資通安全實地稽核項目檢核表(適用公務機關) 修正對照表

版本：v1120512

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
1.2	是否針對重要業務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(如業務調整後對外資訊更新等)？			現行檢核項目1.8移入。
1.3	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？ (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，第三方核發之驗證證書應有我國標準法主管機關委託機構之認證標誌；C級機關：全部核心資通系統2年內完成ISMS導入)	1.2	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？ (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，第三方核發之驗證證書應有TAF認證標誌；C級機關：全部核心資通系統2年內完成ISMS導入)	依資通安全責任等級分級辦法附表一及附表三修正內容，並變更檢核項目項次。
-		1.3	是否盤點核心資通系統，鑑別可能造成營運中斷事件之機率及衝擊影響，且進行營運衝擊分析(BIA)？是否明確訂定核心資通系統之系統復原時間目標(RTO)及資料復原時間點目標(RPO)？	依行政院112年版稽核檢核項目，刪除並移至項目4.5。
-		1.4	是否設置資通系統之備援設備，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？ (資通系統等級中/高等級者適用)	依行政院112年版稽核檢核項目，刪除並移至項目1.6。
1.4	是否定期執行重要資料之備份作業，且備份資料異地存放？存放處所環境是否符合實體安全防護？	1.5	是否定期執行重要資料之備份作業，且備份資料異地存放？存放處所環境是否符合實體安全防護？	變更檢核項目項次。
1.5	是否訂定備份資料之復原程序，且定期執行回復測試，以確保備份資料之有效性？復原程序是否定期檢討及修正？	1.6	是否訂定備份資料之復原程序，且定期執行回復測試，以確保備份資料之有效性？復原程序是否定期檢討及修正？	變更檢核項目項次。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
1.6	資通系統等級中/高等級者，是否設置備援機制，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？			依行政院112年版稽核檢核項目，修正本項目，並由現行檢核項目1.4移入。
1.7	業務持續運作計畫是否已涵蓋全部核心資通系統，並定期辦理全部核心資通系統之業務持續運作演練，包含人員職責應變、作業程序、資源調配及檢討改善等？ (A級機關：每年1次；B、C級機關：每2年1次)	1.7	是否針對核心資通系統制定業務持續運作計畫，並定期辦理全部核心資通系統之業務持續運作演練，包含人員職責應變、作業程序、資源調配及檢討改善等？ (A級機關：每年1次；B、C級機關：每2年1次)	依行政院112年版稽核檢核項目，修正本項目。
-		1.7.1	是否依行政院111年8月警戒專案相關會議指示，機關所轄管資通系統網站(包含學校系所、行政單位網站)內容遭竄改時，備妥應變機制，以利於發現網頁遭竄改後10分鐘內切換為維護公告頁面，並納入業務持續運作計畫演練情境？	依行政院112年版稽核檢核項目，刪除並移至項目7.30.1。
-		1.8	是否針對重要業務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(如業務調整後對外資訊更新等)？	依行政院112年版稽核檢核項目，刪除並移至項目1.2。
1.8	資安治理成熟度評估結果為何？是否進行因應？ (A、B級機關適用，以達到3級為目標)	1.9	是否每年落實辦理資安治理成熟度評估？ (A、B級機關適用)	依行政院112年版稽核檢核項目，修正本項目，並變更檢核項目項次。
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？	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？	依行政院112年版稽核檢核項目，併同現行檢核項目3.5，修正本項目。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
2.4	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？	2.4	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？	依行政院112年版稽核檢核項目，併同現行檢核項目2.5，修正本項目。
-		2.4.1	是否依本部110年12月30日函送之「國立大專校院資通安全維護作業指引」，學校資通安全推動組織宜由資通安全長召集全校各單位主管或副主管組成，每年至少召開會議一次。	刪除現行檢核項目2.4.1。
-		2.5	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？	依行政院112年版稽核檢核項目，刪除並併入至項目2.4。
-		2.5.1	是否依本部110年12月30日函送之「國立大專校院資通安全維護作業指引」，學校置資通安全長，宜指派主任秘書以上人員兼任，以落實推動及監督校內資通安全相關事務。	刪除現行檢核項目2.5.1。
2.5	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？	2.6	是否訂定機關人員辦理業務涉及資通安全事項之考核機制及獎懲基準？	依行政院112年版稽核檢核項目，修正本項目，並變更檢核項目項次。
2.6	是否建立機關內、外部利害關係人清單，並定期檢討其適宜性？	2.7	是否建立機關內、外部利害關係人清單，並定期檢討其適宜性？	變更檢核項目項次。
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、稽核或事件缺失改善所需經費，是否合理配置？	3.1	資安經費占資訊經費比例？資訊經費占機關經費比例？資安經費編列是否符合業務需要？	依行政院112年版稽核檢核項目，修正本項目。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
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)	3.2	資安專職人員配置情形？是否有適切分工？ (A 級機關：4人；B 級機關：2人；C 級機關：1人)	依行政院112年版稽核檢核項目，修正本項目。
-		3.3	是否指定專人或專責單位負責資訊服務請求/事件處理、維運及檢討，且有適切分工？	刪除現行檢核項目3.3。
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？	3.4	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？	變更檢核項目項次。
-		3.5	人員是否瞭解機關之資通安全政策，以及應負之資安責任？	依行政院112年版稽核檢核項目，刪除並併入至項目2.1。
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？	3.6	資通安全專職人員是否每年接受12小時以上之資通安全專業課程訓練或資通安全職能訓練？ (A、B、C 級機關適用)	依行政院112年版稽核檢核項目，併同現行檢核項目3.7及3.8，修正本項目。
-		3.7	資通安全專職人員以外之資訊人員是否每2年接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受3小時以上之資通安全通識教訓練？ (A、B、C 級機關適用)	依行政院112年版稽核檢核項目，刪除並併入至項目3.4。
-		3.8	一般使用者及主管是否每年接受3小時以上之資通安全通識教育訓練？	依行政院112年版稽核檢核項目，刪除並併入至項目3.4。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
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訓練證書各1張以上，且維持其有效性？	3.9	資通安全專職人員是否分別各自持有資通安全專業證照1張以上，且維持證照之有效性？ (A級機關：4張；B級機關：2張；C級機關：1張)	依行政院112年版稽核檢核項目，併同現行檢核項目3.10，修正本項目。
-		3.10	資通安全專職人員是否分別各自持有資通安全職能訓練證書1張以上，且維持證書之有效性？ (A級機關：4張；B級機關：2張；C級機關：1張)	依行政院112年版稽核檢核項目，刪除並併入至項目3.5。
4.1	是否確實盤點資訊資產建立清冊(如識別擁有者及使用者等)，且鑑別其資產價值？	4.1	是否確實盤點資產建立清冊(如識別擁有者及使用者等)，且鑑別其資產價值？	依行政院112年版稽核檢核項目，修正本項目。
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？	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？	依行政院112年版稽核檢核項目，併同現行檢核項目4.5，修正本項目。
-		4.4.1	針對物聯網設備是否採取適當管控機制，如連線控管、變更廠商預設帳密、禁止使用弱密碼、修補安全漏洞？	刪除並移至項目7.17.1。
-		4.5	是否訂定資通安全風險處理計畫，且妥善處理剩餘之資通安全風險？	依行政院112年版稽核檢核項目，刪除並併入至項目4.4。
4.5	核心資通系統是否鑑別可能造成營運中斷事件之機率及衝擊影響，且進行營運衝擊分析(BIA)？是否明確訂定核心資通系統之系統復原時間目標(RTO)及資料復原時間點目標(RPO)？			依行政院112年版稽核檢核項目，修正本項目，並由現行檢核項目1.3移入。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
-		4.6	是否配合新增業務或組織調整時，適時檢視原風險評估作業，以確保相關控制措施之有效性？	刪除現行檢核項目4.6。
4.6	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？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？	4.7	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？是否已禁止使用大陸廠牌資通訊產品？	依行政院112年版稽核檢核項目，修正本項目，並變更檢核項目項次。
-		4.7.1	是否依行政院111年8月警戒專案相關會議指示，透過委外契約或場地租借使用規定，要求對外出租場域不得使用大陸廠牌資通訊產品？	依行政院112年版稽核檢核項目，刪除並併入至項目5.15。
4.7	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？	4.8	是否列冊管理大陸廠牌資通訊產品，並已於110年底前將該產品自公務環境中移除？如該產品仍有與公務環境介接之情況，是否經行政院核定評估同意？	依行政院112年版稽核檢核項目，修正本項目，並變更檢核項目項次。
-		5.1	是否訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？	依行政院112年版稽核檢核項目，刪除並移至項目5.3。
-		5.1.1	是否依行政院111年5月26日函送之「資通系統籌獲各階段資安強化措施」，將所要求之相關措施納入委外安全管理程序?	依行政院112年版稽核檢核項目，刪除並移至項目5.3.1。
-		5.2	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？	依行政院112年版稽核檢核項目，刪除並移至項目5.4。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
-		5.3	委外廠商是否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？	依行政院112年版稽核檢核項目，刪除並移至項目5.5。
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？	5.4	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？	變更檢核項目項次。
-		5.5	是否依委外業務項目之性質允許委外廠商就委外業務項目分(轉)包？如允許分(轉)包，是否注意分(轉)包之範圍，以及分(轉)包之廠商是否具備資通安全維護措施？	依行政院112年版稽核檢核項目，刪除並移至項目5.6。
5.2	是否於採購前識別是否為核心資通系統？並依資通系統分級，於徵求建議書文件(RFP)相關採購文件中明確規範防護基準需求？	5.6	是否依資通系統分級，於徵求建議書文件(RFP)相關採購文件中明確規範防護基準需求？	依行政院112年版稽核檢核項目，修正本項目。
5.3	是否訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？			現行檢核項目5.1移入。
5.3.1	是否依行政院111年5月26日函送之「資通系統籌獲各階段資安強化措施」，將所要求之相關措施納入委外安全管理程序?			現行檢核項目5.1.1移入。
5.4	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？			依行政院112年版稽核檢核項目，修正本項目，並由現行檢核項目5.2移入。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
5.5	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？			依行政院112年版稽核檢核項目，修正本項目，並由現行檢核項目5.3移入。
5.6	委外業務如允許分(轉)包，對分包廠商之資通安全維護措施要求為？如何確認其落實辦理？			依行政院112年版稽核檢核項目，修正本項目，並由現行檢核項目5.5移入。
5.7	對於資通系統之委外廠商，是否針對其人員(如能力、背景等)及開發維運環境之資通安全管理進行評估？	5.7	對於核心資通系統之委外廠商，是否針對其人員(如能力、背景等)及開發維運環境之資通安全管理進行評估？	依行政院112年版稽核檢核項目，修正本項目。
5.8	委外客製化資通系統開發者，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？若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，是否自行或另行委託第三方進行安全性檢測之複測？	5.8	委外客製化資通系統開發者，是否要求委外廠商提供資通系統之安全性檢測證明，並針對非委外廠商自行開發之系統或資源，標示非自行開發之內容與其來源及提供授權證明？若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，是否自行或另行委託第三方進行安全性檢測之複測？	依行政院112年版稽核檢核項目，修正本項目。
5.11	是否訂定委外廠商之資通安全責任及保密規定？	5.11	是否訂定委外廠商之資通安全責任及保密規定，且落實執行？	依行政院112年版稽核檢核項目，修正本項目。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
5.12	是否對委外廠商執行受托業務之資安行為進行檢視？其時機及做法為何？針對查核發現，是否建立後續追蹤及管理機制？	5.12	是否定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務、報告及紀錄等進行管理及安全檢視(如廠商端實地稽核、要求廠商提供異常報告、要求廠商提供相關安全檢測紀錄等)，以利後續追蹤及管理？	依行政院112年版稽核檢核項目，修正本項目。
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、組態管控等相關紀錄？	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)是否建立相關安全管控措施？	依行政院112年版稽核檢核項目，併同現行檢核項目5.15，修正本項目。
-		5.15	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、組態管控等相關紀錄？	依行政院112年版稽核檢核項目，刪除並併入至項目5.13。
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？就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？委外廠商是否為大陸廠商或所涉及之人員是否有陸籍身分？是否於契約內明訂禁止委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等？	5.16	針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內委外廠商是否為大陸廠商或所涉及之人員是否有陸籍身分？是否允許委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等？	依行政院112年版稽核檢核項目，併同現行檢核項目4.7.1，修正本項目，並變更檢核項目項次。
-		6.2	是否落實管理階層(如機關首長、資通安全長等)定期(每年至少1次)審查 ISMS，以確保其運作之適切性及有效性？	刪除現行檢核項目6.2。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
6.2	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？ (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)	6.3	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，且落實執行？ (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)	依行政院112年版稽核檢核項目，併同現行檢核項目6.4，修正本項目，並變更檢核項目項次。
6.2.1	是否依本部110年12月30日函送之「國立大專校院資通安全維護作業指引」，學校辦理內部資通安全稽核，稽核範圍應包含全校各單位。各校得就資通系統（保有個人資料）風險高低、教學單位特性評估訂定推動先後順序，分年分階段規劃辦理，並明訂於各校資通安全維護計畫。 (國立大專校院適用)	6.3.1	是否依本部110年12月30日函送之「國立大專校院資通安全維護作業指引」，學校辦理內部資通安全稽核，稽核範圍應包含全校各單位。各校得就資通系統（保有個人資料）風險高低、教學單位特性評估訂定推動先後順序，分年分階段規劃辦理，並明訂於各校資通安全維護計畫。 (國立大專校院適用)	變更檢核項目項次。
-		6.4	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？	依行政院112年版稽核檢核項目，刪除並併入至項目6.2。
6.3	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？ (中央目的事業主管機關適用)	6.5	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？ (中央目的事業主管機關適用)	變更檢核項目項次。
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？	6.6	是否針對所屬/監督之公務機關及所管之 CI 提供者稽核其資通安全維護計畫實施情形，包含訂定稽核計畫、稽核相關紀錄及提出稽核報告等？且針對實施有缺失或待改善者追蹤其改善情形？	依行政院112年版稽核檢核項目，修正本項目，並變更檢核項目項次。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
6.5	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)	6.7	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)	變更檢核項目項次。
6.6	是否定期針對所屬/監督之公務機關辦理下列演練，且於演練完成後1個月內，送交執行情形及成果報告？(1)每半年規劃及辦理1次社交工程演練？(2)每年規劃及辦理1次資安事件通報及應變演練？	6.8	是否定期針對所屬/監督之公務機關辦理下列演練，且於演練完成後1個月內，送交執行情形及成果報告？(1)每半年規劃及辦理1次社交工程演練？(2)每年規劃及辦理1次資安事件通報及應變演練？	變更檢核項目項次。
7.2	是否針對全部核心資通系統定期辦理滲透測試？ (A級機關：每年1次；B、C級機關：每2年1次)	7.2	是否針對全部核心資通系統定期辦理系統滲透測試？ (A級機關：每年1次；B、C級機關：每2年1次)	依行政院112年版稽核檢核項目，修正本項目。
7.6	是否完成資通安全弱點通報機制(VANS)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？ (A、B級公務機關應於111年8月22日前或核定後1年內完成；C級公務機關應於112年8月22日前或核定後2年內完成)	7.6	是否完成資通安全弱點通報機制(VANS)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？ (A、B級公務機關應於核定後1年內完成；C級公務機關應於核定後2年內完成)	依行政院112年版稽核檢核項目，修正本項目。
7.7	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？ (A、B級公務機關應於112年8月22日前或核定後2年內完成)	7.7	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？ (A、B級公務機關應於核定後2年內完成)	依行政院112年版稽核檢核項目，修正本項目。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
7.12	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？	7.12	是否已確實設定防火牆並定期檢視防火牆規則，有效掌握與管理防火牆連線部署？	依行政院112年版稽核檢核項目，修正本項目。
7.17	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？	7.17	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，並限制使用弱密碼？	依行政院112年版稽核檢核項目，修正本項目。
7.17.1	針對物聯網設備是否採取適當管控機制，如連線控管、變更廠商預設帳密、禁止使用弱密碼、修補安全漏洞？			現行檢核項目4.4.1移入。
7.28	是否訂定網路即時通訊使用原則(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)？			依行政院112年版稽核檢核項目，新增本項目。
7.29	是否訂定即時通訊軟體使用規範、安全需求及購置準則？			依行政院112年版稽核檢核項目，新增本項目。
7.30	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？			依行政院112年版稽核檢核項目，新增本項目。
7.30.1	是否依行政院111年8月警戒專案相關會議指示，機關所轄管資通系統網站(包含學校系所、行政單位網站)內容遭竄改時，備妥應變機制，以利於發現網頁遭竄改後10分鐘內切換為維護公告頁面，並納入業務持續運作計畫演練情境？			現行檢核項目1.7.1移入。

修正項目		現行項目		說明
項次	資通安全稽核檢核項目	項次	資通安全稽核檢核項目	
9.3	是否每年進行1次資安事件通報及應變演練？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？	9.3	是否每年進行1次資安事件通報及應變演練？是否將新興資安議題納入演練情境，以驗證各種資安事件之安全防護及應變程序？	依行政院112年版稽核檢核項目，修正本項目。
9.7	近3年重大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？	9.7	近2年重大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？	依行政院112年版稽核檢核項目，修正本項目。
9.10	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(包含 SLA 水準)確實履約？ (A、B 級機關適用)	9.10	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？ (A、B 級機關適用)	依行政院112年版稽核檢核項目，修正本項目。
9.12	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 相關紀錄日誌(有記錄到 DNS 行為的日誌)？是否有開啟監測內部網路連線至 DMZ 的日誌？	9.12	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？	依行政院112年版稽核檢核項目，修正本項目。