114年資通安全實地稽核_稽核提要（適用公務機關）

項次	資通安全稽核檢核項目	稽核重點	稽核依據	稽核參考基準	稽核 佐證資料	稽核代碼
1.1	是否盤點全機關業務，並進行營運衝擊分析，以識別核心及非核心業務，且盤點對應之資通系統，亦依資通系統防護需求分級原則完成資通系統分級，以及依資通安全管理法施行細則識別核心資通系統？每年是否至少檢視1次分級之妥適性？	機關應於資通安全維護計畫中界定其核心業務	資通安全管理法施行細則第6條：核心業務及其重要性、資訊及資通系統之盤點	1.機關於界定核心業務及非核心業務時，宜辦理營運衝擊分析，並確認所對應之資通系統。 2.核心業務，其範圍如下： （1）公務機關依其組織法規，足認該業務為機關核心權責所在。 （2）各機關維運、提供關鍵基礎設施所必要之業務。 （3）各機關依資通安全責任等級分級辦法第4條第1款至第5款或第5條第1款至第5款涉及之業務。 3.機關應於資通安全維護計畫中界定其核心業務，C級以上機關應每年檢視一次資通系統盤點及分級妥適性 4.定期檢視的方式及相關紀錄。 5.BIA分析結果應能呼應資安風險評鑑之結果與核心資通系統之關鍵性。 6.核心資通系統：支持核心業務持續運作必要之系統、或防護需求等級為高者之資通系統；機關涉及核心業務之資訊系統皆須納入核心系統，再依資通安全責任等級分級辦法附表9進行分級（核心系統資通安全防護等級不一定為高）。 7.依資通安全責任等級分級辦法應辦事項，A、B、C級機關，針對自行或委外開發之資通系統，依附表九完成資通系統分級（CIAL），並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。 8.是否定期檢視範圍的適切性。（ISMS導入範圍係機關維運之全部核心資通系統，依「資通安全責任等級分級辦法應辦事項：管理面之資通系統分級及防護基準」規定，每年至少檢視一次資通系統分級妥適性，爰建議機關於每年盤點核心資通系統時同時檢視ISMS範圍之妥適性。） 9.[資安法FAQ8.4] 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。	核心及非核心業務檢視紀錄、對應之資通系統清冊、資通系統(含核心及非核心資通系統)之盤點及分級清單、分級結果核可紀錄	P1、P6
			資通安全管理法施行細則第7條：核心業務定義 1.公務機關依其組織法規潤該業務微機關核心權責所在。 2.各機關微運、提供關鍵基礎設施所必要之業務。 3.各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第五款涉及之業務。			L1110082307
			資通安全責任等級分級辦法應辦事項：初次核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。			N10100

1.2	是否至少針對核心業務訂定最大可容忍中斷時間(MTPD)，並至少針對防護需求為中等級以上之資通系統，訂定從中斷後至重新恢復服務之可容忍時間要求(RTO)，及可容忍資料損失之時間要求(RPO)？ 是否依RPO訂定資料及系統之備份頻率？	檢視機關所訂定的MTPD、RTO、RPO之適切性 檢視核心資通系統資料備份復原程序、有效性及其落實情形	資通安全責任等級分級辦法附表十資通系統防護基準：營運持續計畫之系統備份 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。（防護需求為中等級以上者） 資通安全責任等級分級辦法附表十資通系統防護基準營運持續計畫： （1）系統備份：訂定系統可容忍資料損失之時間要求。（RPO） （2）系統備援：訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。（RTO）	1.資通系統RTO及RPO之適切性（建議與契約規定相符），宜以業務流程角度評估，評估人員宜包含業務單位、資訊單位，且評估結果應經權責人員核定，核心資通系統之RTO亦不宜大於非核心資通系統之RTO。 2.MTPD(最大可容忍中斷時間)=RTO+WRT(了解機關RTO定義是否包含WRT;工作恢復時間)，需確認設定之合理性，RTO不可大於MTPD。 3.RTO與RPO無直接關係。 4.確認備份週期不可大於RPO設定。	備份機制相關程序或文件、備份復原測試及程序調修改善紀錄、營運衝擊分析結果、營運持續演練成果及滾動調整記錄	C0301 C0301、C0302
1.3	所有資通系統是否定期執行系統源碼與資料備份？ 防護需求為高等級之資通系統，其軟體與其他安全相關資訊是否儲存於與運作系統不同地點之獨立設施或防火櫃中？ 防護需求為中等級以上資通系統之備份資訊，是否定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性？	檢視機關備份措施及應符合其訂定之資安政策、規範	資通安全責任等級分級辦法附表十資通系統防護基準：營運持續計畫之系統備份 （1）應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份（防護需求為高等級者） （2）執行系統源碼與資料備份（全部資通系統）	1.是否依機關資安政策及規範，就資料等級、重要性，規劃不同備份方式、備份媒介與頻率。 2.防護需求等級為高等級之資通系統，軟體及其他安全相關資訊應儲存於與運作系統不同地點之獨立設施或防火櫃，並建議宜有安全距離之異地備份 [FAQ4.11]異地備份建議30公里以上。或防火櫃儲存重要資通系統軟體。 4.針對具機敏性的資料進行加密保護。例如：資料庫機敏資訊欄位進行加密、或採行轉碼、代碼化或機敏資料正規化（資料分割）。 5.防護需求等級中等級以上之資通系統，應依系統分級定期執行各類的備份媒體之可靠性、完整性及可還原性測試，確認是否符合RTO及RPO，並留存相關測試紀錄。 6.檢視回復測試相關紀錄。	備份機制相關程序或文件、備份資料存放紀錄	C0301

1.4	防護需求為中等級以上之資通系統是否設置系統備援，原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務？	檢視機關備援設備之備援能力是否足以支援系統中斷問題	資通安全責任等級分級辦法附表十資通系統防護基準：營運持續計畫之系統備援 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務（防護需求為中等級以上之資通系統）	1.了解防護需求為中等級以上之資通系統架構及其備援機制。 2.備援機制取代時機及作業流程，是否經業務單位確認。 3.備援機制之資源現況及準備度。 4.備援機制在可容忍時間取代之可行性及相關演練紀錄，是否經業務單位確認。	備援機制相關程序或文件，防護需求為中等級以上之資通系統架構圖、營運持續計畫、執行及調修改善紀錄、契約書系統回復、中斷時間（SLA）要求。	C0302
1.5	是否至少對全部核心資通系統訂定營運持續計畫，營運持續計畫內容至少包含人員職責應變、作業程序、資源調度機制及檢討改善措施等，並定期辦理業務持續運作演練？(A級機關：每年1次；B、C級機關：每2年1次)	C級以上之機關應針對其核心資通系統定期辦理業務持續運作演練，並依演練結果滾動調整營運持續計畫。	資通安全責任等級分級辦法應辦事項：全部核心資通系統每年辦理一次業務持續運作演練	1.全部核心資通系統皆應被演練，且留存相關紀錄： （1）A級機關每年至少演練過1次。 （2）B、C級機關每2年至少演練過1次。 2.演練情境是否納入業務單位角色，演練結果與持續營運目標之符合性，亦應經業務單位確認，以確保業務持續運作演練之有效性，並應提報資安長。 3.是否依演練結果滾動調整相關程序及業務持續運作計畫、並提報資安長。 4.建議評估是否需納入複合式演練情境。	營運持續計畫、演練記錄及相關程序調整紀錄及提報資安長紀錄、契約書_系統復原演練要求	N10500

1.6	資安治理成熟度評估等級為何？並依評估結果檢討相關策進作為?評估等級是否經內部簽核程序、召開會議或其他適當方式確認? （A、B級機關適用，以達到3級為目標）	A、B級機關應每年辦理1次資安治理成熟度評估作業	資通安全責任等級分級辦法應辦事項：A、B級公務機關每年辦理一次資安治理成熟度評估	1.依國家資通安全發展方案（110年至113年）所訂分年重要進程（量化目標），113年所有A級政府機關應達第3級以上，80%之B級政府機關應達第3級以上。A級、B級政府機關均應推動資安治理成熟度達第3級，並依評估結果規劃相關策進作為。 2.資安治理成熟度評估結果，宜經內部簽核程序、召開會議或其他適當方式確認。 3.113年度資安治理成熟度評估表，共計有46題評核項目，其中：客觀指標項目（系統依機關回傳結果自動評定）共2題，包含第40題「政府領域資安聯防情資」及第41題「資安事件通報逾時」；其餘各題為機關自評項目。 4.資安治理成熟度達第3級，係指流程構面除「S2資安治理架構」（第4題至第6題）及「S4資安管理監督」（第9題至第11題），其餘各流程構面所有評核項目評分均達3分以上。 5.各評核項目評分等級意義如下： （1）自評0分：指完全未執行或未執行完成檢核項目。 （2）自評1分：指有執行檢核項目。 （3）自評2分：指檢核項目若為資安法應辦事項之要求，完成應辦事項則可評為2分；若非應辦事項之要求，已對檢核項目進行管理或定期檢視。 （4）自評3分：指對檢核項目需具備標準作業程序或相關文件化要求，該文件之內容需清楚說明如何完成執行該檢核項目之步驟或流程，並落實執行。 （5）自評4分：指對檢核項目已訂定質化或量化衡量指標於標準作業	資安治理成熟度評估文件及紀錄	N10600

1.7	是否將全部核心資通系統納入資訊安全管理系統（ISMS）適用範圍？	全部核心資通系統都應納入ISMS適用範圍，A、B級機關並應通過公正第三方驗證（通過我國標準法主管機關委託機構認證之機構：TAF）。	資通安全責任等級分級辦法應辦事項：初次受核定或等級變更後之2年內，全部核心資通系統導入CNS27001或ISO27001，並於3年內完成公正第三方驗證，並持續維持其驗證有效性。	1.A、B級機關：全部核心資通系統2年內完成ISMS導入，3年內通過公正第三方驗證，第三方驗證機構核發之驗證證書應有TAF認證標誌，證書驗證範圍應包括全部核心資通系統，且應為有效之證書。 （1）核心資通系統發生異動後，建議規劃相關ISMS導入（驗證）計畫，ISMS導入範圍應於2年內完成更新；ISMS驗證範圍應於3年內完成更新。 （2）證書有效性的判定原則： A.證明文件於機關維運核心資通系統時應在有效期內。 B.證明文件須顯示出全部核心資通系統在驗證範圍內。 C.ISO 27001：2013證書認列至114年10月31日為止，各機關應於該期限內完成轉版。 2.C級機關：全部核心資通系統2年內完成ISMS導入。 3.[FAQ4.3] 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。	ISMS驗證證書、資安政策、核心資通系統清單、相關執行（會議）紀錄	N10200
2.1	是否訂定資通安全政策及目標，由管理階層核定，並定期檢視且有效傳達其重要性？如何確認人員瞭解機關之資通安全政策，以及應負之資安責任？	檢視機關資安政策之適切性、核定程序及人員對其之瞭解程度	資通安全管理法施行細則第6條：資通安全維護計畫應包含資安政策及目標	1.資安政策與目標適切性、核定、宣導、定期檢討等。 2.人員至少包含機關正式人員（含約聘僱人員）、臨時人員及機關委外人員。 3.包含傳達至機關人員之方式及有效性。 4.了解人員對於資通安全認知程度、資安政策宣導成效、人員落實資安規定等。 5.了解各類人員對於資安應負資安之責任及落實情形。 6.新進人員資安宣導單（如：不使用公務信箱註冊非公務網站帳號、僅使用公務信箱傳遞公務資料、上班時間不連結非公務需要之網站、密碼妥善保存等）。	資安政策核定紀錄、資安宣導紀錄、已簽署之宣導單	P2

2.2	是否指派副首長或適當人員兼任資通安全長，負責推動及督導機關內資通安全相關事務？是否成立資通安全推動組織，負責推動、協調監督及審查資通安全維護計畫及其他資安管理事項？推動組織層級之適切性，且業務單位是否積極參與？	機關資安推動組織架構及資安長對機關資通安全推動事項之參與程度	資通安全管理法施行細則第6條：資通安全維護計畫應包含資通安全推動組織	1.公務機關應設置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。 2.機關資安長之權責說明，是否足以負責推動及督導資安相關業務。資安長係為能分配（提供）資源並做出決策之個體，並有權指派、調度全機關之工作任務及權限。 3.資通安全推動組織、組成架構、參與成員及層級、權責分工情形等 4.組織運作情形，如何運作、人員參與及追蹤列管執行情形，建議跨部門（含業務單位），且參與層級為主管或副主管級以上 5.資通安全推動組織應定期開會，並由資安長或權責人員親自主持情形，並確認是否包含前次會議決議或列管事項辦理情形等。 6.建議於管理審查會議考量下列事項： （1）過往管審會議之決議的處理狀態 （2）內外部議題變更 （3）資通安全績效之回饋，包括其趨勢： A.不符合事項及矯正措施 B.監督及量測結果 C.稽核結果（內外部稽核結果） D.資通安全目標之達成 （4）資通安全維護計畫內容之適切性。 （5）重大資通安全事件之處理及改善情形。 （6）關注方之回饋 （7）風險評鑑結果及風險處理計畫之狀態 （8）持續改善的機會 7.針對是否應於管審會議中審視法遵事項辦理情形，無特別限制。	資安長權責說明、推動組織架構、資安組織圖與職掌說明、資安長主持會議情形、各參與人員出席情形、相關督導管理等紀錄、後續追蹤執行情形	P3
			資通安全管理法施行細則第6條：資通安全維護計畫應包含公務機關資通安全長之配置			P5
			資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制			P13

2.3	是否有文件或紀錄佐證管理階層（如機關首長、資通安全長等）對於ISMS建立、實作、維持及持續改善之承諾及支持？	機關管理階層對ISMS掌握及支持程度	資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制	1.了解機關之ISMS文件管理機制。 2.資安管理文件及紀錄之訂定核定權責人員（如資安政策、程序文件等）。 3.管理階層參與ISMS或相關資安活動情形及落實核定相關文件等紀錄。	管理階層參與資安推動小組會議紀錄、資安管理文件（如ISMS、資安維護計畫）核定資料	P13
2.4	是否訂定資通安全之績效評估方式（如績效指標等），且定期監控、量測、分析及檢視？	檢視機關所訂定資安績效指標之適切性	資通安全管理法施行細則第6條：資通安全維護計畫應包含資通安全政策及目標、資通安全維護計畫與實施情形之持續精進及績效管理機制	1.應訂定資通安全目標，設定量化與質性指標 2.績效指標訂定適切性、可行性 3.定期監控、量測、分析及檢視之方式（何時、方式、依據資訊） 4.機關資通安全目標應與其資通安全政策一致，並考量適用之資安要求事項及風險評鑑、風險處理之結果，針對是否可以設定為法遵事項無特別限制。 5.量化型目標（範例）： （1）核心資通系統可用性達99.99%以上。（中斷時數/總運作時數<=0.1%） （2）知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。 （3）電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於5%及2%。 6.質化型目標（範例）： （1）適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。 （2）達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。 （3）提升人員資安防護意識、有效偵測與預防外部攻擊等。 7.不適當的資通安全目標及績效指標。 （1）納入資安事件發生數。 （2）目標或指標設定太低，無精進效益（如近3年社交工程演練點閱率皆低於3%，惟機關資通安全目標設定為點閱率不超過10%）。	績效指標、定期檢視紀錄	P2、P13

2.5	是否訂定內部資通安全稽核計畫，包含稽核目標、範圍、時間、程序、人員等？是否規劃及執行稽核發現事項改善措施，且定期追蹤改善情形？	機關應實施內部資安稽核，並應有後續追蹤改善機制。	資通安全責任等級分級辦法應辦事項：管理面之內部資通安全稽核(A級每年2次、B級每年1次、C級每2年1次)	1.機關實施內部稽核應以全機關為原則，倘以抽測，應自機關所有內部單位抽測。 [FAQ4.9] 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。 2.A級機關一年需執行至少2次內部稽核，考量內部稽核後之改善措施，需執行一定時間方可足夠紀錄顯示其有效性，爰2次之間宜間隔至少半年以上。 3.稽核人員適切性、獨立性、勝任度等。 4.建議可檢視至少最近2次之內稽紀錄，並實際檢視改善情形、久未結案的原因、後續管考方式及改善紀錄。	內部稽核計畫、內部稽核報告、相關執行紀錄、後續管考紀錄、向資安長報告之紀錄	N10400
			資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制			P13
2.6	是否針對業務涉及資通安全事項之機關人員，進行相關之考核或獎懲？	機關人員業務涉及資通安全事項之考核或獎懲機制及執行情形。	資通安全管理法施行細則第6條：資通安全維護計畫應包含公務機關所屬人員辦理業務涉及資通安全事項之考核機制	1.應訂定考核機制及獎懲基準，範圍不侷限於資訊或資安人員，並應確實傳達同仁週知。 2.實際了解，針對業務涉及資通安全事項之機關人員，視業務執行情形之獎懲情形。	考核機制、獎懲基準等制度文件、獎懲人員清單	P12
			資通安全管理法第15條：公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵			L0107060615
			資通安全管理法第19條：公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。			L0107060619
			公務機關所屬人員資通安全事項獎懲辦法第2條：公務機關就其所屬人員辦理業務涉及資通安全事項之獎懲，得依本辦法之規定自行訂定獎懲基準。			L61100823

2.7	是否建立機關內、外部利害關係人清單及其連絡方式，並定期檢討其適宜性？	機關是否建立內、外部利害關係人清單資料，並定期檢視。	資通安全事件通報及應變辦法第9條第1項第6款：資通安全事件通報窗口及聯繫方式。（公務機關） 資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制	1.機關內、外部利害關係人清單（包括機關內部、上級／監督機關、所屬／所管機關、合作機關、IT服務供應商、民眾等）。 2.利害關係人聯繫及通報機制（時機、連絡人及方式等）。 3.相關資訊正確性、可用性之檢視機制。	資安管理文件（如ISMS、資安維護計畫）、利害關係人清單、聯繫資訊	L3110082309 P13
3.1	資安經費占資訊經費比例？資訊經費占機關經費比例？針對法遵要求作業、資安治理成熟度評估結果、風險評估結果、稽核或事件缺失改善所需經費，是否合理配置？	了解機關資安經費編列情形以及使否妥適運用該經費。	資通安全管理法施行細則第6條：資通安全維護計畫應包含專責人力與經費之配置	1.應配置適合經費推動ISMS。 2.資安經費占資訊經費比例。 3.資訊經費占機關經費比例。 4.資安經費編列是否符合業務需要。 5.資通安全經費、資源之配置情形是否每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查 6.有無針對法遵要求作業、資安治理成熟度評估結果、風險評估結果、稽核或事件缺失改善等事項，規劃配置所需經費(如系統版本過舊已EOS軟體之更新)。	資安需求評估紀錄、年度預算規劃計畫、年度預算審核紀錄、詳細風險評鑑表	P4
3.2	資安專職人員配置情形？是否配置其他資安專責人員？對應機關自身及對所屬資安作業推動，目前之資安人員配置是否進行合理性評估及因應？（A級機關：4位資安專職人員；B級機關：2位資安專職人員；C級機關：1位資安專職人員）	了解資安專職人員業務配置是否對應機關自身資安作業推動	資通安全責任等級分級辦法應辦事項：管理面之資通安全專責人員要求(A級：4位專職人員、B級：2位專職人員、C級：1位專職人員)	1.專職人員，應全職執行資通安全業務者。[FAQ3.2]資安專職人員職務內容。 2.負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責（避免執行及稽核同一人）。 3.建立人力備援制度。 4.專職人員之相關訓練，與專業證照／職能證書取得之關聯性。 5.專職人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。	資安專職成員名單（應含成員的所屬單位）、職務說明書、人力資源分工表[含職務代理人]、相關人力執行業務之紀錄	N10300

3.3	是否訂定人員之資通安全作業程序及權責？是否明確告知保密事項，且簽署保密協議？	機關應訂定作業程序以防止資訊及資訊處理設施遭未經授權之實體存取、損害及干擾	資通安全管理法施行細則第6條：資通安全維護計畫應包含資通安全防護及控制措施	1.人員包含機關正式人員（含約聘僱人員）、臨時人員及機關委外人員。 2.了解機關人員資通安全作業相關規定及文件，如人員資安管理手冊，說明人員資安注意事項，如人員進出規定、設備攜出入規定、個人電腦使用規定、電子郵件使用規定、網路使用規定等。 3.了解保密協議或切結書之簽署情形（人員包括機關人員、約聘僱人員、委外人員等） [FAQ3.16] 資安法提及之一般使用者係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（如臨時人員、派遣人員及志工），建議上開人員皆應了解並簽署保密協議或切結書。	資安管理文件（如ISMS、資安維護計畫）、保密切結書、人員資安管理文件（如員工資安手冊）	P8
3.4	各類人員是否依法規要求，接受資通安全教育訓練並完成最低時數？	各類人員接受資通安全教育訓練情形	資通安全責任等級分級辦法應辦事項：認知與訓練之資通安全教育訓練 (1.資安專責人員：每年至少12小時以上資通安全專業課程訓練或資通安全職能訓練 2.資安專責人員以外之資訊人員：每2年至少接受3小時以上之資通安全專業課程或	1.符合資通安全責任等級分級辦法附表一、三或五，認知與訓練中資通安全教育訓練所列各類人員所應接受課程之時數。 2.資通安全通識教育訓練： （1）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。 （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.查閱方式： (1)針對個人部份，可由「公務人員終身學習入口網」查看資通安全（通識，課程代碼：522）及資通安全（專業、職能，課程代碼：523）之學習總時數，或由該員提供上課證明。 (2)針對全機關，可請機關提供全員時數之相關佐證。 4.[FAQ3.15]資通安全專業課程訓練： （1）係指可對應資安職能訓練發展藍圖中策略面、管理面、技術面之專業課程為原則，其相關時數，可透過以下方式取得： 甲、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、技術相關課程、講習、訓練及研討（習）會。 乙、參加資安專業證照清單上所列之訓練課程。 丙、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： （甲）公私立大專校院。 （乙）依法設立2年以上之職業訓練機構（職業訓練法所稱之職業訓練機構）。	資通安全專業課程訓練與通識訓練教育訓練執行計畫、教育訓練執行紀錄、訓練日期、方式、訓練內容（教	N30101、N30102、N30103

			資通安全職能訓練，且每年接受3小時以上之資通安全通識教育訓練 3.一般使用者及主管：每人每年接受3小時以上之資通安全通識教育訓練）	（丙）依法設立2年以上之短期補習班（短期補習班設立及管理準則所稱之短期補習班）。 （丁）依法設立2年以上之學術研究機構或財團法人，其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）原則應優先以實體課程方式進行，採線上課程方式取得資通安全專業課程訓練時數，每人每年認定上限為6小時。 5.[FAQ 3.16]有關資通安全通識教育訓練： 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。 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。 6.[FAQ3.20] 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。	訓內容（教材）、講者、訓練成效及時數統計資料等	
3.5	資通安全專職人員是否分別各自持有資通安全專業證照及職能	各資通安全專職人員應持有資通安全專業證照	資通安全責任等級分級辦法應辦事項：認知與訓練之資通安全專業證照及職能訓練證書(各自持有證照及證書各1張)	1.符合資安責任等級分級辦法附表一、三、五資通安全專業證照規定。 2.專業證照： （1）需為數發部資安署公告「資通安全專業證照清單」上所列之證照（https://moda.gov.tw/ACS/laws/certificates/676）。 （2）管理類證照ISO/IEC 27001:2013認列至114年10月31日止。 （3）ISO系列主導稽核員（Lead Auditor）相關證照，須提供當年度至少2次實際稽核經驗證明。[FAQ.3.17]參與內部稽核、外部稽核或針對資訊系統委外廠商之稽核。	1.資安專業證照清單上所列之證照、轉版課程證明、稽核經驗證明	N30200

	訓練證書各1張以上，且維持其有效性？	及證書各1張以上，且維持其有效性	113年11月6日資安輔導字第1133001080號函，更新公布於數位發展部資通安全署網站「資安法規專區」之「資安專業證照清單」	對資訊系統安外檢問之稽核。 （4）確認相關人員證照效期是否有效。 （5）ISO系列相關證照之發證機關（構），需為已簽署國際認證論壇（IAF）多邊相互承認協議之認證機構（含TAF），所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構（可至IAF網站查詢：https://iaf.nu/en/accreditation-bodies/）。 3.職能訓練證書：參加本署認證通過之訓練機構或教育體系所開設之資安職能訓練課程，並通過資安職能評量，即取得職能訓練證書。	2.資安職能訓練發展藍圖內課程之資安職能訓練證書	N30200
4.1	是否確實盤點全機關資訊資產建立清冊（如識別擁有者及使用者等），且鑑別其資產價值？	1.資訊資產宜包含與資通訊、資安正常維運相關者，包含硬體、軟體、系統或服務。 2.資訊資產盤點範圍應為全機關及各核心業務與各資訊資產之對應情形。 3.C級以上機關應每年檢視一次資通系統清冊及分級之妥適性，並應有核可紀錄。	資通安全管理法施行細則第6條：資訊及資通系統之盤點，並標示核心資通系統及相關資產	1.資通系統之盤點範圍應涵蓋全機關（含業務單位、輔助單位），建議檢視資通安全維護計畫「資通系統及資訊之盤點」。 2.資訊資產之盤點應涵蓋全機關（含業務單位、輔助單位），不侷限於IT（即OT也應盤點）、不侷限於連網設備（即不連網設備也應盤點）。 [資通系統風險評鑑參考指引] 機關可藉由資通系統所提供的業務流程活動，識別該資通系統之資訊及資通系統資產，包括業務流程活動中之資源保管人、所需使用之資源與規範、執行關鍵活動中所產生的紀錄與最後之輸出及度量標準等。 3.各核心業務與各資通系統或資訊資產之對應情形，核心業務無對應資通系統或資訊資產者之妥適性。 4.依據資通系統防護需求分級原則進行適當分級（支持核心業務持續運作必要系統列為中級以下之妥適性）。 5.核心資通系統：指支持核心業務持續運作必要之系統，或系統防護需求等級為高者，是否有不符情形（例如，系統防護需求等級為高，卻沒有被列為核心資通系統）。 6.機關核心資通系統清單，應經權責人員核定。核定人員建議為資安長或其指派之適階人員。 7.定期檢視的方式及相關紀錄。 8.為執行風險評估，故需識別核心資通系統與資訊資產之關聯，可確認機關是否有相關文件足以描述前開關聯，例如但不侷限於將核心資通系統標示於資訊資產盤點結果，或於系統清冊上標示對應之資訊資產。	資產價值鑑別及分級紀錄、資通系統清單及分級結果核可紀錄	P6
			資通安全責任等級分級辦法應辦事項：對自行或委外開發之資通系統，依附表9完成系統分級，並完成附表10之控制措施；每年至少檢視1次資通系統分級妥適性。			N10100

4.2	是否訂定資產異動管理程序，定期更新資產清冊，且落實執行？	訂定資訊資產異動管理程序，如有異動，應依鎖定程序落實更新。	資通安全管理法施行細則第6條：資通安全維護計畫應包含資訊及資通系統之盤點，並標示核心資通系統及相關資產	1.資產異動管理程序，包括各類資產異動管理，如實體設備回收、繳回、報廢、業務異動權責人員異動等。 2.更新頻率。 3.抽樣（例如機關監視器、刷卡機、無線路由器、OT設備等）確認是否有在資訊資產清冊中。	資產清冊異動、更新紀錄	P6
				1.了解機關所訂定之風險管理程序文件、機關風險評估準則、衝擊準則及風險接受準則等風險管理基本準則，建議檢視機關資通安全維護計畫「資通安全風險評估」。 2.界定風險評估範圍，並清查盤點該範圍內所有相關的資通系統。 3.委外業務項目之風險評估，對於現有資產、流程、作業環境或特殊對機關之威脅造成可能影響。 4.風險評估成員宜包含施政業務與支援該業務之資通系統相關人員，不宜只交由資訊或資安人員負責，以避免產出結果過於主觀，不符合該機關的真實現況。 5.抽樣檢視風險評估適切性。 6.不可接受之風險等級及風險評估結果（包含不可接受風險之資產清		

4.3	是否建立風險準則且執行風險評估作業，並針對重要資訊資產及委外業務項目鑑別其可能遭遇之風險，分析其喪失機密性、完整性及可用性之衝擊？	訂定風險準則，並依據可能遭遇風險鑑別重要資訊資產喪失CIA之衝擊。	資通安全管理法施行細則第6條：資通安全維護計畫應包含資通安全風險評估	單了且經機關管理層級審查並核定。 7.下列方法提供參考： [資通系統風險評鑑參考指引] （1）CNS31010提供風險評鑑方法： A.企業衝擊分析（BIA）：高階風險評鑑。 B.後果/機率矩陣:詳細風險評鑑。 （2）風險值=資訊及資通系統資產價值x脆弱性利用難易度x威脅發生可能性。 （3）資通系統風險管理過程：風險溝通及諮詢、建立全景、風險評鑑、風險處理、風險監控與審查。 （4）高階風險評鑑方法：如資通安全責任等級分級辦法附表九，安全等級分為3級（普、中、高）、4大影響構面（機密性、完整性、可用性、法律遵循性），評定資通系統安全等級。 （5）詳細風險評鑑方法：詳細風險評鑑對於資產進行深度之識別與鑑別作業，並針對資產詳細列出其可能面臨之威脅與可能存在之脆弱性，以做為評鑑其風險與風險處理方法之依據，詳細之步驟需考慮時間、耗費程度及專家意見等。 A.風險識別：資產識別、威脅與脆弱性識別、現有控制措施識別、後果識別。 B.風險分析：後果評鑑（含資訊及資通系統資產價值評鑑）、事件可能性評鑑、決定風險等級。 C.風險評估：決定風險可接受等級。	資產清冊、資訊安全風險列表、風險管理程序	P7

4.4	是否訂定風險處理程序，選擇適合之資通安全控制措施，且相關控制措施經權責人員核可？是否妥善處理剩餘之資通安全風險？	依據所訂風險處理程序，選擇適當之控制措施，並妥善處理剩餘資安風險	資通安全管理法施行細則第6條：資通安全維護計畫應包含資通安全防護及控制措施	1.辦理風險評估及結果（報告）之審核。 2.訂定風險處理程序、風險處理計畫。 3.依風險評估結果，訂定相應之安控措施、時程、權責人員等。 4.就相應之安控措施有效性之驗證機制。 5.風險處理選擇 （1）風險修改（風險降低）：藉由施行、移除或改變安全控制措施，已修訂或降低風險等級，使殘餘風險得被重新評定為可接受。 （2）風險保留：根據風險評估結果，確認無進一步行動，而保留風險之決策。如風險等級符合風險接受準則，則不虛實做額外之控制措施。 （3）風險避免：風險避免係藉由從已規劃或現有活動或一組活動中退出，或變更活動運作的情況，做出完全避免風險的決定。如社交工程攻擊，除進行演練作業外，強化認知訓練及宣導，才是防範社交工程攻擊或進階持續攻擊最有效控制措施。 （4）風險分擔：依據風險評估結果，將部分風險分擔至能有效管理該特定風險之另一方。如資訊硬體損害之風險可利用保險方案加以分擔，於重大事件發生後，可經由理賠以降低損失之程度，包含人員與資產。	程序文件、風險評估結果、風險處理措施及時程規劃、改善追蹤、對於剩餘風險之處理	P8
4.5	針對公務用之資通訊產品，包含軟體、硬體及服務等，是否已禁止使用大陸廠牌資通訊產品？其禁止且避免採購或使用之作法為何？	了解機關是否已禁止使用大陸廠牌資通訊產品（含軟體、硬體及服務）及禁用作法。	行政院秘書長109年12月18日院臺護長字第1090201804A號函 數位發展部111年11月28日數授資綜字第1111000056號函修正「各機關對危害國家資通安全產品限制使用原則」	1.資通訊產品包含軟體、硬體及服務。 2.大陸廠牌資通訊產品之範圍，係指工程會107年12月20日工程企字第1070050131號函所稱「大陸地區廠商」之產品；至原產地部分，依前述工程會函釋，機關可自行於招標文件中明定廠商所提供之財物或勞務之原產地不得為大陸地區，目前並未限制大陸地區製造之財物參與公務機關採購。 3.檢視機關是否有針對公務用大陸廠牌資通訊產品採取禁用措施及實施做法。年度大陸廠牌盤點作業，機關應落實填報，對照前一年度填報內容檢視是否有漏報，或未依機關自行填報預定汰換期程執行之情形。	程序文件、相關紀錄（會議通知、訂定相關使用規定）、契約書	001 001
			行政院秘書長109年12月18日院臺護長字第1090201804A號函	1.確認機關是否遺漏填報大陸廠牌資通訊產品，續針對機關仍有大陸廠牌資通訊產品（含軟體、硬體及服務），確認是否經其機關資安長同意、列冊管理，及有相關管制措施（例如已封存、未與公務環境連接、或採其他管制措施等），並依行政院111年12月26日國家資通安全	資訊資產清	001

4.6	機關如仍有大陸廠牌資通訊產品，是否經機關資安長同意及列冊管理?並於數位發展部資通安全署管考系統中提報?另相關控管措施為何?	機關若仍有大陸廠牌資通訊產品，須經資安長同意，並有相關控管措施。	數位發展部資通安全署111年11月23日資安綜合字第1111000054號函 111年12月26日行政院國家資通安全會報第40次委員會議決議 數位發展部111年11月28日數授資綜字第1111000056號函修正「各機關對危害國家資通安全產品限制使用原則」	會報第40次委員會議決議自行查核管控措施之有效性。 2.機關仍在使用大陸廠牌資通訊產品原因是否合理，有無替代方案及是否規劃報廢時程。依各機關對危害國家資通安全產品限制使用原則，已屆使用年限者，應於停止使用後，即刻辦理財物報廢作業；未達使用年限者，應定明辦理財物報廢作業期程。 3.上級機關是否依行政院111年12月26日國家資通安全會報第40次委員會議決議查核管控措施之有效性。上級機關應查核所屬機關落實執行以下2項決議： （1）公務機關禁止使用危害國家資通安全產品（軟體、硬體、服務），如確需使用，應簽奉資安長及上級資安長同意，並函報數位發展部（資通安全署）核定，且須有資安防護措施，如設定高強度密碼、確實斷網等應處作為。 （2）公眾活動或使用之場地，不得使用危害國家資通訊產品，尤其是傳播影像或聲音功能產品，應將限制事項納入委外契約或場地使用規定中。	冊、大陸廠牌資通訊產品清冊（管考系統）、資安長確認簽名之文件、機關內稽是否使用大陸廠牌資通訊產品之文件，及上級機關查核紀錄。	001 001 001
4.7	是否針對資通系統或資訊處理設施之變更訂定適當之變更管理程序，且落實執行，並定期檢視、審查及更新程序？	訂定資通系統或資訊處理設施之變更管理程序，並定期檢視因應	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.新系統之引進及對既有系統的重大變更，宜遵循議定之規則，以及文件製作、規格、測試、品質控制及受管理的實作之正式過程。宜備妥管理責任及程序，以確保對所有變更進行令人滿意之控制。 2.宜書面記錄並實施變更控制程序，以確保資訊處理設施及資訊系統中資訊之機密性、完整性及可用性，針對由初期設計階段直至所有後續維護工作的整個系統開發生命週期。	變更管理相關文件	P8
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？	針對委外業務項目進行風險評估	資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施 資通安全管理法第9條	1.委外業務項目之風險評估，對於現有資產、流程、作業環境或特殊對機關之威脅，可能影響。 2.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」	風險評估結果及紀錄、防護需求等級評定、經費及資源配置情形、契約書、廠商自評表	P11 L0107060609

5.2	採購前，是否識別資通系統分級？另依資通系統分級，於採購文件明確規範防護基準需求？	是否在需求階段評估核心系統與否及資通系統之分級，並在採購文件內規範系統防護需求等級及配置資	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期委外階段	1.了解委外內容有關資通系統委外開發或維護作業，應依等級將SSDLC安全及防護基準需求納入契約書。 2.資通系統籌獲階段即應評估防護需求等級、估算資安資源需求，並納入採購文件。 3.資通系統防護需求等級評估結果應訂有核定程序。 4.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」。	防護需求等級評定結果、委外服務建議書、委外服務契約、投標廠商說明履約之資安作為	C0506
5.3	委外辦理之資通系統或服務如涉及國家機密，是否記載於招標公告、招標文件及契約？並針對受託人員辦理適任性查核（辦理前是否有取得當事人書面同意，並依規定限制人員出境）？	應對業務涉及國家機密之委外人員進行適任性查核	資通安全管理法施行細則第4條	1.國家機密定義如下： 指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依國家機密保護法核定機密等級者。 2.依資通安全責任等級分級辦法第4條第1款規定，各機關有業務涉及國家機密之情形者，其資通安全責任等級應為A級。 3.依資通安全管理法施行細則第4條第2項規定，委託機關辦理前項第4款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項： （1）曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判決確定，或通緝有案尚未結案。 （2）曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。 （3）曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。 （4）其他與國家機密保護相關之具體項目。 4.盤點涉及國家機密業務、資通系統及委外人員。 5.招標公告、招標文件及契約是否載明委外案需進行適任性查核及查核方式、頻率。 6.進行適任性查核前是否經當事人同意，並據以落實查核。 7.依國家機密保護法之規定，管制人員出境。	契約書、執行紀錄（例如國家機密核定之紀錄，被核定為機密之業務應可對應至契約標的）、適任性查核同意書、國家機密等級核定文件、廠商人員接受適任性查核之同意書、查核相關文件、人員出境經其（原）服務機關或委託機關首長或其授權之人核准之文件	L1110082304 001
			國家機密保護法第2條及第3條			

5.4	委外廠商執行委外作業時，是否確保其具備完善之資通安全管理措施或通過第三方驗證？開發維運環境之資通安全管理進行評估？	資訊委外廠商之評選機制	資通安全管理法施行細則第4條	1.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或通過第三方驗證。 2.了解機關資訊作業委外安全管理程序。 3.了解委外作業流程（委外前、中、後）之安全管理措施及監督內容。 4.了解機關委外資訊業務項目，進一步抽樣檢視近1年訂定之契約，是否有相關要求。 5.機關對委外廠商資安能力的評估機制及實際執行方式。 6.重要資通系統之委外廠商，對其開發維運環境之資安管理進行評估，可參照資通系統籌獲各階段強化措施之廠商自我管理作業資安評估表。 7.[FAQ6.5] 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。 8.[FAQ6.6] 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。 9.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」	投標廠商之資安管理要求、投標廠商專業能力或開發環境之需求資格、資訊作業委外安全管理程序文件、契約書	L1110082304
			資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施			P11
5.5	委外業務如允許複委託，則對複委託之受託者應具備資通安全維護措施要求為何？如何確認其落實辦理？	廠商針對委外業務分包之資安管理作為	資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施	1.機關宜於契約中定有相關規定，明定契約中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。 2.了解機關之委外招標文件，有關委外業務項目複委託之要求，有複委託者，其範圍與資安管理要求。	委外招標文件、委外服務建議書、委外廠商之資安管理要求、契約書	P11
			資通安全管理法施行細則第4條			L1110082304

5.6	是否要求委外廠商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？其要求標準為？機關及委外廠商是否皆已指定專案管理人員，負責推動、協調及督導委外作業之資通安全管理事項？其負責督導的委外作業資通安全管理事項有哪些？	1.委外廠商配置人員之資安證照、職能訓練或相關實務經驗 2.機關及委外廠商宜配置資安專責人員確認履約期間各項資安作為	資通安全管理法施行細則第4條 資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施	1.機關宜於契約中定有相關規定，明定受託者應指定專案管理人員，並評估訂定受託者應配置之資通安全專業人員人數及所需能力，確保廠商有能力承作，並應有評估機制。 2.受託者與機關宜有適當之專案管理人員，配置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。 3.機關配置之資通安全專責人員，宜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。 4.了解機關委外項目對應之專案管理人員之權責。 5.委外廠商更換專案團隊成員時，其專業資格條件應符合RFP之要求。 6.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」	專案管理相關紀錄、資訊作業委外安全管理程序文件、契約書	L1110082304 P11
5.7	委外客製化資通系統開發者，若屬核心資通系統或委託金額達新臺幣一千萬元以上者，委託機關是否自行或另行委託第三方進行安全性檢測？	符合條件者，除要求廠商要提供安全性檢測證明外，機關應自行或另外委託第三方進行安全性檢測	資通安全管理法施行細則第4條	委外客製化資通系統開發者，若為委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者 1.要求廠商提供安全性檢測證明，且機關應自行或另外委託第三方進行安全性檢測。 2.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」 [工程會資訊服務採購契約範本，請委員依實際狀況檢視機關契約內容] 資通安全責任： 本案金額達新臺幣一千萬元以上，廠商交付之軟硬體及文件，應接受委託機關或其所委託之第三方進行安全性檢測	契約書、委外開發系統之驗收程序、檢視廠商提供之安全性檢測紀錄、機關自行或委託第三方執行的安全性檢測紀錄（符合條件者）、資訊作業委外安全管理程序文件	L1110082304
	委外客製化資通系統	委外開發客製化系統，	資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施	1.受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明。 2.涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。	契約書、委外	P11

5.8	開發者，是否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，標示內容與其來源及提供授權證明？	應要求廠商提交安全性檢測，並就非廠商自行開發部分標示內容並應有相關授權證明。	資通安全管理法施行細則第4條	3.委外客製化資通系統開發者，是否要求委外廠商針對非自行開發之系統或資源，標示內容與其來源及提供授權證明？自行開發資通系統者，亦同。 [工程會資訊服務採購契約範本，請委員依實際狀況檢視機關契約內容] 資通安全責任： 涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。	開發系統之驗收程序、檢視安全性檢測紀錄、資訊作業委外安全管理程序文件	L1110082304
5.9	是否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，是否立即通知機關並採行補救措施？	契約內應定有委外廠商違反資安法或知悉資通安全事件時，應採行補救措施相關文字。	資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施 資通安全管理法施行細則第4條	1.受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。 2.機關於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託機關之權責人員或窗口，以指定之方式進行通報。 3.了解機關對於委託項目之資安事件通報及相關規範。 4.比較廠商之資安事件通報及應變規範，與機關內部資安事件管理關聯性。 5.[工程會資訊服務採購契約範本，請委員依實際狀況檢視機關契約內容] 資通安全責任： 廠商提供服務，如違反資通安全相關法令、知悉機關或廠商發生資安事件時，均必須於1小時內通報機關，提出緊急應變處置，並配合機關做後續處理；必要時，得由資通安全管理法主管機關於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。	資安事件通報及相關處理規範、事件通報與處理紀錄、契約書	P11 L1110082304
5.10	委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料？	契約中應對契約終止或解除時，訂有對持有資料之處理機制	資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施 資通安全管理法施行細則第4條	1.契約中對於委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料之規定。 2.了解機關之相關作業及確認方式。如涉屬契約實質內容，建議應逐案確認。 3.[工程會資訊服務採購契約範本，請委員依實際狀況檢視機關契約內容] 資通安全責任： 契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還或移交之，並保留執行紀錄。	機關委外開發系統之驗收程序、相關作業紀錄	P11 L1110082304

5.11	是否對委外廠商執行受託業務之資安作為進行檢視？其時機及做法為何？針對查核發現，是否建立後續追蹤及管理機制？	以稽核或其他方式確認委外廠商之資安執行情形	資通安全管理法施行細則第4條 資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施	1.委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。 2.了解機關對於廠商之管理措施，確保委託業務如期如質執行。 3.檢視範圍應為所有委外廠商，若囿於人力或經費不足無法每年確認所有廠商受託業務辦理情形，建議參照委外金額、涉及核心系統及業務性質等項面擬定相關計畫，並以書面稽核或其他適當方式確認受託業務執行狀況。 4.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」	委外廠商資安監督（稽核）結果、委外廠商改善與追蹤紀錄	L1110082304 P11
5.12	是否訂定委外廠商之資通安全責任及保密規定？	契約書有關資安責任之規定	資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施	1.為符合資安法要求，機關應於契約中訂有對於委外廠商之資通安全責任之相關規定，如保密協議。 2.機關辦理資訊服務採購時得參考資訊服務採購案之資安檢核事項。 3.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」 4.[工程會資訊服務採購契約範本，請委員依實際狀況檢視機關契約內容] 資通安全責任： 廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。此外機關保有依機關與廠商同意之適當方式對廠商及其分包廠商以派員稽核、委由資通安全管理法主管機關籌組專案團隊稽核或其他適當方式執行相關稽核或查核的權利，稽核結果不符合本契約約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲機關通知後應於期限內完成改善，未依限完成者，依第0條第0款約定核計逾期違約金。	委外廠商資安管理文件及執行紀錄、委外廠商之保密簽署紀錄、資通安全及保密之計畫	P11
5.13	委外廠商專案成員進出機關範圍是否被限制？對於委外廠商駐點人員使用之資訊設備（如個人、筆記型、平板電腦、行動電話及智慧卡等）是	機關應對廠商駐點人員有相關管理規範，包含實體進出、	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	1.委外廠商專案人員經核可後始可進出限定場域及時段。 2.委外廠商專案人員攜帶之設備，是否有經核可後始可使用之規定，並應遵守機關相關安控規範。 3.機關是否監督管理委外業務相關紀錄，並應進行檢視與分析（如人員安全管控、媒體與設備安全管控、存取安全、組態管控），並應包	相關管理規範、相關監督	L0107060609

	否建立相關安全管控措施？是否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	資產進出設備管理及存取控管等要求。	資通安全管理法施行細則第4條：受託者應採取之其他資通安全相關維護措施	含委外廠商專案人員所用機關所有或自攜之設備，降低委外廠商對機關資通安全造成影響。 4.就委外業務監督管理機制，是否有檢視妥適性並滾動調整機制。 5.抽樣檢視。	及分析紀錄	L1110082304
5.14	是否訂定委外廠商系統存取程序及授權規定（如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，是否依系統存取授權規定，調整其權限？	機關應定有系統存取控管相關規範，並應包含委外廠商之系統存取及授權規定，且原則應禁止委外廠商遠端維護，例外允許應採短天期並	資通安全責任等級分級辦法附表十資通系統防護基準：存取控制 行政院110年3月2日院臺護字第1100165761號通函各機關委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理	1.委外廠商存取機關各項資源（網路、系統等）之作業程序應符合系統防護基準，另建議不開放遠端連線維護系統，及例外允許相應之控制措施。 2.了解其必要性，給予最小權限（權限限制、登入時段等）。 3.對於廠商專案人員異動之管控時，系統權限是否一併調整。 4.定期監督管理，有檢視妥適性並滾動調整機制。 5.抽樣檢視。	系統存取控管相關規範、申請核可紀錄、異動紀錄	C0101、C0102、C0103 001
5.15	針對涉及資通訊軟體、硬體或服務相關之採購案、具委外營運公眾場域之委外案，契約範圍內是否使用大陸廠牌資通訊產品?針對委外營運公眾場域之委外案，是否於數位發展部資通安全署管考系統填報並經機關資安長確認?委外廠商或所涉及之人員是否為大陸廠商有陸籍身分？是否於契約內明訂禁止委外廠商使用大陸廠牌之資	1.檢視機關採購案或委外案契約範圍內是否使用大陸廠牌資通訊產品。 2.契約是否有訂定相關文字供廠商遵循。	(不得使用陸牌)行政院秘書長109年12月18日院臺護長字第1090201804A號函 (不允許大陸地區廠商、陸籍人士)109年12月18日行政院資通安全會報第36次委員會議決議 (委外營運場地不得使用陸牌)數位發展部資通安全署111年11月23日資安綜合字第1111000054號函 111年12月26日行政院國家資通安全會報第40次委員會議決議	1.大陸廠牌資通訊產品（含軟體、硬體及服務）之範圍，係指工程會107年12月20日工程企字第1070050131號函所稱「大陸地區廠商」之產品；至原產地部分，依前述工程會函釋，機關可自行於招標文件中明定廠商所提供之財物或勞務之原產地不得為大陸地區，目前並未限制大陸地區製造之財物參與公務機關採購。 2.機關對於涉及資通訊軟體、硬體或服務相關之採購契約，應於合約清楚載明禁用大陸廠牌資通訊產品相關文字，並限制下列事項： （1）大陸地區廠商及陸籍人員不得參與。 （2）委外廠商不得使用大陸廠牌之資通訊產品（含軟體、硬體及服務）。 3.如契約尚未加入禁用大陸廠牌資通訊產品相關文字，應已以其他方式（會議記錄、公文等）通知廠商並有預計納入契約之期程。 4.委外營運公眾場域契約應已至行政院管考系統完成填報，並經資安長確認。並依行政院111年12月26日國家資通安全會報第40次委員會議決議自行查核契約書禁用大陸廠牌情形。 5.上級機關應依行政院111年12月26日國家資通安全會報第40次委員會	委外服務契約、相關切結書、會議記錄、公文、資安長確認簽名之文件、機關自行查核記錄、上級機關查核記錄。	001 001 001 001

	通訊產品，包含軟體、硬體及服務等？		數位發展部111年11月28日數授資綜字第1111000056號函修正「各機關對危害國家資通安全產品限制使用原則」	議決議查核契約書禁用大陸廠牌情形。		001
6.1	是否訂定、修正及實施機關資通安全維護計畫，且每年向上級或監督/主管機關提出資通安全維護計畫實施情形？	應訂定且每年滾動式調整資安維護計畫，並每年提出維護計畫實施情形	資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制	1.應訂定、修正及實施機關資通安全維護計畫，資安維護計畫並應經權責人員核定。 2.公務機關應每年向上級或監督提出資通安全維護計畫實施情形，無上級機關者向主管機關提出（實務上為至管考系統提交）。 3.機關資安維護計畫應至少包括施行細則第六條第一項所列事項。 4.維護計畫實施情形應與對應年度之維護計畫吻合。	資安維護計畫訂（修）定及維護計畫實施情形、管理審查會議紀錄	P13
			資通安全管理法第10條：訂定、修正及實施資通安全維護計畫			L0107060610
			資通安全管理法第12條：提出資通安全維護計畫實施情形			L0107060612
6.2	【中央目的事業主管機關適用】 是否針對特定非公務機關之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告提出及其他應遵行事項，訂定相關辦法？	針對特定非公務機關之資通安全管理訂定相關辦法。	資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制	1.特定非公務機關之資通安全維護計畫必要事項、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訂，報請主管機關核定之。 2.了解中央目的事業主管機關對於所管之特定非公務機關之管理規範。 3.管理規範內容適切性。 4.後續精進及績效管理監督機制。	相關管理辦法、相關執行紀錄	P13
			資通安全管理法第17條：資通安全維護計畫必要事項、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，報請主管機關核定之			L0107060617

6.3	是否針對所屬/監督之公務機關及所管之特定非公務機關稽核其資通安全維護計畫實施情形，包含訂定稽核計畫及提出稽核報告等？是否規劃及執行對所屬/監督機關稽核發現事項改善措施，且定期追蹤改善情形？	所屬/監督之公務機關及所管特定非公務機關稽核實施情形及後續追蹤改善	資通安全管理法施行細則第6條：資通安全維護計畫與實施情形之持續精進及績效管理機制	1.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,稽核對象應包含所有所屬或所監督之機關，無規定要在一年內稽核全部，惟應有整體之規劃，且年份不宜過長。 2.中央目的事業主管機關**應**稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形,稽核對象應包含所有所管CI提供者，無規定要在一年內稽核全部，惟應有整體之規劃，且年份不宜過長。 3.中央目的事業主管機關**得**稽核所管關鍵基礎設施提供者以外特定非公務機關（財團法人及公營事業）之資通安全維護計畫實施情形，非所有CI提供者以外的特定非公務機關皆須稽核，惟宜有評估不實施稽核之準則及記錄。 4.對所屬之稽核計畫（如時程、頻率、機關遴選原則、領隊&稽核員、稽核方式等）是否合適。 5.對所屬或所管之資安稽核，應有管考機制。 6.建議參考ISO27001之精神，機關原則於3年內完成所屬或監督之公務機關及所管之特定非公務機關稽核（可採分層分批稽核方式），資通安全責任等級A、B、C級機關建議以實地稽核方式辦理，資通安全責任等級D、E級機關可採書面查核方式辦理。	稽核計畫、稽核報告、相關執行紀錄、後續管考紀錄	P13
			資通安全管理法第13條：應稽核其所屬或監督機關			L0107060613
			資通安全管理法第16條：應稽核所管關鍵基礎設施提供者			L0107060616
			資通安全管理法第17條：得稽核所管關鍵基礎設施提供者以外之特定非公務機關（即公營事業及財團法人 ）			L0107060617
6.4	是否針對所屬/監督之公務機關及所管之特定非公務機關通報之事件於規定時間內完成審核，且於1小時內依指定之方式向上通報？（第一級或第二	除了解監督或中央目的事業主管機關是否依資通安全事件通報應變辦法相關法遵	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制	1.中央目的事業主管機關指定所管特定非公務機關之資安事件通報方式：特定非公務機關包含公營事業、財團法人及關鍵基礎設施提供者，除公營事業及財團法人可直接至國家資通安全通報應變網站上做通報外，關鍵基礎設施提供者係於各領域中央目的事業主管機關建置通報平台上做通報，並經目的事業主管機關審核後1小時內介接至國家資通安全通報應變網站（NCERT）。 2.於接獲所屬或所監督公務機關及所管特定非公務機關通報之資安事件，應依規定時間完成審核資安事件等級，並將審核結果於1小時內通知主管機關： （1）第一級或第二級資通安全事件者，於接獲後8小時內。 （2）第三級或第四級資通安全事件者，於 接獲後2小時內。 3.中央目的事業主管機關審核後，應依下列規定辦理： （1）審核結果為第一級或第二級資通安全事件者，應定期彙整審核結	中央目的事業主管機關指定所管特定非公務機關資安事件之通報方	P9
			資通安全事件通報及應變辦法第5條：對所屬/監督之公務機關通報之事件於規定時間內完成審核			L3110082305
			資通安全事件通報及應變辦法第12條：對所管之特定非公務機關通報之事件於規定時間內完成審核			L3110082312

	報：（第一級或第二級事件：8小時內完成審核；第三級或第四級事件：2小時內完成審核）	時限辦理資安事件外，其所管或所屬是否亦已要求。	行政院資通安全處111年5月6日院臺護字第1110174310號函「國家層級資安聯防機制研商會議」會議紀錄第四條，為即時掌握資安事件，領域CERT接獲所屬CI提供者通報之1、2級資安事件，回傳時間調整為審核後1小時內回傳至N-CERT。	果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。 （2）審核結果為第三級或第四級資通安全事件者，應於審核完成後1小時內，將審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。 （3）依111年4月27日國家層級資安聯防機制會議紀錄第4點，有關各領域CERT接獲資安事件（1、2、3、4級）應於審核後1小時內回傳至N-CERT。 4.近一年是否有審核逾時情形，其改善機制及有效性評估。 5.中央目的事業主管機關審查特定非公務機關第三級及第四級事件之調查、處理及改善報告後提交主管機關。	式、相關紀錄。	001
6.5	【本項僅總統府與中央一級機關之直屬機關及直轄市、縣（市）政府適用】 是否對於其自身、所屬或監督之公務機關，每年辦理1次資安事件通報及應變演練?是否針對表現不佳者有強化作為？是否將新興資安議題、複合式攻擊或災害納入演練情境，以驗證各種資安事件之安全防護及應變程序？	機關演練情境是否足以驗證各種資安事件之應處機制	資通安全事件通報及應變辦法第8條	1.上級／監督機關（總統府與中央一級機關之直屬機關及直轄市、縣市政府）應規劃及辦理資通安全演練作業，並於完成後1個月內，將執行情形及成果報告送交主管機關。 2.完成演練後1個月逕至管考系統填報演練結果（依行政院秘書長108年4月8日院臺護字第1080171277號函）。 3.了解上級／監督對於所屬／所監督之機關之資安事件通報及應變演練規劃（時程、規模、方式、內容、追蹤改善管考等）。 4.機關資安事件通報及應變演練規劃應可與扣合機關資安事件通報及應變作業規範。 5.資安新興議題，包括但不限於針對雲端應用、行動裝置、巨量資料以及物聯網應用等新興應用所驅動之資安議題。 6.複合式攻擊（全災害）情境演練，包括但不限於系統遭駭侵致敏感性資料外洩、機房火災致核心系統失能、DNS遭DDoS攻擊且網頁遭駭侵置換等。 7.演練結果應有相關持續精進及績效管理機制。 8.本項適用範圍請參考附件。	演練計畫、報告及成果、至管考系統填報紀錄。	L3110082308

6.6	【本項僅總統府與中央一級機關之直屬機關及直轄市、縣（市）政府適用】 是否對於其自身、所屬或監督之公務機關，每半年辦理1次社交工程演練？是否針對開啟郵件、點閱郵件附件或連結之人員加強資安意識教育訓練？	演練範圍是否涵蓋自身及所有所屬或所監督之公務機關，是否後續追蹤機制	資通安全事件通報及應變辦法第8條	1.上級／監督機關（總統府與中央一級機關之直屬機關及直轄市、縣市政府）應規劃及辦理社交工程演練作業，並於完成後1個月內，將執行情形及成果報告送交主管機關 2.機關可審酌規模採抽測方式執行，惟抽測之母數應為自身及所有的所屬或所監督的公務機關 3.演練計畫或維護計畫應載明相關目標值，目前並無強制要求開啟率及點閱率的目標值，各機關可依自身資安責任等級及風險評估結果自行訂定目標值。 4.演練結果應有相關持續精進及績效管理機制（例如目標值的妥適性、表現不佳者的改善作為等） 5.完成演練後1個月應將執行情形及成果報告送交主管機關，方式為逕至管考系統填報演練結果（依行政院秘書長108年4月8日院臺護字第1080171277號函）	對自身、所屬/所監督公務機關之演練計畫、演練紀錄、改善措施及追蹤管考紀錄	L3110082308
7.1	是否依法規定期辦理安全性檢測及資通安全健診? 1.全部核心資通系統辦理弱點掃描（A級機關：每年2次；B級機關：每年1次；C級機關：每2年1次） 2.全部核心資通系統辦理滲透測試（A級機關：每年1次；B、C級機關：每2年1次） 3.資通安全健診，包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設	檢視機關執行弱點掃描、滲透測試及資安健診情形。	資通安全責任等級分級辦法應辦事項：技術面之安全性檢測之弱點掃描 資通安全責任等及分級辦法 資通系統防護基準/系統與資訊完整性/漏洞修復	1.機關全部核心資通系統之弱點掃描、滲透測試、資安健診頻率、至少近2次檢測時間、檢測方式、內容、結果。 2.資安健診各項範圍皆應為全機關，倘為抽測，母數範圍應為全機關。 3.是否依機關風險評估及處理原則執行弱點修補（例如機關風險處理原則為中風險以上弱點皆須修補，就須檢視是否有中風險以上未修補也未有經核定之評估紀錄）。 4.比較近2次結果，相同弱點存在時，可探其內容及原因，改善追蹤機制及落實情形。 5.漏洞修復應測試有效性（例如複測）及潛在影響，並定期更新。	機關核心系統清冊（或維護計畫內所載或所填報實施情形中的系統清冊）、弱點掃描報告、執行修補作業與驗證改善	N20101 C0701
7.2	是否針對安全性檢測及資通安全健診結果執行修補作業，且於修補完成後驗證是否完成改善？	檢視機關執行安全性檢測及資安健診後續修補情形。	資通安全責任等級分級辦法 資通系統防護基準/系統與資訊完整性/漏洞修復	1.了解上列安全性檢測及資通安全健診之改善情形。 2.漏洞修復應測試有效性（例如複測）及潛在影響，並定期更新。 3.複測情形。 4.請委員協助檢視審核層級之妥適性。	追蹤改善紀錄、複測報告	C0701

7.3	【A、B級機關適用】 是否完成政府組態基準導入作業？	了解機關之政府組態基準導入現況，針對未能施行的項目之陳核紀錄及相關例外管理是否妥	資通安全責任等級分級辦法應辦事項：技術面之政府組態基準	1.政府組態基準例外清單（未能施行的項目）應經授權主管核定，定期檢討，並留存相關紀錄。 2.主管機關已函文公告（亦公布於資安院網站GCB專區）的政府組態基準，原則皆應導入。	例外管理說明及陳核紀錄、檢討與改善方案、GCB管理工具查詢畫面	N20400
7.4	【A、B級公務機關應於111年8月24日前或核定後1年內完成；C級公務機關應於112年8月24日前或核定後2年內完成】 是否完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？是否針對高風險弱點進行修補或執行其他控制措施?	資通安全弱點通報機制導入作業及持續有效情形	資通安全責任等級分級辦法應辦事項：技術面之資通安全弱點通報機制	1.A、B、C級公務機關皆應依限完成VANS導入及提交資訊資產盤點資料。另因等級變更而新增VANS應辦事項者，係自資安責任等級核定後起算辦理期限；如等級變更前已有VANS應辦事項者，仍依原等級之法遵期限完成。 2.導入範圍： (1)公務機關：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。 (2)建議可請機關登入VANS系統，並查閱機關ISMS資訊資產清冊，自該清冊抽查部分項目是否確實完成上傳。 3.資訊資產上傳頻率： (1)除重大弱點通報或大量資產異動外，建議每個月至少定期上傳1次。 (2)建議可請機關登入VANS系統，並透過資訊查詢功能檢視機關近12個月的上傳歷程紀錄。 4.弱點處置： (1)機關發現高風險以上之弱點，應即時完成修補；於完成修補前，應規劃緩解措施及管理作為，相關弱點處置方式應於1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。 (2)建議確認機關弱點管理相關規定，並瞭解機關針對VANS比對出之高風險弱點是否訂定修補期限；於弱點完成修補前，是否訂定相關防護及管理措施。 (3)建議可請機關登入VANS系統，並檢視機關風險狀態列表（包含資通系統、使用者電腦等2類），且優先查看高風險弱點（風險指數CVSS>=7.0）資產項目之弱點處置填報情形。 (4)屬工控系統之實務建議：工控系統以能持續運作為首要目標，若VANS導入作業會影響相關系統運作，建議先評估是否導入。若導入，則自行開發之程式需盤點至VANS系統上進行資產管理。	VANS系統（如上傳歷程紀錄查詢、資訊資產列表、資產風險狀態等）、高風險以上弱點修補紀錄、資訊資產清冊、工控系統相關評估紀錄	N20500

<table>
<tr>
<td>7.5</td>
<td>【A、B級公務機關應於112年8月24日前或核定後2年內完成】
是否完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定方式提交偵測資料？是否偵測異常事件判定為資安事件後有回傳相關資料?</td>
<td>A、B級機關應依資通安全責任等級公務機關應辦事項辦理「端點偵測及應變機制」相關作業。</td>
<td>資通安全責任等級分級辦法應辦事項：技術面之端點偵測及應變機制</td>
<td>1.了解機關之端點偵測及應變機制導入現況，施行範圍是否妥當，是否有提交偵測資料。
（1）確認其端點偵測及應變機制。
（2）了解A、B級機關是否依照主管機關指定方式提交偵測資料。
（3）辦理內容，如目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄等。
2.機關導入EDR以全機關為目標，如機關囿於經費，可就從事核心業務之主機與電腦、資安風險程度及資訊資產重要性等，逐步完成導入作業。
3.機關EDR偵測到異常活動，並確認成為資安事件時，即須依律定之STIX格式，透由機關SOC回傳管道提交偵測資料。
4.了解近1年機關通報資安事件若屬於非法入侵 （如植入惡意程式、系統遭入侵等），其EDR回傳情形。</td>
<td>EDR相關檢視或執行紀錄</td>
<td>N20600</td>
</tr>
<tr>
<td>7.6</td>
<td>是否完成下列資通安全防護措施？
<table>
<tr><th>安全防護項目</th><th>A級</th><th>B級</th><th>C級</th><th>D級</th></tr>
<tr><td>防毒軟體</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>網路防火牆</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>電子郵件過濾機制</td><td>v</td><td>v</td><td>v</td><td></td></tr>
<tr><td>入侵偵測及防禦機制</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>應用程式防火牆（具有對外服務之核心資通系</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>進階持續性威脅攻擊防禦</td><td>v</td><td></td><td></td><td></td></tr>
</table></td>
<td>資通安全防護措施執行情形</td>
<td>資通安全責任等級分級辦法應辦事項：技術面之資通安全防護</td>
<td>1.了解機關之資通安全防護規範。
2.各責任等級之防護情形。
3.相關防護措施之佈署範圍、防護規則、判斷原則、運作方式、有效性評估（例如防火牆c2清單阻擋之成功率、防毒之阻擋率等）、精進機制。</td>
<td>資通安全防護要求之相關作業程序、執行與查核紀錄</td>
<td>N20701、N20702、N20703、N20704、N20705、N20706</td>
</tr>
</table>

7.7	是否針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則？是否針對電子郵件進行分析，主動發現異常行為且進行改善（如針對大量異常電子郵件來源之IP位址，於防火牆進行阻擋等）？ 是否有電子郵件之使用管控措施，且落實執行？是否依郵件內容之機密性、敏感性規範傳送限制？	電子郵件資安防護及使用管控措施	資通安全責任等級分級辦法應辦事項：技術面之資通安全防護之具有郵件伺服器者，應備電子郵件過濾機制	1.了解機關電子郵件安全管理規範。 2.電子郵件帳號宜定期清查，離職或不在職人員應即停用或刪除帳號。 3.電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。 4.電子郵件過濾原則、發現異常行為之因應。 5.最近1次電子郵件管理檢視情形。 6.機關對於以電子郵件傳送機密性、敏感性資料之規範。 7.下列安全控制措施參考： （1）傳遞機郵件，須以郵件加密傳送，且密碼應以電郵以外方式提供。 （2）電子郵件加簽。 （3）不應使用公務帳號加入網路社群、消費性雲端服務、網路會員購物網站。 （4）建議封鎖圖片自動下載等設定。 （5）預設開啟信件行為建議預設以純文字模式開啟郵件。 （6）可將收信軟體的郵件預覽功能關閉。	電子郵件資安管理措施及管理檢視情形	N20703
			資通安全責任等級分級辦法附表十資通系統防護基準：存取控制之帳號管理			C0101
7.8	是否建立電子資料安全管理機制，包含分級規則（如機密性、敏感性及一般性等）、存取權限、資料安全、人員管理及處理規範等，且落實執行？	電子資料之資安管理機制	資通安全責任等級分級辦法附表十資通系統防護基準：存取控制之帳號管理、系統與通訊保護	1.了解機關對於電子資料管理機制。 2.了解機關資料分級原則。 3.了解對於各級資訊之存取管控。 4.了解機關對於資料處理（包括儲存、傳輸、備份、交換）之安全管理。	相關管理文件、資料分級原則、資料分級處理規範	C0101、C0601、C0602
7.9	是否建立網路服務安全控制措施，且定期檢討？是否定期檢測網路運作環境之安全漏洞？	了解機關網路服務管理相關規範及落實情形	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.網路服務安控措施及定期檢測機制（如網路防護設備等）。 2.安全漏洞相關修補、列管及更新機制。	網路管理文件、相關執行紀錄	P8
			資通安全責任等級分級辦法應辦事項：技術面之資通安全防護之網路防火牆			N20702

7.10	是否已確實設定防火牆並定期檢視防火牆規則，DNS查詢是否僅限於指定DNS伺服器？有效掌握與管理防火牆連線部署？	設定防火牆並定期檢視防火牆規則	資通安全責任等級分級辦法應辦事項：技術面之資通安全防護之網路防火牆	1.機關需掌握防火牆規則清單，並依法遵要求定期檢視。 2.機關防火牆惡意中繼站名單宜定期更新，資安院每週公布一次該院掌握之c2清單，故建議至少每週更新c2清單。 3.限制明碼傳輸（如telnet、FTP等）、任意連線，防火牆最後一條規則應建立Deny all/any等。 4.檢視DNS查詢使用端口應納入防火牆規則清單。 5.是否依機關風險評估結果建立連線行為黑名單（例如有風險的網站、VPN之使用、加密貨幣挖掘、不受信賴的來源等）。	防火牆規則申請單、防火牆規則定期檢視紀錄	N20702
			110年12月7日行政院國家資通安全會報第38次委員會議擴大會議紀錄			001
7.11	針對機關內部同仁及委外廠商進行遠端維護資通系統，是否採「原則禁止、例外允許」方式辦理，並有適當之防護措施？	委外廠商進行遠端維護資通系統採「原則禁止、例外允許」	資通安全責任等級分級辦法附表十資通系統防護基準：存取控制之遠端存取	1.符合資安法施行細則第4條及資安責任等級分級辦法附表十遠端存取相關規定。 2.開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。 3.對於每一種允許之遠端存取類型，均並應經權責人員核可，建立使用限制、組態需求、連線需求及文件化。 4.結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道（如VPN）登入密碼等。 5.遠端存取行為皆應被紀錄且有監控機制，並有查核機制。 6.連線應採用加密機制。	機關訂定之網路管理規範、資通系統存取控制功能之測試紀錄	C0103
			行政院資通安全處110年3月2日院臺護字第1100165761號函			001
			行政院秘書長110年3月2日院臺護長字第1100165761號函			001
			110年12月7日行政院國家資通安全會報第38次委員會議擴大會議紀錄			001
7.12	網路架構設計是否符合業務需要及資安要求？是否依網路服務需要區隔獨立的邏輯網域（如DMZ、內部或外部網路等），且建立適當之防護措施，以管制過濾網域間之資料存取？	了解機關是否針對機關網路服務有做區隔，並建立相關資安防護。	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.了解機關業務與網段區隔的關係。 2.網段區隔落實與有效性。 3.實體隔離的確實性。	網路架構圖、網路管理文件	P8

7.13	是否針對機關內無線網路服務之存取及應用訂定安全管控程序，且落實執行？	了解機關是否依資通安全管理法施行細則、資通安全維護計畫、ISMS等內部管理文件之規定落實辦理。	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.了解機關對於無線網路管理機制。 2.無線區域網路安全政策、無線區域網路安全架構及無線網路安全管理程序等。 3.身分驗證、存取範圍限制。 4.檢核安控執行情形、稽核無線區域網路中異常行為違法使用、系統維護及安全檢查等。 5.建議可以行動裝置檢視稽核現場是否有機關允許以外之無線AP。	資安管理文件（如ISMS、資安維護計畫）、實際檢視	P8
7.14	資通系統重要組態設定檔案及其他具保護需求之資訊是否加密或其他適當方式儲存（如實體隔離、專用電腦作業環境、資料加密等）？是否針對資訊之交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性（如採行識別碼通行碼管制、電子資料加密或電子簽章認證等）？是否針對重要資料的交換過程，保存適當之監控紀錄？	了解機關是否針對系統與資料傳輸之機密性與完整性建立適當之防護措施	資通安全責任等級分級辦法附表十資通系統防護基準：系統與通訊保護之傳輸之機密性與完整性	1.資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 [資通系統防護基準驗證實務2.6.1.2]如資通系統啟用SSL V3、TLS1.0及TLS1.1等通訊協定，或所使用演算法包含RC2、RC4、DES、3DES、MD5及SHA等安全性不足之加密或雜湊演算法，則未符合此控制措施。 2.高防護需求等級資通系統重要組態設定檔案及其他具保護需求之資訊應加密或其他適當方式儲存。 3.使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 4.使用者輸入資料合法性檢查應置放於應用系統伺服器端。 5.發現違反完整性時，資通系統應實施機關指定之安全保護措施。 6.資通系統至少應加密保護資料庫連線位址資訊與連線帳號密碼等機密資訊。 7.了解系統組態設定檔儲存方式，並可檢視系統組態設定檔，不得以明文呈現資料庫連線資訊及帳號密碼等機敏內容，須使用適當加密方式（如檔案加密、組態欄位加密等）確保機密性。 8.若組態設定值僅透過簡單編碼（如Base64編碼等），因無法有效保護機密性，原則上未符合此控制措施。 9.資訊交換相關程序及安控措施，若機關為其他機關之資料領用者（例如機關有向內政部取得戶役政資料等），應配合資料提供機關（例如內政部）之規定，並宜將資料提供機關之規定納入自身之資料交換規範。 10.機關應掌握資料交換項目、交換方式，並應對交換資料的完整性及機密性實施安控措施。 11.資料交換過程應留存相關監控記錄，並有查核機制。	作業規定、組態設定文件、資料傳輸規定、完整性檢查執行紀錄、機關自訂之資料交換之規範、程序、資料交換項目、交換方式清單、保護措施、監控紀錄、資通系統加密連線之測試報告（如Nmap檢測結果）	C0601
			資通安全責任等級分級辦法附表十資通系統防護基準：系統與資訊完整性之軟體及資訊完整性			C0703
			資通安全責任等級分級辦法附表十資通系統防護基準：系統與通訊保護之資料儲存之安全			C0602

7.15	是否建立帳號管理機制，並定期盤點?使用預設密碼登入資通系統時，是否於登入後要求立即變更密碼，並規定密碼強度、更換週期（限制使用弱密碼）？是否是最小權限？是否有使用角色型存取控制？有管理者權限之帳號是否有只用於管理活動？	密碼（應不得使用預設密碼，且強度）應符合政府組態基準（GCB）	資通安全責任等級分級辦法附表十資通系統防護基準：識別與鑑別 資通安全責任等級分級辦法附表十資通系統防護基準：存取控制之帳號管理及最小原則 行政院資通安全處105年11月30日院臺護字第1050185463號函 110年12月7日行政院國家資通安全會報第38次委員會議擴大會議紀錄	1.了解機關對於密碼之管理機制。 2.新建帳號第一次或以預設密碼登入資通系統時，應有強制變更密碼機制。 3.帳號不得為身份證字號。 4.不得配置相同之預設密碼，建議不得為容易取得資料或其排列組合，如統編、身分證字號、機關代碼或身分證後4碼+生日年月日等。 5.了解使用者權限是否最小化，權限應與職務符合。 6.管理者帳號應只用於管理活動。 7.資料查詢有涉及非公開資料者，其驗證方式是否易遭推論（如統編、流水號等）。 8.系統帳號盤點與管理(含離職人員之異動交接)： (1)不共用帳號、啟用多因子認證、內容發佈建立審核和授權機制、避免分享機密或敏感資訊，並應定期檢查帳號登入紀錄。 (2)（建議事項）宜包含社群媒體平臺，如政府機關對外政策溝通應用之管道Facebook、Instagram等，並適用於社群媒體平臺經營者(包含所有管理者、編輯、版主等)。	存取控制文件、機關GCB套用情形、機關GCB例外管理清單、機關訂定之系統發展維護辦法、資通系統功能規格書、資通系統身分驗證功能測試紀錄、帳號權限清單	C0401、C0402、C0403、C0404、C0405 C0101、C0102 001 001
7.16	是否針對電腦機房及重要區域之安全控制、人員進出管控、環境維護（如溫溼度控制）等項目建立適當之管理措施，且落實執行？	應就電腦機房及重要區域訂有相關安全規範或措施之安全措施	資通安全管理法施行細則第6條：資通安全防護及控制措施	下列安全措施提供參考： 1.機關實體安全之安控措施及規範 2.辦公環境及機房應實體隔離 3.機關人員或來訪人員之進出管制，廠商進入機房建議由機關人員全程陪同，或有其他監控機制（例如監視器、側錄廠商執行之行為等） 4.已授權人員名單紀錄 5.人員、設備及媒體進出資料中心及電腦機房應留存紀錄 6.機房環境、動線、雜物、監視設備及有效性 7.定期檢視的方式及相關紀錄 8.檢視機關是否將數位部「政府機關（構）資訊機房環境安全自檢表」納入內稽內控機制。	機關訂定之伺服器連線管理規範、門禁管理紀錄、相關申請紀錄、監視器錄影紀錄、環控紀錄	P8

7.17	是否定期評估及檢查重要資通設備之設置地點可能之危害因素（如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等）？	重要資通設備之設置地點可能之危害因素，應有定期評估、檢查及防護機制。	資通安全管理法施行細則第6條：資通安全防護及控制措施	下列安全措施提供參考： 1.機關資通營運相關實體環境，應包括辦公地點、資通訊機房、發電機、UPS、資通訊機房鄰近空間等。 2.機關資通營運相關實體環境可能之危害因素，應有相對應的安全偵測及防護措施，且應有備援，並應符合相關的法規（例如防火措施應符合消防法規）。 3.資通訊電腦或通訊機房宜設有環境控制機制，各項環境控制之數值應留存紀錄，且有相關檢查、測試及有效性評估之紀錄。	機房環境圖、環控配置圖、相關保養及維護檢查紀錄	P8
7.18	是否針對電腦機房及重要區域之公用服務（如水、電、消防及通訊等）建立適當之備援方案？	資通訊機房及重要區域共用服務應有備援方案	資通安全管理法施行細則第6條：資通安全防護及控制措施	下列安全措施提供參考： 電腦機房及重要區域之公用服務資源應有備援機制，定期維護，並應有演練記錄。	機房環境圖、環控配置圖、相關保養及維護檢查紀錄、備援方案	P8
7.19	是否訂定資訊處理設備作業程序、變更管理程序及管理責任（如相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等），且落實執行？是否訂定資訊設備回收再使用及汰除之安全控制作業程序，以確保任何機密性或敏感性資料已確實刪除？	應就資訊處理設備訂有作業程序	資通安全管理法施行細則第6條：資通安全防護及控制措施	下列安全措施提供參考： 1.機關資訊處理設備，應至少包括個人電腦、伺服器、網路設備、資安防護設備等。 2.資訊處理設備作業程序，應至少包含新增、異動及移除（報廢）程序，並應含管理權責及相關變更作業程序。 3.對機密與敏感性資料之儲存媒體實施防護措施，例如（但不限於）儲存於加密磁碟、置於上鎖之機櫃等。 4.設備安全處理程序（包括報廢程序）及分級標示。 5.資訊及資通系統變更程序應包含設備回收或再利用規範。 6.資訊設備刪除或汰除前應先逐一確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。 7.具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。	資訊處理設備作業程序、變更管理程序、設備移除（報廢）紀錄	P8
7.20	是否針對使用者電腦訂定軟體安裝管控規則？是否確認授權軟體及免費軟體之使用情形，且定期檢查？	機關對於軟體之安裝及使用應有管理及控管規則	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.機關訂定之軟體使用管理機制，應至少包含軟體安裝、合法使用軟體原則、免費軟體下載來源安全及相關管理等 2.宜定期盤查檢視軟體使用管理機制之妥適性	軟體管理程序文件、檢視紀錄、軟體白名單申請及審核紀錄、白名單軟體申請安裝紀錄	P8

7.21	是否針對個人行動裝置及可攜式媒體訂定管理程序，且落實執行，並定期審查、監控及稽核？	機關對於行動裝置及可攜式媒體應定有安全管理措施	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.機關是否訂定個人行動裝置及可攜式媒體之管理機制，至少包含攜入之安全要求、連網限制、存取限制、更新機制等。 2.應有定期盤查、監控及稽核機制。	行動裝置及可攜式媒體程序文件、定期盤查、監控及稽核紀錄	P8
7.22	是否有網路即時通訊管理措施（如機密公務或因處理公務上而涉及之個人隱私資訊，不得使用即時通訊軟體處理及傳送等）？ 是否有即時通訊軟體安全需求及購置準則？	訂定網路即時通訊使用原則、即時通訊軟體管理措施、安全性需求及購置準則	資通安全管理法施行細則第6條：資通安全防護及控制措施	1.了解機關即時通訊軟體使用規範，例如通訊群組管理規範、通訊內容規範、點擊連結前確認、避免在公共使用之電腦登入、資安事件通報用戶端、傳輸端、伺服器端之安全規範等。 2.使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用相符機密等級之保密機制或指定之軟、硬體，並依相關規定辦理。 3.即時通訊軟體之安全性需求，例如身分驗證機制、網路連線安全、通訊紀錄備份機制等。 4.檢視機關訂定即時通訊軟體購置準則，例如避免使用危害國家資通安全產品或具資安風險疑慮之即時通訊軟體、使用機關指定之即時通訊軟體。	網路即時通訊使用原則、機關即時通訊軟體使用規範，安全環境設定、通訊群組管理規範、資安事件通報規範等	P8
7.23	【適用行政院所屬公務機關，不論資安責任等級】 機關所維運對外或為民服務網站，是否採取相關DDOS防護措施（例如靜態網頁切換、CDN、流量清洗或建置DDoS防護設備等），並確認其有效性?	機關所維運之對外或為民服務網站應備妥相關DDOS防護措施（例如靜態網頁切換、CDN、流量清洗或建置DDoS防護設備等，並應透過演練或稽核等方	資通安全管理法施行細則第6條：資通安全防護及控制措施	至少包含下列控制措施之一 1.靜態網頁（可於10分內切換）。 2.CDN啟用程序。 3.流量清洗服務啟用程序。 4.DDoS防護設備。 5.DDoS防護服務啟用程序。	112年1月底所回復盤點資料、程序文件、系統維護或演練相關紀錄	P8
			111年12月26日行政院國家資通安全會報第40次委員會議紀錄（適用院所屬公務機關）			001

7.24	機關是否對雲端服務應用進行相關資安防護管理?	雲端服務應用應針對安全需求實作必要控制措施	資通安全管理法施行細則第6條：資通安全防護及控制措施	下列安全措施提供參考： （參考資安院_政府機關雲端服務應用資安參考指引） 1.雲端服務部署規劃：機關應依業務需求、欲達成目標及風險評鑑結果，評估採自建或租用方式籌獲雲端服務，並對於資料遷移、資通系統遷移、資料保留及退場機制進行詳細規劃。 2.當機關發現所建置或租用之雲端服務發生資安事件或營運中斷時，應備有資安事件管理機制與營運持續計畫，進行雲端服務相關損害控管與業務持續運作之管理程序。 3.可查看虛擬機器資源配置、更新管理、虛擬防火牆管理、身分存取控制、認證管理、雲端資料備份、清除等是否落實管理。 [資安法FAQ8.7] 1.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。 2.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： （1）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。 （2）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。 （3）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。	雲端服務部署規劃、雲端資源配置、更新管理、虛擬防火牆管理、身分存取控制、認證管理、雲端資料備份、清除相關紀錄	P8
8.1	針對自行或委外開發之資通系統是否依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施？	自行或委外開發之資通系統皆應分級且依資通系統防護基準執行控制措施	資通安全責任等級分級辦法附表應辦事項：管理面之資通系統分級及防護基準	1.各機關自行或委外開發之資通系統皆應列於資通系統盤點清冊，且應依「資通系統防護需求分級原則」完成資通系統分級，並依「資通系統防護基準」所定執行控制措施。 2.針對系統安全需求（含機密性、可用性、完整性），宜以檢核表方式進行確認。 3.檢核表內容與防護基準之關聯性（檢核表內容應至少包含該系統之防護等級所對應之控制措施）。	資通系統盤點清冊、資通系統安全檢視表、資通訊系統分級程序文件、契約書	N10100

8.2	資通系統開發程序是否依安全系統發展生命週期（Secure Software Development Life Cycle, SSDLC）納入資安要求？並是否有	自行或委外開發之資通系統各階段應遵循SSDLC	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期需求階段、系統文件	1.SSDLC各階段安全需求（需求確認、風險評估、修正需求、源碼檢測、滲透測試、弱掃、版控、環境區隔、系統文件）皆應納入資通系統安全發展程序。 2.各階段的安全需求達成情形應有檢核機制。	資通系統盤點清冊、資通系統安全發展程序、各階段落實相關紀錄、契約書	C0501~C0508
8.3	資通系統開發前，是否設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形？	安全性需求應於系統開發前設計，並有檢討落實情形	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期設計階段、系統文件	資通系統需求說明文件應納入安全性相關需求（資安威脅及風險識別執行紀錄），設計文件亦應有對應安全性需求之說明，並宜以檢核表方式確認。	資通系統系統需求及設計文件、資通系統輸入合法性檢查之測試紀錄	C0502、C0508、C0703
8.4	資通系統設計階段，是否依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估？	應識別可能影響系統之威脅，進行風險分析及評估	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期設計階段系統文件	針對防護需求等級中、高者，於資通系統設計階段，根據系統功能與要求，應識別可能影響系統之威脅，包含偽冒、竄改、否認行為、機敏資訊外洩、拒絕存取服務及權限提升等，足以危害系統機密性、完整性及可用性之系統存取行為，進行風險分析及評估，且將風險評估結果（風險評估執行紀錄或報告）回饋需求階段之檢核項目，並提出安全需求修正（資通系統安全需求修正紀錄）。	風險評估及處理文件、資通系統安全檢視表、資通系統安全需求修正紀錄	C0502、C0508
8.5	資通系統開發階段，是否針對安全需求實作必要控制措施並避免常見漏洞（如OWASP Top 10等）？且針對防護需求等級高者，執行源碼掃描安全檢測？另是否執行安全性功能測試，且檢討執行情形？	應針對安全需求實作必要控制措施	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期開發階段、系統文件	1.應注意避免軟體常見漏洞及實作必要控制措施，安全需求可能包含機關規定之組態設定，以明確說明允許之功能、埠口、協定及服務等，或是提供必要資安防護能力，如密碼強度要求、加密強度要求、實作存取控制、身分驗證及授權機制等資安功能實作。 2.發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息，以免系統架構被拼湊得知全貌。 3.針對防護需求等級高者之資通系統，應執行「源碼掃描」安全檢測，檢具掃描報告、修補紀錄及複測紀錄，且具備系統嚴重錯誤之通知機制。 4.採用之源碼檢測工具宜具備常見安全弱點（如OWASP Top 10、跨站腳本攻擊及注入攻擊等）檢測能力。 5.安全性功能測試包含但不限於邏輯及安全性驗測、機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試及在各種使用者環境端皆可更新成功並正常執行之測試，並檢討執行情形。	資通系統源碼存取之相關管理程序、相關紀錄（掃描報告、修補紀錄及複測紀錄）	C0503、C0508

8.6	資通系統測試階段，是否執行弱點掃描安全檢測？且針對防護需求等級高者，執行滲透測試安全檢測？	資通系統測試階段應執行安全性檢測	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期測試階段、系統文件	測試階段即應執行安全性檢測 1.皆應執行「弱點掃描」安全檢測，應注意所採用之弱點掃描工具需具備基本之安全弱點（包含但不限於OWASP Top 10、軟體元件版本弱點、通訊協定弱點等）檢測能力。 2.針對防護需求等級高者之資通系統，除弱點掃描外，須另執行「滲透測試」安全檢測。	系統測試管理程序、系統測試計畫、審查紀錄、弱點掃描報告、滲透測試報告、執行修補作業與驗證改善	C0504、C0508
8.7	資通系統開發如委外辦理，是否將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入契約書？	系統發展生命週期各階段之安全需求應納入契約書	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統發展生命週期委外階段、系統文件	1.委外開發之資通系統安全性需求（應至少為該系統之防護需求等級所對應之防護措施）皆應納入契約書。 2.應透過契約書管理確認落實度。 3.可參考行政院111年5月26日院臺護字第1110174630號函訂定「資通系統籌獲各階段資安強化措施」	資通系統安全發展程序、契約書	C0506、C0508
8.8	是否將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安保護措施？	系統開發、測試及正式作業環境應有所區隔，且應有資安防護措施	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之獲得程序、系統文件	1.防護需求等級中級以上系統，其開發、測試及正式作業環境應為區隔（獨立測試環境指實體或邏輯上區隔、運作環境不同之環境，包含其聯集之資料庫），宜切分不同網段。 2.各區之間應有資安防護措施，及相關存取控管機制。	系統開發、測試、實作的環境與設備區隔相關管理程序（系統發展維護辦法）與檢視紀錄	C0507、C0508
8.9	是否儲存及管理資通系統發展相關文件？儲存方式及管理方式為何？	系統相關文件應有管理機制	資通安全責任等級分級辦法附表十資通系統防護基準：系統與服務獲得之系統文件	系統發展各生命週期文件皆應有儲存與管理機制，並應包含文件清單、儲存方式、版本管控方式等。	文件管理程序（機關訂定之文件管理規範）、儲存方式及版本控管	C0508
8.10	資通系統測試如使用正式作業環境之測試資料，是否針對測試資料建立保護措施，且留存相關作業紀錄？	測試資料如使用正式資料，應有保護措施	資通安全責任等級分級辦法附表十資通系統防護基準：系統與通訊保護	1.測試資料應以不使用正式資料為原則，倘需使用正式資料，並應有保護機制（例如遮罩等，並應特別注意敏感測試資料之保護）。 2.測試資料於使用後應即移除並有覆核機制，並留存紀錄。	測試資料來源、測試資料刪除紀錄。	C0602

8.11	是否針對資通系統所使用之外部元件或軟體、韌體，注意其安全漏洞通告，且定期評估更新？系統之漏洞修復是否測試有效性及潛在影響?	外部元件或軟體之安全漏洞通告，應有評估、更新及確認機制	資通安全責任等級分級辦法附表十資通系統防護基準：系統與資訊完整性之漏洞修復	1.宜建立資通系統所使用的外部元件或軟體清單，注意其安全漏洞通告，且定期評估更新，評估及更新均留下紀錄。 2.宜參考美國CISA KEV目錄（Known Exploited Vulnerabilites Catalog)，其所列之CVE漏洞已被積極利用，應優先排入修補期程。 3.於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 4.漏洞修補應有測試及覆核機制（如於測試環境套用更新程式，確認不會對系統服務造成危害後，始於正式環境進行更新，並留有相關紀錄）。	資通系統所使用的外部元件或軟體清單、漏洞修補程序及相關紀錄、設備型號等	C0701
9.1	是否訂定資安事件**通報**作業規範，包含判定事件等級之流程及權責、事件影響及損害評估、內部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式等，並規範於知悉資通安全事件後1小時內進行通報，若事件等級變更時應續行通報？相關人員是否熟悉相關程序，且落實執行？	應依資通安全事件通報應變辦法第4條及第9條落實辦理相關法遵作業。	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制	1.公務機關知悉資通安全事件後，應於1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。 2.依行政院109年4月16日院臺護字第1090170228號函，請公務機關依資通安全事件通報及應變辦法第4條及第6條於相關法定時限內至國家資通安全事件通報應變網站（https://www.ncert.nat.gov.tw/）完成前開各階段應辦理事項。 3.應就資通安全事件之通報訂定作業規範，其內容應包括下列事項： （1）判定事件等級之流程及權責 。 （2）事件之影響範圍、損害程度及機關因應能力之評估。 （3）資通安全事件之內部通報流程。 （4）通知受資通安全事件影響之其他機關之方式。 （5）前四款事項之演練。 （6）資通安全事件通報窗口及聯繫方式。 （7）其他資通安全事件通報相關事項。 4.除依主管機關指定方式通報外，第三級或第四級資通安全事件，應另以電話或其他適當方式通知上級機關或中央目的事業主管機關，無上級機關者，應通知主管機關。 5.檢視機關所訂資通安全事件之通報作業規範，其中對於演練之規定是否落實執行。 6.檢視機關內部教育訓練或宣導文件，確認相關人員熟悉資安事件通報、應處、結報、審核等法遵事項之相關程序。	資安事件通報作業規範、規範內容之落實紀錄	P9
			行政院109年4月16日院臺護字第1090170228號函有關資通安全管理法所稱公務機關之資通安全事件通報方式。			001
			資通安全事件通報及應變辦法第4條：應於1小時內進行通報			L3110082304
			資通安全事件通報及應變辦法第9條：應就資通安全事件之通報訂定作業規範			L3110082309
			數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序			001

9.2	是否訂定資安事件**應變**作業規範，包含應變小組組織、事前之演練作業、事中之損害控制機制，以及事後之復原、鑑識、調查及改善機制、相關紀錄保全等，且落實執行？	機關應依資通安全事件通報應變辦法第10條事項辦理相關應辦事項。	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制 資通安全事件通報及應變辦法第10條：應就資通安全事件之應變訂定作業規範 數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	1.應就資通安全事件之應變訂定作業規範，其內容應包括下列事項： （1）應變小組之組織。 （2）事件發生前之演練作業。 （3）事件發生時之損害控制機制。 （4）事件發生後之復原、鑑識、調查及改善機制。 （5）事件相關紀錄之保全。 （6）其他資通安全事件應變相關事項。 2.視事件需要成立編組，並因應資安事件訂定通報應變機制。 3.檢視機關所訂資通安全事件之應變作業規範，其中對於演練之規定是否落實執行。 4.檢視駭侵類資安事件，後續事件調查及根因釐清是否落實辦理。	資安事件應變作業規範、規範內容之落實紀錄	P9 L3110082310 001
9.3	【參與行政院資通安全會報資通系統實兵演練機關適用】 機關參與行政院資安會報對外資通系統實兵演練，是否就相關系統弱點訂定資安防護改善計畫，並落實	資通系統實兵演練所發現的系統弱點應訂定資安防護改善計畫並落實執行。	年度行政院國家資通安全會報網路攻防演練計畫、資通安全責任等級分級辦法附表十資通系統防護基準：系統與資訊完整性之漏洞修復	1.針對資通系統實兵演練所發現之系統弱點訂定具體可行的資安防護改善計畫，內容宜包含弱點發生原因、造成影響及具體可行的改善規畫期程。 2.資安防護改善計畫須有與改善規畫期程相對應的改善紀錄，證明計畫已被落實執行。 3.改善紀錄須有具體的佐證資料，包含改善計畫執行的結果及系統弱點修復的有效性。	資安防護改善計畫、改善紀錄	C0701
9.4	是否建立資安事件相關證據資料保護措施，以作為問題分析及法律必要依據？	機關應變相關作業規範應包含事件發生後之復原、鑑識、調查及改善	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制 資通安全事件通報及應變辦法第10條：資通安全事件應變規範應包含事件相關紀錄之保全	1.資安事件相關證據資料保護規範。 2.資安事件證據資料保護程序。 [各機關資通安全事件通報及應變處理作業程序 四、跡證保存] 3.發生資通安全事件時，機關應依下列原則進行跡證保存： （1）機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。 （2）若系統無備援機制，應備份受害系統儲存媒介（例如硬碟、虛擬機映像檔）後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。	程序書、相關佐證資料。	P9 L3110082310

		機制。	數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	（3）若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。 （4）若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。		001
9.5	近1年所有資安事件及近3年第3、4級資安事件之通報時間、過程、因應處理及改善措施，是否依程序落實執行？	機關發生資安事件之通報、應點及改善措施之執行情形。	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制	1.了解機關至少近1年之資通安全事件管理情形。除每次稽核意見交換簡報有概述事件內容外，現場亦可查察案件通報內容。 2.近3年若有發生資通安全事件，或同性質重覆發生，應釐清根因、追蹤改善落實情形，並確認改善的有效性。 3.第三級或第四級資通安全事件，應另以密件公文將改善報告送交主管機關及上級或監督機關。	資安事件處理紀錄	P9
			資通安全管理法第14條			L0107060614
			數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序			001
9.6	是否訂定資安事件處理過程之內部及外部溝通程序？	機關應依資通安全事件通報及應變辦法第9條第3、4、6款辦理相關法遵作業。	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制	1.應訂定資安事件內外溝通程序，包含機關內、外部利害關係人清單（包含機關內部、上級/監督機關/所屬及所管機關、合作機關、IT服務供應商等），並應即時更新聯絡資訊，並應且週知相關人員。另國家資通安全通報應變網站帳號是否落實盤點（如資通安全長、資安聯絡人等），且帳號名稱係以可識別命名。 2.新聞官／組：辦理資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息及擬定溝通計畫。 3.內外部溝通相關人員應納入機關內、外部利害關係人清單（包含機關內部、上級/監督機關/所屬及所管機關、合作機關、IT服務供應商等）。 4.第三級或第四級資通安全事件，應另以電話或其他適當方式通知上級機關或中央目的事業主管機關，無上級機關者，應通知主管機關。	相關佐證文件（如：程序書等）、利害關係人清單	P9
			資通安全事件通報及應變辦法第9條			L3110082309
			數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序			001

9.7	針對所有資安事件，是否保留完整紀錄，並與其他相關管理流程連結，應依自身機關資通安全責任等級保存日誌，詳各機關資通安全事件通報及應變處理作業程序表二，且落實執行後續檢討及改善？	機關應依資通安全管理法施行細則第8條落實辦理法遵作業。	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制 資通安全管理法施行細則第8條 數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	1.資安事件相關文件的管理。 2.負責應變之權責人員或緊急處理小組，辦理應變事務並留存應變之紀錄，包括： （1）資安事件之衝擊及損害控制作業。 （2）資安事件所造成損害之復原作業。 （3）資安事件相關鑑識及其他調查作業。 （4）資安事件之調查與處理及改善報告之方式。 （5）資安事件後續發展及與其他事件關聯性之監控。 3.機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。 4.若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。	事件報告、保存紀錄。	P9 L1110082308 001
9.8	**【A、B級機關適用】** 是否建置資通安全威脅偵測管理（SOC）機制？監控範圍是否包括「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄？SOC是否有委外供應商？SOC供應商是否依契約規範（含SLA水準）	了解機關是否依資通安全責任等級分級辦法A、B級機關應辦事項落實情形。	資通安全責任等級分級辦法應辦事項：管理面之資通安全威脅偵測管理機制 資通安全管理法施行細則第6條：資通系統或服務委外辦理之管理措施	1.了解機關SOC是屬於自建或者委外，其建置、管理機制及執行情形。如為委外，契約書之SLA應可對應法遵內容。 2.SOC監控對象、範圍應至少包括「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。 3.SOC運作機制應包含監控機制、監控原則、通報及事件處理之程序	機關訂定之監控作業程序、機關訂定之通報應變作業程序、監控規範及相關紀錄（資安事件分析紀錄）、日誌保存機制、契約書	N20300 P11
9.9	**【A、B級機關適用】** 是否依指定方式提交SOC監控管理資料？	確認A、B級機關是否依主管機關指定之方式提交其SOC監控管理資料之情形。	資通安全責任等級分級辦法應辦事項：管理面之資通安全威脅偵測管理機制 政府領域聯防監控作業規範	1.不論自行或委外監控，在SOC觸發並記錄事件資料時，即需依「政府領域聯防監控作業規範」回傳下列3項SOC監控管理資料至聯防監控平台： （1）監控設備狀況單（每月5日前回傳上月資訊）:納入監控設備之狀況資訊，如設備名稱、型號、資安防護類型及上月觸發次數等，其資安防護類型應包含「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統。 （2）資安監控單（即時回傳）:有監控紀錄即須回傳，其回傳情資須可明確辨識威脅種類（如入侵攻擊、惡意程式等）。 （3）情資分析單（即時回傳）:為SOC分析人員對「資安監控單」進行	SOC監控管理資料、提交紀錄等。	N20300 001

		情況	行政院資通安全處108年8月23日院臺護字第1080186464號函	影響性評估、驗證及關聯分析資訊之情資，如機關綜整評估後無可用情資即無分享。 2.機關可登入資通安全作業管考系統，查詢自身及所屬機關SOC回傳情況。		001
9.10	是否訂定應記錄之特定資通系統事件（如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等）、日誌內容、記錄時間週期及留存政策，且保留日誌至少6個月？是否有啟用DNS及內部網路之相關紀錄日誌日誌時戳是否對應世界協調時間（UTC）或格林威治標準時間（GMT）或相關校時主機?	機關應依資通安全責任等級分級辦法附表十「事件日誌與可歸責性」及系統防護需求等級辦理相關法遵作業。	資通安全責任等級分級辦法附表十資通系統防護基準：事件日誌與可歸責性之記錄事件、日誌紀錄內容、時戳及校時 數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	1.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。 （1）範圍：A級：全部資通系統與各項資通及防護設備、B級：核心資通系統與相連之資通及防護設備、C級核心資通系統。 （2）保存項目：作業系統日誌（OS event log）、網站日誌（web log）、應用程式日誌（AP log）、登入日誌（logon log）。 2.確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 3.應記錄資通系統管理者帳號所執行之各項功能。 4.應定期審查機關所保留資通系統產生之日誌。 5.資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。 6.資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間（UTC）或格林威治標準時間（GMT）。 7.系統內部時鐘應定期與基準時間源進行同步。 8.各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌（log），並建議定期備份至與原稽核系統不同之實體系統。	日誌保存紀錄、相關程序文件。	C0201、C0202、C0205 001
9.11	是否依日誌儲存需求，配置所需之儲存容量，並於日誌處理失效時採取適當行動及提出告警？	確認機關是否依資通安全責任等級分級辦法附表十「事件日誌與可歸責性」及系統防護需求等級落實辦理相關法遵作業。	資通安全責任等級分級辦法附表十資通系統防護基準：事件日誌與可歸責性之日誌儲存容量、日誌處理失效之回應 數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	1.依據日誌儲存需求（至少保留6個月），配置所需之儲存容量。 2.亦可實作其他控制措施以維持可用之儲存空間： （1）定期檢查剩餘容量。 （2）超過容量警戒值時通知相關人員。 （3）定期壓縮或歸檔日誌。 （4）定期刪除超過保存期限之日誌。 3.資通系統於日誌處理失效時，應採取適當之行動。 4.機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	系統備份紀錄與控管文件	C0203、C0204 001

9.12	針對日誌之是否進行存取控管，並有適當之保護控制措施？	確認機關是否依資通安全責任等級分級辦法附表十「事件日誌與可歸責性」及系統防護需求等級落實辦理相關法遵作業。	資通安全責任等級分級辦法附表十資通系統防護基準：事件日誌與可歸責性之日誌資訊之保護	1.對日誌之存取管理，僅限於有權限之使用者（如系統或資料庫管理者等存取日誌檔案或日誌主機）。依附表十辦理。 2.宜運用雜湊或其他適當方式之完整性確保機制。 3.日誌完整性防護又分為事前預防、事中監視及事後驗證等三種面向： （1）事前預防：將日誌以CD-ROM/DVD-ROM或其他具唯獨（Read Only）特性之儲存媒體進行保存，或透過加密處理後保存或備份。 （2）事中監視：市面上推出多款針對檔案、目錄或資料庫專用之監控工具，其功能特性為可即時偵測檔案、目錄或資料庫欄位異動，並提出警示通知。 （3）事後驗證：可利用SHA-256或HMAC-SHA-256等雜湊演算法計算雜湊值，或將日誌備份至原日誌系統不同之實體系統，亦可用來驗證資料完整性。 3.防護等級高等級之系統定期備份日誌至與原系統外之其他實體系統。	相關佐證資料	C0206
			數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序			001
9.13	是否監控資通系統以偵測攻擊與未授權之連線?是否辦理系統軟體及資訊完整性之控制措施?	確認機關是否依資通安全責任等級分級辦法附表十「系統與資訊完整性」及系統防護需求等級落實辦理相關法遵作業。	資通安全責任等級分級辦法附表十資通系統防護基準：系統與資訊完整性之資通系統監控、軟體及資訊完整性	1.應建立資通安全通報機制，當發現資通系統遭不當存取、竄改、毀損等疑似入侵攻擊跡象時，可透過當面告知、電話、簡訊、電子郵件訊息等適當聯絡方式，通知相關人員進行適當處理。 2.驗證已監控防護需求等級中級以上資通系統之連線行為（可使用WAF、IPS、IDS、惡意程式防護工具、日誌監控及網路監控軟體等），確認已具備必要偵測能力，發現潛在惡意攻擊及未授權使用行為，並留有相關紀錄。 3.防護需求等級中級以上系統應驗證其完整性，完整性檢查技術如使用密碼雜湊函數、同位元檢查及循環冗餘檢查等，亦可評估採用目錄檔案監控工具，可自動偵測應用程式與網站目錄或檔案之異動事件，並留有紀錄及示警。	資安事件分析紀錄、完整性驗證工具、相關紀錄	C0702、C0703
	知悉資通安全事件後，是否於規定時間內完成損害控制或復原作業，並持續進行調查及處理(包含根因分	確認機關是否落實辦理資通安全事件通報及應	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制	1.了解機關資通安全事件管理情形，檢視機關最近之資通安全事件是否於規定時間內（第1、2級事件72小時，第3、4級事件36小時）完成損害控制或復原作業並依主管機關指定之方式及對象辦理通知事宜，且持續進行調查及處理，於1個月內送交調查、處理及改善報告。		P9

9.14	析、跡證保存及防範措施等），於1個月內送交調查、處理及改善報告，且落實執行？（第一級或第二級事件：72小時內完成損害控制或復原作業；第三級或第四級事件：36小時內完成損害控制或復原作業）	變辦法第6條法遵及第三級或第四級資通安全事件，應另以密件公文將該報告送交主管機關及上級或監督機關規定。	資通安全事件通報及應變辦法第6條 數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	2.資通安全事件調查、處理及改善報告應包括： （1）事件發生、完成損害控制或復原作業之時間。 （2）事件影響之範圍及損害評估。 （3）損害控制及復原作業之歷程。 （4）事件調查及處理作業之歷程。 （5）事件根因分析。 （6）為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。 （7）前款措施之預定完成時程及成效追蹤機制（機關應評估短、中、長期資安管理改善策略及追蹤管理）。	資通安全事件處理紀錄、資通安全事件調查、處理及改善報告	L3110082306 001
9.15	知悉第三級或第四級資通安全事件後，是否由資通安全長召開會議研商相關事宜，並得請相關機關提供協助？	了解機關是否依資通安全事件通報及應變辦法第7條落實辦理相關作業。	資通安全管理法施行細則第6條：資通安全事件通報、應變及演練相關機制 資通安全事件通報及應變辦法第7條 數位發展部111年11月23日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序	1.公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。 2.了解機關資通安全事件管理情形，檢視機關最近之第3、4級資通安全事件，是否由資通安全長召開會議研商相關事宜。 3.視情況邀請上級機關、中央目的事業主管機關或主管機關出席，並宜至少討論下列事項： （1）資通安全事件概況。 （2）評估受影響範圍。 （3）其他必要之討論事項。	資通安全事件處理紀錄、會議紀錄	P9 L3110082307 001
9.16	是否建立資通安全情資之評估及因應機制，針對所接受之情資(警訊)，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施？	了解機關是否依資通安全情資分享辦法落實辦理相關作業。	資通安全管理法施行細則第6條：資通安全情資之評估及因應機制 資通安全情資分享辦法	1.各機關應訂定資通安全情資之評估及因應機制，就所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。 2.前開資通安全情資之評估及因應機制宜至少包含情資類別（或來源）、評估方式、評估基準、處理方式、分享對象。 3.應留存相關紀錄。	相關機制及執行紀錄	P10 L51100823

9.17	是否適時進行資通安全情資分享？分享哪些資訊？	了解機關是否依資通安全情資分享辦法落實辦理相關作業。	資通安全管理法施行細則第6條：資通安全情資之評估及因應機制	1.公務機關應適時與主管機關進行情資分享（「情資分享」的事項定義在資通安全情資分享辦法第二條所列之任一款資訊，機關依應辦事項回傳SOC資料（如資安監控單等）包含前述資訊，即符合本項規定）；依情資分享辦法，中央目的事業主管機關應適時與其所管特定非公務機關進行情資分享，前揭機關清單詳法規國合組所盤點之全國資安責任等級總表之中央目的事業主管機關一欄。 [FAQ8.5]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，可於資通安全事件通報及應變網站（https://www.ncert.nat.gov.tw/Doc/list.do）以一般機關身分登入後，選擇上方「情資分享功能」填報分享。 2.了解中央目的事業主管機關情資分享方式、情資類別、內容。如情資分享內容包含惡意活動、系統安全漏洞、事件案例分析及安全防護特徵等情資資訊，另情資含有不得分享之內容，得僅就其他部分分享之。 3.了解中央目的事業主管機關所管特定非公務機關如何與其分享情資。應就情資進行分析及整合，得依情資之來源、接收日期、可用期間、類別、威脅指標特性及其他適當項目與內部情資進行關聯分析，並應整合後發現之新型威脅情資進行分享。 4.了解如何管理情資。應就所分享或接收之情資，採取適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。	相關機制及執行紀錄	P10
			資通安全情資分享辦法			L51100823