資通安全管理法常見問題

版本：1151105

問題分類

1. 納管對象及範圍 1
2. 資通安全責任等級分級辦法-責任等級 3
3. 資通安全責任等級分級辦法應辦事項-資安專職人力及證照 5
4. 資通安全責任等級分級辦法應辦事項-其他 12
5. 資通安全維護計畫撰寫及實施情形填報 19
6. 辦理受託業務-受託者之選任及監督 21
7. 資通安全事件通報及應變 24
8. 資通安全事項作業-調度支援 26
9. 其他 27

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. 兼有公務機關與公營事業性質之機關，其納管方式為何？ 1
   1.4. 地方政府之公營事業，其納管方式為何？ 2
   1.5. 里辦公處是否適用資安法？如為適用對象，其辦理作業項目為何？ 2
   1.6. 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辦法-責任等級 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. 只有 1 個官網算不算 C 級機關？ 3
   2.7. 內部不對外的網站，是否屬於 C 級的資通系統？ 3
   2.8. 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？ 3
   2.9. 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
   2.10. 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辦法應辦事項-資安專職人力及證照 5
   3.1. 資通安全專職人員之職務內容為何？ 5
   3.2. 機關配置資通安全專職人員說明？ 6
   3.3. 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
   3.4. 有關資通安全專業證照，所指經主管機關公告之資通安全專業證照，其清單在哪可取得？ 6
   3.5. 資通安全職能訓練證書如何取得？ 7
   3.6. 資通安全專業證照及資通安全職能訓練證書應由誰取得？需不需要每人 1 張？ 7

3.7. 資通安全專職人員應取得之資通安全專業證照及職能訓練證書，如機關責任等級或人員有異動，是否有緩衝期？ 7
3.8. 機關與所屬機關之資通安全專職人員是否可以共用？證照或證書可否上級和所屬機關加起來一起算，還是分開算？ 7
3.9. 資通安全責任等級分級辦法應辦事項中，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？ 7
3.10. 資通安全專職人員，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
3.11. 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？資通安全專職人員是否應接受資通安全通識教育訓練？ 9
3.12. 資通安全專業證照清單中，管理類 Lead Auditor 相關證照，註明「除提出證照外，尚須提供當年度至少 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？ 9
3.13. 資通安全責任等級分級辦法應辦事項中，何謂「資通安全專職人員以外之資訊人員」？ 10
3.14. 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
3.15. 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？ 10
3.16. 資通安全職能訓練是否有修習順序限制？ 10
3.17. 有關資通安全專業證照 ISO/IEC 27001 有效性及認定方式為何？ 10
3.18. 資通安全專職人員為取得資通安全專業證照或資通安全職能訓練證書，機關是否補助參訓之相關費用？ 10
3.19. 資通安全專職人員之全職定義 11
4. 資通安全責任等級分級辦法應辦事項-其他 12
4.1. 資通安全責任等級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，資通安全責任等級分級辦法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. 資通安全責任等級分級辦法應辦事項列表的「資通安全健診」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. 資通安全責任等級分級辦法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果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. 如機關提報資通安全責任等級變更，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. 資通安全責任等級分級辦法附表十有關營運持續計畫高等級防護基準應建立資料「異地備份」機制，有沒有距離要求？ 14
4.12. 資通安全責任等級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. 資通安全責任等級分級辦法應辦事項列表中資通安全弱點管理，所稱「主管機關指定方式」為何？ 15
4.15. 資通安全弱點比對管理範疇為何？作業頻率是否訂有時限？比對方法有哪些？ 15
4.16. 資通安全責任等級分級辦法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？其提交方式為何？ 16
4.17. 資通安全責任等級分級辦法所規定 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？ 17
4.20. 機關因組織調整、新成立致須變更或新增核定資通安全責任等級時，其資通安全責任等級分級辦法應辦事項之法遵期限應如何認列？ 17
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，應完成監控機制建置，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
5. 資通安全維護計畫撰寫及實施情形填報 19
5.1. 資通安全維護計畫之內容要求為何？ 19
5.2. 資通安全維護計畫可否由上級或監督機關代為辦理？ 19
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？ 19
5.4. 資通安全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？ 19
5.5. 資通安全維護計畫是否需按範本的章節填寫？ 19
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？ 19
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？ 20
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？ 20
5.9. 目前機關沒有核心業務，該如何撰寫核心業務？ 20
5.10. 資通安全維護計畫中是否針對個人資料之保護論述不足？ 20
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？ 20
6. 辦理受託業務-受託者之選任及監督 21
6.1. 委外注意事項何時要納入？受託者是否必須通過第三方驗證？第三方驗證之範圍為何？ 21
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？ 21
6.3. 何謂完善的資通安全管理措施？應如何判斷廠商之資通安全管理措施是否「完善」、或由誰來判斷（是採購單位、業務單位、資訊單位還是稽核單位）？ 21
6.4. 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？ 22

6.5. 委外客製化開發資通系統應如何執行安全性檢測？ 22
6.6. 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？ 22
6.7. 請問資安法施行細則第 7 條第 1 項第 4 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，抑或涵蓋軟、硬體及人力？ 22
7. 資通安全事件通報及應變 24
7.1. 資通安全事件通報應變及演練辦法第 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）？此外，1 台 PC 故障，或是 1 個感探器故障，是否要進行通報？ 24
7.2. 公務機關應如何進行資通安全事件之通報？ 24
7.3. 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？ 24
7.4. 有關資通安全事件應於 1 個月內送交調查、處理及改善報告，請問 1 個月如何計算？ 24
7.5. 有關應於知悉資通安全事件後，1 小時內進行資通安全事件之通報，請問應如何判斷「知悉」時間？ 25
7.6. 何謂重大資通安全事件？ 25
8. 資通安全事項作業-調度支援 26
8.1. 調度支援之啟動時機為何？ 26
8.2. 調度支援之內容？ 26
8.3. 主管機關辦理調度支援時，是否須經事發機關或支援機關同意？ 26
8.4. 調度支援之時限？ 26
8.5. 調度支援紀錄由何單位製作？ 26
9. 其他 27
9.1. 資安法施行細則第 7 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？ 27
9.2. 機關如欲與主管機關進行情資分享，其分享方式為何？ 27
9.3. 「危害國家資通安全產品」是否提供清單？ 27
9.4. 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？ 28

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、特定財團法人或受政府控制之事業、團體或機構。 (一)關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關指定，並報行政院核定者。 (二)公營事業：依公營事業移轉民營條例第 3 條各款規定，包含各級政府投資或轉投資經營之事業。 (三)特定財團法人：指符合財團法人法第二條第二項、第三項或第六十三條第一項、第四項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者。 (四)受政府控制之事業、團體或機構：指銓敘部依公務人員退休資遣撫卹法第七十七條第一項第二款第三目及第四目公告之事業、團體或機構，具資通安全重要性，經中央目的事業主管機關指定，並經主管機關核定者；其受地方政府控制者，應經地方主管機關同意後，主管機關始得核定。
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. 兼有公務機關與公營事業性質之機關，其納管方式為何？	資安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>公營事業或特定財團法人），如單一機關兼具二種身分時，依規範強度較高者納管之。 例如：以臺北自來水事業處為例，其兼具公務機

問題	回復
	關與公營事業性質，則以公務機關之身分納管之。
1.4. 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 21 及 24 條及相關子法之規定，該公營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。
1.5. 里辦公處是否適用資安法？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）。
1.6.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辦法-責任等級

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。 個人資料檔案依據個人資料保護法第 2 條第 2 款，指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
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？	機關之官網非屬資通安全責任等級分級辦法第 4 條第 3 款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. 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，機關之資通安全責任等級即為 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。
2.7. 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，機關之資通安全責任等級即為 C 級。
2.8. 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分，故依資通安全責任等級分級辦法第 7 條規定列為 D 級。

問題	回復
2.9. 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 2 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。
2.10. 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 4 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辦法應辦事項-資安專職人力及證照

問題	回復
3.1. 資通安全專職人員之職務內容為何？	一、資通安全專職人員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（或所監督）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、營運持續計畫演練、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（或所監督）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、資通安全監控管理機制、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、機關資通安全專職人員之職務分工建議如下： (一)A 級機關置 4 名專職人員：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 名專職人員：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 名專職人員：統籌機關資安業務。

問題	回復
	三、機關如兼屬資安法之中央目的事業主管機關，應對所管之特定非公務機關辦理下列事項，如資通安全專職人員無法容納，建議由機關權責單位另派人力辦理，資通安全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。
3.2. 機關配置資通安全專職人員說明？	一、依 115 年 1 月 7 日修正公布之《資通安全責任等級分級辦法》附表一至附表六規定，所稱資通安全專職人員，指應全職執行資通安全業務者，亦即資通安全為其主要核心業務，且應優先辦理，各機關得依前述說明進行實務認定。 二、各機關應優先於機關總員額內配置資通安全專職人員，惟為解決機關人力短缺問題，得以約聘僱或委外人員擔任。另鼓勵可優先任用轉職系人員，以提升資安防護能力及留任相關人才。 三、此外，建議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。
3.3. 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。
3.4. 有關資通安全專業證照，所指經主管機關公告之資通安全專業證照，其清單在哪可取得？	一、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」（https://moda.gov.tw/ACS/laws/certificates/676）。 二、本證照清單定期更新，各機關如有新增資通安全專業證照建議，請依數位發展部資通安

問題	回復
	全署網站公告之「資通安全專業證照認可審查作業流程」辦理。
3.5. 資通安全職能訓練證書如何取得？	一、各機關人員參加主管機關辦理之資通安全職能訓練，於完成指定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、自 115 年 4 月起，各機關人員可選擇不參加「資通安全概論」職能訓練課程，逕行報名該科目之免訓評量，通過測驗者即可取得證書。詳細規定請參閱「資安人才培訓服務網」公告。 三、各機關亦得逕洽經主管機關認證之資通安全職能訓練機構申請開設專班，相關資訊請洽主管機關（電話：02-2380-8500）。
3.6. 資通安全專業證照及資通安全職能訓練證書應由誰取得？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職人員至少持有資通安全專業證照或資通安全職能訓練證書 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。
3.7. 資通安全專職人員應取得之資通安全專業證照及職能訓練證書，如機關責任等級或人員有異動，是否有緩衝期？	資通安全責任等級分級辦法規定資通安全專職人員取得資通安全專業證照或職能訓練證書應於機關初次受核定或等級變更後 1 年內完成；人員異動時，亦同。
3.8. 機關與所屬機關之資通安全專職人員是否可以共用？證照或證書可否上級和所屬機關加起來一起算，還是分開算？	資通安全專職人員配置的要求是以機關為單位，人力不能共用計算，證照或證書部分亦須以機關為單位分開計算。
3.9. 資通安全責任等級分級辦法應辦事項中，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	一、「資通安全專業課程訓練」係泛指有助提升資通安全專職人員之資安策略、管理或技術專業知能之課程，以使資通安全專職人員勝任其職務內容。 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。

問題	回復
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？	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，行政院人事行政總處自 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。
3.10. 資通安全專職人員，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，且不得涉及特定資通訊產品宣傳，其相關時數，可透過以下方式取得： (一) 參加主管機關及其所屬機關（含資安院）舉辦或所開設之資通安全策略、管理、技術相關課程、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) 參加機關本身、上級機關或中央目的事業主管機關所開設之資通安全策略、管理或技術訓練課程，且該課程經報請課程開設機關之資安長同意。 (四) 參加公私營訓練機構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。訓練機構以下列型態為限： 1. 公私立大專校院。 2. 經勞動部登記核准在案 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或財團法人，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。 三、資通安全專業課程訓練原則應優先以實體或遠距即時互動課程方式進行，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

問題	回復
	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。
3.11. 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？資通安全專職人員是否應接受資通安全通識教育訓練？	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、有關資通安全教育訓練時數法遵要求，已依人員類型區分為資通安全專職人員、資通安全專職人員以外之資訊人員、一般使用者及主管等 3 類，其中一般使用者及主管指機關組織編制表內人員，或得接觸、使用機關資通系統或服務之各類人員。是以，除資通安全專職人員外，其餘各類人員每人每年應接受 3 小時以上資通安全通識教育訓練。 四、針對資通安全專職人員，由機關視需要適時派訓，如該員為機關新進人員時，仍建議接受機關內部資通安全管理規定之宣導課程。
3.12. 資通安全專業證照清單中，管理類 Lead Auditor 相關證照，註明「除提出證照外，尚須提供當年度至少 2 次實際參與該證照內容有關之稽核經驗證明」，哪些	一、為使資通安全專職人員於取得 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。 二、稽核經驗可以稽核員或觀察員身分，參與內部稽核、外部稽核或針對資通系統委外廠商之稽核，均可納入稽核經驗次數計算。

問題	回復
類稽核可納入 2 次實際參與稽核之計算？	
3.13. 資通安全責任等級分級辦法應辦事項中，何謂「資通安全專職人員以外之資訊人員」？	「資通安全專職人員以外之資訊人員」，指其他實際從事資通安全業務或資訊業務之人員。（詳參資通安全責任等級分級辦法附表一到附表七之備註）。
3.14. 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？	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；而資安通識訓練部分，仍應於當年度年底前完成。
3.15. 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 證照自 114 年 10 月 31 日起已停止認列（機關第三方驗證亦同），最新資通安全專業證照清單詳參本署「資通安全專業證照清單」專區。
3.16. 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。
3.17. 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。
3.18. 資通安全專職人員為取得資通安全專業證照或資通安全職能訓練證書，機關是否補助參訓之相關費用？	依《資通安全責任等級分級辦法》規定，機關指派資通安全專職人員參加培訓課程，以取得資通安全專業證照或資通安全職能訓練證書，屬於執行資安業務的必備要件。故渠等人員參訓之相關費用係屬推動公務所需支出，各機關可本於權責予以補助。

問題	回復
3.19. 資通安全專職人員之全職定義	一、依據《資通安全責任等級分級辦法》，資通安全專職人員，指應全職執行資通安全業務者，亦即資通安全為其主要核心業務，且應優先辦理。 二、上開規定所稱全職，其要件有二，即「資通安全為主要核心業務」與「優先辦理」，非謂資安專職人員僅得辦理資安業務，而不得辦理資安業務以外之其他業務，惟必須符合以下條件： (一)資安業務核心性：資安業務係資安專職人員最重要工作，機關不得使資安專職人員因安排其他業務致排擠資安業務，而使機關資安相關應辦事項與防護措施受影響，藉以落實資安業務作為核心業務之概念。 (二)資安業務優先性：資安專職人員依上開核心性原則，辦完核心業務之餘，可承長官之命辦理其他業務。惟倘發生亟待處理資安事項，資安專職人員應優先處理資安業務，以維機關整體防護。

4. 資通安全責任等級分級辦法應辦事項-其他

問題	回復
4.1. 資通安全責任等級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，資通安全責任等級分級辦法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，資通安全責任等級分級辦法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（詳參資通安全責任等級分級辦法第 11 條第 2 項後段）。
4.6. 資通安全責任等級分級辦法應辦事項列表的「資通	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

問題	回復
安全健診」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？	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。
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？	依資安法施行細則第10條規定之核心資通系統，係指滿足任一條件者（支持核心業務持續運作必要之系統、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），本原則並已列示於資通安全責任等級分級辦法附表一至六之備註一。
4.8. 資通安全責任等級分級辦法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果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，惟是否符合上開「同等或以上效果」，仍需依個案情形審認。 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？	一、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

問題	回復
	核發現之後續追蹤管考機制等，全機關完成稽核之週期不宜過長。 二、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。
4.10. 如機關提報資通安全責任等級變更，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，機關仍應依現行資通安全責任等級辦理附表一至附表八之應辦事項，主管機關原則於收文兩週內完成核定，請機關依函復結果辦理相關事宜。
4.11. 資通安全責任等級分級辦法附表十有關營運持續計畫高等級防護基準應建立資料「異地備份」機制，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；對於異地選址評估，機關可參考「我國電腦機房異地備援機制參考指引」之「電腦機房異地備援選址評分表」(網址：https://gov.tw/8D3)，例如：應避開活動斷層帶及避免位於洪氾高風險區域等，並依據業務關鍵性與成本效益進行評估，作為設置參考依據。
4.12. 資通安全責任等級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、A、B 級公務機關應於初次受核定或等級變更後 1 年內，依公告項目完成 GCB 導入並持續維運；主管機關公告新增項目後，亦應於公告後 1 年內完成導入。 二、GCB 公告項目含括作業系統、瀏覽器、網通設備、應用程式等 4 類，原則均應導入且採

問題	回復
	「專版專用」原則。導入前應先行充分測試，且可依實務進行例外管理，惟須落實例外審核與定期檢討。 三、有關 GCB 相關說明文件、數位教材及部署資源，可參考國家資通安全研究院網站「政府組態基準(GCB)」專區（https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/）。
4.14. 資通安全責任等級分級辦法應辦事項列表中資通安全弱點管理，所稱「主管機關指定方式」為何？	有關資通安全責任等級分級辦法應辦事項列表中資通安全弱點管理，所稱「主管機關指定方式」係指針對安全性檢測、資通安全弱點比對作業及資安警訊等所發現之弱點，應依《各機關基於風險導向之弱點處置期限評估指引》評估風險情境類型，並依該指引及機關內部規範之處理時限，適時修補或採行風險緩解措施，落實弱點管理作為，並得納入機關內部稽核與管理審查等機制，進行檢討與改善。
4.15. 資通安全弱點比對管理範疇為何？作業頻率是否訂有時限？比對方法有哪些？	一、資通安全弱點比對之管理範疇： (一) 公務機關以全機關之資訊資產為原則；其中有關核心資通系統及其他支持核心業務持續運作相關之伺服器主機與使用者電腦，應依應辦事項辦理期限完成。 (二) 關鍵基礎設施提供者至少涵蓋核心資通系統、關鍵資訊基礎設施及其他支持核心業務持續運作相關之伺服器主機與使用者電腦，且應依應辦事項辦理期限完成。 二、資通安全弱點比對之作業頻率：原則依機關內部資通安全管理規範辦理，建議每季至少辦理 1 次，且相關弱點處置方式或改善措施，建議每季完成比對弱點後 1 個月內留存處理紀錄，以強化機關弱點管控作為。 三、資通安全弱點比對之作法：得透過數位發展部資通安全署「資通安全弱點通報系統」（https://vans.nat.gov.tw/）依指定格式提交資訊資產盤點資料，以取得已公開揭露之安全漏洞資訊；或採取其他具有同等或以上效用之作法，至少含括資訊資產盤點管理、與國際權威弱點資料庫查詢或比對是否存在已公開揭露之安全漏洞資訊等內容，並進行後續

問題	回復
	弱點追蹤管理。
4.16. 資通安全責任等級分級辦法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？其提交方式為何？	一、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。 二、請各機關依國家資通安全研究院網站「端點偵測及應變機制(EDR)」專區公告之「資料回傳格式說明」，偵測到異常行為或惡意程式活動，並確認成為資安事件時，透過現有聯防監控資料回傳管道提交至主管機關。（網址：https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/EDR/）
4.17. 資通安全責任等級分級辦法所規定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）。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）。
4.18. 如套裝軟體僅有低度客	資通系統如包含客製化的部分，即屬自行或委外

問題	回復
製化，是否仍屬於自行或委外開發之資通系統？	開發之資通系統，須依資通安全責任等級分級辦法第 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，執行資通安全責任等級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，得由該辦法第 3 條第 1 項後段及第 2 項所定等級提交機關或同條第 1 項前段及第 3 項所定等級核定機關同意，並報請主管機關備查後，免執行該應辦事項或改執行中央目的事業主管機關所定之防護基準。等級提交機關有前段情形者，經主管機關同意後，免予執行；其為等級核定機關者，經報請主管機關備查後，免予執行。（詳參資通安全責任等級分級辦法第 11 條第 4 項）
4.20. 機關因組織調整、新成立致須變更或新增核定資通安全責任等級時，其資通安全責任等級分級辦法應辦事項之法遵期限應如何認列？	一、各機關於初次受核定或等級變更時，依資通安全責任等級分級辦法附表一至附表七各備註內應辦事項辦理期限完成機關責任等級之應辦事項。 二、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。 三、因等級變更新增之應辦事項，係自資通安全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，應完成監控機制建置，並持續維運及依主管機關	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，並即時回傳「資安監控單」及「情資分析單」，另於每個月 5 號前回傳上個月的「監控設備狀況單」。（網址：https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/）

問題	回復
指定之方式提交監控管理資料，其提交方式為何？	

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 9 條第 1 項定有 13 款事項，詳參該法條文。 二、數位發展部資通安全署網站之資安法規專區（網址：https://moda.gov.tw/ACS/laws/documents/680）亦已提供資通安全維護計畫範本。
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 9 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規專區（網址：https://moda.gov.tw/ACS/laws/documents/680）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。(詳參資安法第 20、21 條說明)。
5.4. 資通安全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）。

問題	回復
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？	資通安全維護計畫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。
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. 目前機關沒有核心業務，該如何撰寫核心業務？	資安法施行細則第 10 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. 資通安全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 9 條訂有資通安全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？	各機關應依本身執行情形各自於系統中填報辦理情形，惟考量部分機關人力問題，其上級機關、監督機關或上級政府得協助辦理資料填報作業；前揭填報內容仍應以各該機關之實際執行情形為準，並應分別填報，不可整併或彙整提報。

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？受託者是否必須通過第三方驗證？第三方驗證之範圍為何？	一、依據資安法施行細則第 7 條規定，各機關依資安法第 10 條委外辦理資通系統之建置、維運或資通服務之提供時，即應注意該條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。 二、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。(詳參資安法第 10 條第 2 項)。 三、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。
6.2. 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，機關應依資安法施行細則第 7 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. 何謂完善的資通安全管理措施？應如何判斷廠商之資通安全管理措施是否「完善」、或由誰來判斷（是採購單位、業務單位、資訊單位還是稽核單位）？	一、完善的資通安全管理措施，係指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： (一)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。 (二)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。 二、有關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

問題	回復
	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。
6.4. 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。
6.5. 委外客製化開發資通系統應如何執行安全性檢測？	一、依資安法施行細則第 7 條規定，委外業務涉及客製化資通系統開發者，廠商應提供該資通系統之安全性檢測證明，包含源碼掃描、弱點掃描、滲透測試等安全檢測。(詳參資通安全責任等級分級辦法附表十資通系統防護基準－系統與服務獲得構面，如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)。 二、前述委外業務涉及客製化核心資通系統之開發，或委託金額達新臺幣一千萬元以上者，應由委託機關自行辦理或由委託機關另行委託第三方辦理安全性檢測，以確保該資通系統之安全性。
6.6. 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，廠商應無資安法第 10 條第 2 項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。
6.7. 請問資安法施行細則第 7 條第 1 項第 4 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，抑或涵蓋軟、硬體	有關該款委託金額達新臺幣一千萬元以上者，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。

問題	回復
及人力？	

7. 資通安全事件通報及應變

問題	回復
7.1. 資通安全事件通報應變及演練辦法第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)？此外，1台PC故障，或是1個感探器故障，是否要進行通報？	各機關發生資通安全事件，必須依照資通安全事件通報應變及演練辦法第2條規定進行通報，不論是否屬機關內外因素導致，均須通報。前述通報門檻為第一級以上之資通安全事件，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。
7.2. 公務機關應如何進行資通安全事件之通報？	資通安全事件通報應變及演練辦法第6條第1項規定:「公務機關知悉資通安全事件後，應於一小時內至主管機關指定之系統平臺通報。」 上述規定提及之「主管機關指定之系統平臺」(詳參行政院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。
7.3. 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？	依資通安全事件通報應變及演練辦法第 10 條第1項之規定:「總統府、國家安全會議與五院之直屬機關對其自身、所屬或所監督之公務機關，應規劃及辦理資通安全演練作業，….」及第3項之規定:「直轄市、縣（市）政府應依第一項規定對其自身、所屬、所監督之公務機關及下列機關規劃及辦理資通安全演練作業：一、所轄鄉（鎮、市）公所、直轄市山地原住民區公所與其所屬或所監督之公務機關。二、前款鄉（鎮、市）民代表會、直轄市山地原住民區民代表會。」 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。
7.4. 有關資通安全事件應於1個月內送交調查、處理及改善報告，請問1個月如何計算？	資通安全事件通報應變及演練辦法所稱「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，

問題	回復
	即屬逾時。 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。
7.5. 有關應於知悉資通安全事件後，1 小時內進行資通安全事件之通報，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應變及演練辦法第 2 條各級資通安全事件之時間時，即為機關「知悉」資通安全事件之時間。
7.6. 何謂重大資通安全事件？	依資安法施行細則第 13 條規定，重大資通安全事件指資通安全事件通報應變及演練辦法第 2 條第 4 項及第 5 項規定之第三級、第四級資通安全事件。

8. 資通安全事項作業-調度支援

問題	回復
8.1. 調度支援之啟動時機為何？	依據公務機關所屬人員辦理資通安全事項作業辦法第 11 條規定，調度支援之啟動時機如下： 一、發生重大資通安全事件之機關基於緊急應處所需，向主管機關提出支援請求。 二、主管機關就重大資通安全事件認有必要調度支援時。
8.2. 調度支援之內容？	依據公務機關所屬人員辦理資通安全事項作業辦法第 12 條規定，調度支援之內容包括事件發生時之損害控制及其他資通安全事件應變相關事項。
8.3. 主管機關辦理調度支援時，是否須經事發機關或支援機關同意？	依據公務機關所屬人員辦理資通安全事項作業辦法第 14 條第 1 項規定，主管機關辦理支援調度不須事發或支援機關同意，惟應事先徵詢事件發生機關及支援機關之意見。
8.4. 調度支援之時限？	為避免嚴重影響支援機關及人員業務運行，依據公務機關所屬人員辦理資通安全事項作業辦法第 14 條第 4 項規定，調度期間每次不得逾 7 日，主管機關認有必要時得延長，延長期間不得逾 7 日，並以延長一次為限。
8.5. 調度支援紀錄由何單位製作？	依據公務機關所屬人員辦理資通安全事項作業辦法第 15 條規定，由支援機關參與調度支援人員製作紀錄，內容包含緊急應處執行情形、改善建議及其他相關事項。

9. 其他

問題	回復
9.1. 資安法施行細則第 7 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、資通服務之定義依資安法第 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、資安法第 10 條第 2 項要求應注意受託者「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。
9.2. 機關如欲與主管機關進行情資分享，其分享方式為何？	機關如欲依資通安全情資分享辦法第 3 條第 2 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「情資分享作業」填報分享。
9.3. 「危害國家資通安全產品」是否提供清單？	一、依據「危害國家資通安全產品審查辦法」(下稱審查辦法）第 5 條規定，危害國家資通安全產品認定結果將以情資分享方式讓公務機關知悉。 二、依資安法、審查辦法及行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函，公務機關禁止下載、安裝或使用危害國家資通安全產品（含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： (一)大陸廠牌：指來源為「大陸（含港澳）地區廠商」之產品，而大陸(含港澳)地區廠商，參酌行政院公共工程委員會 107 年 12 月 20 日工程企字第 1070050131 號函示，指依大陸（含港澳）地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體。前述大陸（含港澳）地區廠商倘屬跨國企業於大陸（含港澳）地區依法須設子公司之情形，得視個案予以適當排除，例如由美國輝達母公司 100%持股之香港輝達子公司（實質控制者顯非屬陸港澳)；惟如有其他情形致使用機關認有危害國家資通安全疑慮時，仍得依審查辦法向主管機關提報。 (二)考量實務執行問題，原則係以最終資通訊產品判斷是否屬大陸廠牌。

問題	回復
9.4. 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，雲端服務提供者自行設計之白牌設備暫不納入限制。 (三)機關雲端資料之存取、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。