資料庫技術檢測執行方法

行政院國家資通安全會報技術服務中心
中華民國110年4月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	110/4/1	新編
2			
3			

目　次

1. 前言 1
1.1 適用對象 1
1.2 使用建議 1
1.3 章節結構 1
2. 技術檢測流程 3
3. 前置階段 4
3.1 基本資訊蒐集 4
3.2 回覆基本資訊 6
3.3 確認檢測範圍 6
3.4 確認檢測項目 7
3.5 通知配合事項 7
3.6 編成檢測團隊 9
4. 執行階段 10
4.1 資料庫安全檢測 10
4.2 主機安全檢測 20
4.3 資通系統安全檢測 22
4.4 網路安全檢測 22
5. 結案階段 25
5.1 資料庫安全檢測 25
5.2 主機安全檢測 25
5.3 資通系統安全檢測 25
5.4 網路安全檢測 26
6. 結論 27
7. 附件 28

圖 目 次

圖 1　資料庫技術檢測作業流程 3
圖 2　技術檢測團隊編組架構 9
圖 3　資通系統安全檢測作業流程 22

表 目 次

表 1　基本資訊蒐集重點 4
表 2　檢測範圍挑選原則範例 6
表 3　檢測項目說明 7
表 4　技術檢測配合事項 8
表 5　資料庫安全檢測查檢表 10
表 6　特權帳戶管理檢測項目與檢測重點說明 12
表 7　資料加密檢測項目與檢測重點說明 13
表 8　存取授權項目與檢測重點說明 14
表 9　稽核紀錄檢測項目與檢測重點說明 16
表 10　委外管理檢測項目與檢測重點說明 17
表 11　備份保護檢測項目與檢測重點說明 18
表 12　弱點管理檢測項目與檢測重點說明 19
表 13　主機安全檢測查檢表 20
表 14　網路安全檢測查檢表 23

1. 前言

因應資料外洩事件層出不窮，行政院國家資通安全會報技術服務中心(以下簡稱本中心)發展以資料庫為核心，結合主機安全、資通系統安全及網路安全等面向之技術檢測框架，由內而外逐層檢視資料庫登入、主機登入、系統存取及網路連線等各種資料存取管道之防護情形，以期透過技術檢測掌握資料庫防護現況與可強化面向，以利強化資料庫安全。

本文件藉由說明資料庫技術檢測流程，並詳述包含「資料庫安全檢測」、「主機安全檢測」、「資通系統安全檢測」及「網路安全檢測」等 4 項檢測項目執行方式，以及提醒相關查檢表紀錄內容重點，做為政府機關自我檢測或第三方檢測之參考，以協助政府機關提升資料庫安全防護能力。

1.1 適用對象

本文件適用於政府機關(構)資訊人員執行機關自我檢測或第三方檢測之參考。

1.2 使用建議

本文件主要針對技術檢測各階段作業重點進行說明，提供技術檢測執行之參考，進而掌握各檢測項目與執行上需考量重點，以及執行作業中應留下之紀錄重點。建議先閱讀技術檢測流程，掌握整體執行工作與重點，再接續了解各階段細部工作內容與檢測步驟，以確保可如期如質完成檢測作業。

1.3 章節結構

本文件共分為「前言」、「技術檢測流程」、「前置階段」、「執行階段」、「結案階段」、「結論」及「附件」等 7 個章節，各章節架構與工作項目說明如下：

- 第 1 章：前言

  說明目的、適用對象、使用建議及章節架構，以對檢測重點與本文件架構有全盤性之認知。

- 第 2 章：技術檢測流程

  說明技術檢測前置階段、執行階段及結案階段等各階段之整體流程。

- 第 3 章：前置階段

  說明檢測前需準備之項目，包含基本資訊蒐集、檢測範圍與項目確認、團隊編成、檢測工具及雙方配合事項等。

- 第 4 章：執行階段

  說明「資料庫安全檢測」、「主機安全檢測」、「資通系統安全檢測」及「網路安全檢測」等 4 項之執行重點。

- 第 5 章：結案階段

  說明結果報告中各檢測項目應撰寫之重點。

- 第 6 章：結論

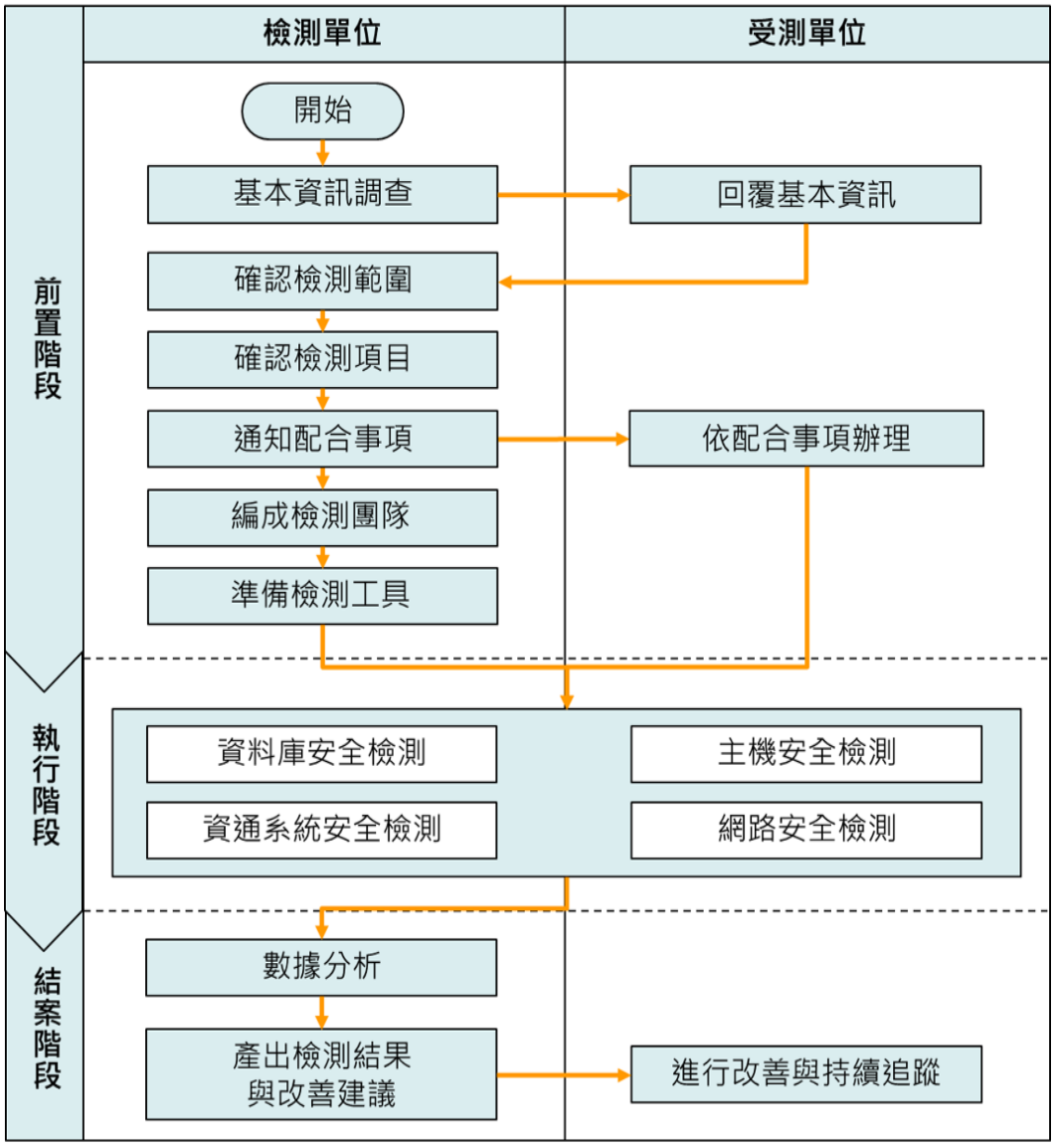
  說明結論與效益。

- 第 7 章：附件

  提供技術檢測所需之基本資訊蒐集表範本。

2. 技術檢測流程

技術檢測作業分為「前置階段」、「執行階段」及「結案階段」等 3 個階段，各階段作業內容詳見圖 1，依據此執行流程對受測資料庫進行資料蒐集與資訊分析，接續執行各面向之技術檢測作業，最後進行數據分析與產出檢測結果，並提供相關改善建議。



資料來源：本中心整理

圖1　資料庫技術檢測作業流程

3. 前置階段

技術檢測執行前須蒐集受測機關基本資訊，以確認檢測範圍、規劃檢測項目、編成檢測團隊及準備檢測工具。同時，受測機關須依檢測配合事項，備妥檢測所需環境，以利後續檢測作業執行。

3.1 基本資訊蒐集

為了解受測機關現行資料庫安全控制措施、網路架構配置及資通系統防護情形等，應於檢測前完成受測機關基本資訊蒐集，以利評估檢測範圍。各檢測項目之蒐集重點詳見表 1，基本資訊蒐集表範本詳見附件。

機關填復基本資訊蒐集表內容後，檢測人員可從表格內容了解機關防護現況與日常維運管理機制，並以此為執行檢測基準，進而檢視實際檢測結果是否與基準相符，以衡量資安防護措施落實情形。

以資料庫安全檢測為例，當機關回覆基本資訊蒐集表「2.6.4.禁止管理者帳戶透過遠端存取」為禁止管理帳戶透過遠端存取，且「2.6.3.限制遠端存取的帳戶」內容為僅限特定且非管理者帳戶可遠端存取時，檢測查檢表之「限制管理者帳戶透過遠端存取」與「限制遠端存取帳戶」兩項即以此回覆內容做為檢測基準，並進行實際檢測。當檢測結果發現實際上管理者帳戶可進行遠端存取，即顯示機關並未落實「限制管理者帳戶透過遠端存取」與「限制遠端存取帳戶」兩項管理措施。

表1　基本資訊蒐集重點

項次	檢測項目	蒐集重點
1	資料庫安全檢測	▪ 受測機關現行資料庫類型與版本 ▪ 資料庫特權帳戶管理、資料加密、備份保護、弱點管理、存取授權、稽核紀錄及委外管理等安全設定狀況

項次	檢測項目	蒐集重點
2	主機安全檢測	資料庫主機資訊，包含主機名稱、內部 IP、作業系統版本、服務應用程式、主機開啟通訊埠及實體主機放置位置等
3	資通系統安全檢測	▪ 資通系統基本資訊，包含系統名稱、簡介、系統網址、系統屬性、服務對象、安全等級、個資含量、系統連線是否具有 Load Balance 機制、使用限制及內部連線經過之防護設備等 ▪ 資通系統存取措施，包含前後台登入介面網址、是否使用單一簽入機制、單一簽入系統管理單位、後台管理登入介面連線方式及後台管理登入角色等 ▪ 資通系統主機資訊，包含主機名稱、主機類型、內部 IP、作業系統版本、服務應用程式、主機開啟通訊埠及實體主機放置位置等
4	網路安全檢測	▪ 受測機關內部服務主機之 IP 與作業系統版本等資訊，包含與資料庫介接之資通系統主機、網域主機、DNS 伺服器、WSUS 伺服器及防毒伺服器等 ▪ 受測機關是否部署防護主機，如資通系統前端是否有 WAF 或 IPS 設備，以及該設備型號與 IP ▪ 受測機關是否建置核心網路設備，如對外線路閘道器、防火牆與核心交換器，以及該設備型號與 IP ▪ 受測機關對外線路 IP ▪ 受測機關是否與其他機關進行資料交換，並敘明交換機關名稱與交換方式 ▪ 受測機關網路環境是否進行網段區隔，如網路管理人員網段、系統管理人員網段、資料

項次	檢測項目	蒐集重點
		庫管理人員網段、程式開發人員網段、系統主機開發、測試網段、虛擬私有網路(VPN)網段、實體隔離網段及網路設備網段等 ▪詳列受測機關使用者網段與對應之使用單位資訊

資料來源：本中心整理

3.2 回覆基本資訊

受測機關承辦人員依資料庫環境現況填完基本資訊項目後，依雙方約定傳送方式與密碼，以安全傳輸方式將基本資訊蒐集表提供予檢測單位，以利進行後續檢測作業。

3.3 確認檢測範圍

機關填復基本資訊蒐集表後，接續依檢測範圍挑選原則(範例詳見表 2)，完成各檢測項目範圍確認。

表2　檢測範圍挑選原則範例

項目	檢測項目	挑選原則
1	資料庫安全檢測	挑選受測機關內保有全國性民眾或公務員個資之核心資料庫
2	主機安全檢測	受測資料庫之主機
3	資通系統安全檢測	與受測資料庫介接，且由機關維運管理之系統
4	網路安全檢測	全機關

資料來源：本中心整理

3.4 確認檢測項目

依據檢測範圍規劃「資料庫安全檢測」、「主機安全檢測」、「資通系統安全檢測」及「網路安全檢測」等 4 項檢測項目內容(詳見表 3)與時程。

表3　檢測項目說明

項次	檢測項目	項目說明
1	資料庫安全檢測	實際訪談與檢測特權帳戶管理、資料加密、存取授權、稽核紀錄、委外管理、備份保護及弱點管理等 7 類別，共 30 項資料庫檢測項目
2	主機安全檢測	檢視資料庫主機之帳戶管理、權限設定及存取管控情形，並進行弱點掃描，以確認弱點防護情形
3	資通系統安全檢測	針對資料庫所介接之資通系統，檢視滲透測試執行情形，並挑選已修補之中高風險項目進行複測，驗證介接資通系統之防護情形
4	網路安全檢測	針對核心資料庫檢視資通系統介接、 VPN 連線管理、防火牆規則、遠端連線管理及存取控制等安全控制措施，進行架構了解與實際設定檢視

資料來源：本中心整理

3.5 通知配合事項

檢測範圍與項目確認後，可將檢測項目配合事項通知受測機關預先準備，針對檢測 IP、系統測試帳戶及通行碼組數，則視檢測人力需求進行申請，技術檢測項目配合事項列表詳見表 4。

表4　技術檢測配合事項

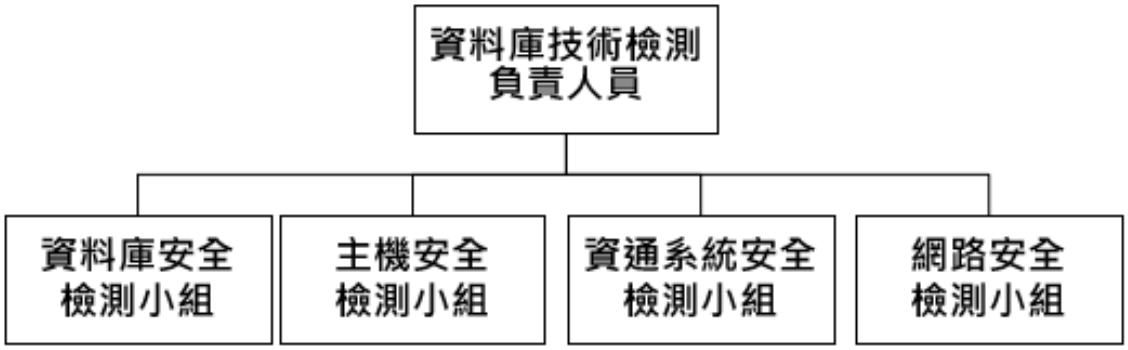
項目	檢測項目	配合事項說明
1	資料庫安全檢測	▪請安排 AP 管理者、DB 管理者及系統操作人員參與資料庫管理訪談，以供檢測人員可確實了解機關料庫安全防護現況 ▪請 DB 管理者備妥可查詢資料庫設定之帳戶權限，於檢測過程協助相關操作
2	主機安全檢測	▪請安排主機管理者參與訪談，以供檢測人員可確實了解主機帳戶管理、權限設定及存取管控情形 ▪請提供至少 1 組與核心資通系統同網段，可對資料庫主機進行弱點掃描之 IP，並確認無防護設備(如防火牆或 WAF)進行阻擋
3	資通系統安全檢測	▪受測資通系統必須為可透過 Ethernet 連線之主機 ▪請提供至少 1 組與機關先前執行滲透測試時相同環境之檢測 IP，以利進行滲透測試複測 ▪受測系統如需使用帳戶、通行碼登入後，方能使用其他功能時，請務必提供機關先前執行滲透測試時所使用之帳戶權限至少 1 組 ▪受測系統如需在 Client 端安裝設備(如讀卡機、憑證卡等)、程式或元件，請先備妥並於檢測當日提供；如需使用憑證登入，請事先備妥測試用憑證，並於檢測當日提供 ▪本項檢測將以機關滲透測試報告中之手法進行複測，確認系統修補狀況，為避免測試過程中發生預期外情況，導致網路、伺服器及資通系統發生當機或資料毀損，因此在執行前應備份受測系統相關資料，或提供與正式環境相同之備援環境進行測試

項目	檢測項目	配合事項說明
4	網路安全檢測	▪請提供至少 1 組與使用者電腦位於同網段之 IP，可執行網路相關檢測 ▪請提供整體網路實體架構圖及網路邏輯架構圖(含網路設備管理 IP、介面 IP 及資安設備如 IPS/IDS)，以及系統連線實體架構圖(含所有經過之網路設備、線路) ▪請安排網路管理者參與網路架構訪談，供檢測人員了解網路架構安全防護現況

資料來源：本中心整理

3.6 編成檢測團隊

為確保各項檢測作業可如期順利完成，依照各檢測項目之需求進行任務編組，任務編組架構詳見圖 2。



資料來源：本中心整理

圖2　技術檢測團隊編組架構

4. 執行階段

技術檢測執行階段將依前置階段所擬定之檢測範圍與任務編組，於檢測時程內，依各檢測項目之執行方法展開檢測作業，並產出相關檢測紀錄。

4.1 資料庫安全檢測

針對資料庫安全檢測，係透過訪談與設定檢視，檢測資料庫之特權帳戶管理、資料加密、存取授權、稽核紀錄、委外管理、備份保護及弱點管理等7類別共30項檢測項目(詳見表5)，各檢測項目與檢測重點說明如下。

表5　資料庫安全檢測查檢表

機關名稱			
資料庫名稱			
檢測日期		____年___月___日	
項次	類別	檢測項目	發現與改善建議
1-1	特權帳戶管理	變更資料庫預設管理帳戶	
1-2		啟用帳戶鎖定次數	
1-3		啟用帳戶鎖定時間	
1-4		啟用通行碼複雜度原則	
1-5		啟用通行碼長度原則	
1-6		啟用通行碼最長有效期限原則	
1-7		限制管理者帳戶透過遠端存取	
2-1	資料加密	資料庫資料具有適當保護機制(加密)	
2-2		資料庫傳輸具有安全機制	
2-3		資料庫加密金鑰具有適當保護機制	
3-1	存取授權	限制資料庫主機服務埠	

機關名稱			
資料庫名稱			
檢測日期		____年___月___日	
項次	類別	檢測項目	發現與改善建議
3-2		限制遠端存取來源	
3-3		限制遠端存取帳戶	
3-4		限制遠端存取操作	
3-5		資料庫帳戶權限最小原則	
4-1	稽核紀錄	啟用資料庫帳戶變更稽核	
4-2		啟用資料庫帳戶登出/登入稽核	
4-3		啟用資料庫結構變更稽核	
4-4		稽核紀錄管理方式	
4-5		資料庫主機時間校時	
4-6		稽核紀錄分析	
5-1	委外管理	委外廠商外部連線方式	
5-2		委外廠商資料存取方式	
5-3		委外廠商帳戶授權方式	
6-1	備份保護	資料庫定期執行備份	
6-2		資料庫備份具有適當保護機制	
6-3		資料庫備份回復測試	
7-1	弱點管理	執行資料庫主機弱點掃描	
7-2		修補資料庫主機弱點項目	
7-3		修補資料庫主機安全性更新項目	

資料來源：本中心整理

●特權帳戶管理

資料庫特權帳戶應妥善進行管理，避免使用預設帳戶，並設置帳戶通行碼保護機制與限制透過遠端操作，特權帳戶管理檢測重點詳見表 6。

表6　特權帳戶管理檢測項目與檢測重點說明

項次	檢測項目	項目說明	檢測方法
1-1	變更資料庫預設管理帳戶	資料庫應變更預設管理帳戶，避免使用已知帳戶，以防成為惡意攻擊之目標。若停用預設管理帳戶，亦符合本項目之要求	▪藉由訪談了解受測資料庫帳戶與權限管理機制 ▪檢視資料庫帳戶與權限列表，確認資料庫預設管理帳戶已變更或停用
1-2	啟用帳戶鎖定次數	資料庫應設定帳戶鎖定次數，避免攻擊者進行暴力破解攻擊	▪藉由訪談了解受測資料庫帳戶管理及通行碼設定規範 ▪檢視帳戶鎖定相關設定，確認帳戶鎖定次數功能已確實啟用，並符合機關規範
1-3	啟用帳戶鎖定時間	資料庫應設定帳戶鎖定時間，避免攻擊者進行暴力破解攻擊	▪藉由訪談了解受測資料庫帳戶管理及通行碼設定規範 ▪檢視帳戶鎖定相關設定，確認帳戶鎖定時間功能已確實啟用，並符合機關規範
1-4	啟用通行碼複雜度原則	資料庫應設定通行碼複雜度，避免因通行碼強度不足而遭破解	▪藉由訪談了解受測資料庫帳戶管理及通行碼設定規範 ▪檢視帳戶通行碼相關設定，確認是否已啟用通行碼複雜度(英數

項次	檢測項目	項目說明	檢測方法
			字、大小寫、特殊符號)原則，並符合機關規範
1-5	啟用通行碼長度原則	資料庫應設定適當通行碼長度，以強化通行碼強度	▪藉由訪談了解受測資料庫帳戶管理及通行碼設定規範 ▪檢視帳戶通行碼相關設定，確認是否已啟用通行碼長度原則，並符合機關規範
1-6	啟用通行碼最長有效期限原則	資料庫應設定通行碼最長有效期限，以確保通行碼定期變更	▪藉由訪談了解受測資料庫帳戶管理及通行碼設定規範 ▪檢視帳戶通行碼相關設定，確認是否已啟用通行碼最長有效期限原則，並符合機關規範
1-7	限制管理者帳戶透過遠端存取	資料庫應限制管理者帳戶無法從非管理者網段進行遠端連線	▪藉由訪談了解資料庫管理者遠端連線機制 ▪檢視遠端連線設定與連線授權紀錄，確認是否已限制管理者帳戶遠端連線之行為

資料來源：本中心整理

●資料加密

資料庫可透過加密方式與設置傳輸安全機制進行資料保護，並針對加密金鑰進行妥善保護，資料加密檢測重點詳見表 7。

表7　資料加密檢測項目與檢測重點說明

項次	檢測項目	項目說明	檢測方法
2-1	資料庫資料具有適當保	資料庫應設置資料保護機制，避	▪藉由訪談了解資料庫資料保護機制(如加密方式、保護資料範圍等)

項次	檢測項目	項目說明	檢測方法
	護機制(加密)	免機敏資料以明文方式儲存	▪針對資料庫存放機敏資料之表單，檢視其設定方式並確認資料欄位內容是否以加密方式予以保護
2-2	資料庫傳輸具有安全機制	資料庫傳輸應設置安全之加密傳輸通道，避免採用不安全方式進行資料傳輸	▪藉由訪談了解資料庫傳輸保護機制 ▪檢視資料傳輸加密方式與設定狀況，確認是否具有安全傳輸機制
2-3	資料庫加密金鑰具有適當保護機制	資料庫加密金鑰應有適當保護機制，以避免加密金鑰遭取得，進而導致資料外洩	▪藉由訪談了解資料庫加密金鑰管理機制，如使用狀況與保管情形等 ▪檢視資料庫加密金鑰保護機制與金鑰使用之管理方式，確認資料庫加密金鑰已妥善保存，且獲授權人員方可存取

資料來源：本中心整理

●存取授權

針對資料庫之存取授權，應限制服務埠、連線來源及連線帳戶，並針對操作行為留存軌跡及秉持最小授權原則，存取授權檢測重點詳見表 8。

表8　存取授權項目與檢測重點說明

項次	檢測項目	項目說明	檢測重點說明
3-1	限制資料庫主機服務埠	資料庫主機應僅開啟允許之服務埠	▪藉由訪談了解資料庫主機連線對象、連線目的及使用之服務埠 ▪檢視資料庫主機是否僅開啟允許之服務埠

項次	檢測項目	項目說明	檢測重點說明
3-2	限制遠端存取來源	資料庫應僅允許授權之來源 IP 可遠端連線	▪藉由訪談了解資料庫遠端存取控管機制 ▪檢視資料庫遠端存取相關來源與連線授權紀錄，確認是否已防止非授權來源 IP 進行連線
3-3	限制遠端存取帳戶	資料庫應僅允許授權之帳戶可遠端存取	▪藉由訪談了解資料庫遠端存取控管機制 ▪檢視資料庫遠端存取相關設定與授權紀錄，確認是否已防止非授權帳戶進行遠端存取
3-4	限制遠端存取操作	資料庫應僅允許授權之遠端存取操作	▪藉由訪談了解資料庫遠端存取控管機制 ▪檢視資料庫遠端存取相關設定與授權紀錄，確認是否已限制非授權之遠端操作行為
3-5	資料庫帳戶權限最小原則	資料庫帳戶權限配置應遵循最小權限原則	▪藉由訪談了解資料庫身分鑑別、存取管理及權限劃分機制 ▪檢視資料庫權限相關申請、審核紀錄及帳戶列表，確認每個資料庫帳戶僅能存取授權之資料內容

資料來源：本中心整理

●稽核紀錄

資料庫應針對資料庫帳戶變更、帳戶登出/登入、資料庫結構變更等啟用稽核紀錄，並建立稽核紀錄管理機制，以及設定主機校時，且定期分析稽核紀錄，稽核紀錄檢測重點詳見表 9。

表9　稽核紀錄檢測項目與檢測重點說明

項次	檢測項目	項目說明	檢測重點說明
4-1	啟用資料庫帳戶變更稽核	資料庫帳戶之新增、刪除應進行稽核	▪藉由訪談了解資料庫稽核紀錄留存項目、保存週期及管理機制 ▪檢視資料庫帳戶異動稽核紀錄設定結果、留存內容及管理方式，確認是否啟用資料庫帳戶變更稽核功能
4-2	啟用資料庫帳戶登出/登入稽核	資料庫帳戶之登入/登出應進行稽核	▪藉由訪談了解資料庫稽核紀錄留存項目、保存週期及管理機制 ▪檢視資料庫帳戶登入/登出稽核紀錄設定結果、留存內容及管理方式，確認是否啟用資料庫帳戶之登入/登出稽核功能
4-3	啟用資料庫結構變更稽核	資料庫結構新增/刪除/修改應進行稽核	▪藉由訪談了解資料庫稽核紀錄留存項目、保存週期及管理機制 ▪檢視資料庫結構異動稽核紀錄設定結果、留存內容及管理方式，確認是否啟用資料庫結構新增/刪除/修改之稽核功能
4-4	稽核紀錄管理方式	資料庫稽核紀錄應妥善保存並定期備份	▪藉由訪談了解資料庫稽核紀錄保存週期、保管方式及管理機制 ▪檢視資料庫稽核紀錄之存取控制與保存紀錄，並確認是否已定期備份稽核紀錄
4-5	資料庫主機時間校時	資料庫主機應進行校時，以確保稽核紀錄時間之正確性	▪藉由訪談了解資料庫主機校時管理機制 ▪檢視資料庫主機校時方式、校時來源及時間正確性，以確認校時功能是否已確實生效

項次	檢測項目	項目說明	檢測重點說明
4-6	稽核紀錄分析	資料庫稽核紀錄應定期進行檢視與分析，確認是否有未經授權之存取與錯誤事件，或與其他紀錄進行關聯分析，以及早發現異常行為並進行因應	▪藉由訪談了解資料庫稽核紀錄分析機制及異常紀錄處理方式 ▪檢視資料庫稽核紀錄分析規則設定、分析紀錄或報告，以及針對異常事件處理方式，確認是否定期進行檢視與分析

資料來源：本中心整理

●委外管理

針對資料庫之委外管理，應限制外部連線、資料存取及帳戶授權，以避免非授權之存取行為，委外管理檢測重點詳見表 10。

表10 委外管理檢測項目與檢測重點說明

項次	檢測項目	項目說明	檢測重點說明
5-1	委外廠商外部連線方式	資料庫應限制委外廠商之外部連線行為	▪藉由訪談了解資料庫委外廠商連線存取控管機制 ▪檢視資料庫委外廠商之外部連線方式設定、授權紀錄及相關防護機制，確認針對連線來源、時間及目的端是否設定存取控制
5-2	委外廠商資料存取方式	資料庫應針對委外廠商資料存取方式，採取相關安全管控措施	▪藉由訪談了解資料庫委外廠商連線存取控管機制

項次	檢測項目	項目說明	檢測重點說明
			▪檢視資料庫委外廠商資料存取方式、授權紀錄及相關防護機制，確認委外廠商存取方式之安全性
5-3	委外廠商帳戶授權方式	應針對資料庫委外廠商帳戶權限申請進行審核	▪藉由訪談了解資料庫委外廠商帳戶權限管理機制 ▪檢視資料庫委外廠商帳戶權限設定與授權紀錄，確認帳戶權限之適當性

資料來源：本中心整理

●備份保護

資料庫應定期執行備份，並予以保護，以及定期測試備份資料之有效性，備份保護檢測重點詳見表 11。

表11 備份保護檢測項目與檢測重點說明

項次	檢測項目	項目說明	檢測重點說明
6-1	資料庫定期執行備份	資料庫應定期執行資料庫備份，並於備份完成後確認備份作業正常執行	▪藉由訪談了解資料庫備份管理機制 ▪檢視資料庫備份方式(如備份時間、週期及方式等)與備份結果，確認備份機制正常運作
6-2	資料庫備份具有適當保護機制	資料庫備份應具備適當保護方式，避免非經授權存取	▪藉由訪談了解資料庫備份檔案之保護機制 ▪檢視資料庫備份之存取控制與保護方式，如異地儲存與內容加密等，確保僅獲授權人員方可存取
6-3	資料庫備份回復測試	資料庫備份應定期執行回復測	▪藉由訪談了解資料庫備份回復測試執行方式與週期

項次	檢測項目	項目說明	檢測重點說明
		試，確保備份資料之可用性，並留存測試紀錄	▪檢視資料庫備份回復測試執行結果與紀錄，確認備份資料之有效性

資料來源：本中心整理

●弱點管理

資料庫應定期執行弱點掃描，以及修補所發現弱點項目，並持續針對資料庫主機之安全性更新進行修補，弱點管理檢測重點詳見表 12。

表12 弱點管理檢測項目與檢測重點說明

項次	檢測項目	項目說明	檢測重點說明
7-1	執行資料庫主機弱點掃描	應定期執行資料庫主機弱點掃描	▪藉由訪談了解資料庫主機弱點掃描執行方式與頻率 ▪檢視資料庫主機弱點掃描紀錄，確認機關落實定期掃描，並掌握風險現況
7-2	修補資料庫主機弱點項目	應定期針對資料庫主機弱點進行修補，並留存紀錄	▪藉由訪談了解資料庫主機弱點修補與追蹤機制 ▪檢視資料庫主機弱點修補紀錄，確認是否已依規定修補所發現之弱點，並針對無法於短期內修補之弱點，是否採取其他替代措施，以降低資安風險
7-3	修補資料庫主機安全性更新項目	資料庫主機應定期安裝作業系統與應用程式之安全性更新項目	▪藉由訪談了解資料庫主機作業系統與應用程式之安全性更新執行方式與頻率

項次	檢測項目	項目說明	檢測重點說明
			▪檢視資料庫主機作業系統與應用程式之安全性更新歷程紀錄，確認已落實執行更新作業

資料來源：本中心整理

4.2 主機安全檢測

主機安全檢測項目係透過訪談與實際檢視資料庫主機作業系統層面安全防護情形，包含帳戶管理、權限設定及存取管控情形(詳見表 13)，並透過弱點掃描方式，確認主機相關弱點管理結果。

表13 主機安全檢測查檢表

機關名稱			
檢測日期		____年___月___日	
項次	檢測類別	檢測項目	發現與改善建議
1-1	帳戶管理	變更預設帳戶	
1-2		啟用帳戶鎖定次數	
1-3		啟用帳戶鎖定時間	
1-4		啟用通行碼長度原則	
1-5		啟用通行碼複雜度原則	
1-6		啟用通行碼最長有效期限原則	
2-1	權限設定	帳戶隸屬群組	
2-2		預設帳戶停用	
2-3		委外廠商帳戶管理	

機關名稱			
檢測日期		____年___月___日	
項次	檢測類別	檢測項目	發現與改善建議
2-4		遠端連線權限設定	
3-1	存取管控	機敏資訊目錄管控機制	
3-2		備份資料目錄管控機制	
4-1	弱點掃描	高風險項目	
4-2		中風險項目	
4-3		低風險項目	

資料來源：本中心整理

●帳戶管理

針對資料庫主機作業系統環境，檢視帳戶與通行碼管理方式，包含變更預設帳戶、啟用帳戶鎖定次數、啟用帳戶鎖定時間、啟用通行碼長度原則、啟用通行碼複雜度原則及啟用通行碼最長有效期限原則，以確保可降低帳戶或通行碼被破解之威脅。

●權限設定

針對資料庫主機作業系統環境，檢視包含帳戶隸屬群組、預設帳戶停用、委外廠商帳戶及遠端連線等權限設定，確認資料庫主機權限設定情形。

●存取管控

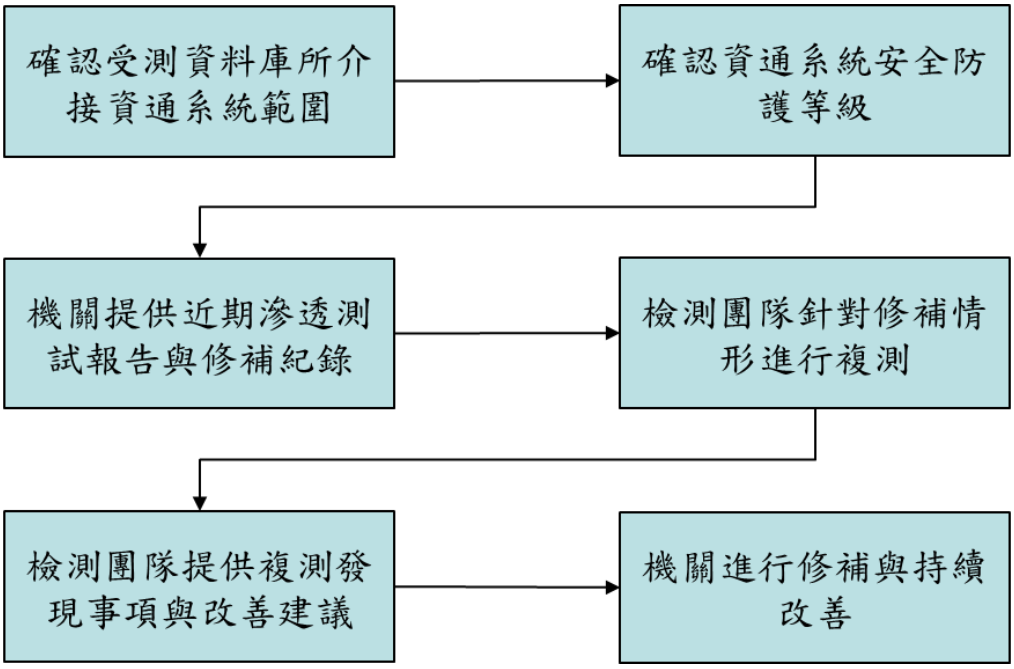
針對資料庫主機作業系統環境，檢視存放機敏資訊或備份資料目錄之存取授權管控方式，避免非經授權之存取行為。

●弱點掃描

使用合法授權之掃描軟體對資料庫主機進行弱點掃描，並針對掃描結果進行驗證與留存紀錄，確認其弱點影響狀況。另檢視受測機關近期資料庫主機弱點掃描報告，以交互比對方式追蹤與確認弱點修補情形。

4.3 資通系統安全檢測

針對受測核心資料庫相關聯之資通系統，若為受測機關自行維運管理，且符合「資通安全責任等級分級辦法」所規範應定期執行系統滲透測試之資通系統，則須請受測機關提供近期滲透測試執行報告與相關修補紀錄。檢測團隊將針對修補內容進行複測，以確認弱點修補落實程度，並記錄未確實修補項目，協助受測機關識別風險並提供改善建議，資通系統安全檢測作業流程詳見圖 3。



資料來源：本中心整理

圖3　資通系統安全檢測作業流程

4.4 網路安全檢測

針對資料庫之網路安全檢測，將透過訪談與實際檢視方式確認網路架構設

計邏輯是否合宜、資料庫主機網路位置是否適當、資通系統與資料庫介接情形、防火牆規則、VPN 連線管理、遠端連線管理與限制及事件記錄設定之適當性，以評估資料庫可能存在之風險，17 項網路安全檢測項目詳見表 14。

表14 網路安全檢測查檢表

機關名稱	
檢測日期	____年___月___日

項次	檢測項目	現況說明與改善建議
1	網路系統架構區域	
2	網路區域間的存取	
3	部署入侵偵測/防禦系統	
4	部署系統本機安全機制	
5	建立實體備援機制	
6	建立服務備援機制	
7	限制內部對外連線	
8	限制外部對內連線	
9	限制服務區域連線	
10	應不包含 Permit All/Any 於任一個規則	
11	應定義 Deny All/Any 於最後一個規則	
12	限制非加密資料傳輸協定	
13	遠端連線存取控制	
14	網路設備存取鑑別	
15	網路設備存取控制	

機關名稱		
檢測日期	____年___月___日	
項次	檢測項目	現況說明與改善建議
16	網路設備 SNMP 設定	
17	網路設備校時設定	

資料來源：本中心整理

5. 結案階段

完成各項檢測後，將依各項檢測紀錄進行彙整與分析，並依分析結果提供改善建議，供受測機關提升資安防護能量，檢測結果報告與改善建議內容重點說明如下。

5.1 資料庫安全檢測

透過訪談與實機檢視，針對各檢測項目提出機關管理作為之脆弱點，於檢測結果報告中詳列受測類別、受測項目、現況說明、檢測結果及強化建議，以利受測機關了解弱點可能造成之影響，並進行後續調整與追蹤。

5.2 主機安全檢測

透過弱點掃描檢視資料庫主機弱點管理情形，並交叉比對機關最近一次弱點掃描與修補情況，確認相關弱點已被識別與控管，於結果報告中詳述弱點資訊、中高風險數量、風險等級及修補建議，以利受測機關了解弱點可能造成之影響並進行修補與追蹤。另透過訪談與實機檢視，針對系統帳戶權限、存取控制及弱點管理等面向之設定進行確認，於檢測結果報告中詳列受測項目、現況說明、檢測結果及強化建議，以利受測機關後續調整。

5.3 資通系統安全檢測

檢視機關最近一次滲透測試報告與修補紀錄，依報告內之滲透測試手法，再次重現與實際驗證，確認修補之有效性，針對未有效修補之弱點，於檢測結果報告中詳列測試標的之弱點名稱、風險等級及實際攻擊成功之檢測畫面，驗證弱點未被確實修補，而針對檢測過程中額外發現之弱點項目，則詳列弱點名稱、風險等級、弱點所在頁面、檢測手法、導致之風險及可能洩漏資訊內容，並說明弱點修補方式，以利受測機關快速掌握弱點成因與影響範圍，並可參考改善方式做為修補參考。

5.4 網路安全檢測

針對檢測標的所發現之中高風險弱點進行統計，詳列發現事項之風險等級、風險說明及改善建議，風險說明詳述問題範圍與可能之影響，並提出具體改善建議，以利受測機關後續修補與調整。

6. 結論

因應資料外洩事件層出不窮，為協助政府機關提升資料庫安全防護能力，本文件針對資料庫安全防護研析相關技術檢測面向、發展各項檢測項目、執行方式及設計標準化作業程序。依所發展之資料庫安全、主機安全、資通系統安全及網路安全等 4 項檢測項目執行方式，提升技術檢測能力，並依規劃之前置、執行及結案等 3 階段標準化作業流程、相關查檢表及紀錄內容重點，以利政府機關自我檢測或第三方檢測時掌握各檢測項目執行重點與留下相關紀錄，以利提升資料庫安全防護程度。

7. 附件

資料庫技術檢測基本資訊蒐集表

1.填表人基本資料			
機關名稱			
填表人姓名			
填表人公務電話		分機	
填表人公務 E-mail			
填表日期	_____年　　月　　日		

2.資料庫安全檢測		
2.1.資料庫基本資訊		
2.1.1.資料庫名稱		
2.1.2.資料庫版本		
2.1.3.官方預設帳戶		
2.2.資料庫帳戶管理		
2.2.1.啟用帳戶鎖定次數	□是，於錯誤　　次後鎖定	□否 (請跳至2.2.3)
2.2.2.啟用帳戶鎖定時間	□是，將鎖定　　分鐘	□否
2.2.3.啟用「通行碼複雜度」原則(可複選)	□是，複雜度原則包含： □英文 □數字 □大小寫 □特殊符號	□否
2.2.4.啟用「最小通行碼長	□是，通行碼長度至少　　個字	□否

度」原則	元	
2.2.5.啟用「資料庫管理帳戶的通行碼最長有效期限」原則	□是，通行碼最長有效期為日	□否
2.2.6.是否停用或變更官方預設帳戶	□是	□否
2.3.資料庫資料保護機制		
2.3.1.是否具備資料保護機制 (可複選)	□是，機制為： □使用資料庫加密 □資料表欄位內容加密 □資料表欄位內容遮罩 □其他，請補充說明：	□否
2.3.2.是否採用第三方加解密工具	□是，工具名稱：	□否
2.4.資料庫備份管理機制		
2.4.1.資料庫備份週期	□是，備份週期為： □每天 □每週 □每月 □其他：	□否
2.4.2.資料庫備份執行方式 (可複選)	□完整備份 □差異備份 □增量備份 □其他：	
2.4.3.資料庫備份儲存方式 (可複選)	□本地備份 □異地備份 □其他：	
2.4.4.資料庫備份保護方式	□是，備份保護方式： □備份檔案加密	□否

	□硬體加密 □實體保護(如儲存資料櫃上鎖) □其他：	
2.4.5.資料庫備份回復測試	□是， ▪ 測試頻率： □每季 □每半年 □每年 □其他： ▪ 最近一次執行日期： 年 月 日	□否
2.5.資料庫弱點管理機制		
2.5.1.執行資料庫主機弱點掃描	□是， ▪ 弱點掃描執行頻率： □每週 □每月 □每季 □其他： ▪ 最近一次掃描日期： 年 月 日 ▪ 執行廠商： ▪ 掃描工具：	□否
2.5.2.定期修補資料庫主機弱點	□是， ▪ 弱點修補頻率： □每月 □每季 □每半年 □其他： ▪ 弱點修補門檻： □僅修補高風險弱點 □修補中風險以上弱點 □修補低風險以上弱點	□否
2.5.3.定期修補資料庫主機安全性更新項目	□是，	□否

	▪更新方式： □集中管控、派送(如中控台) □管理者手動更新 □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	
2.6.資料庫存取與授權		
2.6.1.限制資料庫主機服務埠	□是，僅開啟下列服務埠：	□否
2.6.2.限制遠端存取的 IP 來源	□是，僅允許下列來源 IP 可存取資料庫：	□否
2.6.3.限制遠端存取的帳戶	□是，僅允許下列帳戶可遠端存取資料庫：	□否
2.6.4.禁止管理者帳戶透過遠端存取	□是，限制管理者帳戶直接透過遠端連線進行操作	□否
2.6.5.資料庫帳戶權限最小化原則	□是，依照職務區隔限制資料庫帳戶所需權限	□否
2.6.6.資料庫連線傳輸安全機制	□是，連線傳輸安全機制如下：	□否
2.7.資料庫稽核與紀錄		
2.7.1.啟用資料庫帳戶變更稽核	□是，針對資料庫的帳戶變動(新增、刪除、修改)，留存相關紀錄	□否
2.7.2.啟用資料庫存取稽核	□是，針對資料庫的帳戶登出/登入行為，留存相關紀錄	□否
2.7.3.啟用資料庫結構變	□是，針對資料庫結構新增、刪除、	□否

更稽核	修改等行為，留存相關紀錄	
2.7.4.建立稽核紀錄備份週期	□是，備份週期： □每週 □每月 □每季 □其他：	□否
2.7.5.稽核紀錄備份儲存方式	□本機備份 □異地備份 □其他：	
2.7.6.設定資料庫主機校時	□是，校時主機 IP 如下：	□否
2.7.7.定期分析稽核紀錄	□是， ▪分析稽核紀錄執行頻率： □每週 □每月 □每季 □其他： ▪最近一次分析日期： 年 月 日 ▪分析工具：	□否

3.主機安全檢測	
3.1.資料庫主機基本資訊	
3.1.1.資料庫主機名稱	
3.1.2.資料庫主機 IP	
3.1.3.資料庫主機作業系統版本	
3.1.4.資料庫主機服務應用程式	
3.1.5.資料庫主機開啟通訊埠	
3.1.6.資料庫主機實體存放位置	

3.1.7.資料庫介接系統列表			
系統名稱	來源 IP	內/外部系統	系統說明
		□內部 □外部	
		□內部 □外部	
		□內部 □外部	
		□內部 □外部	
		□內部 □外部	

4.資通系統安全檢測			
4.1.系統基本資訊			
4.1.1.核心資通系統名稱			
4.1.2.系統簡介			
4.1.3.系統首頁網址	□網址： □無		
4.1.4.業務屬性	□行政類	□業務類	
4.1.5.資通系統安全等級	□高	□中	□低
4.1.6.是否含有個資	□含特種個資與一般個資 □僅有一般個資	□僅有特種個資 □無個資	
4.1.7.是否曾執行安全檢	□無	□弱點掃描	

測(可複選)	□滲透測試　　□原碼檢測
4.1.8.系統使用對象	□為民服務(提供一般民眾使用) □內部使用(僅供機關內部同仁使用) □其他：
4.1.9.系統是否具備 Load Balance 機制(否，請跳至 4.1.12)	□是 □否
4.1.10.系統由內網連線是否經過 Load Balance 機制	□所有連線強制通過 Load Balance 機制分配 □僅網頁連線強制通過 Load Balance 機制分配，其餘連線可透過 IP 連線至主機 □所有連線除可通過 Load Balance 機制分配外，亦可透過 IP 連線至主機 □其他：
4.1.11.系統使用限制	▪作業系統版本限制： ▪作業系統位元限制：□32 位元　□64 位元 ▪瀏覽器版本限制： ▪需安裝 Client 端程式：□是　□否 Client 端程式安裝作業系統限制： Client 端程式安裝元件限制： 其他限制：
4.1.12.由內部網路連線至核心資訊系統是否經過相關安全防護設備	□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：
4.2 系統存取管理	
說明：	

系統前台登入介面：係指供使用者登入進行系統操作之介面。 系統後台管理登入介面：係指僅供管理人員登入進行系統管理之介面。 若系統無區分前、後台，使用者與管理人員使用相同登入介面時，請將此登入介面視為系統前台登入介面，並填答 4.2.1~4.2.7 問項。 外部網路：係指機關使用 IP 範圍外之網路。 內部網路：係指機關使用 IP 範圍內之網路。	
4.2.1.系統是否有前台登入介面(若否，請跳至 5.8 作答)	□是　□否
4.2.2.系統前台登入介面網址	□網址： □使用 Client 端應用程式登入 □其他：
4.2.3.系統前台登入是否使用單一簽入機制(若否，請跳至 4.2.5 作答)	□是　□否
4.2.4.單一簽入系統之管理單位	□自行管理　□主管機關管理 主管機關名稱：
4.2.5.系統前台登入介面連線方式	□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
4.2.6.系統前台登入介面之登入方式	□帳戶通行碼登入 □軟體憑證登入 □晶片卡登入
4.2.7.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：
4.2.8.系統是否有後台管理登入	□是　□否

介面(若否，請跳至 4.3 作答)	
4.2.9 系統後台管理登入介面	□網址： □使用 Client 端應用程式登入 □其他：
4.2.10.系統後台管理登入是否使用單一簽入機制(否，請跳至 4.2.12 作答)	□是　　□否
4.2.11.單一簽入系統之管理單位	□自行管理　　□主管機關管理 主管機關名稱：
4.2.12.系統後台管理登入介面連線方式	□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
4.2.13.系統後台管理登入介面登入方式 (可複選)	□帳戶通行碼登入 □軟體憑證登入 □晶片卡登入
4.2.14.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：

4.3 系統主機資訊　※項次不足請自行增加

類型 (可複選)	主機名稱	內部 IP	作業系統版本	服務應用程式	主機開啟 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						

5.網路安全檢測					
5.1.服務主機資訊蒐集　※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	AD Server	☑			
範例 2	AD Server	□	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
1	AD Server	□	1		
			2		
2	內部 Mail Server	□	1		
			2		
3	外部 Mail Server	□	1		
			2		

4	內部 DNS Server	☐	1		
			2		
5	外部 DNS Server	☐	1		
			2		
6	WSUS Server	☐	1		
			2		
7	防毒伺服器	☐	1		
			2		

5.2.防護主機資訊蒐集　※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	IP
範例 1	核心資訊系統前端是否有 WAF 設備	☑			
範例 2	核心資訊系統前端是否有 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
1	核心資訊系統前端是否有 WAF 設備	☐	1		
			2		
2	核心資訊系統前端是否有 IPS 設備	☐	1		
			2		
3	惡意中繼站 IP 部署位置	☐	1		
			2		
4	惡意中繼站 DN 部署	☐	1		

	位置		2		
5.3.核心網路設備資訊蒐集　※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
1	對外線路閘道器	☐	1		
			2		
2	防火牆	☐	1		
			2		
3	核心交換器	☐	1		
			2		
5.4.線路資訊蒐集　※項次不足請自行增加					
5.4.1	對外線路	▪ ISP 名稱：　　，配發 IP： ▪ ISP 名稱：　　，配發 IP： ▪ ISP 名稱：　　，配發 IP： ▪ ISP 名稱：　　，配發 IP：			
5.4.2	是否與其他機關資料交換	☐是， ▪ 機關名稱： ▪ ISP 名稱： ☐否			

5.5.網段資訊蒐集　※項次不足請自行增加				
編號	項目	無此網段	項次	網段
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
1	是否有網路管理人員網段	☐	1	
			2	
2	是否有系統管理人員網段	☐	1	
			2	
3	是否有資料庫管理人員網段	☐	1	
			2	
4	是否有程式開發人員網段	☐	1	
			2	
5	是否有系統主機開發、測試網段	☐	1	
			2	
6	是否有虛擬私有網路(VPN)網段	☐	1	
			2	
7	是否有實體隔離網段	☐	1	
			2	
8	是否有網路設備網段	☐	1	
			2	

5.6 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			