109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說明會

資安技術檢核

計畫辦公室：教育體系資安檢核技術服務中心

執行單位：國立交通大學 資訊技術服務中心

報告人(協同主持人)：交大資訊中心 副主任 高義智 博士

2020/08

目錄
CONTENT

[01]

教育體系因應資通安全管理法之作業說明

教育體系因應資通安全管理法之作業說明–(1/4)

資通安全管理法

- 總統107年6月6日公布**資通安全管理法**。
- 行政院107年11月21日發布相關子法：
  - 資通安全管理法施行細則
  - 資通安全責任等級分級辦法
  - 資通安全事件通報及應變辦法
  - 特定非公務機關資通安全維護計畫實施情形稽核辦法
  - 資通安全情資分享辦法
  - 公務機關所屬人員資通安全事項獎懲辦法
- 行政院107年12月05日函定自**108年1月1日施行**。

教育體系因應資通安全管理法之作業說明–(2/4)

➢ 單位等級應辦項目–技術面

★依照資通安全責任等級分級辦法第11條訂定。

辦理項目	辦理內容	A	B	C
安全性檢測 全部核心資通系統	網站安全弱點檢測	每年2次	每年1次	每2年1次
	系統滲透測試	每年1次	每2年1次	
資通安全健診	網路架構檢視、網路惡意活動檢視、使用者電腦惡意活動檢視、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	每年1次	每2年1次	
資通安全威脅偵測管理機制	完成威脅偵測機制建置，並持續維運	1年內		×
	依行政院指定方式提交監控管理資料	○	○	×
資通安全防護 (啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內		
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆(WAF)	1年內		×
	APT攻擊防禦	1年內	×	
政府組態基準 (GCB)	依主管機關公告之項目，完成GCB導入作業，並持續維運(公務機關)	1年內		×

教育體系因應資通安全管理法之作業說明–(3/4)

稽核依據

- **資通安全管理法**
  - 第13條第1項
    - 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。(e.g.國立大專院校、部屬機關)
  - 第17條第3項
    - 中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。
- **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。
    - 本部得每年擇定特定非公務機關，以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。(e.g.教育部捐助之財團法人)

教育體系因應資通安全管理法之作業說明–(4/4)

稽核準則

- 資通安全管理法及其子法。
- CNS 27001:2014或ISO 27001:2013等資訊安全管理系統標準。
- 受稽機關之資通安全維護計畫。
- 個人資料保護法及其子法。
- 教育體系資通安全暨個人資料管理規範。
- 臺灣學術網路管理規範。
- 其他適用之行政院或本部資通安全政策或規範。

[02]

資安檢核技術服務簡介

資安檢核技術服務簡介 – 背景

自108年5月起教育部委由**國立交通大學**執行**教育體系資安檢核技術服務計畫**，成立「**教育體系資安檢核技術服務中心**」，針對資安技術面為推動方向，配合辦理教育機關(構)資通安全檢測項目之檢核，並培育專業資安技術人才，強化網路資安進階及資訊管理鑑識技術能力，協助全國教育體系機關(構)進行資安檢核作業。

資安檢核技術服務簡介 – 作業模式

教育體系資通安全稽核作業

[03]

資安檢核作業說明

資安檢核作業說明–(1/14)

檢核方式

- 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：

	技術檢測	實地稽核
公務機關（部屬機關(構)、國立大專校院）	V	V
特定非公務機關（本部捐助之財團法人）	X	V

資安檢核作業說明–(2/14)

檢核作業流程–機關自評

- 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)。

檢核作業流程–技術檢測結果

- 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核人員提交「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。

資安檢核作業說明–(3/14)

➢ 檢核團隊

項目	檢核人員	人員配置	項目分工	人員總計
檢核團隊	高級技術檢核員(主導)	1名	統籌團隊運作及技術指導	6~8名
	副級、正級、高級技術檢核員	3~5名	根據檢核項目分成： - 網路惡意活動檢視 - 網路架構檢測 - 物聯網設備檢測 - 使用者電腦安全檢測 - 核心資訊系統安全檢測 - 網域主機安全防護檢測 - 組態設定安全檢測	
	佐級技術檢核員	2名	各項檢測協助與支援	

資安檢核作業說明–(4/14)

➢實地檢核

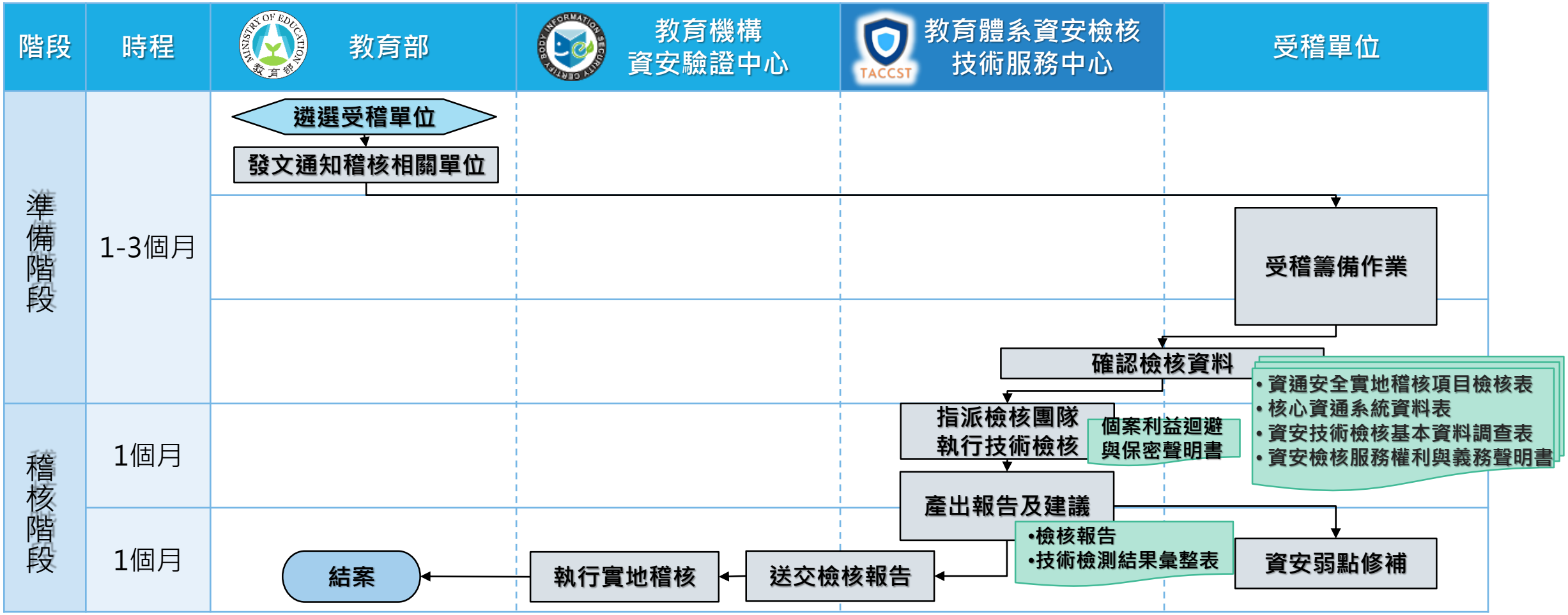
本年度配合教育部進行教育機關(構)資安稽核之技術檢核作業，說明實地檢核時程、七大檢測項目對應技能及工具，並於後續提供技術檢核報告。

Day 1 【實地檢核】	
時間	檢核內容
09:30 – 09:50	啟始會議
09:50 – 10:00	驗證範圍實體環境瀏覽
10:00 – 10:10	小組會議討論
10:10 – 12:00	【網路架構檢核】 【網路惡意活動檢核】 【使用者電腦安全檢核】
12:00 – 13:30	中午休息
13:30 – 15:30	【網路架構檢核】 【使用者電腦安全檢核】 【物聯網設備探測與檢核】
15:30 – 16:30	小組討論、檢核發現及報告彙整
17:00 – 17:30	檢核發現簡要說明

Day 2 【實地檢核】	
時間	檢核內容
09:30 – 12:00	【網路架構檢核】 【網域主機安全防護檢核】 【核心資通系統安全檢核】
12:30 – 13:30	中午休息
13:30 – 16:00	【網路惡意活動檢視】 【核心資通系統安全檢核】
16:00 – 16:30	小組討論、檢核發現及報告彙整
16:30 – 17:00	檢核發現簡要說明
17:00 – 17:30	總結會議(檢核發現說明)

資安檢核作業說明–(5/14)

➢ 作業流程概況–技術檢核



資安檢核作業說明–(6/14)

➢資安稽核之技術檢核項目配分方式–教育體系 部屬機關(構)

項次	檢測項目	子項目	配分	檢測範圍
1	使用者電腦安全	使用者電腦弱點掃描	10	50台使用者電腦
		使用者電腦安全防護檢測	20	5台使用者電腦
2	網路惡意活動	惡意中繼站連線阻擋檢測	5	最新中繼站名單
3	核心資通系統安全	核心資通系統內網滲透測試	20	1個核心資通系統
		核心資通系統防護基準檢測	5	
4	網路架構	網路架構檢測	10	機關網路架構
5	目錄伺服器安全	目錄伺服器安全防護檢核	5	1台目錄伺服器
6	物聯網設備	網路攝影機、門禁設備、網路印表機、無線AP/無線路由器、環控系統	10	5台物聯網設備
7	組態設定安全	作業系統組態、瀏覽器組態、網通設備組態、應用程式組態檢測	15	5台伺服器主機
合計			100	※若單位無該檢核項目，則將技術檢測分數依比例調整。

資安檢核作業說明–(7/14)

➢資安稽核之技術檢核項目範圍–國立大專院校

稽核範圍 [配分]

項次	檢測項目	子項目	配分	電算中心 (40%)	行政單位 (20%)	教學單位 (20%)	計畫單位 (20%)
1	使用者電腦安全	弱點掃描	10	管理人員 20台	行政人員 10台	系所人員 10台	計畫人員 10台
		安全防護	20	管理人員 2台	行政人員 1台	系所人員 1台	計畫人員 1台
2	網路惡意活動		5	單位網段	單位網段	單位網段	查看單位資料
3	核心資通系統安全	滲透測試	20	1個			
		防護基準	5				
4	網路架構		15	網路架構	網路架構	網路架構	網路架構
5	目錄伺服器安全		10	1台			
6	物聯網設備		10	2台	1台	1台	1台
7	組態設定安全		5	伺服器主機 2台	行政人員 1台	系所人員 1台	計畫人員 1台
合計			100	※若無該項目則將技術檢核分數依比例調整。			

資安檢核作業說明–(8/14)

➢資安稽核之技術檢核說明–(1/7)

項次	項目	子項目	執行方式
1	**使用者電腦安全檢測**	•使用者電腦弱點掃描	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**。
		•使用者電腦安全防護檢測	依弱點掃描結果之風險程度排序，**挑選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。

資安檢核作業說明–(9/14)

➢資安稽核之技術檢核說明–(2/7)

項次	項目	子項目	執行方式
2	**網路惡意活動檢視**	•惡意中繼站連線阻擋檢測	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，針對機關使用者網段及核心系統管理員網段進行檢測。

資安檢核作業說明–(10/14)

➢資安稽核之技術檢核說明–(3/7)

項次	項目	子項目	執行方式
3	**核心資通系統安全檢核**	•核心資通系統內網滲透測試	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。
		•核心資通系統防護基準檢測	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。

資安檢核作業說明–(11/14)

➢資安稽核之技術檢核說明–(4/7)

項次	項目	子項目	執行方式
4	**網路架構檢測**	•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。

資安檢核作業說明–(12/14)

➢資安稽核之技術檢核說明–(5/7)

項次	項目	子項目	執行方式
5	**網域主機安全防護檢測**	•防毒軟體檢測 •安全性更新檢視 •惡意程式檢測	透過實際檢測方式，針對機關之網域主機進行**防毒軟體、安全性修補程式更新及惡意程式檢測**。

資安檢核作業說明–(13/14)

➢資安稽核之技術檢核說明–(6/7)

項次	項目	子項目	執行方式
6	**物聯網設備檢測**	•網路攝影機檢測 •門禁系統檢測 •網路印表機檢測 •無線AP/路由器檢測 •環控系統檢測	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。

資安檢核作業說明–(14/14)

➢資安稽核之技術檢核說明–(7/7)

項次	項目	子項目	執行方式
7	**組態設定安全檢測**	•作業系統組態檢測 •瀏覽器組態檢測 •應用程式組態檢測 •網通設備組態檢測	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。

[04]

教育訓練說明

教育訓練說明–(1/2)

➢資安技術檢核訓練課程

本中心因應教育部辦理資安技術檢核人員之培訓，以增進教育部屬機關構資安技術能力。

基礎課程 40小時(線上)	核心技術課程 18小時	進階技術課程 18小時	線上測驗
資安健診	資安健診	資安進階技術與工具應用	資安技術實務測驗
弱點掃描	弱點掃描	資安進階實務演練 I	
滲透測試	滲透測試	資安進階實務演練 II	
資安鑑識	資安鑑識		
法律與管理			

理論 +工具應用 +實務演練

教育訓練說明–(2/2) ➢人員培訓說明

<table>
<tr><th colspan="3">項目 ＼ 身分</th><th>佐級技術檢核員</th><th>副級技術檢核員</th><th>正級技術檢核員</th><th>高級技術檢核員</th></tr>
<tr><td rowspan="4">具備條件</td><td rowspan="3">累計條件</td><td>參與檢核作業</td><td>通過資安檢核技術實務測驗</td><td>1次</td><td>3次</td><td>5次</td></tr>
<tr><td>完成檢核分項報告</td><td></td><td>1項</td><td>4項</td><td>7項</td></tr>
<tr><td>技術檢核點數</td><td></td><td>20點</td><td>50點</td><td>100點</td></tr>
<tr><td colspan="2">主導檢核作業資格</td><td></td><td></td><td></td><td>經高級技術檢核員評核通過。</td></tr>
<tr><td rowspan="2">頒證條件(期效3年)</td><td colspan="2">首次頒證</td><td rowspan="2">• 該身份不頒證</td><td colspan="2">• 完成技術檢核人員該階段之身份條件。</td><td rowspan="2">主導技術檢核作業至少3次</td></tr>
<tr><td colspan="2">重新頒證</td><td colspan="2">• 參與技術檢核至少3次。
• 技術檢核點數累計至少20點。
• 參與檢核交流研討會至少1次。</td></tr>
</table>

※七大檢核項目：

1. 使用者電腦安全檢測
2. 網路惡意活動檢視
3. 核心資通系統安全檢測
4. 網路架構檢測
5. 網域主機安全防護檢測
6. 物聯網設備檢測
7. 組態設定安全檢測

※點數累計方式：

完成技術檢核，其點數依CVE等資安弱點風險等級給予：

- 極高：20點(驗證漏洞並入侵)
- 高　：15 點(驗證漏洞)
- 中　：10點(驗證漏洞)
- 低　： 5 點(驗證漏洞)

Q&A

Thank you.

教育體系資安檢核技術服務中心：https://www.taccst.moe.edu.tw/