資通安全管理法常見問題

版本：1091124

問題分類

目錄

1. 納管對象及範圍

議題	回應
1.1. 資通安全管理法(以下簡稱資安法)之納管對象為何？	資安法納管對象包含公務機關及特定非公務機關。 一、公務機關：指依法行使公權力之中央、地方機關(構)或公法人，但不含軍事及情報機關。 二、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 相關定義可參考資安法第 3 條第 5 至 9 款條文。
1.2. 公立醫療機構委託民間辦理，是否屬資安法納管對象？	依行政院衛生署 95 年 8 月 24 日衛署醫字第 0950036702 號函示，公立醫療機構委託民間辦理或公設民營機關〈構〉，既係委由民間辦理，其屬性不適合予以定位為公立醫療機構。 因此爰引上述函釋，公立醫療機構如委託民間辦理，可視為非屬本法所稱公務機關之範疇，惟其後續如經衛福部指定為「緊急救援與醫院類」之關鍵基礎設施提供者，則仍屬資安法納管對象。
1.3. 資安法中對政府捐助財團法人之定義，與財團法人法中不同，應以何為準？	資安法於送立法院審議期間，財團法人法尚未完成立法，對於資安法所稱政府捐助之財團法人之定義，已於第 3 條第 9 款中明定，並以該定義為準。
1.4. 地方政府捐助之財團法人是否為資安法納管對象？	地方政府捐助之財團法人非屬資安法第 3 條第 9 款所稱「營運及資金運用計畫應依預算法第 41 條第 3 項規定送立法院」、「年度預算書應依同條第 4 項規定送立法院審議之財團法人」，故非屬資安法納管對象。
1.5. 兼有公務機關與公營事業性質之機關，其納管方式為何?	資通安全管理法針對不同納管對象訂有不同程度之規範強度（公務機關>關鍵基礎設施提供者>公營事業或政府捐助之財團法人），如單一機關兼具二種身份時，依規範強度較高者納管之。 例如：以台北市自來水事業處為例，其兼具公務機關與公營事業性質，則以公務機關之身分納管之。
1.6. 地方政府之公營事業，其納管方式為何？	地方政府之公營事業屬資安法之特定非公務機關，依資安法第 17 及 18 條及相關子法之規定，該事業應受中央目的事業主管機關(各部會)之監督與管理。而地方政府則應督促所屬公營事業，依中央目的事業主管機關所定規定，辦理各項法遵業務。

議題	回應
1.7. 所有公務機關是否都應置資通安全長?資通安全長由誰來擔任?	依資安法第 11 條規定，公務機關皆應設置資通安全長；資通安全長由機關首長指派副首長或適當人員兼任。
1.8. 特定非公務機關是否應指定資安長/資通安全管理代表? 其資安長/資通安全管代表之層級是否有要求?	目前資安法本文中，並未明定特定非公務機關應指定資安長/資通安全管理代表。 惟為確保有效推動資通安全維護事項，建議特定非公務機關可指定資安長/資通安全管理代表。
1.9. 中央目的事業主管機關得否要求特定非公務機關指定一定層級之人員擔任資安長/資通安全管理代表?	資安法第 16 條第 6 項、第 17 條第 4 項中規定，「…資通安全維護必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬定，請主管機關核定」，故各中央目的事業主管機關基於資安防護整體考量，得要求其所管特定非公務機關指定適當層級之人員擔任資安長/資通安全管理代表，相關規定並得訂定於相關管理辦法中。
1.10. 里辦公處是否適用資通安全管理法？如為適用對象，其辦理作業項目為何？	里辦公處為里長與里幹事辦公之處所，隸屬於所在區公所並為其之派出單位，應適用本法，並配合所在鄉(鎮、市、區)公所辦理資通安全相關作業。(行政院資安處 109 年 3 月 30 日院臺護字第 1090169297 號函)

2. 資通安全責任等級分級

議題	回應
2.1. 資通安全責任等級分級辦法第 4 條中，全國性民眾或公務員個人資料檔案，其認定標準為何?	全國性民眾或公務員個人資料檔案，指含括全國大部分民眾或公務員之個人資料檔案。
2.2. 資通安全責任等級分級辦法第 5 條中，區域性、地區性民眾個人資料檔案，其認定標準為何?	區域性或地區性民眾個人資料檔案，指含括跨直轄市、縣(市)或單一直轄市、縣(市)地域範圍內之大部分民眾之個人資料檔案。
2.3. 機關的官方網站是提供資訊給全國民眾，是否屬於全國性的民眾服務?	機關之官網非屬本法所稱全國性民眾服務之範圍，全國性民眾服務通常為中央機關為執行法定職掌，統一規劃及提供予全國民眾或全國公務機關使用之申辦服務，如戶籍登記、地籍登記、工商登記、報稅等。
2.4. 市立的中醫醫院是否也屬於公立區域醫院或地區醫院，其資通安全責任等級為何?	市立中醫醫院屬於公立區域醫院或地區醫院，依資通安全責任等級分級辦法第 5 條，其資通安全責任等級原則上列為 B 級。
2.5. 目前部立醫院、區域醫院都被要求是 B 級，可是有些醫院規範不大，是否可以調降其資通安全責任等級?	機關可依資通安全責任等級分級辦法第 10 條，彈性調整各機關之等級，惟應敘明調整之理由。
2.6. 資通安全責任等級 C 級與 D 級機關的差異為何?	資通安全責任等級 C 級及 D 級的差異在於是否維運自行或委外開發之資通系統，若有，則機關之資通安全責任等級至少為 C 級(請參閱資通安全責任等級分級辦法第 6、7 條)。
2.7. 只有一個官網算不算 C 級機關？	官網如係屬機關自行或委外開發之資通系統，則符合資通安全責任等級第 6 條 C 級機關之條件，機關之資安責任等級即為 C 級。 建議類此機關，宜積極進行資通系統向上集中，減少機關維運負擔，連帶調降機關資通安全責任等級。
2.8. 內部不對外的網站，算不算自行或委外開發之資通系統?	內部不對外的網站，如屬自行或委外開發之資通系統，即符合資通安全責任等級第 6 條 C 級機關之條件，機關之資安責任等級即為 C 級。

議題	回應
2.9. 機關只有自行維護個人電腦及印表機等設備，是否可列為 E 級機關?	機關如僅自行維護個人電腦及印表機等設備，仍屬自行辦理資通業務之一部份，故依資通安全責任等級分級辦法第 7 條規定列為 D 級。
2.10.依責任等級分級辦法第 3 條，直轄市政府應提交所屬機關資通安全責任等級，是否包含學校?	依資通安全責任等級分級辦法第 3 條第 3 項規定，市立學校的資通安全責任等級由地方政府彙整提交。

3. 資通安全責任等級分級之應辦事項-資安專職人力及證照

議題	回應
3.1. 何謂資通安全專職人員？	資通安全專職人員，指全職執行資通安全業務者(請參閱資通安全責任等級分級辦法附表一備註四說明) 。
3.2. 資安專職人員之職務內容為何？	一、資安專職人力之職務內容分策略面、管理面及技術面等三大面向，各面向內容如下： (一)策略面： 1. 機關(及所屬)資安政策、資源分配及整體防護策略之規劃。 2. 機關導入資安治理成熟度之協調與推動。 3. 資通安全維護計畫實施情形之績效評估與檢討。 4. (屬上級或監督機關者)稽核所屬(或監督)公務機關之資通安全維護計畫實施情形。 (二)管理面： 1. 訂定、修正及實施資通安全維護計畫並提出實施情形。 2. 訂定及建立資通安全事件通報及應變機制。 3. 辦理下列機關資通安全責任等級之應辦事項：資訊安全管理系統之導入及通過公正第三方之驗證、業務持續運作演練、辦理資通安全教育訓練等。 4. (屬上級或監督機關者)針對所屬(或監督)公務機關，審查其資通安全維護計畫及實施情形、辦理其資通安全事件通報之審核、應變協處與改善報告之審核。 (三)技術面： 1. 整合、分析與分享資通安全情資。 2. 配合主管機關辦理機關資通安全演練作業。 3. 辦理下列機關資通安全責任等級之應辦事項：安全性檢測、資通安全健診、資通安全威脅偵測管理機制、政府組態基準、資通安全防護等。 4. (屬上級或監督機關者)針對所屬(或監督)公務機關，規劃及辦理資通安全演練作業。 二、機關資安專職人力之職務分工建議如下： (一)A 級機關置 4 名專職人力：1 名負責策略面工作，1 至 2 名負責管理面工作，另 1 至 2 名負責技術面工作。 (二)B 級機關置 2 名專職人力：1 名負責策略面及管理面工作，另 1 名負責技術面工作。 (三)C 級機關置 1 名專職人力：統籌機關資安業務。

議題	回應
	三、機關如兼屬資安法之中央目的事業主管機關，應對所轄之特定非公務機關辦理下列事項，如資安專職人力無法容納，建議由機關權責單位另派人力辦理，資安專職人員提供必要之協助。 (一) 審查其資通安全維護計畫及其實施情形。 (二) 稽核其資通安全維護計畫實施情形。 (三) 辦理其資通安全事件之通報審核、應變協處、改善報告審核。 (四) 訂定及修正機關特定非公務機關管理辦法。 (五) 指定關鍵基礎設施提供者及訂定其防護基準。 (六) 分享資通安全情資。
3.3. 機關規模不大且沒有資訊單位，如何在短時間配置資通安全專職人員？	1. 資安法施行後，各機關應優先於機關總員額內配置資安專職人力，惟為解決機關人力短時間調配問題，並配合數位專責機關籌設，如暫無缺額人力可支配，可先以約聘僱或委外人員擔任，至本法施行 4 年後(111 年底)，再以正式人員配置。 2. 此外，建議資訊業務規模小之機關可考慮將資通系統及資源向上集中，由上級機關統籌辦理，減少機關自行維運之負擔。
3.4. 資通安全專職人員是否要求要在資訊單位，或是否要求資訊職系?	資通安全專職人員並未要求配置在資訊單位，也未要求由資訊職系人員擔任，惟機關應給予資通安全專職人員足夠的教育訓練，取得適當之資通安全專業證照及職能證書。
3.5. 資通安全專職人力，如果分散在好幾人的身上，可以用 0.5+0.5=1 的方式配置嗎?	此無法達成專職專人之設置意義，機關應指定專人全職執行資通安全業務。
3.6. 有關資通安全專業證照，子法中指由主管機關認可之國內外發證機關(構)所核發之資通安全證照，相關認定何時可訂出?	資通安全專業證照清單已公布於國家資通安全會報網站資安管理法專區中（網址：https://nicst.ey.gov.tw/Page/EB237763A1535D65），並依資通安全專業證照認可審查作業流程，按季定期受理各機關（構）新增資通安全專業證照建議，經審查認可之資通安全專業證照，將定期更新資通安全專業證照清單。

議題	回應
3.7. 資通安全職能評量證書如何取得?	國家資通安全會報技術服務中心將每年遴選通過評鑑之教育訓練機構，於北中南各地開設資安職能評量證書課程，各機關同仁可報名上課，通過評量後即可取得證書。
3.8. 資通安全專業證照及資通安全職能評量證書應由誰取得?需不需要每人1張？	資通安全專職(責)人員至少應取得 1 張資通安全專業證照及資通安全職能評量證書，至於其他資訊或資安相關人員，機關也應鼓勵同仁踴躍參加資安相關教育訓練，提升專業能力。
3.9. 技服中心開設之資通安全職能評量證書課程，未來是否可開放特定非公機關參加?	技服中心開設的課程係針對公務機關專職人員開設，將優先提供名額予公務機關同仁。後續會視實際開課及報名情形，再檢討是否開放給特定非公務機關參加。
3.10. 108 年 1 月 1 日正式施行後，針對資安專職人力應取得之資通安全專業證照及職能練證書，是否有緩衝期?	資安法規定專業證照及職能練證書之取得於初次受核定或等級變更後 1 年內完成，故有 1 年緩衝期。
3.11.機關與所屬機關之資安專職人力是否可以共用?證照可否上級和所屬機關加起來一起算，還是分開算?	專職人力配置的要求是以機關為單位，人力不能共用計算，證照部分亦須以機關為單位分開計算。
3.12.特定非公務機關是否要配置專職人力，專職和專責人力差異在那?	依據資通安全責任等級分級辦法附表二、四、六等之規定，特定非公務機關須配置資安專責人員。資安專責人力是指機關應有專人負責資通安全事務，負責資通安全事務的人員即為專責人員，並無全職投入人力之要求，此與公務機關須配置專職人員之人力要求不同。(請參閱資通安全責任等級分級辦法附表一備註四說明)
3.13.資通安全專職人力如有異動，應多久內補齊專業證照?	資通安全專職人力如有異動，應於異動發生後立即派員受訓取得專業證照及職能證書。
3.14. 「資通安全責任等級分級辦法部分條文修正」附表中，資通安全教育訓練分為「資通安全專業課程訓練」、「資通安	1.「資通安全專業訓練」係泛指有助提升資通安全專責人員之資安管理或技術訓練之課程，以使資安專責人力勝任其職務內容。 2. 「資通安全職能訓練」指經行政院資通安全處認證之資安訓練機構舉辦之資安職能訓練課

議題	回應
全職能訓練」及「資通安全通識教育訓練」，三類課程意指為何？另相關課程時數是否可以從公務人員終身學習入口網站中統計？	程。 3.「資通安全通識教育訓練」係指資通安全相關之通識性概念課程，或機關內部資安全管理規定之宣導課程。 為利資安課程時數統計，人事行政總處將自 110 年 1 月 1 日起，於公務人員終身學習入口網站增加資安課程類別：資通安全(通識)、資通安全(專業、職能)及其對應代碼，屆時各機關於時數登錄時，對應其代碼即可分類計算相關時數。
3.15. 資通安全專職(責)人員，每人每年需 12 小時、資通安全專職人員以外之資訊人員每人每 2 年需 3 小時之資通安全專業課程訓練或資通安全職能訓練，時數應如何取得？	資通安全專業課程訓練或資通安全職能訓練相關時數，可透過以下方式取得： 1. 參加經行政院資通安全處認證之資安訓練機構舉辦之資安職能訓練。並請參考資安職能訓練發展藍圖(https://ctts.nccst.nat.gov.tw/about/Training)，由共通、基礎至進階循序學習，由淺入深逐步具備相關技能。 2. 參加技服中心舉辦之政府資通安全防護巡迴研討會，或所開設之資通安全管理、技術相關課程。 3. 參加資通安全專業證照清單上所列之訓練課程。 4. 參加國內外之公私營訓練機構所開設或受委託辦理之資通安全管理或技術訓練課程。 前述第 4 種辦理之訓練機構以下列型態為限： 1. 公私立大專校院。 2. 依法設立 2 年以上之職業訓練機構。 3. 依法設立 2 年以上之短期補習班。 4. 依法設立 2 年以上之學術研究機構、行政法人或財團法人，其設立章程宗旨與人才培訓相關，且有辦理人才培訓業務。
3.16. 資通安全專職人員以外之資訊人員、一般使用者及主管，每人每年需 3 小時之資通安全通識教育訓練，時數應如何取得？其中「一般使用者及主管」的範圍為	1.資通安全通識教育訓練時數，可透過以下方式取得： (1) 由機關自行辦理資通安全教育訓練。 (2) 至數位學習資源整合平臺「e 等公務園+學習平臺」(https://elearn.hrd.gov.tw)線上修習包含資安管理制度、社交工程攻擊防護、個人資料保護、行動裝置使用安全、物聯網資安威脅等資安課程。

議題	回應
何？	2.一般使用者及主管，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。
3.17.ISO/IEC27001:2013 ISMS LA 這張證照註明「除提出證照外，當須提供當年度至少 2 次實際參與該證照內容有關之稽核經驗證明」，那些類稽核可納入 2 次實際參與稽核之計算?	為使資安專職人員於取得 LA 相關證照後，持續維持稽核能力，爰要求提供當年度至少 2 次實際參與該證照內容有關之稽核經驗證明。 稽核經驗可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之稽核，均可納入稽核經驗次數計算。
3.18.資通安全責任等級分級辦法部分條文修正案中，何謂「資通安全專責人員以外之資訊人員」?	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。
3.19.機關如暫以委外人力擔任機關資安專職人力，該委外人員能否參加資安職能訓練課程？	如機關於本法施行過渡期間暫以委外人員擔任機關資安專職人員，該人員可以參加資安職能訓練課程，並取得資安職能證書。請該人員於報名時，加註敘明其所擔任資安專職人員之服務機關，供報名審查即可。

4. 資通安全責任等級分級應辦事項-其他

議題	回應
4.1. 附表備註中「資通安全健診」亦得採取經主管機關、中央目的事業主管機關認可之其他具有同等或以上效用之措施；主管機關何時會認可此類同等或以上效用之措施？	本項規定係因應未來科技發展所保留多元作業方式之彈性，公務機關或特定非公務機關針對特定之技術如有認定之需要，可以個案方式提出，由主管機關與中央目的事業主管機關認定。
4.2. C 級機關如無核心資通系統，應辦事項中針對核心資通系統之項目是否須辦理?	C 級機關如無核心資通系統，應辦事項中針對核心資通系統之項目則無須辦理。
4.3. C 級核心資通系統若皆委由外單位維運(自行維運非核心系統)，是否仍須導入 CNS27001 及相關安全性檢測？	核心資通系統不論是委外或自行維運，皆須導入 CNS27001 及相關安全性檢測。
4.4. ISMS 導入的範圍，因實體空間之限制(例如機關使用雲端機房)，機關應如何進行導入？	依資通安全責任等級分級辦法之規定，C 級以上機關 ISMS 導入的範圍為「全部核心資通系統」，不因系統是否在雲端機房有所不同。 雲端服務同樣可取得 ISO27001 驗證，機關如需使用雲端服務，請選擇通過 ISO 27001 驗證之雲端服務商。
4.5. 資通系統檢測目前是否以 IT 設備為主，OT 設備是否納入？	A、B、C 級機關之核心資通系統，不論其屬 IT 或 OT，皆應依分級辦法附表 1 至 6 之規定，辦理安全性檢測。 惟中央目的事業主管機關得就特定類型資通系統之防護基準認有另為規定之必要者，自行擬定防護基準(詳參分級辦法第 11 條第 2 項後段)。
4.6. 應辦事項列表的「資安健診」中「使用者端電腦惡意活動檢視」，請問有規定檢視的比例嗎？機關沒有那麼多經費可以檢視 100%的電腦怎麼辦?	資通安全健診對於使用者端電腦惡意活動檢視並無明確比例之規定，原則上檢測範圍為全機關，機關如囿於經費，可將部分非從事核心業務之使用者電腦，分年完成使用者電腦檢測，惟檢測週期不宜逾 2 年。 另建議機關單位正副主管以上及機要人員、資訊單位同仁、委外廠商駐點人員、維護機關核心資通系統之承辦同仁等電腦，應加強檢測頻率，以利及早掌握資安威脅狀態。

議題	回應
4.7. 核心資通系統的選定，是否就機關內支持核心業務運作必要之系統，及資通系統防護需求等級為高者，擇一標準來選定即可？	依施行細則第七條規定之核心資通系統，係指滿足任一條件者(支持核心業務運作必要之系統、或資通系統防護需求等級為高)，都為核心資通系統。 如該資通系統屬由其他機關提供之共用性系統，則由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統，本原則並已列示於分級辦法附表一至六備註處。
4.8. 應辦事項列表中的資通安全管理系統之導入及通過公正第三方驗證，提到全部核心資通系統需導入 CNS27001 或 ISO27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準；請問如何認定同等或以上效用之資訊安全管理系統或標準？ **另所謂公正第三方驗證之「公正第三方」，是指那些機構?**	1. 同等或以上效用之資訊安全管理系統或標準，係指資安法納管對象針對其特殊事業領域已有國際或國內慣用之特定資通安全管理系統標準，且效用同等或高於 CNS27001 或 ISO27001 者。 2. 有關公正第三方係指通過我國標準法主管機關(經濟部)委託機構(財團法人全國認證基金會，TAF)認證之機構，可參考 TAF 官網之管理系統驗證機構認證名錄(https://www.taftw.org.tw/wSite/sp?xdUrl=/wSite/taf/cbalab.jsp&ACCID=CBA_MS_ID&mp=1)
4.9. 機關內部資安稽核的範圍，是否僅限資訊單位？或需涵蓋全機關各單位？針對無資通系統之單位，應如何稽核？	機關內部資安稽核應涵蓋全機關，非僅限資訊單位，另建議先擬定整體稽核計畫，確認各單位之稽核頻率、稽核委員組成及稽核發現之後續追蹤管考機制等。 針對無建置資通系統之單位，稽核重點可針對同仁對資通系統之使用行為、社交工程演練落實情形及資安意識訓練等。

5. 資通安全維護計畫撰寫

議題	回應
5.1. 資通安全維護計畫之內容要求為何?	1. 資安法施行細則第 6 條第 1 項已訂有 13 款內容，詳細可參閱子法條文。 2. 國家資通安全會報網站之資安法專區亦已提供範本。
5.2. 資通安全維護計畫可否由上級或監督機關代為辦理?	1. 依資安法施行細則第 6 條第 3 項規定，公務機關之資通安全維護計畫可由上級或監督機關代為辦理。 2. 特定非公務機關之資通安全維護計畫可由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或經中央目的事業主管機關同意，由其所管特定非公務機關辦理。
5.3. 上級或監督機關是否需提供維護計畫範本？中央目的事業主管機關是否需提供維護計畫範本?	1. 有關公務機關資通安全維護計畫內容，行政院已提供範本，並置於國家資通安全會報網站之資安法專區中。 2. 至於上級或監督機關、中央目的事業主管機關是否需提供維護計畫範本由機關自行視需要提供。(參閱資安法第 16、17 條說明)。
5.4. 維護計畫的內容如援引機關內部文件，是否需做摘錄?提交時，相關文件是否需以附件提報?	資通安全維護計畫援引之文件，原則上應做為附件一併提交，惟如機關已通過 CNS27001(ISO27001)驗證，所援引之文件係 CNS27001(ISO27001)相關文件者，應說明文件名稱及章節，除另有要求外，原則不需提交。
5.5. 資通安全維護計畫是否需按範本的章節填寫?	建議機關依資通安全維護計畫範本之章節次序撰寫，各機關如有特殊考量仍得依實務需求微調，惟仍應包含所有規定項目。
5.6. 資通安全維護計畫中之資通安全推動組織，必須由機關自行成立新推動組織嗎？能否併入現行相關推動組織辦理？或併同其他機關共同成立？	若機關已有相關資安推動組織，應於現行體制運作融入法規要求並進行調整即可，無須另成立新推動組織；至於是否宜合併他機關組織進行運作，仍須視實務可行性而定(如機關資通業務多已向上級機關集中，則可行性較高)。
5.7. 資通安全維護計畫範本中之資安防護措施，機關是否可依需要進行調整？	範本中所列之控制措施多為基本資安防護作業，機關可依自身需求增加資安防護措施，如機關經整體風險評估後，認為部分資安防護措施已有其他替代措施或不適用，亦可調整。

議題	回應
5.8. 未來針對風險評鑑方法論，是否須參考「資通系統風險評鑑參考指引」進行?	建議公務機關依此文件進行資安風險評鑑作業，俾利建立公務機關間一致性之作法與基準。
5.9. 目前沒有核心業務如何撰寫核心業務?	資安法第 7 條已明定核心業務之範圍，建議機關依此定義辨識機關之核心業務，另外，機關亦可參考現行內部控制制度所選定業務項目或經業務衝擊影響分析(BIA)後所辨識之重要業務作為核心業務。
5.10. 維護計畫中是否針對個人資料之保護論述不足？	資安法施行細則第 6 條訂有資安維護計畫之內容框架，計畫內容則由機關依業務特性研擬資安防護作為，個人資料保護屬機關資料保護範圍之一環，相關保護措施可併入現有資料防護作業辦理，機關如經評估有強化個資保護之必要，可增強防護措施並呈現於資安維護計畫內。

6. 辦理受託業務-受託者之選任及監督

議題	回應
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。
6.2. 資安法施行前已存在的委外契約，是否適用委外管理之規定？	資安法施行後，機關應依施行細則第 4 條所定之委外注意事項，檢視現行委外作業之適法性，如有須調整者，建議透過專案管理或變更契約等方式辦理。
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。
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、資訊單位還是稽核單位)？	廠商的管理措施是否"完善"，係視機關委外業務之防護需求及等級而定。機關可在招標文件中述明，以作為選商的評判依據。另外，前述防護需求所需之"完善"管理措施，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。
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	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

議題	回應
在驗證範圍?	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。
6.7. 客製資通系統開發，是否須第三方安全性檢測?	委外開發之資通系統如屬委託機關之核心資通系統，或委託案件金額在 1,000 萬元以上，委託機關應自行或另行委託第三方進行安全性檢測。
6.8. 第三方安全性檢測包含那些事項？	第三方安全性檢測建議包含弱點掃描、滲透測試等，源碼掃描可視系統重要性及經費資源額外辦理。 另依資通安全責任等級分級辦法附表十資通系統防護基準中，針對系統與服務獲得之構面，要求系統防護需求分級為「高」之系統，須執行源碼掃描、滲透測試及弱點掃描。
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，此情形受託者辦理受託業務之相關程序及環境都在機關內，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？	1. 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。 2. 惟採購套裝軟體或硬體，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，以降低潛在的資安威脅及弱點。
6.10. 請問資通安全管理法施行細則第四條第 1 項第 5 款之規定，其委託金額達新臺幣一千萬元以上者，是僅有硬體設備，亦或涵蓋軟、硬體及人力？	受託業務包括客製化資通系統開發者之委託金額達一千萬元以上者，係指該採購案之採購金額，並未再區分軟硬體或服務之金額。

7. 資通安全事件通報及應變

議題	回應
7.1. 資安事件通報及應變辦法第二條第二項中，如影響系統可用性是非外力（非機關外的駭客）造成的，是不是要通報？（例如 UPS 造成的中斷）	不論是否屬機關內外因素導致，均須通報。
7.2. 1 台 PC 故障，或是 1 個感探器故障，是否要進行通報？	需視其是否影響核心或非核心業務運作，或造成機關日常作業影響而定，如已造成前述事項之影響，則須通報。
7.3. 公務機關應如何進行資通安全事件之通報？	資通安全事件通報及應變辦法第四條第一項之規定:「公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。」。 上述規定提及之「主管機關指定之方式」,即利用國家資通安全通報應變網站(https://www.ncert.nat.gov.tw/)辦理通報業務，相關網站使用問題，請參考該網站之「通報網站常見問題集」等說明文件。
7.4. 直轄市山地原住民區公所及其區民代表會是否須配合上級或監督機關執行演練作業？	是的，資通安全事件通報及應變辦法第八條第一項之規定：「總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關」,即直轄市山地原住民區公所及直轄市山地原住民區民代表會須配合上級或監督機關執行演練作業，例如臺中市和平區民代表會應配合臺中市政府執行演練作業。

8. 其他

議題	回應
8.1. 資安法施行後，如執行不力公務人員是否會被記過?	機關人員未依資安法、資安法授權訂定之法規或機關內部規範辦理資安事項，經主管機關、上級或監督機關評定績效不良，且疏導無效情節重大者，始可能進行懲處，機關人員如已依規定辦理者，不致受懲。
8.2. 資通安全和資訊安全的差異在那?	資通安全涵蓋資訊與通信，範圍較資訊廣泛，目前多以資通安全稱之。
8.3. 施行細則第 4 條有關委外辦理資通系統建置或資通服務提供，資通服務提供的定義為何？PC 維護案是否屬之？須不須有第三方驗證？	1. 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。 2. 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。
8.4. 若系統資料含特種個資，該系統防護需求等級是否一定要列為"高"？若含一般個資，系統防護需求等級是否一定要列為"中"以上？或是依系統所含個資種類、數量等，是否有建議的系統防護需求分級參考？	各機關應依資通安全責任等級分級辦法附表 9 資通系統防護需求分級原則，就機關業務屬性、系統特性及資料持有情形等，訂定較客觀及量化之衡量指標，據以一致性評估機關資通系統之防護需求。