



教育部  
Ministry of Education

# 教育部113年度資通安全稽核 技術檢測 行前說明會

---

— 第一梯次 受稽單位 —

檢測時間：113年5~6月

# 大綱

1. 作業時程
2. 團隊介紹
3. 依據與目的
4. 作業說明
5. 檢測範圍
6. 技術檢測項目範圍及配分
7. 技術檢測項目
8. 配合事項
9. 技術檢測追蹤流程說明



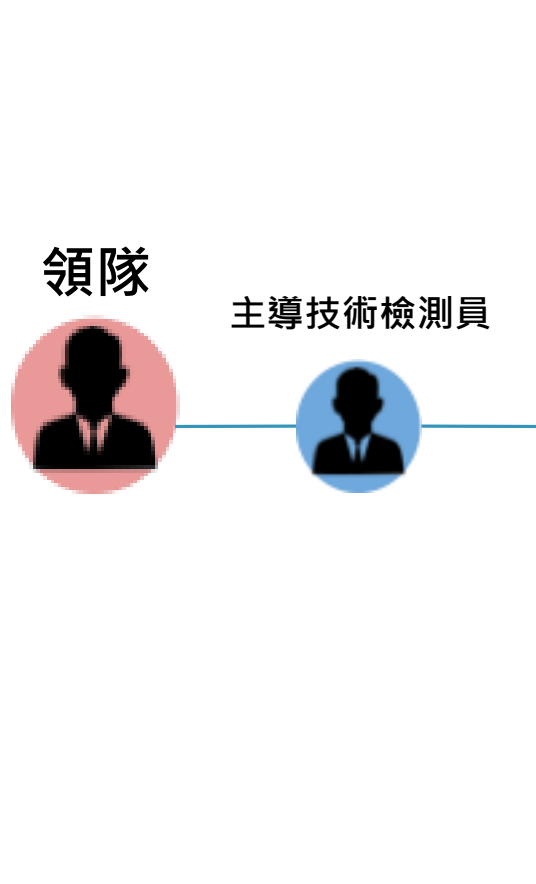
# 1. 作業時程 – 第一天

時間	工作項目
9:30 - 10:00	啟始會議： <ul style="list-style-type: none"><li>● 受稽代表致詞、介紹出席人員</li><li>● 技術檢測團隊領隊致詞、介紹技術檢測團隊</li><li>● 技術檢測作業說明(20分鐘) <b>[報告單位: 教育體系資安檢測技術服務中心(TACCST)]</b></li></ul>
10:00 - 10:10	檢測範圍實體環境瀏覽
10:10 - 10:30	檢測團隊檢測前意見交換 <b>[內部會議，請受檢方暫時離席]</b>
10:30 - 12:00	分組檢測
12:00 - 13:30	中午休息
13:30 - 16:00	分組檢測
16:00 - 17:00	檢測團隊意見交換

# 1. 作業時程 – 第二天

時間	工作項目
9:00 - 12:00	分組檢測
12:00 - 13:30	中午休息及彙整發現
13:30 - 15:00	分組檢測
15:00 - 16:00	檢測團隊意見交換、檢測發現及報告彙整
16:00 - 17:00	<b>總結會議：</b> <ul style="list-style-type: none"><li>● 受稽代表致詞</li><li>● 技術檢測團隊領隊致詞</li><li>● 技術檢測結果說明(20分鐘)</li></ul> <b>[報告單位: 教育體系資安檢測技術服務中心(TACCST)]</b>

## 2. 團隊介紹



技術檢測員



技術檢測員



技術檢測員



技術檢測員



技術檢測員



佐級技術檢測員



工作人員



工作人員



佐級技術檢測員



### 技術檢測員

- 主要執行技術檢測項目
- 提交稽核發現
- 撰寫項目報告書

### 佐級技術檢測員

- 協助核心資通系統安全檢測
- 協助物聯網安全檢測
- 檢測觀察作業

### 工作人員

- 協助執行技術檢測工具
- 協助檢測作業相關事宜

# 3. 依據與目的

## ○依據

- 資通安全管理法第13條第1項及第17條第3項。
- 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。

## ○目的

教育部為實施「教育部113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」，委由教育體系資安檢測技術服務中心 (TACCST) (以下稱本中心) 辦理資安稽核技術檢測作業。





## 4. 作業說明

- 第1組：本部所屬公務機關之今年度重點稽核對象。
- 第2組：第1組以外之受稽核對象。

### ①機關自評

- 受稽方填寫「資通安全實地稽核項目檢測表」、「受稽方現況調查表」、「技術檢測基本資料調查表」(第1組)及「核心資通系統調查表」(第1組)等作業表單。



### ②技術檢測

- 進行2至3天技術檢測（第1組適用）。
- 技術檢測結果作為實地稽核參考。



### ③實地稽核

- 由稽核領隊帶領稽核團隊進行實地稽核。



### ④獎勵及改善

- 對於各組別成績表現優良者，函請受基稽關行政獎勵及頒發獎狀。
- 函送資安稽核報告予受稽機關，請其就待改善事項研議因應作為及辦理時程。

## 5. 檢測範圍

---

- 檢測日期：113年6月6日(四)、6月7日(五)
- 檢測時間：上午9:00至下午17:00 (16:00閉幕會議；可依受檢單位調整)
- 受稽單位：國立中央大學
- 資通安全責任等級：B級
- 受稽範圍：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。



## 6. 技術檢測項目範圍及配分

### 網路安全

網路惡意活動檢測

網路架構檢測

### 系統安全

核心資通系統  
安全檢測

目錄伺服器安全檢測

組態設定安全檢測

資料庫安全檢測

### 端點安全

使用者電腦  
安全檢測

物聯網設備  
安全檢測

## 6. 技術檢測項目範圍及配分

項次	項目	子項目	配分	檢測計分範圍
1	使用者電腦安全檢測	弱點掃描	5	50臺
		安全防護	10	5-10臺
2	網路惡意活動檢視		5	1個Server farm網段、1個管理網段、3個User farm網段
3	核心資通系統安全檢測	滲透測試	15	全核心資通系統遴選至少2個（依檢測實施天數抽測）
		防護基準	10	
4	網路架構檢測		10	全單位
5	目錄伺服器安全檢測		10	1台
6	物聯網設備檢測		15	20臺（10臺單位提供清單、10臺內外部掃描結果）選5台
7	組態設定安全檢測		10	伺服器主機5台、使用者電腦5台
8	資料庫安全檢測		10	2個核心資料庫
9	準備作業配合度		倒扣，最多扣10分	應備文件及相關紀錄完整性
合計			100	※若無該項目則將技術檢測分數依比例調整。

# 7. 技術檢測項目





## 7.1 使用者電腦安全檢測 — a.弱點掃描

- 執行範圍：全單位
- 主要使用工具：Nmap、Nessus、Shodan
- 執行方式：
  - 本次檢測針對受檢單位進行全單位網段端口掃描(Portscan)，並依端口掃描結果，挑選可能存在較高風險之50台使用者電腦進行弱點掃描（VA）。

※若因特殊原因無法進行全單位網段端口掃描(Portscan)，將直接進行全單位網段弱點掃描（VA），並依單位比例挑選50台風險最高之使用者電腦列入計分。



## 7.1 使用者電腦安全檢測 — a.弱點掃描

- 計分範圍：使用者網段內之50台使用者電腦
- 計分方式（5分）
  - 計算規則
    - 每個高風險弱點扣 1 分
    - 每個中風險弱點扣 0.5 分
  - 計算公式
    - 本項得分 =  $5 - [\text{高風險弱點數}] * 1 - [\text{中風險弱點數}] * 0.5$  ※最低扣至 0 分。
  - 其它事項
    - 受稽機關應於檢測前提供全機關之使用者電腦清單(包含 IP 位址、單位名稱、人員姓名(可遮罩)、職稱、所在地點等資訊)。前述清單之完整性及正確性，列入準備作業配合度之計分範圍。



## 7.1 使用者電腦安全檢測 – b.安全防護

- 執行範圍：5-10台使用者電腦
- 主要使用工具：ProcessExplorer、ProcessMonitor、TCPView、Autoruns
- 執行方式
  - 再依弱點掃描結果，抽樣5-10台較高風險使用者電腦進行深度檢測，檢測項目主要為：
    - 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
    - 瀏覽器安全性更新
    - 惡意程式檢測
  - 其中作業系統安全性更新及應用軟體安全性更新部分，**若單位無定義將直接採用最新版本號列入評分。**



# 7.1 使用者電腦安全檢測 – b.安全防護

- 計分範圍：5-10台使用者電腦
- 計分方式（10分）
  - 計算規則
    - $X = \text{防毒軟體未更新(或未安裝)電腦數} + \text{安全性修補程式未更新電腦數} + \text{應用軟體(含瀏覽器、Java、Adobe Reader等)未更新電腦數} + \text{具惡意程式電腦數}$
    - 使用者電腦安全防護不符合率：
      - $Z = X / (\text{受測電腦台數} * 4) * 100\%$
  - 計算公式
    - 本項得分 = 使用者電腦安全防護不符合率(Z)對應之得分

得分	使用者電腦安全防護不符合率(Z)
10	0%
9	$0\% < X \leq 11\%$
8	$11\% < X \leq 22\%$
7	$22\% < X \leq 33\%$
6	$33\% < X \leq 44\%$
5	$44\% < X \leq 55\%$
4	$55\% < X \leq 66\%$
3	$66\% < X \leq 77\%$
2	$77\% < X \leq 88\%$
1	$88\% < X < 100\%$
0	100%



## 7.2 網路惡意活動檢測

- 執行範圍
  - 抽選共5個網段，含1個Server farm網段、1個管理網段（如網路管理/系統管理/程式開發等）、3個User farm網段。
- 使用工具：PingPlotter
- 執行方式
  - 檢測名單：國家資通安全研究院最新提供之惡意中繼站名單
  - 檢測標準：受測單位主機 traceroute 中繼站名單越過單位網路邊界，即存在風險。
  - 惡意連線紀錄分析（複驗）
    - 於單位核心資通系統伺服器網段前端抽選一台防火牆或單位DNS Server之一個月Log，並挑選最新5筆中繼站進行複驗。





# 7.2 網路惡意活動檢測

- 計分範圍
  - 抽選共5個網段，含1個Server farm網段、1個管理網段（如網路管理/系統管理/程式開發等）、3個User farm網段。
- 計分方式（5分）
  - 計算規則
    - 一般使用者(X)a、b、c網段中繼站未阻擋率：
      - $Xa、Xb、Xc = (\text{未阻擋中繼站數} / \text{檢測中繼站總數}) * 100\%$
    - 管理用途使用者(Y)、伺服器(Z)網段中繼站未阻擋率：
      - $Y、Z = (\text{未阻擋中繼站數} / \text{檢測中繼站總數}) * 100\%$
    - 不符合率(Z) =  $(Xa + Xb + Xc + Y + Z) / 5$ 。
      - 若無管理用途使用者網段，則不計Y，如不符合率(Z) =  $(Xa + Xb + Xc + Z) / 4$ ，以此類推。
  - 計算公式
    - 本項得分 = 中繼站未阻擋率(Z)對應之得分

得分	中繼站未阻擋率(Z)
5	0%
4	$0\% < Z \leq 25\%$
3	$25\% < Z \leq 50\%$
2	$50\% < Z \leq 75\%$
1	$75\% < Z < 100\%$
0	100%



## 7.3 核心資通系統安全檢測

- 執行範圍：全核心資通系統

- 遴選原則：依據單位核心資通系統之個資筆數、機敏性、功能項目（如系統複雜度、介接系統及共用資料庫等）優先序進行挑選，其餘系統則依資安疑慮、檢測能量作為預備標的。

- 執行方式

- 內網滲透測試：
  - 由於核心系統為線上環境，請務必確認該系統是否已完成備份，或提供與正式環境相同之備援環境進行測試。
  - 本次採灰箱測試，單位需先準備測試帳號，確認是否已開啟與其權限相對應之功能，並於測試結束後協助測試功能是否正常，且確認本次執行測試帳號是否刪除。
  - 基於核心資訊系統重要性，所有核心系統「相關資訊資產（如伺服器主機及介接之系統）」，皆列入評分依據。
- 系統防護基準等級：
  - 依核心資通系統相應防護基準等級進行實體驗證，如存取控制、事件日誌與可歸責性、識別與鑑別、系統與服務獲得、系統與資訊完整性及其子項目。



# 7.3 核心資通系統安全檢測

- 計分範圍：至少2個核心資通系統
  - 計分數量：依檢測日程數挑選資通系統個數計分，如檢測日程排定2日，將遴選2個資通系統計分。
  - 計分範圍以外之核心資通系統，相關發現列入檢測報告但不扣分。

- 計分方式：
  - 計算規則：每個核心資通系統分別計算。
    - 內網滲透測試（15分）：
      - 每個高風險弱點扣2分
      - 每個中風險弱點扣0.5分
    - 系統防護基準等級（10分）：
      - 資通系統防護基準不符合率
        - $X = (\text{資通系統防護基準不符合項數} / \text{系統防護基準檢測總數}) * 100\%$
  - 計算公式：
    - 本項得分 = 資通系統防護基準不符合率(X)對應之得分

得分	資通系統防護基準不符合率(X)
10	0%
9	$0% < X \leq 11\%$
8	$11\% < X \leq 22\%$
7	$22\% < X \leq 33\%$
6	$33\% < X \leq 44\%$
5	$44\% < X \leq 55\%$
4	$55\% < X \leq 66\%$
3	$66\% < X \leq 77\%$
2	$77\% < X \leq 88\%$
1	$88\% < X < 100\%$
0	100%



## 7.4 網路架構檢測

- 執行範圍：全單位
- 執行方式
  - 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
    - 資通系統管理與防護情形



## 7.4 網路架構檢測

- 計分範圍：全單位
- 計分方式（10分）
  - 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 =  $10 - [\text{高風險弱點數}] * 2 - [\text{中風險弱點數}] * 1$  ※最低扣至0分。
  - 其它事項：
    - 受稽機關應於檢測當日提供網路實體架構圖、網路邏輯架構圖及相關系統連線實體架構圖。前述文件之完整性及正確性，列入準備作業配合度之計分範圍。



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
1	網路系統架構區域 規劃網路區域，如同伺服器區、資料庫區	未規劃網路區域	高
		未依規劃置放系統服務	中
		未明確劃分網路區域	建議
2	網路區域間的存取 各區域間部署防火牆、配置相關存取控制	未配置網路區域間的存取	高



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
3	部署入侵偵測/防禦系統	未部署入侵偵測/防禦系統	中
4	部署系統本機安全機制 如HIDS、HIPS、本機防火牆	未部署系統本機安全機制	低
5	建立實體備援機制 從主機端至服務出口端經過的設備	重要系統未建立實體備援機制	中
		系統備援失效仍可維持基本網路服務	低



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
6	建立服務備援機制 網域名稱服務、系統服務	重要服務未建立服務備援機制	中
7	限制內部對外連線	未限制內部對外部連線	中
		內部對外部連線服務過於寬鬆	建議
8	限制外部對內連線	未限制外部對內部連線	高





# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
9	限制服務區域連線	未限制服務區域連線	高
		服務區域內部對外部連線服務過於寬鬆	建議
10	應不包含Permit All/Any於任一個規則	包含Permit All/Any	高
11	應定義Deny All/Any於最後一個規則	未定義Deny All/Any	高



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
12	限制非加密資料傳輸協定	資料傳輸未使用加密協定並未限制外部端點	中
		資料傳輸未使用加密協定並未限制內部端點	建議
13	遠端連線存取控制	未配置遠端連線存取控制	高
14	網路設備存取鑑別	未配置網路設備存取鑑別	中
		管理者帳號未進行區分控管	建議



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
15	網路設備存取控制	未配置外網網路設備存取控制	高
		未配置內網網路設備存取控制	中
		已配置存取控制，但未生效	中



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
16	網路設備SNMP設定	配置可寫SNMP，使用預設通行碼	高
		配置唯讀SNMP，使用預設通行碼	中
		使用預設通行碼，但有配置存取控制	低



# 網路架構檢測檢測內容

項次	檢測內容	檢測結果	風險基準
17	網路設備校時設定	未配置校時設定	中
		已配置校時設定，但未生效	中
		未部署校時伺服器	低



## 7.5 目錄伺服器安全檢測

※若單位為無目錄伺服器環境，則該項次不計分。

- 執行範圍：1台
- 執行方式：
  - 本項檢測針對受測目錄伺服器，執行安全防護檢測：
    - 安全性更新
    - 防毒軟體
    - 異常程序檢測
    - 存取控制：帳號管理（如密碼原則/最小授權等），檢視LDAP做ACL或網路相關防護機制。



## 7.5 目錄伺服器安全檢測

※若單位為無目錄伺服器環境，則該項次不計分。

- 計分範圍：1台
- 計分方式（10分）：
  - 計算規則：
    - 防毒軟體更新得分 = 目錄伺服器防毒軟體已安裝且病毒碼已更新則得2分
    - 安全性修補程式更新得分 = 目錄伺服器安全性修補程式更新皆已安裝則得2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
    - 身分鑑別管理得分 = 目錄伺服器身分鑑別已設定安全性原則得2分
    - 身分授權管理得分 = 目錄伺服器身分授權採最小權限原則得2分
  - 計算公式：
    - 本項得分 = 防毒軟體病毒碼更新得分 + 安全性修補程式更新得分 + 惡意程式檢測得分 + 身分鑑別管理得分 + 身分授權管理得分



## 7.6 物聯網設備檢測

- 執行範圍：總計20台，遴選5台進行深度檢測
  - 遴選原則：依單位提供之物聯網設備清單抽選10台；未列於單位物聯網設備清單中之設備抽選10台，總計20台，若未滿則由單位提供清單設備遞補至滿台數，並從中依風險程度挑選5台進行深度檢測。
- 使用工具：Nessus、Forescout、Shodan
- 執行範圍
  - 安全防护深度檢測內容如下：
    - 物聯網設備軟體版本（包含是否具有重大CVE風險）
    - 管理介面存取控制策略
    - 連線存取控制策略
    - 加密傳輸保護及管理控制策略





## 7.6 物聯網設備檢測

- 計分範圍：總計20台，遴選5台進行深度檢測
  - 遴選原則：依單位提供之物聯網設備清單抽選10台；未列於單位物聯網設備清單中之設備抽選10台，總計20台，若未滿則由單位提供清單設備遞補至滿台數。並從中依風險程度挑選5台進行深度檢測。
- 計分方式（15分）
  - 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 =  $15 - [\text{高風險弱點數}] * 2 - [\text{中風險弱點數}] * 1$  ※最低扣至0分。
  - 其它事項：
    - 受稽機關應於檢測前提供全機關之物聯網設備清單（包含IP位址、管理單位、設備類別、設備名稱、廠牌型號/作業系統、放置位置等資訊）。
    - 前述清單之完整性及正確性，列入準備作業配合度之計分範圍。



## 7.7 組態設定安全檢測

- 執行範圍：
  - ※採A、B級單位進行計分，C級單位檢測結果作為備存。
- 遴選原則：挑選伺服器主機5台、使用者電腦5台，總計10台進行檢測。
- 執行方式：
  - 依據受檢單位自訂定之政府組態規則進行GCB工具檢測。



# 7.7 組態設定安全檢測

● 執行範圍： ※採A、B級單位進行計分，C級單位檢測結果作為備存。

○ 遴選原則：挑選伺服器主機5台、使用者電腦5台，總計10台進行檢測。

● 計分方式：

○ 計算規則：

■  $X = (\text{組態設定不符合項數} / \text{組態設定檢測總數}) * 100\%$

○ 計算公式：

■ 本項得分=組態設定項目不符合率(x)對應之得分

得分	組態設定項目不符合率(X)
10	0%
9	$0\% < X \leq 11\%$
8	$11\% < X \leq 22\%$
7	$22\% < X \leq 33\%$
6	$33\% < X \leq 44\%$
5	$44\% < X \leq 55\%$
4	$55\% < X \leq 66\%$
3	$66\% < X \leq 77\%$
2	$77\% < X \leq 88\%$
1	$88\% < X < 100\%$
0	100%



## 7.8 資料庫安全檢測

- 執行範圍：2個核心資料庫
- 執行方式

※若單位無核心資料庫，則該項次不計分。

- 透過訪談及實際檢視方式，依據防護基準等級抽測10項資料庫安全機制項目，確認資料庫安全管理與防護狀況，包含：
  - 特權帳號管理
  - 資料加密
  - 備份保護
  - 弱點管理
  - 存取授權
  - 稽核紀錄
  - 委外管理



## 7.8 資料庫安全檢測

※若單位無核心資料庫，則該項次不計分。

- 執行範圍：2個核心資料庫
- 計分方式（10分）
  - 計算規則：每個核心資料庫分別計算。
    - 每個不符合項目扣1分
    - 得分= 10 - (不符合項目 \* 1) ※最低扣至0分。
  - 計算公式：
    - 本項得分= 個別核心資料庫得分之加總 / 檢測核心資料庫總數



# 資料庫安全檢測檢核內容

項次	檢測類別	檢測項目
1	特權帳號管理	變更資料庫預設管理帳號
2		啟用帳號鎖定次數
3		啟用帳號鎖定時間
4		啟用密碼複雜度原則
5		啟用密碼長度原則
6		啟用密碼最常有效期限原則
7		限制管理者帳號透過速端存取



# 資料庫安全檢測檢核內容

項次	檢測類別	檢測項目
8	資料加密	資料庫資料具有適當保護機制(包含加密、不可識別處理)
9		資料庫傳輸具有安全機制
10		資料庫加密金鑰具有適當保護機制
11	存取授權	限制資料庫主機服務埠
12		限制遠端存取來源
13		限制遠端存取帳號
14		限制遠端存取操作
15		資料庫帳號權限最小原則



# 資料庫安全檢測檢核內容

項次	檢測類別	檢測項目
16	稽核紀錄	啟用資料庫帳號變更稽核
17		啟用資料庫帳號登出/登入稽核
18		啟用資料庫結構變更稽核
19		稽核紀錄管理方式
20		資料庫主機時間校時
21		稽核紀錄分析





# 資料庫安全檢測檢核內容

項次	檢測類別	檢測項目
22	委外管理	委外廠商外部連線方式
23		委外廠商資料存取方式
24		委外廠商帳號授權方式
25	備份保護	資料庫定期執行備份
26		資料庫備份具有適當保護機制
27		資料庫備份回復測試



# 資料庫安全檢測檢核內容

項次	檢測類別	檢測項目
28	弱點管理	資料庫主機定期弱點檢測
29		修補資料庫主機弱點項目
30		修補資料庫主機安全性更新項目



# 7.9 準備作業配合度

- 計分範圍：應備文件及相關紀錄完整性
- 計分方式
  - 計算規則：
    - 技術檢測基本資料調查表：未提供者倒扣3分；提供內容如不完整，視情況倒扣1至2分。
    - 核心資通系統調查表：未提供者倒扣3分；提供內容如不完整(如各類角色權限功能不齊全等)，視情況倒扣3至5分。
    - 受檢測應備文件清單所列項目（包含使用者電腦清單、物聯網設備清單、網路架構圖等）：各項未提供者各倒扣2分；提供內容如不完整，倒扣1分。
  - 計算公式：
    - 採倒扣，至多扣減10分 ※最低扣至0分。
  - 其它事項：
    - 本部將提供受檢測應備文件清單，受稽機關應依要求時程提供或於現場備好，以避免耽誤檢測時程。

## 8. 配合事項





## 8.1 原則與環境

### ● 原則

- 基於檢測作業客觀中立原則，本中心團隊不宜接受受測單位招待及饋贈，敬請配合。
- 為確認教育體系教職員生資料受資通安全保護情形，請配合檢測作業，避免受測期間暫時關閉資通訊設備。

### ● 用餐

- 午餐委請貴單位代訂，由本中心團隊支付費用，並請於後續提供午餐收據，統編：87557573（國立陽明交通大學）。

### ● 環境

- 檢測場地：需具備至少20個實體網孔、20條網路線、5條延長線。
- 會議場地：請貴單位製作人員桌排，須具備投影設備（可與檢測場地同地點）。



## 8.2 會議與簽署文件

- 與會人員

- 啟始及結束會議，由貴單位受稽代表與本中心團隊領隊共同主持，建議邀請機關資安推動組織之成員、行政幕僚及各單位代表共同參與。
- **總結會議簡報內容為稽核範圍（全機關）之技術檢測初步發現彙整**，列入後續技術檢測總報告；技術檢測評分結果另依選定範圍統整計算。

- 簽署文件

- 請貴單位提供「**資安檢測服務權利與義務聲明書**」用印後之版本。
- 本中心團隊統一簽署本案檢測作業之「**保密切結書**」及「**簽到表**」，檢測作業結束後，將提供掃描檔供貴單位留存。



## 8.3 技術檢測

### ● 使用者電腦安全檢測

- 【使用者電腦清單】：全機關各單位使用者電腦清單，內容含網路位址、職稱、人員姓名、單位名稱、所在地點等，並**確保檢測當日電腦為開機狀態**。
- 【資安健診結果報告】：請提供最近一次資安健診結果報告。
- 【使用者電腦檢測用網路位址】：請提供至少6組可連線至所有使用者電腦網段、未受網路設備阻擋之IP，以確保弱點掃描作業順利實施。

### ● 網路惡意活動檢測

- 〔開啟Traceroute功能〕：請確認是否開啟Traceroute功能，如tracert 8.8.8.8。
- 【日誌資料】：提供檢測前一個月防火牆log或DNS Server log資料。
- 【網路惡意活動檢測用網路位址】：至少3組與使用者電腦、2組與管理者（如網路管理/系統管理/程式開發等）、2組與伺服器叢集同網段，且可對外連線之IP。



## 8.3 技術檢測

### ● 核心資通系統安全檢測

- **【掃描/測試報告】**：請提供最新系統弱點掃描、滲透測試、源碼掃描報告。
- **【系統授權碼】**：請提供測試用帳號密碼，含前後台、不同使用者權限各4組，並確認各類角色權限功能是否齊全。
- **〔完成備份作業〕**：請於檢測前完成備份作業，或提供與正式環境相同之備援環境進行測試。
- **【核心資通系統安全檢測用網路位址】**：請提供至少8組可連線至核心資通系統網段，可進行內網滲透測試之IP，並確認無防護設備(如防火牆或WAF)進行阻擋。

### ● 網路架構檢測

- **【網路架構圖】**：請提供整體網路實體\網路邏輯\系統連線實體架構圖。
- **【VPN授權碼】**：請提供VPN連線測試帳號密碼3組。





# 8.3 技術檢測

## ● 物聯網設備檢測

- 【物聯網設備清單】：請提供全機關各單位完整物聯網設備清單。
- 【物聯網設備檢測用網路位址】：請提供至少6組可連線至物聯網設備之IP。

## ● 組態設定安全檢測

- 【組態GPO】：請單位提供組態GPO設定檔。

## ● 資料庫安全檢測

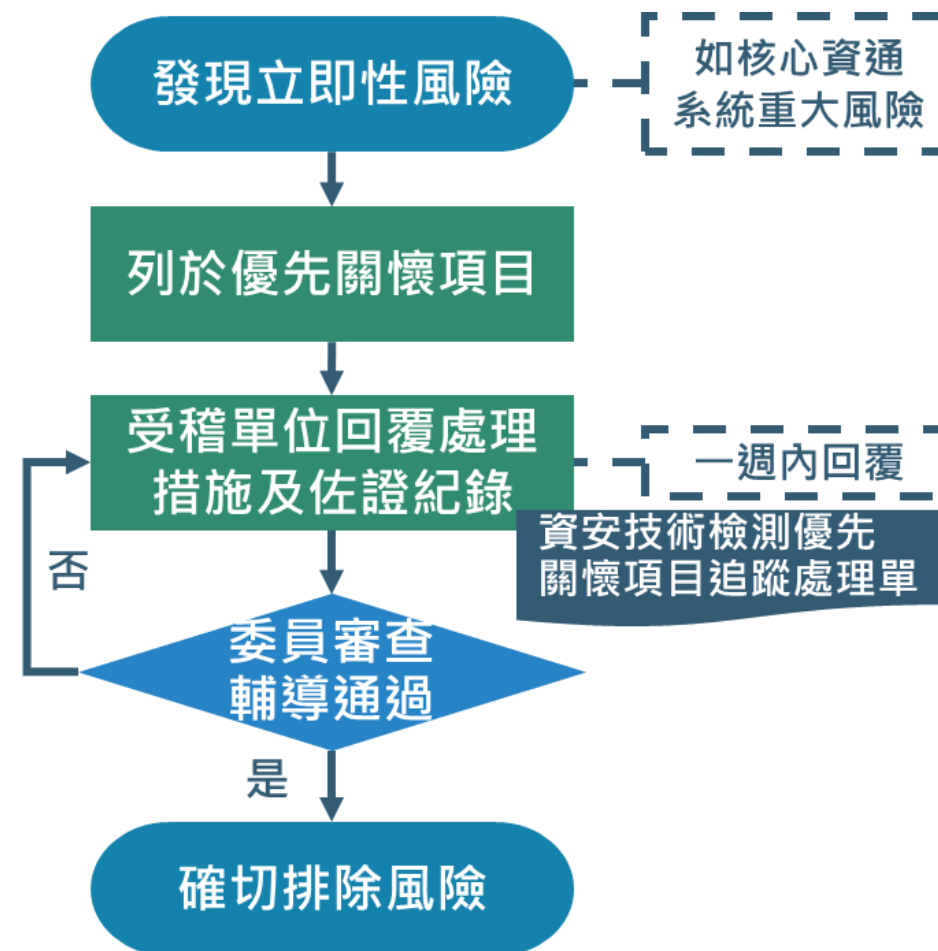
- 【演練/掃描/修補報告】：請於檢測當日提供最近一次資料庫備份還原演練報告、資料庫主機弱點掃描報告及弱點修補紀錄。
- 【權限帳號】：請資料庫管理者備妥可查詢資料庫設定之帳號權限，於檢測過程協助相關操作。

## 9. 技術檢測追蹤流程說明

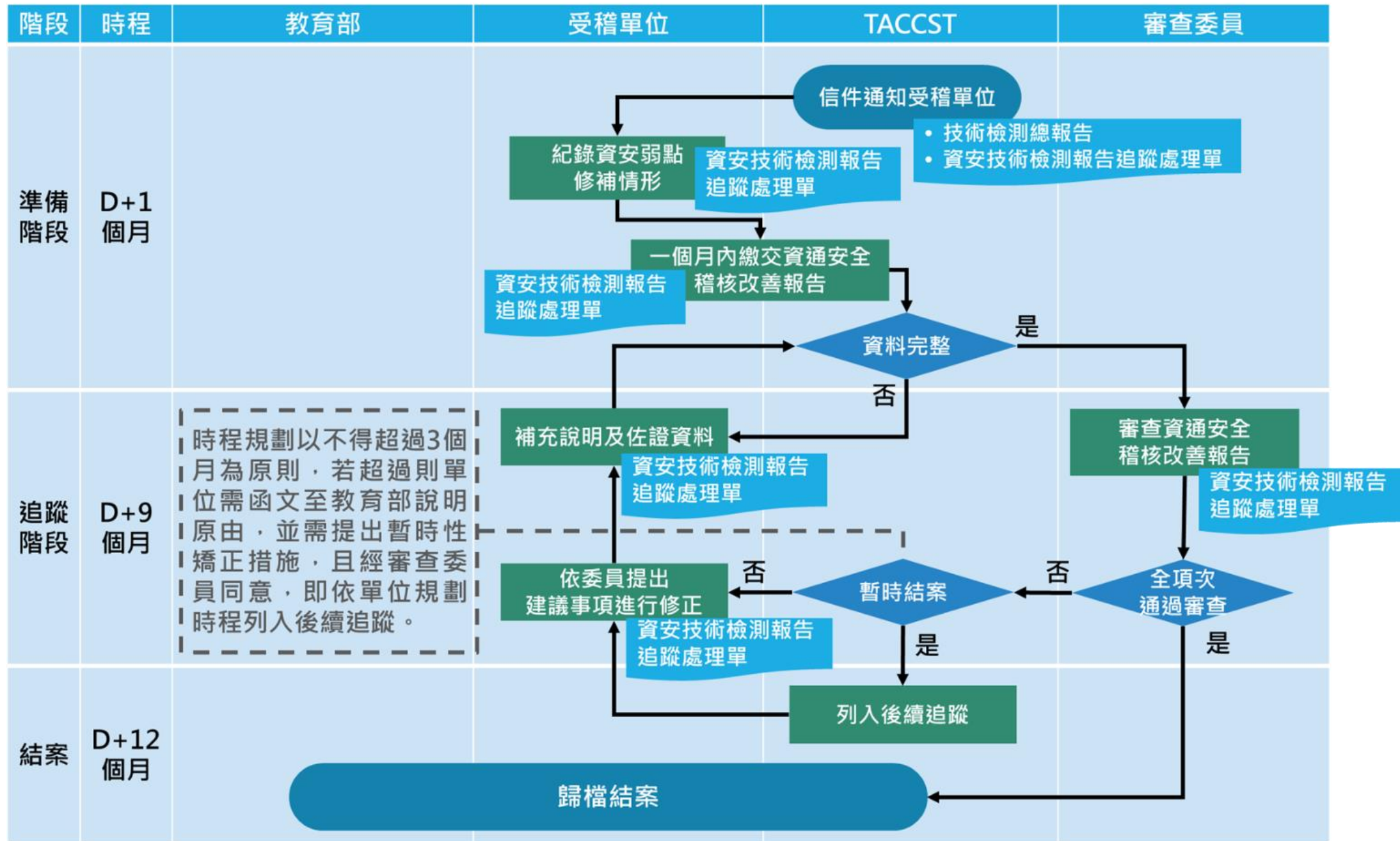


# 優先關懷追蹤流程

執行技術檢測作業發現立即性風險，如個資外洩等高風險項目，單位需於檢測後一週內提交矯正措施及相關佐證紀錄，安排參與實地稽核技術面委員進行審查，確認後即排除風險。



# 改善追蹤流程



※D為總報告提供日期。

# 10. 技術檢測平台說明





# 10. 平台簡介

---

- 簡介

- 為使技術檢測作業簡化，受稽單位能夠更了解技術檢測流程。從今年度開始檢測前的資料上傳、下載、弱點改善追蹤都在此平台上進行。

- 功能

- 帳號註冊
- 公佈欄
- 時間軸
- 檔案列表
- 弱點改善追蹤



# 10.1 帳號註冊

## ● 介紹

- 即日起開放註冊。
- 註冊網址：  
<https://tas.moe.edu.tw/account/signup/>
- 同一單位僅需一名稽核負責窗口申請。
- 信箱請務必填寫正確。

- 密碼至少10碼
- 密碼不可全是數字
- 密碼不可是常見的組合

Password

\* 密碼

Password check

\* 重新輸入密碼

03-3000000 #000

\* 電話 #分機

0900000000

手機

聯絡地址

聯絡地址

國立陽明交通大學

\* 服務單位

資訊技術服務中心

\* 服務處室

組長

\* 職稱

Register





# 10.1 帳號註冊

- 介紹

- 註冊後，請等待工作人員審核後並開通您申請的帳號。



“註冊成功，管理員審核後會開通您的帳號。”

— 聯絡電話: #52885、#52891、#52861、#31268



# 10.1 帳號註冊

## ● 介紹

- 審核通過後，收到寄信通知，即可登入系統。
- 第一次登入系統，請先認證信箱，以開啟完整功能。

Taccst Audit

帳號

王小明  
受稽人員

> 公佈欄  
> 技術檢測  
> 弱點改善

▼ 帳戶  
帳戶設置  
重設密碼  
登出

王小明  
受稽單位  
國立陽明交通大學 資訊技術服務中心  
修改資料

帳戶名稱	test123
名稱	王小明
身份	受稽單位
信箱	@nycu.edu.tw
服務單位	國立陽明交通大學
服務處室	資訊技術服務中心
職稱	技術員
電話	03-30000000
手機	09-00000000
聯絡地址	

送驗證信



# 10.2 公佈欄

- 公告總覽
  - 公佈總覽內會公告技術檢測相關的最新消息，工作人員聯絡資訊也可在此查詢。

王小明

受稽人員

✓ 公佈欄

公告總覽

常見問題

✓ 技術檢測

檢測管理

✓ 弱點改善

弱點改善回報

> 帳戶

公告總覽

系統公告

系統說明：  
請尚未驗證信箱的使用者至[帳戶設置](#)驗證信箱。  
  
若對技術檢測流程有相關問題，請聯絡負責人。

- 何小姐：(03) 571-2121 #52885
- 呂小姐：(03) 571-2121 #52891
- 廖先生：(03) 571-2121 #52861
- 陳小姐：(03) 571-2121 #31268

  
若系統功能出現異常請聯繫負責人。

- 廖先生：(03) 571-2121 #52861
- 劉先生：(03) 571-2121 #52822

置頂公告

標題：  
教育體系資安檢測技術服務中心網站  
  
內容：  
檢測中心簡介可參考網站連結 <https://www.taccst.moe.edu.tw/>  
  
發佈日期：  
若系統功能出現異常請聯繫負責人。  
  
標題：  
改善追蹤注意事項  
  
內容：  
依教育部規定技術檢測所發現之弱點需於開始追蹤起3個月內完成改善，如無法於時程規劃內完成，需請函文至教育部說明並提出暫時性矯正措施。函文範本：[https://www.taccst.moe.edu.tw/file/public\\_file/](https://www.taccst.moe.edu.tw/file/public_file/)

教育部113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 技術檢測

59



# 10.2 公佈欄

- 常見問題

- 技術檢測中心會整理技術檢測常見的問題，以O&A的方式呈現。

Taccst Audit

王小明  
受稽人員

公佈欄

公告總覽

**常見問題**

> 技術檢測

> 弱點改善

> 帳戶

常見問題

Q: 技術檢測作業目的

A: 為配合教育部實施「教育部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」，委由教育體系資安檢測技術服務中心辦理資安稽核技術檢測作業，進行1至3天之技術檢測（部屬機關(構)、國立大專校院適用），技術檢測結果作為實地稽核參考。

Q: 技術檢測作業目依據

- 資通安全管理法第13條第1項及第17條第3項。
- 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。

Q: 技術檢測項目

- 使用者電腦安全檢測
- 物聯網設備安全檢測
- 網路架構檢測
- 網路惡意活動檢測
- 核心資通系統安全檢測
- 目錄伺服器安全檢測
- 組態設定安全檢測
- 資料庫安全檢測

# 10.3 時間軸

- 介紹
  - 為使受稽單位能了解整體技術檢測時程及各階段需要繳交與下載之所有文件。
  - 時間軸內將顯示開放及截止日期，並可直接點選檔案列表至文件下載區。

檔案列表

王小明  
受稽人員

✓ 公佈欄  
公告總覽  
常見問題

✓ 技術檢測  
檢測管理

✓ 弱點改善  
弱點改善回報

> 帳戶

技術檢測文件

2024-05-31 09:00 ~ 2024-05-31 17:00

一、教育部提供文件：  
教育部113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

二、本中心提供附件：  
TACCST-B-02-02\_資安技術檢測基本資料調查表\_v3.1  
TACCST-B-02-03\_核心資通系統調查表\_v3.1  
TACCST-B-02-05\_資安技術檢測計畫  
附件01\_資安技術檢測交通位置表  
附件02\_技術檢測參與人員清單  
附件03\_資安檢測服務權利與義務聲明書  
附件04\_出席會議人員名單  
附件05\_資安技術檢測作業說明  
附件06\_項目負責人聯絡清單

123-1 國立測試大學 技術檢測時程圖

教育部113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 技術檢測

61



# 10.4 檔案列表

- 下載檔案

- 技術檢測前應繳的資料及檢測後的會議簡報及總報告，都會在此列表供受稽單位下載。

檢測管理 > 時間軸 > 檔案列表

上傳

檢測中心提供清單

- 1 - 前置文件
- 2 - 會議簡報
- 3 - 總報告
- 4 - 其它

受稽單位應繳清單

- 1 - 應繳附件
- 2 - 其它

# 10.4 檔案繳交

- 上傳檔案

- 進入上傳檔案頁面後，  
依據檔案內容上傳至各  
分區。

檢測管理 > 時間軸 > 檔案列表 > 上傳檔案

上傳檔案大小: 單個檔案10MB以內

上傳檔案類型: pdf、docx、odt、xlsx、ods、png、jpeg、jpg、zip

上傳檔案數量: 最多30個

## 檢測中心提供清單

### 1 - 應繳附件

- 00\_TACCST-B-02-05\_資安技術檢測計畫.pdf
- 附件01\_資安技術檢測交通位置表.docx
- 附件02\_技術檢測參與人員清單.pdf
- 附件03\_資安檢測服務權利與義務聲明書.pdf
- 附件04\_出席會議人員名單.docx
- 附件05\_資安技術檢測作業說明.pdf
- 附件06\_項目負責人聯絡清單.docx
- 附件07\_資安檢測使用網路位址清單.docx
- 附件08\_使用電腦安全檢測清單.docx
- 附件09\_資安技術檢測之測試帳號及密碼.xlsx
- 附件10\_事前作業查核表.docx
- TACCST-B-02-02\_資安技術檢測基本資料調查表\_v3.1.docx
- TACCST-B-02-03\_核心資通系統調查表\_v3.1.docx

### 2 - 會議簡報

## 受稽單位應繳清單

### 1 - 應繳附件

未選擇任何檔案

### 2 - 交通資訊

未選擇任何檔案

### 3 - 其它

未選擇任何檔案




## 10.5 弱點改善追蹤

- 介紹

- 技術檢測作業完成後，會以信件通知實施後續的弱點改善追蹤。
- 請單位收到通知信後，在期限內登入系統回復修補狀況，並提供佐證資料。

[教育體系資安檢測技術服務中心] 國立陽明交通大學-弱點追蹤回報-優先關懷項目

 taccst@nycu.edu.tw <taccst@nycu.edu.tw>  
上午 11:20

收件者: @nycu.edu.tw

王小明老師您好：

感謝貴單位參與教育部技術檢測，在檢測中有發現貴單位存有風險項目，建議貴機關對資訊資產風險進行修補，以避免資安風險。請於 2023-05-30 17:30 前登入系統並回報，以利本中心掌握修補情況，謝謝！

系統連結：<https://tas.moe.edu.tw/>

- 此封信為系統自動寄發，請勿直接回信 -

教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology

- 聯絡電話：(03)-5712121 #52885、#52891、#52861、#31268
- 地址：30010 新竹市大學路 1001 號(國立陽明交通大學 資訊技術服務中心 1F)



# 10.5 弱點改善追蹤

- 介紹
  - 優先關懷項目: 針對高風險的弱點。請在一個星期內修補並回報。
  - 追蹤改善項目: 依據單位規劃的時程，進行改善並回報。

Tacst Audit

王小明  
受檢人員

> 公佈欄

> 技術檢測

> 弱點改善

- 弱點改善回報

> 帳戶

弱點改善回報

優先關懷項目

追蹤改善項目

追蹤中

Show 10 entries

Search:

年度	場次	單位	開始追蹤時間	單位回覆期限	狀態	聯絡窗口	動作
115	1	國立陽明交通大學	2023-05-24	2023-05-30 17:30	待單位回覆	王小明	<div>檢視</div> <div>回覆</div>

Showing 1 to 1 of 1 entries

Previous 1 Next

已完成追蹤

Show 10 entries

Search:

年度	場次	單位	開始追蹤時間	結束追蹤時間	聯絡窗口	動作
----	----	----	--------	--------	------	----

No data available in table

Showing 0 to 0 of 0 entries

Previous Next

教育部113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 技術檢測

65





# 10.5 弱點改善追蹤

弱點改善回報 > 回覆表單

送出

## 115-1 國立陽明交通大學 優先關懷項目

上傳檔案大小限制: 單個檔案5MB以內

項次	風險等級	系統名稱 / 事件IP / 網段	風險位置	檢測發現	改善方式	時程規劃日期	佐證資料	審查意見	建議修正事項	歷程概要
1	使用者電腦安全檢測									
1-1	高風險	111.111.0.25	-	外網可透過遠端登入，且無設定密碼。	已限制該電腦僅內網可存取，並設定強密碼。	2023-05-31	<a href="#">佐證資料一.docx</a> 選擇檔案 未...檔案	建議修正		2023/05/24 11:20 請單位進行矯正回覆。
2	核心資訊系統安全檢測									
2-1	高風險	111.111.0.50	https://tas.moe.edu.tw/	可透過sql injection登入系統	已在登入密碼時，於前端篩選字元，防止sql語法。	2023-05-31	<a href="#">佐證資料二.docx</a> 選擇檔案 未...檔案	建議修正		2023/05/24 11:20 請單位進行矯正回覆。

儲存



# 10.5 弱點改善追蹤

送出

115-1 國立陽明交通大學 優先關懷項目

上傳檔案大小限制: 每個檔案5MB以內

項次	風險等級	系統名稱 / 事件IP / 網段	風險位置	檢測發現	改善方式	時程規劃日期	佐證資料	審查意見	建議修正事項	歷程概要
1	使用者電腦安全檢測									
1-1	高風險	111.111.0.25	-	外網可透過遠端登入，且無設定密碼。	已限制該電腦僅內網可存取，並設定強密碼。	2023-05-31	佐證資料一.docx 選擇檔案 未...檔案	同意	-	2023/05/24 11:20 請單位進行矯正回覆。 2023/05/24 11:56 單位提供回覆及佐證資料。 2023/05/24 13:55 審查人員同意受檢單位回覆資訊。
2	核心資訊系統安全檢測									
2-1	高風險	111.111.0.50	https://tas.moe.edu.tw/	可透過sql injection登入系統	已在登入密碼時，於後端篩選字元，防止sql語法。	2023-05-31	佐證資料二.docx 選擇檔案 未...檔案	建議修正	請於後端進行字元篩選。	2023/05/24 11:20 請單位進行矯正回覆。 2023/05/24 11:56 單位提供回覆及佐證資料。 2023/05/24 13:55 請單位依照委員回覆進行建議修正，並提供佐證資料。

儲存



# 10.5 弱點改善追蹤

- 介紹

- 審查委員皆同意所有修正。
- 工作人員會將追蹤表單歸檔，受稽單位可以檢視歷年的弱點追蹤結果。

Taccst Audit

王小明

受稽人員

> 公佈欄

> 技術檢測

> 弱點改善

> 弱點改善回報

> 帳戶

弱點改善回報

優先關懷項目

追蹤改善項目

追蹤中

Show 10 entries

Search:

年度

場次

單位

開始追蹤時間

單位回覆期限

狀態

聯絡窗口

動作

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

已完成追蹤

Show 10 entries

Search:

年度

場次

單位

開始追蹤時間

結束追蹤時間

聯絡窗口

動作

115

1

國立陽明交通大學

2023-05-24

王小明

檢視

Showing 1 to 1 of 1 entries

Previous

1

Next

教育部113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 技術檢測

68