附表三　　# 資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：＿年＿月＿日

查　核　項　目	自我評審			查核員評量			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
1 資訊安全政策				☐	☐	☐	☐
1.1管理階層是否瞭解資訊安全目的並予支持？	☐	☐	☐	☐	☐	☐	☐
1.2貴機關之資訊安全政策文件是否由管理階層核准並正式發布且轉知所有員工？	☐	☐	☐	☐	☐	☐	☐
1.3貴機關是否訂有資訊安全政策的說明文件及資料(如作業程序、資訊安全控管文件、使用者應遵守的安全規則)？	☐	☐	☐	☐	☐	☐	☐
1.4資訊安全政策文件是否包括資訊安全定義、目標、涵蓋範圍、實施內容、執行組織、權責分工、員工責任、事件通報程序、處理流程等？	☐	☐	☐	☐	☐	☐	☐
1.5資訊安全政策文件是否就一般使用人員與專責人員之權責分項說明？	☐	☐	☐	☐	☐	☐	☐
1.6是否指定專人或專責單位進行資訊安全政策的維護及檢討工作？	☐	☐	☐	☐	☐	☐	☐
1.7資訊安全政策是否定期評估，並作必要調整？	☐	☐	☐	☐	☐	☐	☐
1.8是否定期對單位人員及資訊設備進行安全評估，以確定其是否遵守機關資訊安全政策及相關規定？	☐	☐	☐	☐	☐	☐	☐
1.9是否訂有違反資訊安全規定之處理程序？	☐	☐	☐	☐	☐	☐	☐
1.10與外單位簽訂資料存取之契約中是否包含資料保護、服務水準、智慧財產權、事故發生處理方式等條款？	☐	☐	☐	☐	☐	☐	☐
1.11委外契約中有關安全需求內容是否包含法律需求(如電腦處理個人資料保護法)、界定雙方有關人員權責、使用何種實體與邏輯安全控管措施、對委外廠商稽核權、得依實際需要隨時修改安全控管措施及作業程序等？	☐	☐	☐	☐	☐	☐	☐
2 建立資訊安全組織				☐	☐	☐	☐
2.1是否指定高級主管人員或成立跨部門組織負責推動、協調及監督資訊安全管理事項？	☐	☐	☐	☐	☐	☐	☐
2.2是否指定專人或專責單位負責規劃、執行與控管資訊安全工作？	☐	☐	☐	☐	☐	☐	☐
2.3是否指定單位辦理風險評估、安全分級、系統安全控管措施？	☐	☐	☐	☐	☐	☐	☐
2.4是否訂定規範員工的資訊安全作業程序與權責(含經管使用設備及作業須知)？	☐	☐	☐	☐	☐	☐	☐
2.5是否訂定各項資訊設備的安全作業程序？	☐	☐	☐	☐	☐	☐	☐
2.6是否訂定有關資訊安全狀況授權處理層級？	☐	☐	☐	☐	☐	☐	☐
2.7是否對資訊計畫內容進行資訊安全政策符合性檢查？	☐	☐	☐	☐	☐	☐	☐
2.8單位內因業務需要開放給外單位(含其他機關、上下游業者、顧問、維護廠商、委外承包商、臨僱人員)使用之資訊，其存取權限是否嚴加控管？	☐	☐	☐	☐	☐	☐	☐
2.9單位內開放給外單位作資料存取是否辦理風險評估？	☐	☐	☐	☐	☐	☐	☐
2.10單位內開放給外單位作資料存取是否訂定控管程序？	☐	☐	☐	☐	☐	☐	☐
2.11單位內開放給外單位作資料存取於契約中是否訂定雙方權利義務及違約處分方式？	☐	☐	☐	☐	☐	☐	☐

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：__年__月__日

查　　核　　項　　目	自我評審			查核員評量			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
3 人員安全與管理				□	□	□	□
3.1對人員之進用及調派，是否作適當之安全評估？	□	□	□	□	□	□	□
3.2對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有妥適分工，分散權責？	□	□	□	□	□	□	□
3.3對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否實施人員輪調？	□	□	□	□	□	□	□
3.4對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有建立人力備援制度？	□	□	□	□	□	□	□
3.5針對人員之調動、離職或退休，是否立即取消其各項識別碼、通行碼？	□	□	□	□	□	□	□
3.6是否對員工品德、行爲、家庭狀況等加以考核？	□	□	□	□	□	□	□
3.7員工是否瞭解單位之資訊安全政策？	□	□	□	□	□	□	□
3.8是否依員工職務層級進行適當的資訊安全講習？	□	□	□	□	□	□	□
3.9是否隨時公告資訊安全相關訊息？	□	□	□	□	□	□	□
3.10下班後員工是否將經辦之機密性或敏感性資料，妥善收藏？	□	□	□	□	□	□	□
3.11是否對員工的私人資訊設備作必要之安全控管程序？	□	□	□	□	□	□	□
3.12單位是否派員參與外界舉辦相關訓練、研討會、產品展示會？	□	□	□	□	□	□	□
4 資產分類與控管				□	□	□	□
4.1重要的資產(含資訊、軟體、實體)是否均指定專人負責？	□	□	□	□	□	□	□
4.2是否建置資產清冊且隨時更新？	□	□	□	□	□	□	□
4.3資訊是否分級(區分機密性、敏感性及一般性)？是否建立資訊安全等級之分類標準？	□	□	□	□	□	□	□
4.4是否配合資訊分級，建立一套符合需要的資訊保護措施？	□	□	□	□	□	□	□
4.5系統文件、顯示螢幕、儲存媒體、電子訊息及檔案資料等是否作安全等級分類？	□	□	□	□	□	□	□
4.6對於安全等級要求高的各類資訊，是否標示清楚？	□	□	□	□	□	□	□
5實體及環境安全管理				□	□	□	□
5.1資訊設備之設置是否作安全上之考量？	□	□	□	□	□	□	□
5.2機密性工作站是否專人管理？	□	□	□	□	□	□	□
5.3需特別保護之設備是否與一般設備區隔？	□	□	□	□	□	□	□
5.4是否檢查及評估火、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害？	□	□	□	□	□	□	□
5.5電腦作業區(含機房)是否落實執行禁止抽煙及飲用食物？	□	□	□	□	□	□	□
5.6電源之供應及備援電源是否作安全上考量？	□	□	□	□	□	□	□
5.7通訊線路及電纜線是否作安全保護措施？	□	□	□	□	□	□	□
5.8設備之維護是否由授權之維護人員執行？	□	□	□	□	□	□	□
5.9攜帶型的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)並落實執行？	□	□	□	□	□	□	□
5.10設備報廢前是否先將機密性、敏感性資料及有版權軟體移除？	□	□	□	□	□	□	□
5.11電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	□	□	□	□	□	□

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：＿年＿月＿日

查　核　項　目	自我評審			查核員評量			
	是	否	不適用	完整性 非常	尚屬	不盡	不適用
5.12電腦機房內是否嚴禁存放易燃物及未經核准之電器或其他物品？	□	□	□	□	□	□	□
5.13電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	□	□	□	□	□	□	□
5.14電腦機房操作人員是否熟悉自動滅火系統操作方法及滅火機位置？	□	□	□	□	□	□	□
5.15各項安全設備是否定期檢查？員工有否施予適當的安全設備使用訓練？	□	□	□	□	□	□	□
5.16是否制訂資訊安全緊急應變處理程序？有否定期演練及測試？	□	□	□	□	□	□	□
5.17公文及磁片長時間不使用及下班後是否妥爲存放？機密性、敏感性資訊是否妥爲收存？	□	□	□	□	□	□	□
5.18棄置之手寫或影印公文廢紙及已過保存期限之公文，若爲機密性、敏感性者是否予以銷毀？	□	□	□	□	□	□	□
5.19個人電腦及終端機不使用時是否有關機、登出、設定螢幕密碼或是以其他控制措施進行保護？	□	□	□	□	□	□	□
5.20對於資訊財產攜出辦公處所，是否訂有安全之攜出管理規則？	□	□	□	□	□	□	□
6 通訊與操作管理				□	□	□	□
6.1資訊處理設備，是否訂有操作程序及管理責任？	□	□	□	□	□	□	□
6.2是否建立系統變更之程序？	□	□	□	□	□	□	□
6.3是否訂定電腦當機及服務中斷後之緊急處理程序？	□	□	□	□	□	□	□
6.4是否訂有資訊安全事件通報程序並確實依規定通報？	□	□	□	□	□	□	□
6.5資訊安全事件處理的過程是否均留有完整記錄？	□	□	□	□	□	□	□
6.6對安全要求高的資訊業務是否將資訊安全管理及執行的責任分散？	□	□	□	□	□	□	□
6.7業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否授權分由不同的人員執行？	□	□	□	□	□	□	□
6.8系統開發及正式作業是否在不同的處理器、不同的系統環境處理？	□	□	□	□	□	□	□
6.9系統開發及正式作業是否使用不同的登入程序？	□	□	□	□	□	□	□
6.10是否與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款？	□	□	□	□	□	□	□
6.11資訊委外服務契約是否包含對於機密性、敏感性資料之雙方權責及作業程序？	□	□	□	□	□	□	□
6.12伺服器及個人電腦是否採行必要的事前預防及保護措施？	□	□	□	□	□	□	□
6.13是否遵守軟體授權規定，禁止使用未取得授權的軟體？	□	□	□	□	□	□	□
6.14是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	□	□	□	□
6.15是否即時公告有關病毒最新資訊？	□	□	□	□	□	□	□
6.16是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	□	□	□	□
6.17是否對單位員工辦理資訊安全宣導講習(含防毒、備份及一般機密保護規定)？	□	□	□	□	□	□	□

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：__年__月__日

查　核　項　目	自我評審			查核員評量			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
6.18對於外來及內容不確定的磁片在使用前，是否先作電腦病毒掃瞄？	□	□	□	□	□	□	□
6.19是否對重要的資料及軟體定期作備份處理？	□	□	□	□	□	□	□
6.20備份資料是否異地存放?存放處所環境是否合於電腦機房安全標準？	□	□	□	□	□	□	□
6.21重要資料的備份是否保留三代以上？	□	□	□	□	□	□	□
6.22是否定期測試備份資料以確保備份資料之可用性？	□	□	□	□	□	□	□
6.23是否檢查更正作業妥適與否？確保更正作業未破壞系統原有的安控措施及更正作業係依正當的授權程序辦理。	□	□	□	□	□	□	□
6.24是否定期檢討電腦網路安全控管事項之執行？	□	□	□	□	□	□	□
6.25是否使用網路防火牆(Fire Wall)？	□	□	□	□	□	□	□
6.26是否定期檢測網路運作環境之安全漏洞？	□	□	□	□	□	□	□
6.27有關電腦網路安全之事項是否隨時公告？	□	□	□	□	□	□	□
6.28對於敏感性資訊之傳送是否採取資料加密等保護措施？	□	□	□	□	□	□	□
6.29媒體儲存的資料不再繼續使用時是否將儲存的內容消除？	□	□	□	□	□	□	□
6.30儲存媒體是否依保存規格要求存放在安全的環境？	□	□	□	□	□	□	□
6.31內含機密性或敏感性資料的媒體報廢時是否指定專人處理？	□	□	□	□	□	□	□
6.32敏感性資料報廢時是否紀錄處理時機、方式、人員？	□	□	□	□	□	□	□
6.33輸出及輸入機密性、敏感性資料是否有處理程序及標示？	□	□	□	□	□	□	□
6.34收受機密性、敏感性資料是否有正式收受紀錄？	□	□	□	□	□	□	□
6.35機密性、敏感性資料在儲存媒體上是否明確標示資料機密等級？	□	□	□	□	□	□	□
6.36系統文件發送對象是否經系統負責人的授權？	□	□	□	□	□	□	□
6.37系統文件是否有適當的存取保護措施？	□	□	□	□	□	□	□
6.38對於資料及軟體之交換使用是否均有相關文件？	□	□	□	□	□	□	□
6.39重要電腦資料媒體(含報表)是否有專人負責運送並記錄運送時間及內容？	□	□	□	□	□	□	□
6.40儲存機密及敏感性資料的電腦媒體是否採取特別的安全保護措施(如使用加密技術)？	□	□	□	□	□	□	□
6.41採行電子交換之資料交換是否視資料之安全等級採行帳號密碼管制、電子資料加密或電子簽章認證等保護措施？	□	□	□	□	□	□	□
6.42是否要求員工接收電子郵件後立即自郵件伺服器中刪除？	□	□	□	□	□	□	□
6.43敏感性、機密性資料的處理過程是否有嚴密的安全保護機制(如數位簽章、認證及加解密等)？	□	□	□	□	□	□	□
7 存取控制	□	□	□	□	□	□	□
7.1是否訂有資訊存取控制政策及相關說明文件？	□	□	□	□	□	□	□
7.2資訊存取控制政策是否符合資料保護等相關法令與契約規定？	□	□	□	□	□	□	□
7.3資訊存取控制政策是否依工作性質與職務分別訂定？	□	□	□	□	□	□	□
7.4是否將資訊存取說明文件列入員工手冊？							
7.5對於多人使用之資訊系統，是否建立使用者註冊管理程序及紀錄？							

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：__年__月__日

查　核　項　目	自我評審			查核員評量			
	是	否	不適用	完整性 非常	尚屬	不盡	不適用
7.6使用者及外單位人員是否取得正式存取授權？	□	□	□	□	□	□	□
7.7是否依個別應用系統安全需求制定安全等級與分類？	□	□	□	□	□	□	□
7.8是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	□	□	□	□	□	□	□
7.9資訊系統與服務是否儘量避免使用共同帳號？	□	□	□	□	□	□	□
7.10使用者存取權限的檢視，是否訂有嚴格管制程序？	□	□	□	□	□	□	□
7.11是否保留與隨時更新使用者註冊資料？	□	□	□	□	□	□	□
7.12是否定期檢查並刪除重覆或閒置的使用者帳號？	□	□	□	□	□	□	□
7.13是否嚴格管制使用者初次登入電腦系統後必須立即更改預設之密碼？	□	□	□	□	□	□	□
7.14對於忘記密碼之處理，是否有嚴格的身份確認程序？	□	□	□	□	□	□	□
7.15預設之密碼是否以規定之安全程序轉交於使用者，使用者取得密碼確認無誤後回應系統管理者？	□	□	□	□	□	□	□
7.16是否定期複檢(建議每六個月一次)或在變更權限後立即稽核？	□	□	□	□	□	□	□
7.17密碼長度是否超過七個字元？	□	□	□	□	□	□	□
7.18密碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	□	□	□	□
7.19密碼輸入錯誤，是否訂有三次以下之限制？	□	□	□	□	□	□	□
7.20是否避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）當做密碼？	□	□	□	□	□	□	□
7.21是否依照規定的期限或使用的次數變更密碼？	□	□	□	□	□	□	□
7.22是否於不使用時用上鎖或密碼等管制措施不讓電腦或終端機遭非法使用？	□	□	□	□	□	□	□
7.23應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？	□	□	□	□	□	□	□
7.24是否有界定網域的範圍與在該網域上可利用的網路連線服務？	□	□	□	□	□	□	□
7.25是否建立完整的網路服務使用授權程序？	□	□	□	□	□	□	□
7.26是否規劃建置使用者連線使用資訊系統的方式(如專線或固定號碼撥接)？	□	□	□	□	□	□	□
7.27是否規劃運作將特定輸出入埠(port)之使用者自動連線到指定的應用系統或安全閘道(Security Gateway)做認證或其他安全辨識的工作再進入系統？	□	□	□	□	□	□	□
7.28是否依環境或業務需要，於網路防火牆作適當之設定？	□	□	□	□	□	□	□
7.29是否依業務性質或任務分配來建置邏輯性網域的存取權限機制(如虛擬私有網路VPN)？	□	□	□	□	□	□	□
7.30對外連線是否有使用密碼技術(Cryptographic based technique)、硬體符記(Hardware token)、挑戰/回應(Challenge/Response)協定或透過檢查專線用戶位址的設備等鑑別方法以找出連線作業的來源？	□	□	□	□	□	□	□
7.31對外連線是否有建置回撥(Dial-back)作業程序與控管措施及相關測試？	□	□	□	□	□	□	□
7.32網路中繼節點設備是否列入管制與鑑別的範疇並有適當的鑑別方法？	□	□	□	□	□	□	□

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：＿年＿月＿日

查　核　項　目	自我評審			查核員評量			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
7.33是否有製訂遠端維護用輸出入埠的存取作業規範並確實遵行(如用鑰匙鎖住，軟硬體維護支援人員須通過查驗或稽核始能進行)？	□	□	□	□	□	□	□
7.34是否依據服務性質區隔出獨立的邏輯網域，每個網域都有既定的防護措施並有通訊閘道管制過濾網域間資料的存取(如網路防火牆)？	□	□	□	□	□	□	□
7.35是否管制使用者的連線功能(如網路通訊閘道所設定的規則)？	□	□	□	□	□	□	□
7.36是否針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段做通盤連線控管考量？	□	□	□	□	□	□	□
7.37是否設有檢測連線的來源位址與目的位址網路路由之控管措施？	□	□	□	□	□	□	□
7.38提供網路服務的供應廠商是否對網路中繼設備的特性與安全政策提供清楚的說明與設定方式？	□	□	□	□	□	□	□
7.39是否限制登入失敗次數的上限(建議三次)並中斷連線？	□	□	□	□	□	□	□
7.40是否限制登入失敗次數超過上限時需經過一段時間或重新取得授權後才可再登入？	□	□	□	□	□	□	□
7.41是否限制登入作業，在一定期間未操作時，即予中斷連線？	□	□	□	□	□	□	□
7.42對於異常的登入程序，是否留有紀錄(LOG FILE)，並有專人定期檢視？	□	□	□	□	□	□	□
7.43是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資料？	□	□	□	□	□	□	□
7.44使用者是否均有專屬的識別碼？	□	□	□	□	□	□	□
7.45是否採用適當的加解密與生物測定技術提供身份辨別(Identification)鑑別	□	□	□	□	□	□	□
7.46密碼是否分由不同單位分配與保管？	□	□	□	□	□	□	□
7.47是否將輸入的密碼顯示在螢幕上？	□	□	□	□	□	□	□
7.48是否將密碼檔與應用系統的資料檔分開儲存？	□	□	□	□	□	□	□
7.49密碼檔是否以單向加密演算法(One-way encryption algorithm)儲存？	□	□	□	□	□	□	□
7.50軟體安裝完畢後是否立即更新廠商所預設之密碼？	□	□	□	□	□	□	□
7.51是否必須經過身份認定程序才能使用系統公用程式？	□	□	□	□	□	□	□
7.52是否將系統公用程式與應用程式隔離存放？	□	□	□	□	□	□	□
7.53是否訂定系統公用程式授權程序？	□	□	□	□	□	□	□
7.54是否訂定系統公用程式授權等級？	□	□	□	□	□	□	□
7.55是否訂定系統公用程式使用期限？	□	□	□	□	□	□	□
7.56是否保存系統公用程式使用紀錄？	□	□	□	□	□	□	□
7.57是否對風險性高的應用程式限制其連線作業需求？	□	□	□	□	□	□	□
7.58是否依據使用者身分控制應用程式的存取？	□	□	□	□	□	□	□
7.59是否指定專人管理應用程式原始碼、資料庫及執行檔？	□	□	□	□	□	□	□
7.60是否將應用程式原始碼、資料庫及執行檔分別存放？	□	□	□	□	□	□	□
7.61是否將開發中及正式作業之應用程式及資料庫分開存放及處理？	□	□	□	□	□	□	□
7.62是否將程式目錄清單、資料及相關電子檔作備份並異地存放？	□	□	□	□	□	□	□

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：__年__月__日

查　核　項　目	自我評審			查核員評量			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
7.63是否保有應用系統各種更新版本？	☐	☐	☐	☐	☐	☐	☐
7.64機密及敏感性資料的處理是否於獨立或專屬的電腦作業環境中執行？	☐	☐	☐	☐	☐	☐	☐
7.65例外事件及資訊安全事件是否建立紀錄？	☐	☐	☐	☐	☐	☐	☐
7.66事件之記錄內容是否包括使用者識別碼、登入登出系統之日期時間、電腦的識別資料或其網址及事件描述等事項？	☐	☐	☐	☐	☐	☐	☐
7.67對於系統存取異常時，是否留有紀錄並作必要處置？	☐	☐	☐	☐	☐	☐	☐
7.68是否查核系統存取特別權限的帳號使用及配置情形？	☐	☐	☐	☐	☐	☐	☐
7.69是否追蹤特定的系統存取？	☐	☐	☐	☐	☐	☐	☐
7.70敏感性資料的存取情形是否留有紀錄？	☐	☐	☐	☐	☐	☐	☐
8 系統開發與維護				☐	☐	☐	☐
8.1應用系統在規劃分析時是否將安全需求納入考量？	☐	☐	☐	☐	☐	☐	☐
8.2安全控管方式是否採用系統自動控管及人工控管兩種方式處理？	☐	☐	☐	☐	☐	☐	☐
8.3對高敏感性的資料在傳輸或儲存過程中是否使用加密技術？	☐	☐	☐	☐	☐	☐	☐
8.4應用程式執行碼更新作業是否限定只能由授權的管理人員才可執行？	☐	☐	☐	☐	☐	☐	☐
8.5有無建立應用程式執行碼的更新紀錄？	☐	☐	☐	☐	☐	☐	☐
8.6系統變更後是否立即更新系統文件？	☐	☐	☐	☐	☐	☐	☐
8.7版本更新是否保留舊版軟體及系統文件？	☐	☐	☐	☐	☐	☐	☐
8.8是否避免以真實資料進行測試？如須用真實資料是否於事前將足以辨識個人身份的資料去除？	☐	☐	☐	☐	☐	☐	☐
8.9開發、測試與正式作業是否分開使用不同主機？	☐	☐	☐	☐	☐	☐	☐
8.10系統變更後其相關控管措施與程序是否檢查仍然有效？	☐	☐	☐	☐	☐	☐	☐
8.11系統變更後，是否主動公告異動的範圍、時間、可能的影響？	☐	☐	☐	☐	☐	☐	☐
8.12修改套裝軟體是否確認有無涉及廠商的版權問題？	☐	☐	☐	☐	☐	☐	☐
8.13系統上線前是否檢查程式碼有無後門或木馬程式？	☐	☐	☐	☐	☐	☐	☐
8.14系統安裝後是否管制程式碼？	☐	☐	☐	☐	☐	☐	☐
8.15委外開發合約中是否對著作權之歸屬訂有規範內容？	☐	☐	☐	☐	☐	☐	☐
8.16訂約時是否簽訂履行條款與相關罰則？	☐	☐	☐	☐	☐	☐	☐
8.17是否定期對使用軟體實施病毒偵測？	☐	☐	☐	☐	☐	☐	☐
9 永續經營管理				☐	☐	☐	☐
9.1是否已擬訂關鍵性業務及其風險評估、衝擊影響、優先順序？	☐	☐	☐	☐	☐	☐	☐
9.2是否檢討業務停頓的企業損失和備援措施？	☐	☐	☐	☐	☐	☐	☐
9.3是否指定適當層級主管負責永續經營政策之執行與協調？	☐	☐	☐	☐	☐	☐	☐
9.4是否分析造成業務停擺的可能危機及損失？	☐	☐	☐	☐	☐	☐	☐
9.5是否定期作風險評估並調整永續經營政策？	☐	☐	☐	☐	☐	☐	☐
9.6永續經營計畫是否配合業務、組織及人員之變更而更新？	☐	☐	☐	☐	☐	☐	☐
9.7是否建立資訊安全事件之通報作業程序及應變措施？	☐	☐	☐	☐	☐	☐	☐
9.8是否訂有緊急應變計畫？	☐	☐	☐	☐	☐	☐	☐
9.9緊急應變程序是否涵蓋有往來外單位之應變規劃？	☐	☐	☐	☐	☐	☐	☐

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。

表三　　資通安全外部稽核（自我評審）表

受查單位：＿＿＿＿＿＿＿＿＿＿＿＿　　稽查日期：__年__月__日

查　核　項　目	自我評審			查核員評量			
	是	否	不適用	完整性 非常	尚屬	不盡	不適用
9.10緊急應變程序是否設有對外發言的處理機制？是否結合相關單位及地方警消單位？	☐	☐	☐	☐	☐	☐	☐
9.11緊急應變程序是否有異地場所、設備、處理程序及時限？	☐	☐	☐	☐	☐	☐	☐
9.12緊急應變計畫是否定期演練與修正？	☐	☐	☐	☐	☐	☐	☐
9.13緊急應變之作業程序與流程是否書面化？	☐	☐	☐	☐	☐	☐	☐
9.14緊急應變計畫是否納入內部教育訓練？	☐	☐	☐	☐	☐	☐	☐
9.15緊急應變計畫復原程序是否測試無誤？	☐	☐	☐	☐	☐	☐	☐
9.16永續經營管理是否保持人員異動的取代更替？	☐	☐	☐	☐	☐	☐	☐
9.17永續經營管理是否隨法令更新？	☐	☐	☐	☐	☐	☐	☐
10 內部稽查及其他				☐	☐	☐	☐
10.1是否定期稽查資訊安全事項辦理情形？	☐	☐	☐	☐	☐	☐	☐
10.2稽查範圍是否涵括資訊系統、供應商、資訊資產負責人、使用者和管理階層？	☐	☐	☐	☐	☐	☐	☐
10.3是否訂有資訊安全作業稽查計畫(含稽查內容、範圍、程序、人員)，並公布？	☐	☐	☐	☐	☐	☐	☐
10.4稽查人員是否經過訓練並作事前工作分配？	☐	☐	☐	☐	☐	☐	☐
10.5稽查時是否需要額外的資源支援？	☐	☐	☐	☐	☐	☐	☐
10.6稽查時的存取行為是否經過監控與記錄？	☐	☐	☐	☐	☐	☐	☐
10.7稽查結果是否製成文件？	☐	☐	☐	☐	☐	☐	☐
10.8稽查結果是否包括背景描述、稽查項目、過程、結果、改進建議等內容？	☐	☐	☐	☐	☐	☐	☐
10.9是否清查過系統內與資訊安全相關的記錄檔案？	☐	☐	☐	☐	☐	☐	☐
10.10與資訊安全相關的記錄檔案是否訂有保存規範？	☐	☐	☐	☐	☐	☐	☐
10.11是否定期審閱資訊安全相關的記錄檔案？	☐	☐	☐	☐	☐	☐	☐
10.12是否專人負責管理與資訊安全相關的記錄檔案？	☐	☐	☐	☐	☐	☐	☐
10.13與資訊安全相關的記錄檔案是否足以追蹤駭客入侵的證據？	☐	☐	☐	☐	☐	☐	☐
10.14是否使用合法軟體？	☐	☐	☐	☐	☐	☐	☐
10.15是否訂有軟體採購作業程序？	☐	☐	☐	☐	☐	☐	☐
10.16是否擬訂合法使用軟體規範及違規罰則，並作宣導？	☐	☐	☐	☐	☐	☐	☐
10.17是否妥善保存授權證明、原版程式、使用手冊？	☐	☐	☐	☐	☐	☐	☐
10.18對於以使用者人數為基礎的授權合約是否確實履行使用人數限制？	☐	☐	☐	☐	☐	☐	☐
10.19是否確定個人電腦中只載入合法軟體？	☐	☐	☐	☐	☐	☐	☐
10.20是否使用適當稽查軟體工具檢查所有個人電腦內使用之軟體？	☐	☐	☐	☐	☐	☐	☐
10.21是否訂定軟體使用記錄和資料的儲存、處理和報廢的規則？	☐	☐	☐	☐	☐	☐	☐
10.22是否訂定軟體使用記錄和資料的保存時限？	☐	☐	☐	☐	☐	☐	☐
10.23是否建立軟體目錄？	☐	☐	☐	☐	☐	☐	☐
10.24是否即時辦理軟體異動登記？	☐	☐	☐	☐	☐	☐	☐
10.25是否指派專人負責有關個人資料保護法規之蒐集、公告、實施作為？	☐	☐	☐	☐	☐	☐	☐
10.26是否依照「電腦處理個人資料保護法」規定辦理？	☐	☐	☐	☐	☐	☐	☐

※前述查核項目，於自我評審如答「否」時，請填寫表四資通安全行動計畫表，便於控管加強辦理；紅色字為實地稽核重點項目。