教育部109至110年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫

109年8月

壹、依據

一、資通安全管理法第13條第1項及第17條第3項。

二、教育部所管特定非公務機關資通安全管理作業辦法第5條第1項。

貳、目的

依資通安全管理法第10條及第17條第1項規定，公務機關及關鍵基礎設施（Critical Infrastructure，以下簡稱CI）提供者以外之特定非公務機關應訂定、修正及實施資通安全維護計畫。依資通安全管理法第13條第1項規定，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，另依資通安全管理法第17條第3項規定，中央目的事業主管機關得稽核所管CI提供者以外之特定非公務機關資通安全維護計畫實施情形。

教育部（以下簡稱本部）為落實前述法令規定，規劃每年自所屬公務機關及所管特定非公務機關擇定受稽核對象，查核其資通安全管理法及其子法相關法遵事項符合情形與資通安全維護計畫實施情形，以協助機關強化資安防護工作之完整性及有效性，並透過持續改善降低資安風險。

受稽機關之資通安全維護計畫實施有缺失或待改善者，應依資通安全管理法第13條第2項及教育部所管特定非公務機關資通安全管理作業辦法第10條規定提出改善報告，以確保資通安全維護計畫之合宜性、適切性及有效性。

參、對象及期間

一、部屬機關(構)、資通安全責任等級A級之本部捐助財團法人

（一)範圍為部屬機關（國民及學前教育署、青年發展署、體育署）、部屬機構（國家教育研究院、國家圖書館、國立海洋生物博物館、國

立自然科學博物館、國立科學工藝博物館、國立臺灣科學教育館、國立教育廣播電臺、國立公共資訊圖書館、國立臺灣圖書館、國立臺灣藝術教育館、國立海洋科技博物館）及資通安全責任等級A級之本部捐助財團法人（計有大學入學考試中心基金會等1家）。

(二)實地稽核頻率為3年1次。

二、國立大專校院、資通安全責任等級B級至E級之本部捐助財團法人

(一)範圍為國立大專校院（計48家）及資通安全責任等級B級至E級之本部捐助財團法人（計10家）

(二)遴選原則

1、依資通安全管理法規定，本部應辦理稽核者。

2、資通安全責任等級A、B級者。

3、本(109)年或近1年曾發生資通安全事件者。

4、近1年本部實施社交工程演練成果不佳者。

5、近3年未曾接受行政院或本部稽核，或其稽核結果建議持續關注協助者。

6、其他未完成資安應辦事項或執行情形不佳者（如資通安全維護計畫及其實施情形/資通安全防護/資通安全健診等）。

三、專案實地稽核

考量近期國內、外資安事故頻繁發生，造成機關之機敏資料外洩、系統服務中斷等重大衝擊，為協助機關重要業務相關資通系統或服務發掘潛在資安風險，本部得視情況籌組稽核團隊辦理專案稽核。

四、書面查核

除已實地稽核者，另辦理機關資通安全維護計畫實施情形之書面查核，頻率為3年1次。

肆、作業階段及時程

本案資安稽核作業，分為準備作業、前置作業、實施作業及檢討作業等 4 階段，各階段作業時程及重點工作詳見表 1。

表 1、各階段作業時程及重點工作

階段	作業時程	重點工作
1	準備作業 (6~8 月)	(1)研擬及確認稽核計畫（含受稽機關遴選原則及查檢項目） (2)研擬稽核委員建議名單
2	前置作業 (8~9 月)	(1)確認受稽機關與時程 (2)確認稽核委員與觀察員名單 (3)辦理候選機關說明會、稽核啟始會議、稽核委員及觀察員作業說明會等相關會議
3	實施作業 (109 年 9 月~110 年 10 月)	進行技術檢測及實地稽核 第一梯次：109 年 9 月~109 年 11 月 第二梯次：110 年 12 月~110 年 4 月 第三梯次：110 年 5 月~110 年 7 月 第四梯次：110 年 8 月~110 年 10 月
4	檢討作業 (110 年 11 月~110 年 12 月)	(1)提出稽核結果及共同與個別發現事項 (2)建議表揚優良機關（另擇期辦理優良機關表揚工作）

伍、稽核委員

由本部考量稽核之需求，邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者擔任稽核小組成員（稽核委員）。

稽核小組成員之調派，由本部委請教育機構資安驗證中心(ISCB)及教育體系資安檢核技術服務中心(TACCST)辦理，並由本部資訊安全管理制度輔導廠商協辦。

如受稽機關為教育機構資安驗證中心(ISCB)及教育體系資安檢核技術服務中心(TACCST)之主辦單位，由本部主導稽核小組成員之調派。

陸、稽核團隊

各場次技術檢測及實地稽核團隊組成如下（稽核團隊員額配置如表 2）：

一、領隊：本部資安與個資管理會召集人、副召集人、執行秘書或稽核分組組長，並得由策略面委員代理。

二、稽核委員：每個受稽機關依其資通作業環境之規模與性質，分配 4 至 7 名委員進行資安實地稽核作業，分別為策略面 1 至 2 名、管理面 1 至 2 名及技術面 2 至 3 名。

三、觀察員：自本部及部屬機關(構)人員遴選，每場次至多 2 名。

四、技術檢測團隊：由教育體系資安檢核技術服務中心(TACCST)擔任，每場次 4 至 6 名。如受稽機關為教育體系資安檢核技術服務中心(TACCST)之主辦單位，由本部另行召集技術檢測團隊。

表 2、稽核團隊員額配置

項目	稽核團隊	人員配置	人員總計
技術檢測	技術檢測團隊人員 ▪主導檢核員 ▪檢核員	 1 名 3~5 名	4~8 名
	觀察員	0~2 名	
實地稽核	領隊	1 名	7~13 名
	稽核委員 ▪策略面 ▪管理面 ▪技術面	共 4 至 7 名 ▪ 1 至 2 名 ▪ 1 至 2 名 ▪ 2 至 3 名	
	觀察員	0~2 名	
	工作人員	2 至 3 名	

受稽機關為本部所管特定非公務機關者，稽核團隊如有涉及教育部所管特定非公務機關資通安全管理作業辦法第 8 條第 3 項各款之情形，應提早通知本部並主動迴避。

柒、稽核準則

一、資通安全管理法及其子法。

二、CNS 27001:2014 或 ISO 27001:2013 等資訊安全管理系統標準。

三、受稽機關之資通安全維護計畫。

四、個人資料保護法及其子法。

五、教育體系資通安全暨個人資料管理規範。

六、臺灣學術網路管理規範。

七、其他適用之行政院或本部資通安全政策或規範

捌、稽核範圍

稽核範圍為受稽機關資通安全維護計畫所包括之全機關及核心資通系統各項資安管理政策、程序等。

玖、稽核及評分方式

一、資通安全管理法授權本部稽核所屬公務機關及所管特定非公務機關，本年資安稽核依受稽機關類型實施項目如下：

(一)公務機關（部屬機關(構)、國立大專校院）：採技術檢測及實地稽核方式進行。

(二)特定非公務機關（本部捐助之財團法人）：採實地稽核方式進行。

二、評分方式

(一)第 1 階段：技術檢測

1、本項僅針對公務機關實施。

2、技術檢測分為 7 大檢測項目，各檢測項目之配分說明，部屬機關(構)如表 3-1，國立大專校院如表 3-2。（技術檢測評分表，請參閱附件 6）

表 3-1、技術檢測項目及配分（部屬機關(構)）

項次	檢測項目	配分
1	使用者電腦安全檢測	30
2	網路惡意活動檢測	5
3	核心資通系統安全檢測	25
4	網路架構檢測	10
5	目錄伺服器安全檢測	5
6	物聯網設備安全檢測	10
7	組態設定安全檢測	15
	合計	100
※若無該項目則將技術檢核分數依比例調整。		

表 3-2、技術檢測項目及配分（國立大專校院）

項次	檢測項目	配分
1	使用者電腦安全檢測	30
2	網路惡意活動檢測	5
3	核心資通系統安全檢測	25
4	網路架構檢測	15
5	目錄伺服器安全檢測	10
6	物聯網設備安全檢測	10
7	組態設定安全檢測	5
	合計	100
※若無該項目則將技術檢核分數依比例調整。 ※國立大專校院之技術檢測，將涵括資訊單位（電算中心）、行政單位、教學單位與計畫單位（如涉及公務機關捐助、資助或研發之敏感科學技術資訊安全維護及管理者）及其相關行政人員。		

(二)第 2 階段：實地稽核

實地稽核分策略面、管理面及技術面 3 構面，各構面之稽核項目及配分說明如表 4，總分合計 100 分。（實地稽核評分表，請參閱附件 7）

表 4、實地稽核各構面稽核項目配分

構面	稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資訊及資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、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	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10

國立大專校院之實地稽核，將涵括資訊單位（電算中心）、行政單位、教學單位與計畫單位（如涉及公務機關捐助、資助或研發之敏感科學技術資訊安全維護及管理者）及其相關行政人員，如機關之資通安全維護計畫實施範圍未完整，則相關稽核項目予以扣分。

(三)總分計算

1、公務機關（部屬機關(構)、國立大專校院）：

整體總成績 = 技術檢測得分 × 20% ＋ 實地稽核得分 × 80%。

2、特定非公務機關（本部捐助之財團法人）：

整體總成績 = 實地稽核得分 × 100%。

壹拾、作業說明

一、機關自評

(一)受稽機關填寫「資通安全實地稽核項目檢核表」(附件 1)、「受稽機關現況調查表」(附件 2)、「技術檢測基本資料調查表」(附件 3)及「核心資通系統調查表」(附件 4)。

(二)建議受稽機關先行辦理資安健診作業，俾利預先了解資安現況，並進行改善作為（資安健診服務已納入共同供應契約）。

二、技術檢測

於實地稽核公務機關（部屬機關(構)、國立大專校院）前，將先進行 1 至 3 天之技術檢測，檢視受稽機關之安全防護情形，並於檢測完畢後由技術檢測人員提交「技術檢測結果彙整表」(附件 5)，除據以進行技術檢測評分外，並作為實地稽核之參考。技術檢測重點說明如下：

(一)使用者電腦安全檢測

針對受稽機關檢核範圍進行全網段連接埠掃描（port scan），藉由掃描結果挑選可能存在風險之使用者電腦進行弱點掃描，再依弱點掃描結果之風險程度排序，挑選 5 台高風險及不同作業系統版本之使用者電腦進行深度檢測，其檢測項目包含防毒軟體、安全性修補程式更新、應用程式更新及惡意程式檢測。

(二)網路惡意活動檢測

依照行政院國家資通安全會報技術服務中心每週公布之惡意中繼站名單，針對機關各類型（部屬機關(構)為一般使用者及核心資通系統；國立大專校院為資訊單位(電算中心)、行政單位、教學單位及計畫單位）網段進行檢測。

(三)核心資通系統安全檢測

1. 針對核心資通系統進行內網滲透測試，其檢測項目包含資通系統之權限存取、應用程式及系統弱點、系統通訊保護等，若資通系統使用單一簽入進行權限控管，則亦納入檢測範圍。
2. 依資通系統防護需求等級(普、中、高)，針對核心資通系統之存取控制、識別及鑑別、系統及服務獲得、系統及資訊完整性與系統及

通訊保護等控制措施進行檢測，並檢視源碼掃描、弱點掃描及滲透測試等檢測報告及修補紀錄，以及安全需求檢核結果。

(四)網路架構檢測

透過訪談與實際檢視方式，驗證網路與系統之管理控制措施、網路與系統之安全控制措施、網路與系統架構之備援機制、防火牆規則及存取控制，並確認資通系統管理與防護情形。

(五)目錄伺服器安全檢測

透過實際檢測方式，針對機關之目錄伺服器進行防毒軟體、安全性修補程式更新及惡意程式檢測。

(六)物聯網設備安全檢測

針對網路印表機、門禁系統、網路攝影機、無線網路基地台(AP)/無線路由器及環控系統等物聯網設備進行檢測，透過內部網路或臨機操作方式執行檢測作業，其檢測項目包含傳輸加密保護、身分鑑別與授權、用戶端與管理端網頁介面之安全性、軟體及韌體之安全性更新等。

(七)組態設定安全檢測

針對已公告之政府組態基準(GCB)項目，就網通設備、作業系統、瀏覽器及應用程式進行抽測。

三、實地稽核

(一)由領隊帶領稽核團隊至受稽機關進行實地稽核(實地稽核時程規劃如表 5)，如受稽機關為本部捐助之財團法人，將請其業務主管單位派員出席（如：大學入學考試中心基金會，請高等教育司派員陪同受稽）。實地稽核項目依據資通安全管理法及各子法法遵事項，整併為三大構面、九大稽核項目，詳參附件「資通安全實地稽核項目檢核表」。

(二)實地稽核時間將依機關業務複雜度、機關辦公場域數量、重要資通系統數量等因素，彈性調整稽核時程。稽核啟始/結束會議之受稽

機關代表建議由機關資通安全長出席，以帶領機關之資安管理及追蹤改善。

表 5、實地稽核當天議程

時間	工作項目	參與人員
9:00~9:30	啟始會議 ➢ 受稽機關代表致詞、介紹出席人員（5 分鐘） ➢ 稽核團隊領隊致詞、介紹稽核團隊（5 分鐘） ➢資安稽核作業說明（5 分鐘） ➢受稽機關資安推動情形(15 分鐘)	▪稽核團隊 ▪受稽機關 ▪業務主管單位
9:30~9:45	稽核團隊稽核前意見交換	稽核團隊
9:45~12:30	實地稽核	▪稽核團隊 ▪受稽機關 ▪業務主管單位
12:30~13:30	午餐(註)及彙整稽核發現	稽核團隊
13:30~16:30	實地稽核	▪稽核團隊 ▪受稽機關 ▪業務主管單位
16:30~17:00	稽核團隊意見彙整	稽核團隊
17:00~17:30	結束會議 ➢稽核結果報告 ➢意見交流	▪稽核團隊 ▪受稽機關 ▪業務主管單位

註：午餐委請受稽機關代訂，由稽核團隊支付費用。

壹拾壹、獎勵及改善作業

資安稽核作業結束後，依受稽機關屬性分為部屬機關(構)及國立大專校院 2 組，對於分組成績表現優良者，本部將函請受稽機關行政獎勵。（本部捐助之財團法人不列入評比）

一、行政獎勵

依據稽核分組各受稽機關成績，擇取排序後前四分之一（未達整數以四捨五入計），且稽核成績須達 75 分(含)以上之受稽機關評為績優機關，本部將函請績優機關，針對有功人員予以敘獎（嘉獎或記功）。

二、績優機關限制條件

個別分組之受稽機關未達獎勵標準時，名額從缺。

三、稽核改善作業

(一)本部將於每季稽核結束後函送資安稽核報告予受稽機關，並請機關就報告中待改善或建議事項研議因應作為及辦理時程，於期限內填報並函復本部，後續本部將通知受稽機關定期回復。

(二)公務機關所屬人員未遵守資通安全管理法規定者，應依資通安全管理法第 19 條規定辦理之；本部所管特定非公務機關之稽核結果，如有資通安全管理法第 20 條及第 21 條所述情形，本部將依法辦理之。

(三)本次資安稽核作業結束後，本部將彙整所有受稽機關之稽核結果，並提出本次資安稽核共同發現事項及建議，供本部所屬公務機關及所管特定非公務機關參考改進。

壹拾貳、受稽機關配合事項

一、本部於稽核前 1 個月通知受稽機關，另將個別通知受稽機關稽核期程，請受稽機關於文到後 2 週內填復「資通安全實地稽核項目檢核表」、「受稽機關現況調查表」及「技術檢測基本資料調查表」、「核心資通系統調查表」及，並提供機關最新版之資通安全維護計畫，俾利稽核團隊辦理作業。

二、本部將分北、中、南三區辦理資安稽核說明會，以及辦理稽核委員及觀察員作業說明會，其辦理時程、地點及相關事項另行通知；為因應 COVID-19（武漢肺炎）疫情，並請配合各場次相關防疫措施。

壹拾參、其他資通安全稽核相關事宜

一、其他非本部直屬教育體系機關之資通安全稽核

為協助其他非本部直屬教育體系機關提升資通安全防護之完整性及有效性，本部將適時協助相關機關檢視資通安全維護計畫實施情形，屬跨領域主管機關者，將協請相關領域主管機關共同辦理資安稽核。

壹拾肆、附件

附件	附件名稱	說明
1	資通安全實地稽核項目檢核表	機關之資通安全維護計畫實施情形，資料將提供實地稽核之稽核委員參考
2	受稽機關現況調查表	受稽機關現況說明，包括機關組織、辦公地點、系統管理者存取核心資通系統地點、目錄伺服器放置地點等資訊
3	技術檢測基本資料調查表	技術檢測所需之相關資訊，如受檢測電腦配置、軟體安裝資訊、組態設定等資訊
4	核心資通系統調查表	核心資通系統之防護現況及系統配置等資訊
5	技術檢測結果彙整表	技術檢測結果說明
6	技術檢測評分表	技術檢測項目配分說明
7	實地稽核評分表	實地稽核項目配分說明

資通安全實地稽核項目檢核表(適用公務機關)

機關名稱：_____

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(一) 核心業務及其重要性							
1.1	是否界定機關之核心業務，完成資通系統之盤點及分級，且每年至少檢視 1 次分級之妥適性？						
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；C 級機關：全部核心資通系統 2 年內完成 ISMS 導入)						
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)？						
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)						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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)						
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)？						
1.9	是否每年辦理 1 次資安治理成熟度評估？(A、B 級機關適用)						
(二) 資通安全政策及推動組織							
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？						
2.2	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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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？						
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？						
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？						
(三)、專責人力及經費配置							
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？						
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)						
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？						
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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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)						
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)						
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？						
3.9	資安專職人員是否符合資通安全專業證照要求，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)						
3.10	資安專職人員是否符合資通安全職能評量證書要求，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)						
(四) 資訊及資通系統盤點及風險評估							
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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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？						
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？						
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？						
(五) 資通系統或服務委外辦理之管理措施							
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？						
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？						
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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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？						
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？						
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？						
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？						
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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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？						
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？						
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？						
(六) 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							
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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)						
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？						
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】						
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？						
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)						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
(七) 資通安全防護及控制措施							
7.1	是否針對全部核心資通系統定期辦理網站安全弱點檢測？(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)						
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)						
7.3	是否定期辦理資通安全健診，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定檢視等？(A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)						
7.4	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？						
7.5	是否建置資通安全威脅偵測管理(SOC)機制？ (A、B 級機關適用)						

<table>
<tr><th>稽核項目</th><th>資通安全稽核檢核項目</th><th>符合</th><th>部分符合</th><th>不符合</th><th>不適用</th><th>簡述符合、部分符合、不符合或不適用之原因</th><th>紀錄文件</th></tr>
<tr><td>7.6</td><td>是否依指定方式提交 SOC 監控管理資料？
(A、B 級機關適用)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7.7</td><td>是否針對資通系統及相關設備，建立適當之監控措施(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)？是否針對日誌建立適當之保護機制，以避免遭到竄改，且落實執行並定期稽核？</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7.8</td><td>是否建立電子資料使用紀錄、軌跡資料及證據保存相關管理機制？</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7.9</td><td>是否完成政府組態基準導入作業？(A、B 級機關適用)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7.10</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>v</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統者)</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></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.11	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)？						
7.12	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？						
7.13	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？						
7.14	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？						
7.15	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？						
7.16	是否針對機密及敏感性資料之處理及儲存建立適當之防護措施(如實體隔離、專用電腦作業環境、資料加密等)？是否針對系統與資料之完整性建立適當之防護措施？						
7.17	是否訂定電子郵件之使用規則，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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.18	是否每半年進行 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？						
7.19	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？						
7.20	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)？						
7.21	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？						
7.22	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？						
7.23	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，且落實執行？						
7.24	是否針對電子資料相關設備進行安全管理(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)？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.25	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？						
7.26	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？						
7.27	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？						
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)？						
7.29	是否訂定即時通訊軟體使用規範，包含安全環境設定、通訊群組管理規範、資安事件通報規範等？						
7.30	是否訂定即時通訊軟體之安全性需求及購置準則，包含用戶端、傳輸端、伺服器端之安全規範(如網路連線安全、通訊紀錄備份機制、通訊內容，與公務相關、點擊連結前確認、避免在公共使用之電腦登入等)？						
(八) 資通系統發展及維護安全							
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.2	資通系統開發過程請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？						
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？						
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？						
8.5	資通系統開發階段，是否避免常見漏洞(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？						
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？						
8.7	資通系統上線前，是否執行安全性要求測試，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測試等，且檢討執行情形？						
8.8	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)納入委外契約？						
8.9	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.10	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？						
8.11	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？						
8.12	是否針對資通系統所使用之外部元件或軟體，注意其安全漏洞通告，且定期評估更新？						
(九) 資通安全事件通報應變及情資評估因應							
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？						
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、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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
9.5	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？						
9.6	是否訂定資安事件處理過程之內部及外部溝通程序？						
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，且落實執行後續檢討及改善？						
9.8	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，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)						
9.9	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？						
9.10	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，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？						
9.11	是否適時進行資通安全情資分享？分享哪些資訊？						

受稽機關現況調查表

受稽機關(構)	辦公地點	辦公單位	使用者電腦數量	核心資通系統名稱	系統管理員存取核心資通系統之地點	目錄伺服器放置地點(若無目錄伺服器則不需填寫)	目錄伺服器管理者存取該主機地點
○○委員會 (範例 1)	臺北市中正區 寶慶路○○號 (會本部)	綜合規劃處 秘書室 人事室 政風室 主計室	300	無	無	目錄伺服器主機與濟南路辦公室相同	目錄伺服器主機與濟南路辦公室相同
	臺北市中正區 濟南路○○號 (濟南路辦公室)	○○事務處	200	A 系統	濟南路辦公室	○○機房	濟南路辦公室
	某機房	無	0	B 系統 E 系統	濟南路辦公室	無	無
○○部 (範例 2)	臺北市信義區 ○○路○○號	綜合規劃組 政風室 人事室 主計室 秘書室	300	A 系統 B 系統 C 系統 D 系統 E 系統	○○中心	2F 機房	○○中心

受稽機關(構)	辦公地點	辦公單位	使用者電腦數量	核心資通系統名稱	系統管理員存取核心資通系統之地點	目錄伺服器放置地點(若無目錄伺服器則不需填寫)	目錄伺服器管理者存取該主機地點

附件 3 技術檢測基本資料調查表

1.填表人基本資料		
機關(構)名稱		
填表人姓名		
填表人公務電話		
填表人公務 Email		
填表日期	_____年_____月_____日	
2.使用者電腦安全檢測-使用者電腦弱點掃描		
2.1.	使用者電腦作業系統版本(可複選)	□Microsoft Windows XP _____台 □Microsoft Windows 7 _____台 □Microsoft Windows 8 _____台 □Microsoft Windows 8.1 _____台 □Microsoft Windows 10 _____台 □其他：_____共____台
2.2.	是否定期執行使用者電腦弱點掃描作業?	□是： ■最近一次掃描日期：___年___月___日 ■執行廠商：_____ ■掃描工具：_____ ■掃描方式： □由 1 組固定 IP 進行跨網段弱點掃描 □無法跨網段掃描，改由每個網段設定 1 組 IP 進行弱點掃描 □其他：_____ □其他情況說明：_____ □否(請跳至 3.1)
2.3.	針對使用者電腦弱點掃描結果是否定期進行修補?	□是： ■最近一次修補日期：___年___月___日 ■修補弱點類型： □僅修補高風險弱點 □修補高、中風險弱點 □其他：_____ □其他情況說明：_____ □否

3. 使用者電腦安全檢測-使用者電腦安全防護檢測		
3.1	使用者電腦是否安裝 Java 軟體?	□是，安裝版本：_____ □否(請跳至 3.3)
3.2	使用者電腦 Java 軟體是否有更新政策?	□是， ■政策文件名稱：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □修補程式發布後就更新 □其他：_____ ■最近更新時間：____年___月___日 ■更新方式： □使用者手動下載更新與安裝 □自動下載更新，使用者決定是否安裝 □中控台集中派送 □其他：_____ ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
3.3	使用者電腦是否安裝 Adobe Flash Player 軟體?	□是，安裝版本：_____) □否(請跳至 3.5)
3.4	使用者電腦 Adobe Flash Player 是否有更新政策?	□是， ■政策文件名稱：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □修補程式發布後就更新 □其他：_____ ■最近更新時間：____年___月___日 ■更新方式： □自動安裝更新 □自動下載更新，使用者決定是否安裝

		□中控台集中派送 □其他：_____ ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
3.5	使用者電腦是否安裝 Adobe Reader 軟體?	□是，安裝版本：_____ □否(請跳至 3.7)
3.6	使用者電腦 Adobe Reader 是否有更新政策?	□是， ■政策文件名稱：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □修補程式發布後就更新 □其他：_____ ■最近更新時間：____年___月___日 ■更新方式： □自動安裝更新 □自動下載更新，使用者決定是否安裝 □使用者手動下載更新與安裝 □中控台集中派送 □其他：_____ ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
3.7	使用者電腦是否安裝防毒軟體?	□是， ■防毒軟體名稱：_____ ■防毒軟體版本：_____ □否(請跳至 3.9)

3.8	使用者電腦防毒軟體病毒碼是否有更新政策?	□是， ■政策文件名稱：_____ ■更新方式： □集中管控、派送(如防毒軟體中控台) □使用者手動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
3.9	使用者電腦作業系統相關安全修補程式是否有更新政策?	□是， ■政策文件名稱：_____ ■更新來源： □微軟更新伺服器 □機關內部 WSUS 伺服器 □其他：_____ ■更新方式： □使用者手動下載與更新 □自動下載，使用者決定是否更新 □自動下載，設定排程安裝更新 □自動下載，自動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄：

		□是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否 □其他情況說明：_____
3.10	使用者電腦之 Microsoft Office 與其他微軟應用程式是否有更新政策?	□是， ■政策文件名稱：_____ ■更新來源： □微軟更新伺服器 □機關內部 WSUS 伺服器 □其他：_____ ■更新方式： □使用者手動下載與更新 □自動下載，使用者決定是否更新 □自動下載，設定排程安裝更新 □自動下載，自動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否 □其他情況說明：_____
3.11	機關是否已具備資產管理系統?	□是， ■資產管理系統名稱（依字母筆劃排序）： □IP-guard 端點安全管控系統 □SmartIT □WinMatrix IT 資源管理系統

		□X-Fort 電子資料監控系統 □神網電腦終端防護系統 □其他：_____ ■資產管理系統涵蓋範圍： □使用者電腦（□包括軟體） □伺服器主機（□包括軟體） □網路設備（□包括軟體） □其他：_____ □否
4.組態設定安全檢測		
4.1	機關是否已導入政府組態基準(GCB) □是(請勾選導入項目，可複選)　□否(請跳至 4.4)	
	4.1.1 作業系統(使用者電腦)	
	□Microsoft Windows 7	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Microsoft Windows 8.1	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____

	□Microsoft Windows 10	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	4.1.2 作業系統(網域主機主機)	
	□Microsoft Windows Server 2008 R2	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Microsoft Windows Server 2012 R2	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Microsoft Windows Server 2016	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度：

		□測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□RedHat Enterprise Linux 5	■導入方式(可複選)： □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	4.1.3 瀏覽器	
	□Microsoft Internet Explorer 8	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Microsoft Internet Explorer 11	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____

	□Google Chrome	■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Mozilla Firefox	■導入方式(可複選)： □透過網域主機進行派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Microsoft Edge	■導入方式(可複選)： □透過網域主機進行派送 □逐台設定 □其他：_____ ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 ■□補充說明：_____
	4.1.4 網通設備	
	□Juniper Firewall	■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台

		■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Fortinet Fortigate	■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Cisco Firewall	■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□無線網路	■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	4.1.5 應用程式	

	□Exchange Server 2013	■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
	□Microsoft IIS 8.5	■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■目前導入進度： □測試中，預計於___年___月完成 □部分導入，預計於___年___月完成 □已於___年___月完成導入 □補充說明：_____
4.2	機關組態設定值與 GCB 建議值不同時，需訂定例外管理項目並紀錄變更事由及相關配套措施 機關是否已訂定例外管理項目? □是， ■作業系統 ➢Microsoft Windows 7 已訂定____條例外管理項目 ➢Microsoft Windows 8.1 已訂定____條例外管理項目 ➢Microsoft Windows 10 已訂定____條例外管理項目 ➢Microsoft Windows Server 2008 R2 已訂定____條例外管理項目 ➢Microsoft Windows Server 2012 R2 已訂定____條例外管理項目 ➢Microsoft Windows Server 2016 已訂定____條例外管理項目 ➢RedHat Enterprise Linux 5 已訂定____條例外管理項目 ■瀏覽器 ➢Microsoft Internet Explorer 8 已訂定____條例外管理項目 ➢Microsoft Internet Explorer 11 已訂定____條例外管理項目	

<table>
<tr><td></td><td>
➢Google Chrome 已訂定____條例外管理項目
➢Mozilla Firefox 已訂定____條例外管理項目
➢Mozilla Edge 已訂定____條例外管理項目
■網通設備
➢Juniper Firewall 已訂定____條例外管理項目
➢Fortinet Fortigate 已訂定____條例外管理項目
➢Cisco Firewall 已訂定____條例外管理項目
➢無線網路 已訂定____條例外管理項目
■應用程式
➢Exchange Server 2013 已訂定____條例外管理項目
➢Microsoft IIS 8.5 已訂定____條例外管理項目
(例外管理項目請列於 4.3)
□否(請跳至 4.4)
</td></tr>
<tr><td>4.3</td><td>
4.3.1 Windows 7 例外管理清單 ※項次不足請自行增加
<table>
<tr><th>項次</th><th>CCE-ID</th><th>原則設定名稱</th><th>GCB 建議值</th><th>機關設定值</th><th>變更事由</th><th>配套措施</th><th>適用範圍</th></tr>
<tr><td>範例</td><td>CCE-9193-4</td><td>密碼最長使用期限</td><td>90 天以下</td><td>180 天</td><td>依 ISMS 規範辦理</td><td>增加密碼長度並要求需符合密碼複雜度，提升安全性</td><td>全機關</td></tr>
<tr><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
4.3.2 Windows 8.1 例外管理清單 ※項次不足請自行增加
<table>
<tr><th>項次</th><th>CCE-ID</th><th>原則設定名稱</th><th>GCB 建議值</th><th>機關設定值</th><th>變更事由</th><th>配套措施</th><th>適用範圍</th></tr>
<tr><td>範例</td><td>CCE-34907-6</td><td>密碼最長使用期限</td><td>90 天以下</td><td>180 天</td><td>依 ISMS 規範辦理</td><td>增加密碼長度並要求需符合</td><td>全機關</td></tr>
</table>
</td></tr>
</table>

							密碼複雜度，提升安全性	
	1							
	2							
	3							
	4.3.3 Windows 10 例外管理清單 ※項次不足請自行增加							
	項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
	範例	CCE-43535-4	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
	1							
	2							
	3							
	4.3.4 Windows Server 2008 R2 例外管理清單 ※項次不足請自行增加							
	項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
	範例	CCE-10562-7	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
	1							
	2							

3							

4.3.5 Windows Server 2012 R2 例外管理清單　※項次不足請自行增加

項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	CCE-37167-4	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
1							
2							
3							

4.3.6 Windows Server 2016 例外管理清單　※項次不足請自行增加

項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
1							
2							
3							

4.3.7 RedHat Enterprise Linux 5 例外管理清單　※項次不足請自行增加

項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
1							
2							
3							

4.3.8 Internet Explorer 8 例外管理清單　※項次不足請自行增加

項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	CCE-10052-9	即使簽章無效也允許執行或安裝軟體	啟用	停用	導致會計系統線上報表無法列印使用	以受信任網站方式進行限制	會計室
1							
2							
3							

4.3.9 Internet Explorer 11 例外管理清單　※項次不足請自行增加

項次	CCE-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	CCE-32251-1	即使簽章無效也允許執行或安裝軟體	停用	啟用	導致會計系統線上報表無法列印使用	以受信任網站方式進行限制	會計室
1							
2							
3							

4.3.10 Google Chrome 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	設定擴充功能安裝黑名單	啟用	停用	(機關系統)需使用 Chrome 的多憑證安控模組擴充套件	針對允許使用的擴充功能進行管控	全機關
1						
2						
3						

4.3.11 Mozilla Firefox 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	啟用自動下載更新與安裝	true	false	為避免資產盤點問題，不允許自動下載更新與安裝	由資訊室統一進行版本更新派送	全機關
1						
2						
3						

4.3.12 Mozilla Edge 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
1						
2						
3						

4.3.13 Juniper Firewall 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	密碼需要最少 4 種不同的字元符號	設置 4 種密碼複雜組合	設置 2 種密碼複雜組合	經內部審核流程決議調整密碼複雜度為小寫英文字母及數字	將密碼長度限制 8 字元調整為 12 字元，以提升安全性	全機關 Juniper Firewall 設備
1						
2						
3						

4.3.14 Fortinet Fortigate 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	密碼最長使用期限	90 天	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關 Fortinet Fortigate 設備
1						
2						
3						

4.3.15 Cisco Firewall 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍

4.3.16 無線網路 例外管理清單　※項次不足請自行增加

項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	變更出廠預設值的密碼內容	12 字元以上	8 個字元以上	依據 ISMS 規定辦理	規範密碼需符合複雜性要求，提升安全性	全機關無線網路設備
1						
2						
3						

4.3.17 Exchange Server 2013 例外管理清單　※項次不足請自行增加

	項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
	範例	密碼到期期限	90 天以上	180 天以上	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關 Exchange Server 2013 設備
	1						
	2						
	3						
	4.3.18 Microsoft IIS 8.5 例外管理清單 ※項次不足請自行增加						
	項次	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
	1						
	2						
	3						
5.網路惡意活動檢視-惡意中繼站連線阻擋檢測							
5.1	是否可取得技服中心所公布之惡意中繼站名單?	□是， ■技服中心惡意中繼站名單取得方式： □從「國家資通安全通報應變網站」下載 □上級機關提供 □廠商提供 □其他：_____ ■最近收到名單日期：____年___月___日 □否					
5.2	是否部署技服中心所公布之惡意中繼站名單?	□是， ■部署週期： □每天 □每週 □每月 □其他：_____					

		■最近一次部署日期：____年____月____日 □否
5.3	對外連線	■　　網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____ ■　　網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____ ■　　網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____ ■　　網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____ ■　　網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____
6. 目錄伺服器安全防護檢測		
6.1	是否建置目錄伺服器?	□是 □否(請跳至 7.1)
6.2	目錄伺服器之作業系統版本?	□Windows Server 2003_____台 □Windows Server 2008_____台 □Windows Server 2008 R2_____台

		□Windows Server 2012_____台 □Windows Server 2012 R2_____台 □Windows Server 2016_____台 □Windows Server 2019_____台 □其他：_____
6.3	目錄伺服器防毒軟體病毒碼是否有更新政策?	□是， ■政策文件名稱：_____更新方式： □集中管控、派送(如防毒軟體中控台) □使用者手動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：____年___月____日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
6.4	目錄伺服器作業系統與微軟應用程式之相關修補程式是否有更新政策?	□是， ■政策文件名稱：_____ ■更新來源： □微軟更新伺服器 □機關內部 WSUS 伺服器 □其他：_____ ■更新方式： □使用者手動下載與更新 □自動下載，使用者決定是否更新 □自動下載，設定排程安裝更新 □自動下載，自動更新 □其他：_____

		■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否

7.網路架構檢測-服務主機資訊調查　※項次不足請自行增加

編號	服務主機類型	無此類型主機	項次	IP	OS 版本
範例 1	目錄伺服器	☑			
範例 2	目錄伺服器	□	1	10.10.10.1	Windows Server 2008 R2
			2	10.10.10.2	Windows Server 2012 R2
			3	10.10.10.3	Windows Server 2012
7.1	目錄伺服器	□	1		
			2		
7.2	內部 Mail Server	□	1		
			2		
7.3	外部 Mail Server	□	1		
			2		
7.4	內部 DNS Server	□	1		
			2		
7.5	外部 DNS Server	□	1		
			2		
7.6	WSUS Server	□	1		
			2		
7.7	防毒伺服器	□	1		

			2		
8.網路架構檢測-防護主機資訊調查　※項次不足請自行增加					
編號	防護主機類型	無此類型主機/無部署	項次	設備型號/類型	IP
範例 1	核心資通系統前端是否有 WAF 設備	☑			
範例 2	核心資通系統前端是否有 WAF 設備	☐	1	iMperva X2010	192.168.1.1
			2	iMperva X2010	192.168.1.2
範例 3	惡意中繼站 IP 部署位置	☐	1	防火牆 1	192.168.1.3
			2	防火牆 2	192.168.1.4
8.1	核心資通系統前端是否有 WAF 設備	☐	1		
			2		
8.2	核心資通系統前端是否有 IPS 設備	☐	1		
			2		
8.3	惡意中繼站 IP 部署位置	☐	1		
			2		
8.4	惡意中繼站 DN 部署位置	☐	1		
			2		
9.網路架構檢測-核心網路設備資訊調查　※項次不足請自行增加					
編號	網路設備類型	無此類型設備	項次	設備型號	IP
範例 1	對外線路閘道器	☑			

範例 2	防火牆	□	1	FG-1000D	10.10.10.1
			2	FG-1000D	10.10.10.2
9.1	對外線路閘道器	□	1		
			2		
9.2	防火牆	□	1		
			2		
9.3	核心交換器	□	1		
			2		

10.網路架構檢測-線路資訊調查　※項次不足請自行增加		
10.1	對外線路	(1) ISP 名稱：_____， (如:GSN Internet) 配發 IP：_____ (2) ISP 名稱：_____， 配發 IP：_____ (3) ISP 名稱：_____， 配發 IP：_____ (4) ISP 名稱：_____， 配發 IP：_____
10.2	是否與其他機關資料交換	□是， ■機關名稱：_____ ■ISP 名稱：_____ (如:GSN VPN) □否

11.網路架構檢測-網段資訊調查　※項次不足請自行增加				
編號	項目	無此網段	項次	網段 IP
範例 1	是否有網路管理人員網段	☑		
範例 2	是否有網路管理人員網段	☐	1	192.168.1.1-20
			2	192.168.2.0/24
11.1	是否有網路管理人員網段	☐	1	
			2	
11.2	是否有系統管理人員網段	☐	1	
			2	
11.3	是否有資料庫管理人員網段	☐	1	
			2	
11.4	是否有程式開發人員網段	☐	1	
			2	
11.5	是否有系統主機開發、測試網段	☐	1	
			2	
11.6	是否有虛擬私有網路(VPN)網段	☐	1	
			2	
11.7	是否有實體隔離網段	☐	1	
			2	
11.8	是否有網路設備網段	☐	1	
			2	

12.網路架構檢測-使用者電腦網段配置(User Farm 網段) ※項次不足請自行增加			
項次	IP 網段	使用處室	說明

範例 1	192.168.0.0/24	全機關	全機關使用同一網段 IP，未針對處室進行 VLAN 劃分
範例 2	10.0.1.0/24	資訊處	資訊處專屬網段
範例 3	10.0.2.0/24	人事室	10.0.2.1~10.0.2.200 為使用者電腦 IP，10.0.2.201 後為網路印表機等設備 IP
1			
2			
3			
4			
5			

13. 物聯網設備檢測　※項次不足請自行增加

※請填覆機關內所有的「網路印表機」、「門禁設備」、「網路攝影機」、「無線網路基地台/無線路由器」、「環控系統」五類設備，項次不足請自行增加，若無某類型設備時，則不需填覆該類型設備

※檢測標的為下列可直接使用 RJ45 進行連線之設備:

- 網路印表機：提供紙張輸出功能 (範例:印表機、多功能事務機、影印機等)
- 網路攝影機：提供影像錄製功能 (範例:攝影機)
- 門禁設備：提供門禁開關功能 (範例:指紋機、指掌靜脈機、門禁卡機等)
- 無線網路基地台/無線路由器：提供無線網路分享功能 (範例:無線網路基地台、無線路由器)
- 環控系統：提供監控機房溫度或濕度功能 (範例:機房溫度監控伺服器)

編號	類別	無此類別設備	項次	設備名稱	網址（內部 IP）	廠牌型號/作業系統	放置位置
範例 1	網路印表機	□	1	HP 網路印表機	192.168.5.101	HP LaserJet 4300	資訊處 5 樓辦公室
			2	HP 網路印表機	192.168.5.102	HP LaserJet 4400	資訊處 6 樓辦公室
			3	HP 網路印表機	192.168.5.103	HP LaserJet 4500	資訊處 7 樓辦公室

	門禁設備	□	1	怡群科技門禁卡機	192.168.20.11	怡群科技 Bic-301	人事室 1 樓辦公室
			2	怡群科技門禁卡機	192.168.20.12	怡群科技 Bic-302	人事室 2 樓辦公室
	網路攝影機	□	1	AXIS 網路攝影機	192.168.10.11	AXIS P1354	資訊處 6 樓機房
			2	AXIS 網路攝影機	192.168.10.12	AXIS M1033_W	1 樓電梯口
			3	AXIS 網路攝影機	192.168.10.13	AXIS Q1635	2 樓電梯口
	無線網路基地台/無線路由器	□	1	ASUS 無線路由器	192.168.0.1	ASUS RT-AC86U	第 1 會議室
			2	ASUS 無線路由器	192.168.0.2	ASUS RT-AC53	第 2 會議室
	環控系統	□	1	Advantech 水位計伺服器	192.168.140.55	Advantech WebAccess ver 2.1	資訊處 6 樓機房
範例 2	網路印表機	□	1	HP 網路印表機	192.168.5.101	HP LaserJet 4300	資訊處 5 樓辦公室
			2	HP 網路印表機	192.168.5.102	HP LaserJet 4400	資訊處 6 樓辦公室
			3	HP 網路印表機	192.168.5.103	HP LaserJet 4500	資訊處 7 樓辦公室
			4	HP 網路印表機	192.168.5.104	HP LaserJet 4600	資訊處 8 樓辦公室
			5	HP 網路印表機	192.168.5.105	HP LaserJet 4700	資訊處 9 樓辦公室

			6	HP 網路印表機	192.168.5.106	HP LaserJet 4800	資訊處 10 樓辦公室
	門禁設備	■	1				
	網路攝影機	□	1	AXIS 網路攝影機	192.168.10.11	AXIS P1354	資訊處 6 樓機房
			2	AXIS 網路攝影機	192.168.10.12	AXIS M1033_W	1 樓電梯口
			3	AXIS 網路攝影機	192.168.10.13	AXIS Q1635	2 樓電梯口
	無線網路基地台/無線路由器	□	1	D-link 無線路由器	192.168.0.1	D-link AC3900	貴賓室
	環控系統	■	1				
13.1	網路印表機	□	1				
			2				
			3				
13.2	門禁設備	□	1				
			2				
			3				
13.3	網路攝影機	□	1				
			2				
			3				
13.4	無線網路基地台/無線路由器	□	1				
			2				
			3				

13.5	環控系統	□	1				
			2				
			3				

附件四、核心資通系統調查表

填表日期：　　年　月　日

1.　資通系統基本資訊	
1.1 系統名稱	
1.2 系統簡介	
1.3 是否含有個資 （可複選）	□含一般個資，個資檔案類型：_____ □含特種個資，個資檔案類型：_____ □無個資
1.4 系統來源	□自行開發 □委外開發，廠商名稱：_____ □其他：_____
1.5 防護需求等級	□普　□中　□高
1.6 防護基準實施情形	請填寫附表一
1.7 系統性質	□網站 □本地端程式 □資料庫系統(非應用系統) □其他：_____
1.8 系統使用者	□為民服務(提供一般民眾/學生使用) □內部使用(僅供機關內部同仁/教職員使用) □其他：
1.9 安全性檢測情形 （可複選）	□無 □滲透測試，前次掃描日期：　年　月　日 □弱點掃描，前次掃描日期：　年　月　日 □源碼掃描，前次掃描日期：　年　月　日
1.10 系統連線經過之安全防護設備	□入侵偵測系統(IDS) □入侵防禦系統(IPS) □網頁應用程式防火牆(WAF) □防火牆(FW) □其他：

1.11Web 伺服器軟體	□無 □有， □Apache HTTP Server，版本：_____ □Apache Tomcat Server，版本：_____ □Microsoft IIS，版本：_____ □Nginx，版本：_____ □其他，名稱：_____，版本：_____
2.　資通系統存取管理	
2.1 系統登入介面/網址	□前台登入介面/網址：_____ □後台管理登入介面/網址： _____ □無 說明： ● 前台：指供使用者登入進行系統操作之介面。 ● 後台管理：指供管理者登入進行系統管理之介面。 ● 若系統無區分前、後台，即使用者與管理者使用相同登入介面時，請將此登入介面視為前台登入介面
2.2 系統前台登入介面連線方式	□單一簽入機制 □僅能透過外部網路連線至系統前台登入介面進行操作 □允許透過內部與外部網路連線至系統前台登入介面進行操作 □僅能透過內部網路連線至系統前台登入介面進行操作
2.3 系統前台登入介面登入方式	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.4 系統前台登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：
2.5 系統後台管理登入介面連線方式	□單一簽入機制 □僅能透過外部網路連線至系統後台管理登入介面進行操作 □允許透過內部與外部網路連線至系統後台管理登入介面進行操作 □僅能透過內部網路連線至系統後台管理登入介面進行操作

2.6 系統後台管理登入介面登入方式（可複選）	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.7 系統後台管理登入介面允許登入之使用者角色類別（可複選）	□一般使用者　□系統管理員 □業務承辦使用者　□其他：

3. 資通系統主機資訊　**※項次不足請自行增加**

類型（可複選）	主機名稱	IP 位址	作業系統及版本	服務應用程式	開啟連接埠(Port)	實體主機放置位置
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						

附表一、資通系統防護基準實施情形

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
存取控制	帳號管理	一、建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	普/中/高	□是，具備以下程序： □帳號申請程序 □帳號開通程序 □帳號停用程序 □帳號刪除程序 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、已逾期之臨時或緊急帳號應刪除或禁用。	中/高	□是，進行方式： □系統自動判別 □人工審查 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、資通系統閒置帳號應禁用。	中/高	□是，進行方式： □系統自動判別 □人工審查 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	中/高	□是，審核頻率為_____ □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。	高	□是， □系統於閒置_____分鐘後自動登出 □可使用期限為_____ □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		六、應依機關規定之情況及條件，使用資通系統。	高	□是， □限定系統使用時段 □限定 IP 位址來源 □其他方式：_____ □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
		七、監控資通系統帳號，如發現帳號違常使用時回報管理者。	高	□是，請於備註欄說明監控及通知機制為何 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	最小權限	一、採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。	中/高	□是，有依最小權限開放使用者存取權限 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	遠端存取	一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。	普/中/高	□是，組織有遠端存取 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、應監控資通系統遠端連線。	中/高	□是，請於備註欄說明監控方式 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、資通系統應採用加密機制。	中/高	□是， □HTTPS □SSH □VPN □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
稽核與可歸責性	稽核事件	一、依規定時間週期及紀錄留存政策，保留稽核紀錄(Audit Logs)。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。	普/中/高	□是，稽核以下事件： □帳號異動 □更改密碼 □登錄失敗 □資訊系統存取失敗 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、應稽核資通系統管理者帳號所執行之各項功能。	普/中/高	□是，請於備註欄說明稽核頻率 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、應定期審查稽核事件	中/高	□是，審查頻率約為_____ □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	稽核紀錄內容	一、資通系統產生之稽核紀錄(Audit Logs)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，並採用單一日誌紀錄機制，確保輸出格式之一致性。	普/中/高	□是，包含以下資訊： □事件類型 □發生時間 □發生位置 □任何與事件相關之使用者之身分識別 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、資通系統產生之稽核紀錄(Audit Logs)，應依需求納入其他相關資訊。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	稽核儲存容量	一、依據稽核紀錄(Audit Logs)儲存需	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
		求，配置稽核紀錄所需之儲存容量。			
	稽核處理失效之回應	一、資通系統於稽核處理失效時，應採取適當之行動。	普/中/高	□是， □關閉資通系統 □覆寫最舊的稽核紀錄 □停止產生稽核紀錄 □通知管理者進行故障排除作業 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	高	□是， □Email 通知 □簡訊通知 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	時戳及校時	一、資通系統應使用系統內部時鐘產生稽核紀錄(Audit Logs)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)。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。	中/高	□是， □依機關 NTP 校時伺服器進行校時 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	稽核資訊	一、對稽核紀錄(Audit Logs)之存取管理，僅限於有權限之使用者。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
	之保護	二、應運用雜湊或其他適當方式之完整性確保機制。	中/高	□是， □提供稽核資訊之雜湊值 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、定期備份稽核紀錄(Audit Logs)至與原稽核系統不同之實體系統。	高	□是， □手動備份 □自動備份至 Log 伺服器(如 syslog) □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
營運持續計畫	系統備份	一、訂定系統可容忍資料損失之時間要求。	普/中/高	□是，RPO 設定為_____ □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、執行系統源碼與資料備份。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、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。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、應將備份還原，作為營運持續計畫測試之一部分。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、應在與運作系統不同處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。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統備援	一、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。	中/高	□是，RTO 為_____ □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
		二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
識別與鑑別	內部使用者之識別與鑑別	一、資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、對帳號之網路或本機存取採取多重認證技術。	高	□是， □使用密碼 □使用黑/白名單限制存取來源 IP □使用自然人憑證或晶片卡 □使用生物特徵，如指紋 □其他：請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	身分驗證管理	一、使用預設密碼登入系統時，應於登入後要求立即變更。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、身分驗證相關資訊不以明文傳輸。	普/中/高	□是，使用_____加密傳輸機制 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	普/中/高	□是：帳戶鎖定機制為失敗達_____次，則_____分鐘內不得再登入 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
		四、基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	普/中/高	□是， □密碼長度_____個字元以上 □已要求密碼組成複雜度 □最短效期_____天 □最長效期_____天 □其他：請於備註欄說 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		七、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	中/高	□是， □採用驗證碼(CAPTCHA) □其他：請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		八、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	中/高	□是， □EMAIL 驗證連結 □簡訊驗證碼 □其他：請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	鑑別資訊回饋	一、資通系統應遮蔽鑑別過程中之資訊。	普/中/高	□是， □密碼輸入欄位預設以「*」顯示或不顯示 □使用憑證或 QR 碼進行鑑別 □其他：請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
				□否，請於備註欄說明原因 □不適用，請於備註欄說明	
	加密模組鑑別	一、資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	非內部使用者之識別與鑑別	一、資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
系統與服務獲得	系統發展生命週期需求階段	一、針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
	系統發展生命週期開發階段	一、應針對安全需求實作必要控制措施。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、應注意避免軟體常見漏洞及實作必要控制措施。	普/中/高	□是， □源碼已防範 OWASP 所公布之最新 OWASP TOP 10 安全風險 □已進行源碼檢測，並確認中、高風險弱點已修復 □其他控制措施:請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、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。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、執行「源碼掃描」安全檢測。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、具備系統嚴重錯誤之通知機制。	高	□是， □電子郵件 □簡訊 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統發展生命週期測試階段	一、執行「弱點掃描」安全檢測。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、執行「滲透測試」安全檢測。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
	系統發展生命週期部署與維運階段	一、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。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、資通系統相關軟體，不使用預設密碼。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、於系統發展生命週期之維運階段，須注意版本控制與變更管理。	中/高	【版本控制：如 git、svn 管理】 □是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
				【變更管理: 如應用系統維護紀錄單】 □是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統發展生命週期委外階段	一、資通系統開發如委外辦理，應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）納入委外契約。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	獲得程序	一、開發、測試及正式作業環境應為區隔。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統文件	一、應儲存與管理系統發展生命週期之相關文件。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
系統與通訊保護	傳輸之機密性與完整性	一、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。	高	□是， □使用 HTTPS，支援 SSLv3 以下、TLS v1.0 或 TLS 1.1 □使用 HTTPS，支援 TLS v1.2 以上 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、使用公開、國際機構驗證且未遭破解之演算法。	高	□是，未使用已被破解之加密演算法，如 RC4、3DES、MD5、SHA-1…等 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、支援演算法最大長度金鑰。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、加密金鑰或憑證週期性更換。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	資料儲存之安全	一、靜置資訊及相關具保護需求之機密資訊應加密儲存。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
系統與資	漏洞修復	一、系統之漏洞修復應測試有效性及潛在影響，並定期更新。	普/中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	措施內容	填寫等級	機關檢視結果	備註
訊完整性		二、定期確認資通系統相關漏洞修復之狀態。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	資通系統監控	一、發現資通系統有被入侵跡象時，應通報機關特定人員。	普/中/高	□是，依機關相關程序通報 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	軟體及資訊完整性	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。	中/高	□是 □否， □未檢查 □僅於前端網頁(如JavaScript)檢查 □不適用，請於備註欄說明	
		三、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。	中/高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、應定期執行軟體與資訊完整性檢查。	高	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

附件 5　技術檢測結果彙整表

1.1.使用者電腦安全檢測-使用者電腦弱點掃描			
高風險弱點總數			
中風險弱點總數			
項次	受測電腦 IP 位址	高風險弱點數量	中風險弱點數量
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			

45			
46			
47			
48			
49			
50			

1.2.使用者電腦安全檢測-使用者電腦安全防護檢測

項次	受測電腦IP位址	防毒軟體更新符合機關規定	安全性更新缺漏筆數	應用程式更新符合機關規定			是否有惡意程式
				Java	Adobe Reader	Adobe Flash Player	
1		□是 □否	筆	□是 □否	□是 □否	□是 □否	□是 □否
2		□是 □否	筆	□是 □否	□是 □否	□是 □否	□是 □否
3		□是 □否	筆	□是 □否	□是 □否	□是 □否	□是 □否
4		□是 □否	筆	□是 □否	□是 □否	□是 □否	□是 □否
5		□是 □否	筆	□是 □否	□是 □否	□是 □否	□是 □否

2.惡意中繼站連線阻擋檢測

惡意中繼站阻擋率	_____%

項次	網段未阻擋惡意中繼站名單	網段未阻擋惡意中繼站名單	網段未阻擋惡意中繼站名單	網段未阻擋惡意中繼站名單
1				
2				
3				
4				

5				

3.1.核心資通系統安全檢測-核心資通系統內網滲透測試					
高風險弱點總數					
中風險弱點總數					
項次	系統	弱點名稱	風險等級	弱點說明	改善建議
1					
2					
3					
4					
5					

3.2.核心資通系統安全檢測-核心資通系統防護基準檢測			
系統	防護需求等級	不符合總數	系統防護不符合項目

4.網路架構檢測			
高風險弱點總數			
中風險弱點總數			
低風險弱點總數			
建議風險弱點總數			
項次	風險說明	風險等級	改善建議
1			
2			
3			
4			

5			

5.目錄伺服器安全防護檢測			
IP	防毒軟體更新符合機關規定	安全性更新缺漏筆數	是否有惡意程式
	□是 □否	筆	□是 □否

6.物聯網設備安全檢測					
高風險弱點總數					
中風險弱點總數					
項次	設備名稱	弱點名稱	風險等級	弱點說明	改善建議
1					
2					
3					
4					
5					

7.1 組態設定安全防護檢測-作業系統類			
項次	受測電腦 IP	受測電腦類型	組態設定不符合機關規定總數
1		□使用者電腦 □伺服器主機	筆
2		□使用者電腦 □伺服器主機	筆
3		□使用者電腦 □伺服器主機	筆
4		□使用者電腦 □伺服器主機	筆

5		□使用者電腦 □伺服器主機	筆
6		目錄伺服器	筆
7.2 組態設定安全防護檢測-瀏覽器類			
項次	受測電腦 IP	受測瀏覽器類型	組態設定不符合機關規定總數
1		IE8/IE11/Google Chrome/Mozilla Firefox/Microsoft Edge	筆
2		IE8/IE11/Google Chrome/Mozilla Firefox/Microsoft Edge	筆
3		IE8/IE11/Google Chrome/Mozilla Firefox/Microsoft Edge	筆
4		IE8/IE11/Google Chrome/Mozilla Firefox/Microsoft Edge	筆
5		IE8/IE11/Google Chrome/Mozilla Firefox/Microsoft Edge	筆
7.3 組態設定安全防護檢測-網通設備類			
項次	受測設備 IP	受測設備類型	組態設定不符合機關規定總數
1		Juniper Firewall	筆
2		Fortinet Fortigate	筆
3		Cisco Firewall	筆
4		Wireless	筆
7.4 組態設定安全防護檢測-應用程式類			
項次	受測電腦 IP	受測應用程式類型	組態設定不符合機關規定總數

1		Exchange Server 2013	筆
2		Microsoft IIS 8.5	筆

附件 6-2　技術檢測評分表（國立大專校院）

受稽機關(構)	
技術檢測日期	年　月　日至　月　日

項次	技術檢測項目	技術檢測子項	檢測範圍	分數	評分
1	使用者電腦安全檢測	使用者電腦弱點掃描	50 台使用者電腦	10	
		使用者電腦安全防護檢測	5 台使用者電腦	20	
2	網路惡意活動檢測	惡意中繼站連線阻擋檢測	年　月　日 中繼站名單	5	
3	核心資通系統安全檢測	核心資通系統內網滲透測試	1 個核心資通系統	20	
		核心資通系統防護基準檢測		5	
4	網路架構檢測	網路架構檢測	機關網路架構	15	
5	目錄伺服器安全檢測	目錄伺服器安全防護檢測	1 台目錄伺服器	10	
6	物聯網設備安全檢測	網路印表機檢測	5 台物聯網設備	10	
		門禁設備檢測			
		網路攝影機檢測			
		無線網路基地台/無線路由器檢測			
		環控系統檢測			
7	組態設定安全檢測	作業系統組態檢測	5 台伺服器主機	5	
		瀏覽器組態檢測			
		網通設備組態檢測			
		應用程式組態檢測			
得　分(滿分 100)分)					

技術檢測結果摘要：

執行人員：＿＿＿＿＿＿、＿＿＿＿＿＿、＿＿＿＿＿＿、＿＿＿＿＿＿、

＿＿＿＿＿＿、＿＿＿＿＿＿

技術檢測項目配分說明

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">使用者電腦安全檢測</td><td>使用者電腦弱點掃描</td><td>50 台使用者電腦
其中包含：
1.資訊單位(電算中心)-管理行政人員 20 台
2.行政單位-行政人員 10 台
3.教學單位-系所行政人員 10 台
4.計畫單位-計畫行政人員 10 台</td><td>10</td><td>計算規則：
• 每個高風險弱點扣 2 分
• 每個中風險弱點扣 1 分
計算公式：
本項得分 = 10 – [高風險弱點數] * 2 – [中風險弱點數] * 1
(最低扣至 0 分)</td></tr>
<tr><td>使用者電腦安全防護檢測</td><td>5 台使用者電腦
其中包含：
1.資訊單位(電算中心)-管理行政人員 2 台
2.行政單位-行政人員 1 台
3.教學單位-系所行政人員 1 台
4.計畫單位-計畫行政人員 1 台</td><td>20</td><td>計算規則：
分為防毒軟體病毒碼更新、作業系統安全性更新、應用軟體安全性更新、惡意程式檢測等 4 個項目，每項目 5 分。
<table><tr><th>得分</th><th>不符合率(X)區間</th></tr><tr><td>5</td><td>0%</td></tr><tr><td>4</td><td>0% < X≦25%</td></tr><tr><td>3</td><td>25% < X≦50%</td></tr><tr><td>2</td><td>50% < X≦75%</td></tr><tr><td>1</td><td>75% < X < 100%</td></tr><tr><td>0</td><td>100%</td></tr></table>計算公式：
(1)計算不符合率(X)
• 防毒軟體病毒碼未更新率：
X = (防毒軟體病毒碼未更新(或未安裝)電腦數 / 受測電腦總數) * 100%
• 作業系統安全性未更新率：</td></tr>
</table>

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>X =(作業系統未安全性更新電腦數 / 受測電腦總數) * 100%
• 應用軟體安全性未更新率：
X =(應用軟體未安全性更新電腦數 / 受測電腦總數) * 100%
• 惡意程式感染率：
X =(具惡意程式電腦數 / 受測電腦總數) * 100%
(2)套用不符合率(X)區間計分，
本項得分= [防毒軟體病毒碼更新得分] + [作業系統安全性更新得分] + [應用軟體安全性更新得分] + [惡意程式檢測]</td></tr>
<tr><td>2</td><td>網路惡意活動檢測</td><td>惡意中繼站連線阻擋檢測</td><td>中繼站名單
其中包含：
1.資訊單位(電算中心)網段
2.行政單位網段
3.教學單位網段
4.計畫單位網段</td><td>5</td><td>計算規則：
<table><tr><th>得分</th><th>惡意中繼站未阻擋率(Z)</th></tr><tr><td>5</td><td>0%</td></tr><tr><td>4</td><td>0% < Z≦25%</td></tr><tr><td>3</td><td>25% < Z≦50%</td></tr><tr><td>2</td><td>50% < Z≦75%</td></tr><tr><td>1</td><td>75% < Z < 100%</td></tr><tr><td>0</td><td>100%</td></tr></table>• 資訊單位(電算中心)網段惡意中繼站未阻擋率：
X = (未阻擋惡意中繼站數 / 檢測惡意中繼站總數)*100%
• 行政單位網段惡意中繼站未阻擋率：
Y = (未阻擋惡意中繼站數 / 檢測惡意中繼站總數)*100%
• 教學單位網段惡意中繼站未阻擋率：
A = (未阻擋惡意中繼站數 / 檢測惡意中繼站總數)*100%</td></tr>
</table>

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>• 計畫單位網段惡意中繼站未阻擋率：B = (未阻擋惡意中繼站數 / 檢測惡意中繼站總數)*100%
• 不符合率(Z) = (X + Y + A + B) / 2，若無計畫單位網段，則不計 B，不符合率(Z) = (X + Y + A) / 2，以此類推
計算公式：
本項得分=惡意中繼站未阻擋率(Z)對應之得分</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">核心資通系統安全檢測</td><td>核心資通系統內網滲透測試</td><td rowspan="2">1 個核心資通系統</td><td>20</td><td>計算規則：
• 每個高風險弱點扣 2 分
• 每個中風險弱點扣 1 分
計算公式：
本項得分 = 20 – (高風險弱點數 * 2)– (中風險弱點數 * 1)
(最低扣至 0 分)</td></tr>
<tr><td>核心資通系統防護基準檢測</td><td>5</td><td>計算規則：
<table><tr><th>得分</th><th>資通系統防護基準不符合率(X)</th></tr><tr><td>5</td><td>0%</td></tr><tr><td>4</td><td>0% < X≦25%</td></tr><tr><td>3</td><td>25% < X≦50%</td></tr><tr><td>2</td><td>50% < X≦75%</td></tr><tr><td>1</td><td>75% < X< 100%</td></tr><tr><td>0</td><td>100%</td></tr></table>• X=(資通系統防護基準不符合項數/資通系統防護基準檢測總數)*100%
計算公式：
本項得分 = 資通系統防護基準不符合</td></tr>
</table>

項次	檢測項目	檢測子項	檢測範圍	配分	配分計算方式
					率(X)對應之得分
4	網路架構檢測	網路架構檢測	機關網路架構 其中包含： 1.資訊單位(電算中心)-網路架構 2.行政單位-網路架構 3.教學單位-網路架構 4.計畫單位-網路架構	15	**計算規則：** • 每個高風險弱點扣 2 分 • 每個中風險弱點扣 1 分 **計算公式：** 本項得分= 15 – [高風險弱點數] * 2 – [中風險弱點數] * 1 (最低扣至 0 分)
5	目錄伺服器安全檢測	目錄伺服器安全防護檢測	1 台目錄伺服器	10	**計算規則：** • 防毒軟體病毒碼更新得分 = 目錄伺服器防毒軟體已安裝且病毒碼已更新則得 4 分 • 安全性更新得分 = 目錄伺服器安全性更新皆已安裝則得 4 分 • 惡意程式檢測得分 = 目錄伺服器未發現惡意程式則得 2 分 **計算公式：** 本項得分 = 防毒軟體病毒碼更新得分 + 安全性更新得分 + 惡意程式檢測得分
6	物聯網設備安全檢測	物聯網設備安全檢測	5 台物聯網設備(網路印表機、門禁設備、網路攝影機、無線網路基地台(AP)/無線路由器、環控系統) 其中包含：	10	**計算規則：** • 每個高風險弱點扣 2 分 • 每個中風險弱點扣 1 分 **計算公式：** 本項得分= 10 – [高風險弱點數] * 2 – [中風險弱點數] * 1 (最低扣至 0 分)

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td>1.資訊單位(電算中心)-2 台
2.行政單位-1 台
3.教學單位-1 台
4.計畫單位-1 台</td><td></td><td></td></tr>
<tr><td>7</td><td>組態設定安全檢測</td><td>組態設定安全檢測</td><td>5 台伺服器主機
其中包含：
1.資訊單位(電算中心)-2 台
2.行政單位-1 台
3.教學單位-1 台
4.計畫單位-1 台</td><td>5</td><td>計算規則：
<table><tr><th>得分</th><th>組態設定項目不符合率(X)</th></tr><tr><td>5</td><td>0%</td></tr><tr><td>4</td><td>0% < X≦25%</td></tr><tr><td>3</td><td>25% < X≦50%</td></tr><tr><td>2</td><td>50% < X≦75%</td></tr><tr><td>1</td><td>75% < X <100%</td></tr><tr><td>0</td><td>100%</td></tr></table>• X=(組態設定不符合項總數/組態設定檢測總數)*100%
計算公式：
本項得分=組態設定項目不符合率(X)對應之得分</td></tr>
<tr><td colspan="4">得　分　總　計
(滿分 100 分)</td><td></td><td>計算公式：
得分總計= (檢測項目總得分/檢測項目總分)*100
• 若為無目錄伺服器環境，則不計第 5 項 [目錄伺服器安全檢測]，得分總計= (檢測項目 1~4、6~7 項總得分 / 95) * 100</td></tr>
</table>

實地稽核評分表

頁次：1

受稽機關：＿＿＿＿＿＿＿＿＿＿＿＿日期：　/　/

稽核構面	稽核項目	評分
策略面	**一、核心業務及其重要性(10 分)：** 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
	二、資通安全政策及推動組織(10 分)： 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
	三、專責人力及經費配置(10 分)： 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
管理面	**四、資訊及資通系統盤點及風險評估(10 分)：** 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
	五、資通系統或服務委外辦理之管理措施(10 分)： 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
	六、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(10 分)： 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
技術面	**七、資通安全防護及控制措施(20 分)：** 優(20-17 分)、良(16-13 分)、佳(12-9 分)、可(8 分)、待改進(7 分(含)以下)	
	八、資通系統發展及維護安全(10 分)： 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
	九、資通安全事件通報應變及情資評估因應(10 分)： 優(10-9 分)、良(8-7 分)、佳(6-5 分)、可(4 分)、待改進(3 分(含)以下)	
得　　分(滿分 100 分)		

法遵符合情形：

待改善或建議事項：

委員簽名：＿＿＿＿＿＿＿＿＿＿