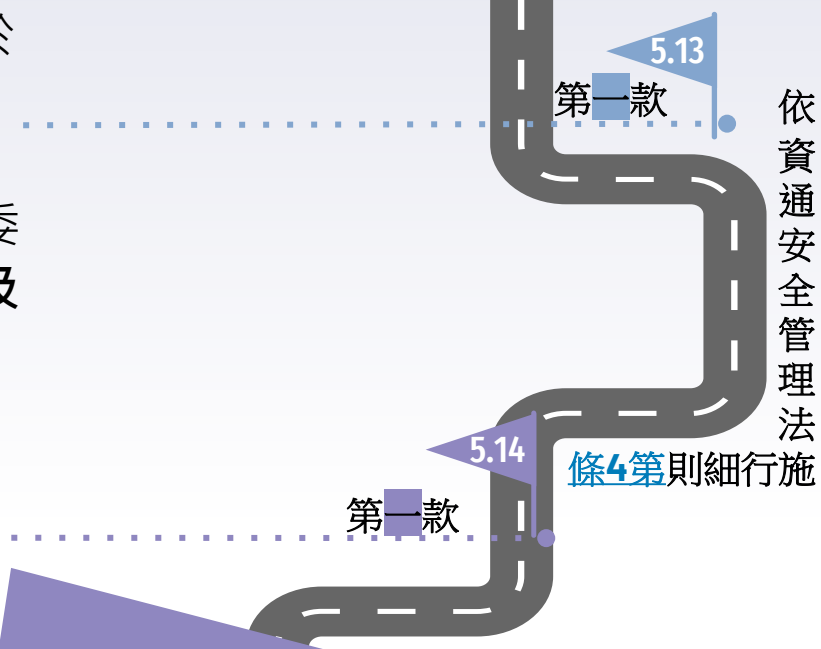
5.13 委外廠商專案成員**進出機關範圍被限制**？對於委外廠商駐點人員使用**資訊設備** (個人、筆記型、平板電腦、行動電話及智慧卡等) 建立相關安全**管控措施**？**定期檢視**並分析資訊作業委外之**人員安全、媒體保護管控、使用者識別及鑑別、組態管控**等相關紀錄？

5.14 訂定委外廠商**系統存取程序及授權**規定(限制其可接觸之系統、檔案及資料範圍等)？委外廠商專案**人員調整及異動**，依系統存取授權規定，調整其權限？



5.13 委外廠商專案成員進出機關範圍被限制？對於委外廠商駐點人員使用資訊設備 (個人、筆記型、平板電腦、行動電話及智慧卡等) 建立相關安全管控措施？定期檢視並分析資訊作業委外之**人員安全、媒體保護管控、使用者識別及鑑別、組態管控**等相關紀錄？

5.14 訂定委外廠商系統存取程序及授權規定(限制其可接觸之系統、檔案及資料範圍等)？委外廠商專案人員調整及異動，依系統存取授權規定，調整其權限？



- ✓ 基於「資通安全管理法施行細則」第4條第1項第1款：「一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施。」
- ✓ 當廠商人員進入機關環境進行作業時，完善的管理措施當然就是指廠商要符合機關的資安程序書規定，而機關程序書一定會有實體安全、可攜式設備管理、系統存取授權等規範，而5.13、5.14即是檢核是否有對委外廠商要求配合這些規範，應有的資安文件就要留下紀錄做為佐證。

5.13 委外廠商專案成員**進出機關範圍被限制**？對於委外廠商駐點人員**使用資訊設備** (個人、筆記型、平板電腦、行動電話及智慧卡等) 建立相關安全**管控措施**？**定期檢視**並分析資訊作業委外之**人員安全、媒體保護管控、使用者識別及鑑別、組態管控**等相關紀錄？

5.13 第？款

依資通安全管理法

5.14 條4第則細行施

目前公務機關已全面禁止使用大陸廠牌資通訊產品，是否須要求委外廠商人員攜入機房設備登記廠牌，禁用大陸廠牌並管控連網安全?

✓ 並無法規要求廠商使用設備之廠牌，若稽核要求機關管控廠商攜入設備廠牌，可能出現爭議。但機關程序書或委外維運合約有相關規定，當然應該落實。

✓ 可建議機關於程序書或委外維運合約訂定維護作業時的連網原則，針對廠商所攜帶設備，註明基於何種原因連網，以及可查核連網紀錄，足以於發生資安事件時追蹤根因。

5.13 委外廠商專案成員**進出機關範圍被限制**？對於委外廠商駐點人員使用**資訊設備** (個人、筆記型、平板電腦、行動電話及智慧卡等) 建立相關安全**管控措施**？**定期檢視**並分析資訊作業委外之**人員安全、媒體保護管控、使用者識別及鑑別、組態管控**等相關紀錄？

- ✓ 基於「資通安全管理法施行細則」第4條第1項：「各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供，選任及監督受託者時，應注意下列事項：一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施。」
- ✓ 所謂的「**定期檢視**」就是要看機關如何落實「**監督**」受託者做好業務之相關程序，當然包含人員安全、媒體保護管控、使用者識別及鑑別、組態管控等必要的資通安全管理措施是否完善。
- ✓ 機關有權要求委外廠商，將委外人員異動管控、儲存媒體管控記錄、帳號異動及人員進出記錄、伺服器主機系統組態更新異動記錄等，定期提出相關報告備查。

5.13 第？款

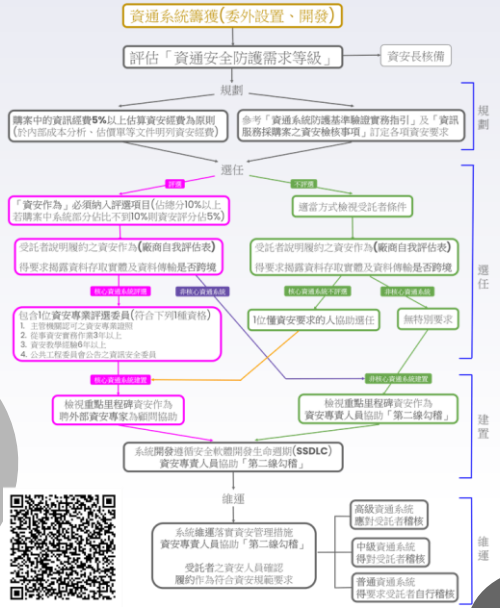
5.14

依資通安全管理法第4條第1項施行細則

行政院111年5月26日院臺護字第1110174630號函「資通系統籌獲各階段資安強化措施」

流程圖

重點表



行政院秘書長110年7月13日院臺護長字第1100177483號函，要求各機關資通訊相關採購案，應參考公共工程委員會「投標須知範本」及「資訊服務採購契約範本」，落實「資訊服務採購案之資安檢核事項」相關要求。

E3

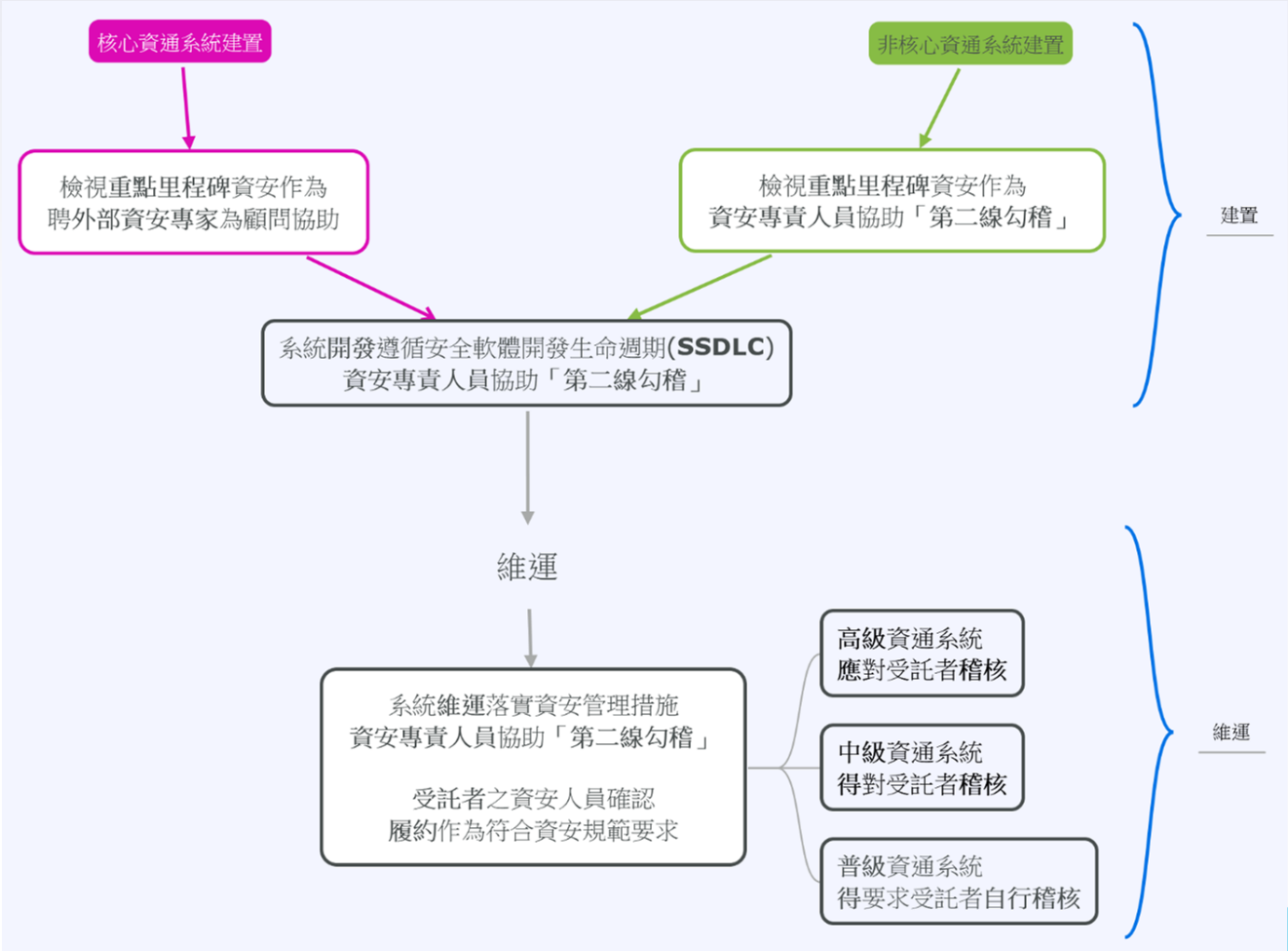
關於**選任**適當受託者，「**資通系統籌獲各階段資安強化措施**」對於建置階段之要求如右表所列。

一	委託機關之**資通安全專責人員**應**以適當方式協助**資通系統籌獲需求單位監督、確認開發團隊於系統開發時遵循安全軟體開發生命周期(**SSDLC**)。(註：資安專責人員適當方式協助是指負責做第二線勾稽確認，主要監督、確認之責仍為管理及需求單位人員。)
二	資通系統籌獲案之**重點里程碑**，應有委託機關之**資通安全專責人員協助**資通系統籌獲需求單位確認。
三	委託機關之**核心**資通系統籌獲案，應聘請**外部資安專家**為顧問或委員，協助機關於專案重點里程碑中，檢視履約(執行)程序與成果之相關資安管理作為。
四	為確保**核心**資通系統品質，針對受託業務包括委託機關之核心資通系統且委託金額達新臺幣一千萬元以上者，委託機關應評估導入**獨立驗證與認證機制**(IV&V)，評估結果應經委託機關**資通安全長**確認。

關於**選任**適當受託者，「**資通系統籌獲各階段資安強化措施**」對於維運階段之要求如右表所列。

一	委託機關之**資通安全專責人員**應**協助**資通系統管理單位，確認資通系統維運作業確實依委託機關之**資安管理措施落實**辦理，例如登入維護、資料備份、效能調校、主機環境及系統版本更新等。(註：資安專責人員協助確認是指負責做第二線勾稽確認，主要訂定、監督、確認之責仍為管理及需求單位人員。)
二	受託者應配置適當之**資通安全專責人員協助**確認履約(執行)階段作業符合委託機關及受託者雙方之資安管理規範
三	委託機關得依資通系統籌獲案之規模及性質，要求受託者應就受委託範圍**自行**辦理資安**稽核**作業；資通系統防護需求等級為「**高級**」之資通系統籌獲，委託機關**應**以適當方式定期或不定期對受託者辦理資安**稽核**；資通系統防護需求等級為「**中級**」之資通系統籌獲，委託機關**得**視需求以適當方式定期或不定期對受託者辦理資安**稽核**，確認受託者落實資安要求；受託者執行受託業務知悉資安事件，且經審核為重大資安事件時，委託機關應辦理資安稽核，並應將稽核結果送交資安主管機關。

關於**選任**適當受託者，「**資通系統籌獲各階段資安強化措施**」對於建置階段、維運階段之要求，這部分的流程圖如右所示。



機關及委外廠商皆有PM

- 5.1 委外業務風險評估
- 5.2 RFP規範防護基準
- 5.6 分(轉)包資安措施
- 5.7 廠商資安管理評估
- 5.13 定期檢視人員媒體

5.4

廠商ISMS人員

5.5

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 受託業務資安檢視
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.3 委外安全管理程序：選商、監督

5.10 終止解除

5.3 訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定。

5.10 委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀持有資料？

委外業務風險評估 5.1

RFP規範防護基準 5.2

分(轉)包資安措施 5.6

廠商資安管理評估 5.7

定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

建議以「風險評估記錄(或相關會議記錄)」來做佐證，確認委外業務對於現有資產、流程、作業環境或特殊威脅之影響。

在稽核時可以據此要求委外承辦人提出佐證，該「資通系統」或「資通服務」**是否有評估過適合委外嗎**？譬如系統需要與校務資訊整合，校務系統需要配合委外系統的資料交換方式是否有考量過？資安面的管控方式如何呢？例如某個系統的歷史資料需要補建，評估過資料敏感度合適委外處理嗎？

5.1 針對委外業務項目進行**風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？

委外業務風險評估 5.1

RFP規範防護基準 5.2

分(轉)包資安措施 5.6

廠商資安管理評估 5.7

定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

建議可參考國家資通安全研究院的「資通系統委外開發RFP」

- 資通系統委外開發RFP資安需求範本(V3.0)
- 附件1資通系統資安需求項目查檢表
- 附件2機關日常維運管理需求
- 附件3機關日常維運管理需求項目查檢表

p.s. 上述查檢表整併後也就是現在的「資通安全責任等級分級辦法」之附表十「資通系統防護基準」。最簡單的方式，就是在RFP增加一節「資安需求」有這樣的文字: 本專案之系統開發或維運，必須依據本機關對該系統訂定等級(普/中/高)，完成「資通安全責任等級分級辦法」附表十「資通系統防護基準」之該等級全部適用項目要求。

5.2 於採購前識別是否為核心資通系統？依資通系統分級，於**徵求建議書文件(RFP)**相關採購文件中明確規範防護基準需求。

E3

委外業務風險評估 5.1

RFP規範防護基準 5.2

分(轉)包資安措施 5.6

廠商資安管理評估 5.7

定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

服務建議書宜具體說明已實施下列資安管理作為

資通系統或服務委外辦理之管理措施

資通安全防護及控制措施

SSDLC

委外廠商查核項目表

專案成員具備資安專業

5.2 於採購前識別是否為核心資通系統？依資通系統分級，於**徵求建議書文件(RFP)**相關採購文件中明確規範防護基準需求。

E3

委外業務風險評估 5.1

RFP規範防護基準 5.2

分(轉)包資安措施 5.6

廠商資安管理評估 5.7

定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

依「資通安全管理法施行細則」第四條第一項第三款：受託者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。

p.s. 建議在RFP的「資安需求」有這樣的文字: 本專案允許複委託範圍，複委託之廠商亦須具備本專案受託廠商相同的資通安全維護措施。

5.6 委外業務如允許分包，對**分包廠商**資通安全維護措施要求為？如何確認其落實辦理？

委外業務風險評估 5.1

RFP規範防護基準 5.2

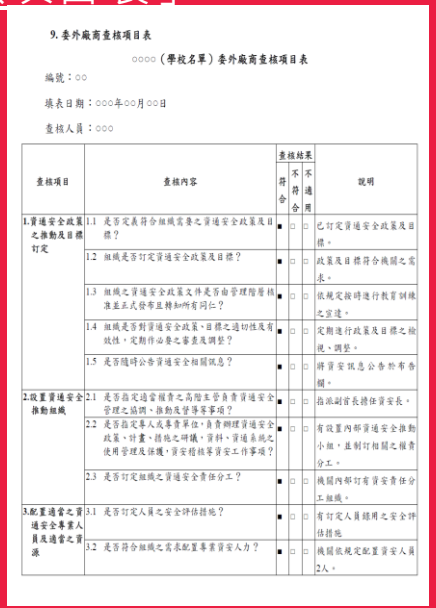
分(轉)包資安措施 5.6

廠商資安管理評估 5.7

定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

建議可參考資通安全維護計畫範本參考附件9「委外廠商查核項目表」



9. 委外廠商查核項目表

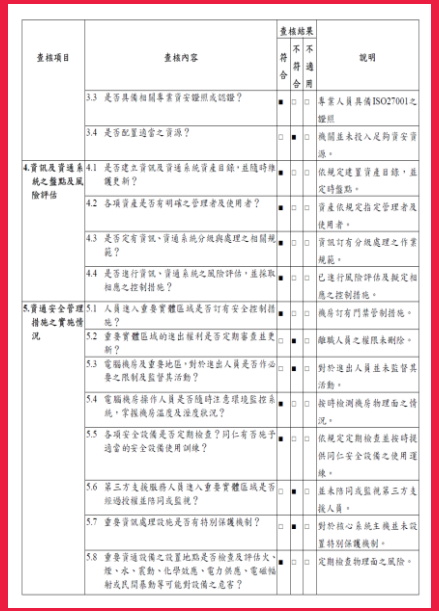
○○○○（學校名單）委外廠商查核項目表

編號：○○

填表日期：○○○年○○月○○日

查核人員：○○○

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	■	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	■	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	■	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	■	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	■	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	■	□	□	指派副首長擔任資安長，
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	■	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	■	□	□	機關內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	■	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專責資安人力？	■	□	□	機關依規定配置資安人員2人。



查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	3.3 是否具備相關專業資安證照或認證？	■	□	□	專業人員具備ISO27001之證照
	3.4 是否配置適當之資源？	□	■	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	■	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	■	□	□	資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	■	□	□	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	■	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	■	□	□	機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	■	□	離職人員之權限未刪除。
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	■	□	對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及濕度狀況？	■	□	□	按時檢測機房物理面之情況。
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	■	□	□	依規定定期檢查並按時提供同仁安全設備之使用運練。
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	■	□	並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？	□	■	□	對於核心系統主機並未設置特別保護機制。
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁輻射或民間基動等可能對設備之危害？	■	□	□	定期檢查物理面之風險。

p.s. 建議在RFP的「資安需求」有這樣的文字: 本專案之受託廠商必須於服務建議書提出時附上「委外廠商資訊安全自評表」。

5.7 對於資通系統之委外廠商，針對其人員(如能力、背景等)及開發維運環境之**資通安全管理**進行**評估**？

- 委外業務風險評估 5.1
- RFP規範防護基準 5.2
- 分(轉)包資安措施 5.6
- 廠商資安管理評估 5.7
- 定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

「委外廠商查核項目表」

1.政策目標
2.推動組織
3.人員資源
4.資產盤點及風險評估
5.管理措施
6.資安事件通報應變
7.宣導訓練
8.資安稽核
9.資安維護計畫

5.7 對於資通系統之委外廠商，針對其人員(如能力、背景等)及開發維運環境之**資通安全管理**進行**評估**？

委外業務風險評估 5.1

RFP規範防護基準 5.2

分(轉)包資安措施 5.6

廠商資安管理評估 5.7

定期檢視人員媒體 5.13

5.3 委外安全管理程序 選商

委外人員之監督管理的落實度與適切性，要能降低委外廠商對機關資通安全造成影響。

5.13 委外廠商專案成員.....相關安全管控措施？**定期檢視**並分析資訊作業委外之**人員安全、媒體保護管控、使用者識別及鑑別、組態管控**等相關紀錄？

- 委外業務風險評估 5.1
- RFP規範防護基準 5.2
- 分(轉)包資安措施 5.6
- 廠商資安管理評估 5.7
- 定期檢視人員媒體 5.13

關於委外人員異動管控、儲存媒體管控記錄、帳號異動及人員進出記錄、伺服器主機系統組態更新異動記錄等依委託機關所訂週期提出相關報告備查

5.3 委外安全管理程序 選商

5.13 委外廠商專案成員.....相關安全管控措施？**定期檢視**並分析資訊作業委外之**人員安全、媒體保護管控、使用者識別及鑑別、組態管控**等相關紀錄？

專案管理人員負責委外專案之執行成效監督方式，如時程管控、安全管控等。

機關及委外廠商皆有PM

5.4

廠商ISMS人員

5.5

監督

5.10 終止解除

依「資通安全管理法施行細則」第四條第一項第二款：受託者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。

5.4 機關及委外廠商皆已指定**專案管理人員**，負責委外作業之資通安全管理事項。

5.5 委外廠商配置擁有資通安全專業**證照**或具有類似業務經驗**資通安全專業人員**。

E5

建議以「委外人員管理規範」、「保密切結書」、「徵求建議書文件(RFP)之保密條款」、「系統存取申請記錄」來做佐證

以程序書規定來看，可以檢視委外程序書有無訂定委外廠商作業資訊安全要求、委外服務交付管理等相關條文(以符合ISO 27001:2022 A.5.19供應者關係中之資訊安全及A.5.20於供應者協議中闡明資訊安全)，以供委外承辦人員及廠商有所依循。

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 受託業務資安檢視
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.11 訂定委外廠商之**資通安全責任及保密**規定，且落實執行？

E
8

「訂定資安事件通報及相關處理規範」，這部分通常是資訊中心及資安專職人員負責，而且機關的程序必須符合「資通安全事件通報及應變辦法」之相關要求。

重點概念要加強教育訓練讓委外承辦人員知悉，而委外承辦人員就是要了解程序並告知廠商依程序配合。

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 受託業務資安檢視
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.9 訂定委外廠商對於機關委外業務之**資安事件通報**相關處理規範？委外廠商違反資通安全相關法令或知悉**資通安全事件**時，立即通知機關並採行補救措施？

E7

對「資安行為進行檢視」受託業務之執行情形，宜列入RFP聲明具權利可對受託者進行資安稽核，如此就可以用來佐證。

具有權利以「資安行為進行檢視」受託業務之執行情形，不一定就代表每個委外案都要在進行過程中對廠商進行稽核。至於「時機及做法」可以自訂，譬如知悉委外廠商發生可能影響委外作業之資通安全事件時，才是真正需要對廠商進行稽核的必要時機。拿到相關的報告、紀錄由專業人員進行安全檢視也是找出問題的可行做法，不一定就是要大張旗鼓對廠商進行稽核。

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 受託業務資安檢視
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.12 對委外廠商執行受託業務之**資安**行為進行**檢視**？其**時機及做法**為何？針對查核發現，建立**後續追蹤及管理**機制？

E 9

委外人員之進出機關之管理規範、進出範圍、設備使用等相關管理文件，以及申請及核可記錄。

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 定期或異常時稽核
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.13 委外廠商專案成員**進出機關範圍被限制**？對於委外廠商駐點人員**使用資訊設備**建立相關安全**管控措施**？定期檢視.....相關紀錄？

委外人員之系統存取程序與授權規定相關管理文件，以及申請及核可記錄。

當廠商人員進入機關環境進行作業時，完善的管理措施當然就是指廠商要符合機關的資安程序書規定，而機關程序書一定會有實體安全、可攜式設備管理、系統存取授權等規範，而5.13、5.14即是檢核是否有對委外廠商要求配合這些規範，應有的資安文件就要留下紀錄做為佐證。

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 受託業務資安檢視
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.14 訂定委外廠商**系統存取程序及授權**規定(如限制可接觸系統、檔案及資料範圍)？
委外廠商專案**人員調整及異動**，依系統存取授權規定，調整其權限？

分級為「高」之系統才需要執行源碼掃描、滲透測試，「中」級以下系統僅要求執行弱點掃描。

通常資通系統不全然都是廠商自行開發的，開發過程可能引用了一些框架、套件、外掛程式等，若在交付系統沒列出這些非自行開發的來源，就可能忽略存在的安全風險及版權合法性，後續在系統維運時也就不會關注必要的漏洞修補及版本更新。

5.11 資安責任保密規定

5.9 資安事件通報處理

5.12 受託業務資安檢視

5.13 廠商進出範圍限制

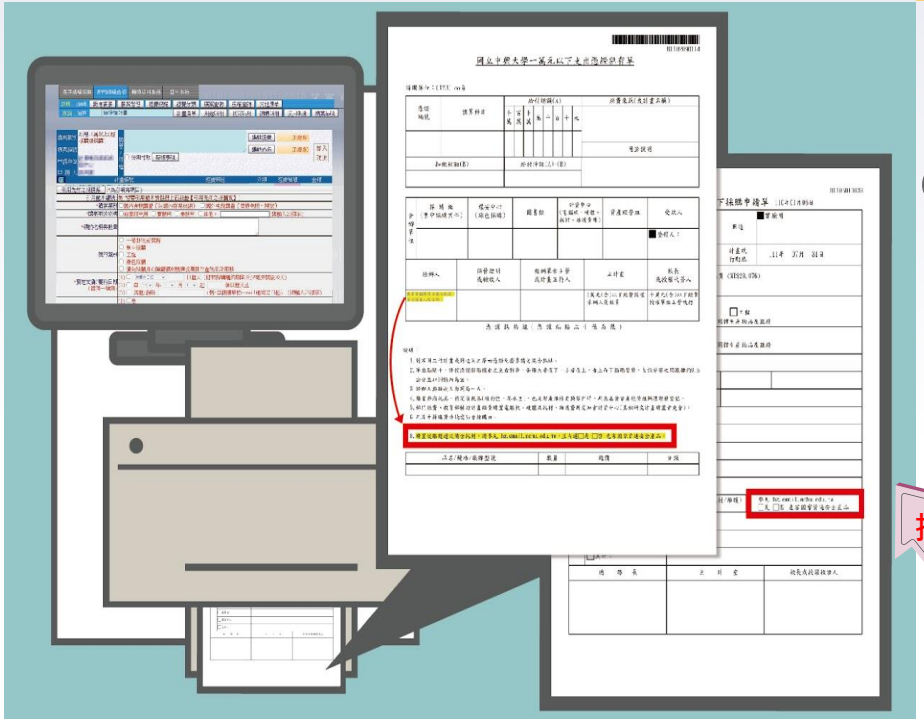
5.14 系統存取程序授權

5.8 系統安全檢測證明

5.8 客製化資通系統開發要求委外廠商提供資通系統之**安全性檢測證明**，並針對**非自行開發**之系統或資源，**標示其來源及提供授權證明**？

E6

108.4.18 各機關對危害國家資通安全產品限制使用原則



該從108年起就開始限制採購，所有大陸廠牌者無論其原產地於我國、大陸地區或第三地區等，均列入限制使用範圍，要落實這樣的管制最重要就是**從採購程序把關**，譬如資通訊設備採購及核銷都能會辦資訊中心，由資訊中心檢核購案中是否有任何大陸廠牌產品，一發現就與採購單位溝通說明並退件。

D6 4.6 公務用資通訊產品，已**禁止**使用大陸廠牌資通訊產品，禁止且避免採購**作法**為何？

D7 4.7 如仍有此類須資安長同意及**列冊管理**，至資安署**管考系統提報**？**相關控管措施**為何？

E13 5.15 **委外營運公眾場域**不得有**大陸廠商**(或陸籍)，於**契約**明訂**禁止**大陸廠牌通訊產品？

108.4.18 各機關對危害國家資通安全產品限制使用原則

四、各機關**自行或委外營運**，提供**公眾活動或使用之場地**，不得使用.....。機關應將前段規定事項納入**委外契約**或**場地使用規定**中，並督導管理。

...必須採購或使用...**列冊管理**：

(一)應指定**特定區域**及**特定人員**使用，不得傳播影像或聲音供不特定人士直接收視或收聽。

(二)購置理由消失，或使用年限屆滿應立即**銷毀**。

111.11.28

D6 4.6 公務用資通訊產品，已**禁止**使用大陸廠牌資通訊產品，禁止且避免採購**作法**為何？

D7 4.7 如仍有此類須資安長同意及**列冊管理**，至資安署**管考系統提報**？**相關控管措施**為何？

E13 5.15 **委外營運公眾場域**不得有**大陸廠商**(或陸籍)，於**契約**明訂**禁止**大陸廠牌通訊產品？

108.4.18 各機關對危害國家資通安全產品限制使用原則

111年數位發展部數授資綜字第1111000056號函文「數位發展部修正各機關對危害國家資通安全產品限制使用原則」，在公文的說明中特別要求落實控管措施如左圖所示。

111.11.28

D6 4.6 公務用資通訊產品，已**禁止**使用大陸廠牌資通訊產品，禁止且避免採購**作法**為何？

D7 4.7 如仍有此類須資安長同意及**列冊管理**，至資安署**管考系統提報**？**相關控管措施**為何？

E13 5.15 **委外營運公眾場域**不得有**大陸廠商**(或陸籍)，於**契約**明訂**禁止**大陸廠牌通訊產品？

禁止使用大陸地區(含港澳)雲端服務

境外雲端服務之人員安全管控機制通過國際標準驗證

[資通安全法常見問題8.7](#)

禁止使用大陸地區(含港澳)雲端服務，境外雲端服務之人員安全管控機制通過國際標準驗證。雲端服務使用的資通訊產品不得為大陸廠牌、成員不得有陸籍人士、存取/備份/備援不得在大陸地區且不得跨該境傳輸。

111.11.28

D6 4.6 公務用資通訊產品，已**禁止**使用大陸廠牌資通訊產品，禁止且避免採購**作法**為何？

D7 4.7 如仍有此類須資安長同意及**列冊管理**，至資安署**管考系統提報**？**相關控管措施**為何？

E13 5.15 **委外營運公眾場域**不得有**大陸廠商**(或陸籍)，於**契約**明訂**禁止**大陸廠牌通訊產品？

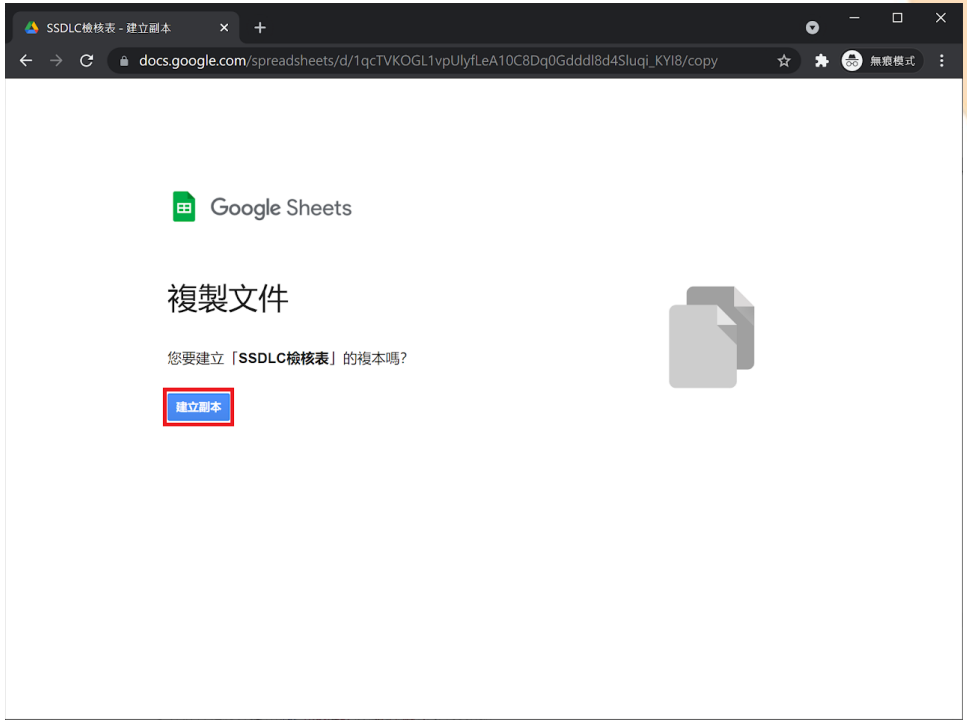
資通安全防護及控制措施

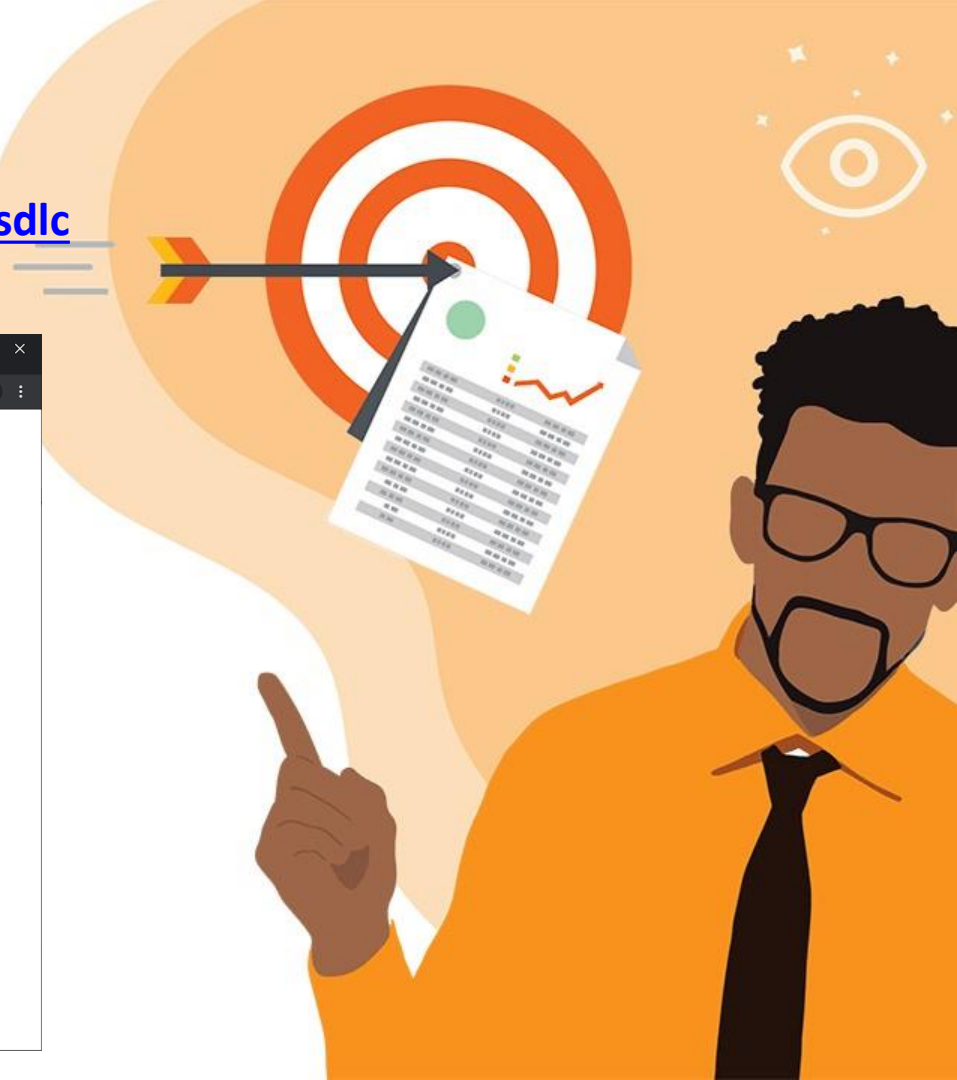
資通安全責任等級分級辦法
附表十
附表三

資通系統發展及維護安全

SSDLC檢核表

https://sites.google.com/email.nchu.edu.tw/ssdlc





資安的價值往往在事件發生後才凸顯

資安作為，是一種出事才能看出效果的投資，而且經常被視為是企業的成本，而不是價值。

「沒有發生資安事故」，背後其實做了多大、多深的努力和投入($)，是一種做得比別人更好的實質競爭力，用資安成就好名聲。

THANKS!

此簡報開放各界重製改作