資通安全管理法常見問題

版本：1130628

問題分類

1. 納管對象及範圍 1
2. 資通安全責任等級分級 3
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 5
4. 資通安全責任等級分級應辦事項-其他 12
5. 資通安全維護計畫撰寫及實施情形填報 18
6. 辦理受託業務-受託者之選任及監督 20
7. 資通安全事件通報及應變 22
8. 其他 24

目錄

1. 納管對象及範圍 1
   1.1. 資通安全管理法（以下簡稱資安法）之納管對象為何？ 1
   1.2. 公立醫療機構委託民間辦理，是否屬資安法納管對象？ 1
   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？ 1
   1.4. 地方政府捐助之財團法人是否為資安法納管對象？ 1
   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？ 1
   1.6. 地方政府之公營事業，其納管方式為何？ 2
   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？ 2
   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/資通安全管理代表之層級是否有要求？ 2
   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？ 2
   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？ 2
   1.11. 由資安法納管對象所設立或管理之任務編組，是否受資安法納管？其資安權責為何？ 2
2. 資通安全責任等級分級 3
   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？ 3
   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？ 3
   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？ 3
   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？ 3
   2.5. 目前部立醫院、區域醫院都被要求是 B 級，可是有些醫院規模不大，是否可以調降其資通安全責任等級？ 3
   2.6. 資通安全責任等級 C 級與 D 級機關的差異為何？ 3
   2.7. 只有 1 個官網算不算 C 級機關？ 3
   2.8. 內部不對外的網站，是否屬於 C 級的資通系統？ 3
   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？ 4
   2.10. 依資通安全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？ 4
   2.11. 各機關如有因組織或業務調整致須變更原資通安全責任等級，或新設

機關之情形，其上級機關應於多久內提報該機關之資通安全責任等級或解除納管？ 4
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 5
3.1. 何謂資通安全專職人員？ 5
3.2. 資安專職人員之職務內容為何？ 5
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？ 6
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？ ..6
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？ 6
3.6. 有關資通安全專業證照，所指由主管機關認可之資通安全證照，其清單在哪可取得？ 7
3.7. 資通安全職能訓練證書如何取得？ 7
3.8. 資通安全專業證照及資通安全職能訓練評量證書應由誰取得？需不需要每人 1 張？ 7
3.9. 資通安全職能訓練是否可開放特定非公務機關參加？ 7
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訓練證書，是否有緩衝期？ 7
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？ 7
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為何？ ..8
3.13. 資通安全專職人力如有異動，應多久內補齊專業證照？ 8
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？ 8
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？ 8
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？是否能以資通安全專業課程訓練時數相抵？其中「一般使用者及主管」的範圍為何？ 10
3.17. ISO/IEC 27001:2013 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」，哪些類稽核可納入 2 次實際參與稽核之計算？ 10
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」？ 10
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？ 10
3.20. 有關資安法對於資安教育訓練時數之要求，如同仁年底才到職，來不及上課，該年度是否得以排除？ 10
3.21. 國際標準組織ISO已於111年10月26日公告新版ISO/IEC 27001:2022，相關人員取得之 ISO/IEC 27001:2013 資通安全專業證照是否有轉版緩衝期？ 11
3.22. 資通安全職能訓練是否有修習順序限制？ 11
3.23. 有關資通安全專業證照 ISO/IEC 27001 有效性及認定方式為何？ 11
4. 資通安全責任等級分級應辦事項-其他 12
4.1. 分級辦法附表一至六備註中「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、中央目的事業主管機關何時會認可此類同等或以上效用之措施？ 12
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？ 12
4.3. 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 CNS 27001 或 ISO 27001 等資訊安全管理系統標準，並進行相關安全性檢測？ 12
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？ 12
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？ 12
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？ 12
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？AD 或防火牆等系統是否亦須標識為核心資通系統？另由他機關提供之共用性系統，使用機關需再辦理系統防護需求分級嗎？ 13
4.8. 應辦事項列表中的資訊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 CNS 27001 或 ISO 27001 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？ 13
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？ 13
4.10. 如機關提報資安責任等級變更，於待核定期間之相關應辦事項，應依原等級辦理或依待核定之新等級辦理？ 14
4.11. 分級辦法附表十有關營運持續計畫高等級防護基準於「不同地點」備

份，有沒有距離要求？ 14
4.12. 分級辦法附表十所要求資通系統應保存日誌（log）之項目為何？ ... 14
4.13. 有關政府組態基準（GCB）導入作業，其應完成期限為何？導入有哪些應注意事項？ 14
4.14. 應辦事項列表中資安弱點通報機制（VANS）應導入範圍為何？是否有建議之上傳頻率？針對高風險以上弱點是否有訂定相關修補時間？ .15
4.15. 應辦事項列表中資安弱點通報機制（VANS）所謂應依主管機關指定方式提交資訊資產盤點資料，所稱「資訊資產」為何？如何執行盤點作業？是否有相關參考資料供導入參考？ 15
4.16. 應辦事項列表中端點偵測及應變機制（EDR）應導入範圍為何？若機關現階段尚未編列足夠的經費，應如何導入？ 15
4.17. 分級辦法所規定 ISMS 取得公正第三方驗證，驗證證書須有 TAF 標誌，但如機關已有驗證證書，但沒有 TAF 標誌應如何處理？ 16
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？ 16
4.19. 公務機關如果有維運特定類型資通系統（如工控系統等），可否改用其他資通系統防護基準來執行相關控制措施？ 16
4.20. 機關因組織調整、新成立致須變更或新增核定資安責任等級時，其應辦事項之法遵期限應如何認列？ 16
4.21. 有關資通安全責任等級分級辦法附表一、附表三應辦事項規定，A、B 級公務機關於初次受核定或等級變更後之 1 年內，應完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料，其提交方式為何？ 17
4.22. 行政院國家資通安全會報年度資安稽核計畫是否公告周知？稽核頻率為何？ 17
5. 資通安全維護計畫撰寫及實施情形填報 18
5.1. 資通安全維護計畫之內容要求為何？ 18
5.2. 資通安全維護計畫可否由上級或監督機關代為辦理？ 18
5.3. 上級或監督機關、中央目的事業主管機關是否需提供資通安全維護計畫範本？ 18
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？ 18
5.5. 資通安全維護計畫是否需按範本的章節填寫？ 18
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？ 18
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？ 18

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？ 19
5.9. 目前沒有核心業務如何撰寫核心業務？ 19
5.10. 維護計畫中是否針對個人資料之保護論述不足？ 19
5.11. 有關資通安全維護計畫實施情形填報，是否可由上級機關統一提報？ 19
6. 辦理受託業務-受託者之選任及監督 20
6.1. 委外注意事項何時要納入？ 20
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？ 20
6.3. 受託者是否必須通過第三方驗證？第三方驗證之範圍？ 20
6.4. 何謂完善的資通安全管理措施？ 20
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）？ 20
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？ 20
6.7. 客製資通系統開發，是否須第三方安全性檢測？ 21
6.8. 第三方安全性檢測包含那些事項？ 21
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？ 21
6.10. 請問資通安全管理法施行細則第 4 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？ 21
7. 資通安全事件通報及應變 22
7.1. 資安事件通報及應變辦法第 2 條第 2 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） 22
7.2. 1 台 PC 故障，或是 1 個感探器故障，是否要進行通報？ 22
7.3. 公務機關應如何進行資通安全事件之通報？ 22
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？ 22
7.5. 有關資安事件應於 1 個月內送交調查、處理及改善報告，請問 1 個月如何計算？ 22
7.6. 有關應於知悉資通安全事件後，1 小時內進行資安事件通報，請問應如何判斷「知悉」時間？ 23
7.7. 何謂重大資安事件？ 23
8. 其他 24

8.1. 資安法施行後，如執行不力公務人員是否會被記過？ 24
8.2. 資通安全和資訊安全的差異為何？ 24
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？ ..24
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？.....24
8.5. 機關如欲與主管機關進行情資分享，其分享方式為何？ 24
8.6. 有關「限制使用危害國家資通安全產品」是否會提供相關清單？此外，在未公布清單前是否有相關參考作法？ 24
8.7. 有關雲端服務是否會提供相關參考指引？且是否有相關限制？ 25

1. 納管對象及範圍

問題	回復
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。 其中公營事業係依「公營事業移轉民營條例」第 3 條規定，包含中央及地方政府投資經營之公營事業： 一、各級政府獨資或合營者。 二、政府與人民合資經營，且政府資本超過百分之五十者。 三、政府與前二款公營事業或前二款公營事業投資於其他事業，其投資之資本合計超過該投資事業資本百分之五十者。
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。

問題	回復
	例如：以臺北自來水事業處為例，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。
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/資通安全管理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（行政院資通安全處 109 年 3 月 30 日院臺護字第 1090169297 號函）。
1.11. 由資安法納管對象所設立或管理之任務編組，是否受資安法納管？其資安權責為何？	一、任務編組之業務屬於其設立機關或管理機關之一部分，爰應受資安法納管，配合設立機關或管理機關，執行資通安全業務。 二、設立機關或管理機關之資通安全維護計畫，應將該任務編組之核心業務、資通系統納入。

2. 資通安全責任等級分級

問題	回復
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，可是有些醫院規模不大，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 級的差異在於是否有維運自行或委外設置、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 1 個官網算不算 C 級機關？	官網如係屬機關自行或委外設置、開發，即符合資通安全責任等級分級辦法第 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，是否屬於 C 級的資通系統？	內部不對外的網站，如為自行或委外設置、開發，即符合資通安全責任等級分級辦法第 6 條 C 級機關之條件，機關之資安責任等級即為 C 級。

問題	回復
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. 依資通安全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。
2.11. 各機關如有因組織或業務調整致須變更原資通安全責任等級，或新設機關之情形，其上級機關應於多久內提報該機關之資通安全責任等級或解除納管？	機關如有下列情形，其上級機關應於 1 個月內，依資通安全責任等級分級辦法第 3 條第 6 項辦理等級異動作業： 1. 機關裁撤（自行政院人事行政總處函生效日起）。 2. 機關因組織或業務調整（自行政院人事行政總處函生效日起）。 3. 成立籌備處（自籌備處組織規程發布日起）。 4. 新設機關（自組織法施行日起）。

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

問題	回復
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三、附表三備註三、附表五備註二說明）。
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。 5. 委外廠商管理與稽核。 (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

問題	回復
	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。 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？	一、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，如暫無缺額人力可支配，得先以約聘僱或委外人員擔任。 二、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。向上集中辦理之經費，於實務上有上級機關統編或由各使用機關分攤等方式。
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	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。

問題	回復
置嗎？	
3.6. 有關資通安全專業證照，所指由主管機關認可之資通安全證照，其清單在哪可取得？	資通安全專業證照清單已公布於數位發展部資通安全署「資安法規專區」之「資安專業證照清單」（網址：https://moda.gov.tw/ACS/laws/certificates/676）。 各機關如有新增資通安全專業證照或調整建議，請依資通安全專業證照認可審查作業流程，主管機關將按季受理審查，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。
3.7. 資通安全職能訓練證書如何取得？	一、各機關可透過參加主管機關委由國家資通安全研究院統籌辦理之資通安全職能訓練，且完成指定上課時數並通過評量測驗後，即可取得資通安全職能訓練證書。 二、各機關亦可逕洽經主管機關認證之教育訓練機構申請開設資通安全職能訓練專班課程，相關申請資訊：資安人才培訓服務網 https://ctts.nics.nat.gov.tw/DownloadDetail/66。
3.8. 資通安全專業證照及資通安全職能訓練評量證書應由誰取得？需不需要每人 1 張？	公務機關資通安全專職(責)人員至少持有資通安全專業證照及資通安全職能訓練證書各 1 張以上、特定非公務機關資通安全專責人員至少持有資通安全專業證照 1 張以上，並維持其證照或證書之有效性。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. 資通安全職能訓練是否可開放特定非公務機關參加？	資通安全職能訓練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，其次開放給特定非公務機關人員參加，惟無法進行相關補助。
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訓練證書，是否有緩衝期？	資安法規定專業證照及職能訓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	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。

問題	回復
屬機關加起來一起算，還是分開算？	
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為何？	依據資通安全責任等級分級辦法附表二、四、六之規定，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三、附表三備註三、附表五備註二說明）
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？	一、「資通安全專業課程訓練」係泛指有助提升資通安全專責人員之資安策略、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。 二、「資通安全職能訓練」指經主管機關認證之資安訓練機構舉辦之資安職能訓練課程。 三、「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，或機關內部資通安全管理規定之宣導課程。 四、為利資安課程時數統計，人事行政總處自 110 年 1 月 1 日起，於公務人員終身學習入口網站之公務人員學習紀錄增加資安課程代碼：資通安全（通識）代碼 522、資通安全（專業、職能）代碼 523，各機關於統計學習時數時，可依代碼計算相關時數。
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？	一、資通安全職能訓練時數取得方式，係參加經主管機關認證之資安訓練機構舉辦之資安職能訓練。 二、資通安全專業課程訓練係指可對應資安職能訓練發展藍圖中策略面、管理面、技術面（https://ctts.nics.nat.gov.tw/about/Training）之專業課程為原則，其相關時數，可透過以下方式取得： (一) 參加主管機關舉辦政府資通安全防護巡迴研討會，或所開設之資通安全策略、管理、技

問題	回復
	術相關課程、講習、訓練及研討（習）會。 (二) 參加資通安全專業證照清單上所列之訓練課程。 (三) 參加公私營訓練機構聘請符合資格講師所開設或受委託辦理之資通安全策略、管理或技術訓練課程。 1. 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，設立章程宗旨與資通安全人才培訓相關，且有辦理資通安全人才培訓業務。 2. 講師需具備資通安全課程實際授課經驗，且應符合下列各款資格之一，持有資通安全職能訓練證書者尤佳： (1) 為國內、外碩士以上資訊或理工相關系所畢業，並具有 5 年以上與資通安全領域專業相關實務經驗之專業工作年資；或為國內、外大專以上資訊或理工相關系所畢業，並具 10 年以上與資通安全領域專業相關實務經驗之專業工作年資。 (2) 政府機關（構）薦任第九職等或相當職務以上從事與資通安全相關業務人員。 (3) 其他在資通安全相關領域（如：技術）上有特殊造詣，檢具足以擔任授課師資之相關證明文件，經主管機關認可者。 三、資通安全專業課程訓練原則應優先以實體課程方式進行，惟為因應機關特定需求，符合下列各項條件者，同意採線上課程方式取得資通安全專業課程訓練時數，惟每人每年認定上限為 6 小時： (一) 課程須上架至數位學習資源整合平臺「e 等公務園+學習平臺」。 (二) 課程內容須定期更新，課後須辦理評量，且評量內容應涵蓋授課範圍、具辨識度且定期

問題	回復
	調整。 (三) 線上課程應提供「問題提問或諮詢」機制，其方式不拘。
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？是否能以資通安全專業課程訓練時數相抵？其中「一般使用者及主管」的範圍為何？	一、資通安全通識教育訓練時數，可透過以下方式取得： (一) 由機關自行辦理資通安全教育訓練。 (二) 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。 二、資通安全通識教育訓練與資通安全專業課程訓練性質及目的不同，爰資通安全專業課程訓練時數不可抵資通安全通識教育訓練時數。 三、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/IEC 27001:2013 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」，哪些類稽核可納入 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，在其持續擔任資通安全專職（責）人員期間，要求提供每年度須至少 2 次實際參與該證照內容有關之稽核工作或經驗證明。 稽核經驗可以稽核員或觀察員身分，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設置、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。
3.20. 有關資安法對於資安教育訓練時數之要求，如同仁年底才到職，來不	考量資安專業/職能訓練實體課程，有開課、報名及參訓等議題，故機關同仁當年在職未滿 90 天者得免納入當年度時數要求名單；而資安通識訓練

問題	回復
及上課，該年度是否得以排除？	部分，仍應於當年度年底前完成。
3.21. 國際標準組織 ISO 已於 111 年 10 月 26 日公告新版 ISO/IEC 27001:2022，相關人員取得之 ISO/IEC 27001:2013 資通安全專業證照是否有轉版緩衝期？	ISO/IEC 27001:2013 資通安全專業證照認列至 114 年 10 月 31 日止，請於該期限前完成轉版。（備註：機關轉版期限亦同）
3.22. 資通安全職能訓練是否有修習順序限制？	依「資安職能訓練發展藍圖」規劃學習路徑（核心→專業），須持有核心科目「資通安全概論」評量有效證書者，始得報名其他「專業」科目。
3.23. 有關資通安全專業證照 ISO/IEC 27001 有效性及認定方式為何？	有關屬於國際認證論壇（International Accreditation Forum, IAF）正式會員之認證機構所核發之 ISO/IEC 系列資通安全專業證照，其歷年版次及轉版之有效性及認定方式，請逕洽原核發機構確認。通過英國皇家品質協會（Chartered Quality Institute, CQI）與國際認證稽核員註冊機構（International Register of Certificated Auditors, IRCA）獨立審查與認證之 ISO/IEC 27001 證照，亦屬主管機關認可之資通安全專業證照。

4. 資通安全責任等級分級應辦事項-其他

問題	回復
4.1. 分級辦法附表一至六備註中「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、中央目的事業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. 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 CNS 27001 或 ISO 27001 等資訊安全管理系統標準，並進行相關安全性檢測？	核心資通系統不論是委外或自行維運，皆須導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準，並進行相關相關安全性檢測。
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 CNS 27001 或 ISO 27001 等驗證，機關如需使用雲端服務，請選擇通過 ISMS 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，皆應依資通安全責任等級分級辦法附表一至六之規定，辦理安全性檢測。 惟特定非公務機關之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，得自行擬訂防護基準（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	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

問題	回復
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？	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。
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？AD 或防火牆等系統是否亦須標識為核心資通系統？另由他機關提供之共用性系統，使用機關需再辦理系統防護需求分級嗎？	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，核心資通系統的擇選範圍以應用系統為原則。 如該資通系統屬由其他機關（含上級機關）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（系統防護需求分級亦同），本原則並已列示於分級辦法附表一至六之備註一。
4.8. 應辦事項列表中的資訊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 CNS 27001 或 ISO 27001 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？	一、同等或以上效果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訊安全管理系統標準，且效果同等或高於 CNS 27001 或 ISO 27001 者。 二、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，可至 TAF 官網之「認證名錄」查詢「管理系統驗證機構」（ https://www.taftw.org.tw/directory/scheme/msv）。 三、考量第三方驗證作業之公正性及獨立性，機關如委外辦理 ISMS 輔導及驗證時，輔導案及驗證案之服務契約，應分別招標。
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？	考量資安法納管對象為全機關，並確保內部稽核有效性，機關內部資安稽核範圍應涵蓋機關資通安全維護計畫之適用範圍，而非僅限資訊單位，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

問題	回復
	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。
4.10. 如機關提報資安責任等級變更，於待核定期間之相關應辦事項，應依原等級辦理或依待核定之新等級辦理？	未核定變更前，機關仍應依現行之資安責任等級辦理，主管機關原則於收文兩周內完成核定，請機關依函復結果辦理相關事宜。
4.11. 分級辦法附表十有關營運持續計畫高等級防護基準於「不同地點」備份，有沒有距離要求？	有關不同地點備份，宜朝「不遭受同一風險或事件影響」的方向考量，目前並未設置距離要求；有關距離建議，機關亦可參考「我國電腦機房異地備援機制參考指引」中，異地備份/備援機制提及之主機房與異地備援機房之距離應距離 30 公里以上，做為參考依據，以期在發生地震等區域性毀損時，仍能夠保存完整之備份資料及縮短回復時間。
4.12. 分級辦法附表十所要求資通系統應保存日誌（log）之項目為何？	各機關於日常維運資通系統時，應訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月，其保存項目建議如下： 1. 作業系統日誌（OS event log） 2. 網站日誌（web log） 3. 應用程式日誌（AP log） 4. 登入日誌（logon log） 另為確保資通安全事件發生時，各機關所保有跡證足以進行事件根因分析，相關日誌紀錄建議定期備份至與原日誌系統不同之實體，詳參國家資通安全研究院發布之「資通系統防護基準驗證實務」2.2.1.記錄事件章節之內容（https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/）。
4.13. 有關政府組態基準（GCB）導入作業，其應完成期限為何？導入有哪些應注意事項？	一、依資通安全責任等級分級辦法，A、B 級公務機關應於初次受核定或等級變更後 1 年內，依主管機關公告之項目，完成 GCB 導入作業，並持續維運。 二、主管機關如有公告新增項目，A、B 級公務機關應於公告 1 年內，完成新增項目 GCB 之導入。 三、GCB 係規範資通訊終端設備的一致性安全設定，套用原則為專版專用，各機關導入 GCB

問題	回復
	時，應充分進行測試後再套用，以避免發生預期外之狀況。各機關得依實務需求進行例外管理，並落實審核及定期檢討。
4.14. 應辦事項列表中資安弱點通報機制(VANS)應導入範圍為何？是否有建議之上傳頻率？針對高風險以上弱點是否有訂定相關修補時間？	一、公務機關 VANS 導入範圍以全機關之資訊資產為原則，有關支持核心業務持續運作相關之資通系統主機與電腦應於規定時限內完成導入；關鍵基礎設施提供者 VANS 之導入範圍至少應涵蓋關鍵資訊基礎設施及營運持續運作必要相關資通系統。 二、有關資訊資產盤點資料上傳頻率，除重大弱點通報或大量資產異動外，建議每個月定期上傳 1 次，並應針對發現弱點設定修補期限。 三、機關發現高風險以上之弱點，應即時完成修補；弱點完成修補前，應規劃緩解措施及管理作為，加強監控、防護配套與異常偵測，確保弱點管理之即時性及有效性，以降低資安風險；相關弱點處置方式應於一週內至 VANS 系統填寫，並納入機關內部稽核與管理審查等機制進行管理，確認弱點改善措施之有效性。
4.15. 應辦事項列表中資安弱點通報機制(VANS)所謂應依主管機關指定方式提交資訊資產盤點資料，所稱「資訊資產」為何？如何執行盤點作業？是否有相關參考資料供導入參考？	一、「資訊資產」係指伺服器主機及使用者電腦之作業系統及應用程式等軟體資訊。 二、導入 VANS 之資訊資產盤點資料，為彙總性之盤點資料，僅含比對所需之必要欄位資訊，包含「資產名稱」、「資產廠商」、「資產版本」及「數量」等。 三、提交作業流程可參考國家資通安全研究院網站-VANS 專區（https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/VANS/）之實作訓練數位教材，教材內容包含資訊資產盤點、正規化、資產登錄等相關作業。
4.16. 應辦事項列表中端點偵測及應變機制（EDR）應導入範圍為何？若機關現階段尚未編列足夠的經費，應如何導入？	有關支持核心業務持續運作相關之資通系統主機與電腦應於規定時限內完成導入，機關如囿於經費，可考量與核心業務之關聯性、資安風險程度及資訊資產重要性等，優先擇定並分年完成導入。

問題	回復
4.17. 分級辦法所規定ISMS取得公正第三方驗證，驗證證書須有 TAF 標誌，但如機關已有驗證證書，但沒有 TAF 標誌應如何處理？	現有證書要更換成具財團法人全國認證基金會（Taiwan Accreditation Foundation, TAF）標誌之證書，經詢驗證機構，主要有以下方式，請機關洽委託機構確認： 1. 機關現行證書上沒有國際認證論壇（International Accreditation Forum, IAF）認可的 AB[1]標誌，如要取得 TAF 標誌的證書，需重新進行初次驗證。 2. 機關現行證書上有 IAF 認可的 AB 標誌（但不是 TAF），有 2 種方式可取得具 TAF 標誌的證書。 (1) 原驗證機構進行驗證，併同年度稽核提出轉換認證單位或是增列認證單位的需求。 (2) 向具有 TAF 認證的 CB[2]申請轉證，取得 TAF 認證標誌證書。 註： [1]AB：認證機構（Accreditation Body）。如 TAF、UKAS 等。 [2]CB：驗證機構（Certification Body）。如 SGS、BSI、TUV、AFNOR、TCIC 等。
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。
4.19. 公務機關如果有維運特定類型資通系統（如工控系統等），可否改用其他資通系統防護基準來執行相關控制措施？	公務機關如維運特定類型之資通系統，執行分級辦法附表一至附表八所定事項或附表十之控制措施顯有困難者，得由其資通安全責任等級提報機關同意，並報請主管機關備查後，免執行該事項或控制措施。【資通安全責任等級分級辦法第 11 條第 3 項】。
4.20. 機關因組織調整、新成立致須變更或新增核定資安責任等級時，其應辦事項之法遵期限應如何認列？	一、未規定「初次受核定或等級變更後 O 年內」之應辦事項，辦理期限係採週年計算起訖期間。例如某 A 級機關於 112 年 9 月 30 日成立，則該機關應於 113 年 9 月 30 日前（即機關成立 1 年內）辦理 2 次內部資通安全稽核作業。 二、因等級變更新增之應辦事項，係自資安責任等級核定後起算辦理期限，其餘應辦事項仍依原等級之法遵期限完成。例如：某 C 級機

問題	回復
	關本應於 112 年 8 月 23 日完成 VANS 導入作業，嗣於 112 年 4 月 12 日經核定調升為 B 級，該項作業之辦理期限仍應於 112 年 8 月 23 日前完成。
4.21. 有關資通安全責任等級分級辦法附表一、附表三應辦事項規定，A、B 級公務機關於初次受核定或等級變更後之 1 年內，應完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料，其提交方式為何？	請各機關依國家資通安全研究院網站「國家資安聯防監控中心（N-SOC）」專區公告之「政府領域聯防監控作業規範」辦理提交。（網址：https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/）
4.22. 行政院國家資通安全會報年度資安稽核計畫是否公告周知？稽核頻率為何？	一、年度資通安全稽核計畫及相關表單公開刊載於資安署網站（https://moda.gov.tw/ACS/operations/drill-and-audit/652）。 二、目前針對行政院所屬二級機關稽核頻率以二年一次為原則；針對其他機關稽核頻率，由資安署評估資安責任等級、重大資安事件、稽核頻率及稽核量能遴選相關受稽機關。

5. 資通安全維護計畫撰寫及實施情形填報

問題	回復
5.1. 資通安全維護計畫之內容要求為何？	一、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。 二、數位發展部資通安全署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？	一、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。 二、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、中央目的事業主管機關是否需提供資通安全維護計畫範本？	一、有關公務機關資通安全維護計畫內容，已置於數位發展部資通安全署網站之資安法專區中。 二、上級或監督機關、中央目的事業主管機關亦得視需要提供維護計畫範本供所屬或所管機關參用。(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 CNS 27001（ISO 27001）驗證，所援引之文件係 CNS 27001（ISO 27001）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。

問題	回復
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。詳參國家資通安全研究院發布之「資通系統風險評鑑參考指引」（https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/）。
5.9. 目前沒有核心業務如何撰寫核心業務？	資安法施行細則第 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。
5.11. 有關資通安全維護計畫實施情形填報，是否可由上級機關統一提報？	資通安全維護計畫實施情形，各機關應依本身執行情形各自填報辦理情形，不可整併或彙整提報。惟考量部分機關人力問題，其上級、監督機關或上級政府可協助其至系統中填寫機關實施情形。

6. 辦理受託業務-受託者之選任及監督

問題	回復
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 CNS 27001 或 ISO 27001 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

問題	回復
在驗證範圍？	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。
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，或委託案件金額在一千萬元以上，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？	一、如受託者辦理受託業務之相關程序及環境都在機關內，廠商應無資通安全管理法施行細則第 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、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 4 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

問題	回復
7.1. 資安事件通報及應變辦法第 2 條第 2 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」(參行政院 109 年 4 月 16 日院臺護字第 1090170228 號函），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所在地直轄市政府執行演練作業，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。
7.5. 有關資安事件應於 1 個月內送交調查、處理及改善報告，請問 1 個月如何計算？	本法所稱「1 個月」之計算，皆依據行政程序法第 48 條規定辦理。 如機關於 3 月 31 日完成損害控制或復原作業，則從 4 月 1 日起算 1 個月，至 4 月 30 日屆滿，若機關於 5 月 1 日送交調查、處理及改善報告，即屬逾時；

問題	回復
	如機關於 3 月 30 日完成損害控制或復原作業，則從 3 月 31 日起算 1 個月，依行政程序法第 48 條第 3 項規定至 4 月 30 日屆滿，若機關於 5 月 1 日送交調查、處理及改善報告，即屬逾時。 如機關於 1 月 30 日完成損害控制或復原作業，則從 1 月 31 日起算 1 個月，依行政程序法第 48 條第 3 項至 2 月 28 日或 29 日屆滿，若機關於 3 月 1 日送交調查、處理及改善報告，即屬逾時。
7.6. 有關應於知悉資通安全事件後，1 小時內進行資安事件通報，請問應如何判斷「知悉」時間？	當機關發現有導致機關系統、服務或網路狀態之機密性（C）、完整性（I）或可用性（A）受影響，符合資通安全事件通報及應變辦法第 2 條各級資安事件之時間時，即為機關「知悉」資通安全事件之時間。
7.7. 何謂重大資安事件？	依資通安全管理法施行細則第 10 條規定，重大資通安全事件指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。

8. 其他

問題	回復
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為何？	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？	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「具備完善之資通安全管理措施」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九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。
8.5. 機關如欲與主管機關進行情資分享，其分享方式為何？	行政院已於 110 年第 2 季提供線上填報情資功能，供機關運用，機關如欲依資通安全情資分享辦法第 3 條第 3 項進行情資分享，可於國家資通安全通報應變網站（https://www.ncert.nat.gov.tw）以一般機關身分登入後，選擇上方「情資分享功能」填報分享。
8.6. 有關「限制使用危害國家資通安全產品」是否會提供相關清單？此外，在未公布清單前是否有相關參考作法？	一、考量危害國家資通安全產品由主管機關核定廠商清單效益有限，後續將由主管機關透過跨部會協調平臺與各機關溝通，推動危害國家資通安全產品之限制使用事宜。 二、現階段係請各公務機關依行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函，禁止使用及採購大陸廠牌資通訊產品（含軟體、硬體及服務），其相關注意事項如下：

問題	回復
	(一) 大陸廠牌：指行政院公共工程委員會 107 年 12 月 20 日工程企字第 1070050131 號函所稱「大陸地區廠商」，至於「第三地區含陸資成分廠商」及「在臺陸資廠商」原則非屬上述範圍，惟各機關於辦理採購案時，如屬經濟部投資審議委員會公告「具敏感性或國安含資安疑慮之業務範疇」，應確實於招標文件中載明不允許經濟部投資審議委員會公告之陸資資訊服務業者參與。 (二) 陸籍人士：指委外廠商執行標案之團隊成員不得為大陸地區人民，針對多重國籍部分，如其一屬大陸地區人民，亦為限制範圍；此外，針對香港居民及澳門居民非屬上述限制範圍。 (三) 考量實務執行問題，現行僅限制其最終資通訊產品不可為大陸廠牌，暫未限制大陸廠牌零組件。 (四) 各機關辦理資通訊相關採購，得依個案特性及實際需要於採購文件中評估限制委外廠商及其分包廠商不得提供大陸地區廠商所生產或製造零組件。
8.7. 有關雲端服務是否會提供相關參考指引？且是否有相關限制？	一、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」（https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/），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。 二、為使政府機關於建置或使用雲端服務時，降低可能之風險，相關資安要求事項如下： (一) 應禁止使用大陸地區（含香港及澳門地區）廠商之雲端服務運算提供者。 (二) 提供機關雲端服務所使用之資通訊產品（含軟硬體及服務）不得為大陸廠牌，執行委外案之境內團隊成員（含分包廠商）亦不得有陸籍人士參與，就境外雲端服務之執行團隊成員，至少應具備相關國際標準之人員安全管控機制，並通過驗證。另，雲端服務提供

問題	回復
	者自行設計之白牌設備暫不納入限制。 (三) 機關應評估機敏資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區（含香港及澳門地區），且不得跨該等境內傳輸相關資料。