論　述

資通安全稽核解析

資訊運用普及之同時，也帶來資訊安全之危機，在於預防勝於治療的前提下，執行各項資訊安全必要基礎保護措施，已是使用者必須具備之責任與義務，然而每個使用者是否落實資安保護措施，則有賴實施資安稽核，本文對資安稽核程序及標準提出解說，期望對推動資安工作有所助益。

◉ **李茂基**（行政院主計處電子處理資料中心分析師）

壹、前言

藉著資訊與網路之結合，政府可以利用電腦透過網路提供即時之服務，並且不受時空的限制，提高服務績效及服務品質；企業可以強化競爭力，增加經營績效及降低管理成本；一般民眾可以即時知道國際最新情勢，隨時獲得日常生活常識，不再求助無門，減少蒐尋資料摸索時間，爲人們帶來了太多的便利。然而資訊與網路的結合，也讓我們面臨資通安全的威脅，威脅的來源日益廣泛，有電腦病毒侵襲、電腦駭客入侵、服務的網站突然停止提供服務、個人隱私資料外洩、網路詐騙層出不窮。因此，如何妥善保護資訊，以達到資料之可用性、完整性和機密性等安全必備要件，並建立可信賴的網路環境，已是資訊化社會所面臨最關切的問題；因此政府機關及民間企業均積極建立資訊安全管理系統，進行資安防護工作。惟其資安工作推動是否落實，能否達到預期效益，則有賴資安稽核之實施。

貳、稽核程序

資安稽核執行流程依序爲研擬稽核計畫、籌組稽核團隊、準備稽核檢查表、實施稽核、報告稽核結果、確定矯正措施及追蹤列管等七大步驟。在稽核計畫中首先要界定稽核範圍，擇定稽核標準，選定稽核區域，排定稽核日期

●94年度政府機關資通安全外部稽核會議

及決定稽核方式。稽核團隊則優先考量具有資安稽核專業或受過訓練之人員。爲便於資安稽核順利進行，宜事先準備稽核檢查表，將資安標準或資安規範轉成問項，使稽核者及受稽者清楚資安稽核目標及重點。檢查表亦爲確保稽核深度及稽核持續性之重要輔助工具，故其訂定應足以涵蓋稽核事項。實施稽核之執行程序自召開起始會議、進入稽核區域、確認資料、紀錄稽核發現、隨時告知被稽核者狀況、準備稽核發現報告。於稽核過程如有發現資安缺失，或違反組織之資安規定等，則被評爲不符合事項並納入稽核總結報告，稽核總結報告將於稽核結束會議中提出。受稽核方對於稽核報告中所提之不符合事項或改善意見須提出矯正預防措施及預定完成時間，並自行追蹤管制，稱爲一個稽核循環。

在稽核一個組織之資安時，首先須了解該組織是否已建立符合其業務活動之資安管理系統，是否定義其資安政策，有無評鑑風險之系統化方法及鑑別各項資訊資產風險，各項資產是否鑑別出可能被利用之脆弱點及可能遭受之威脅及衝擊；依據風險評鑑結果，決定可接受之風險等級後擬定風險管理計畫，採用合於成本效益的控制措施，以有效的阻止或降低可能發生之風險；並對各項控制措施執行監控與定期審查，以確定其有效性。因此在資安系統建立過程中相關文件，如資安政策、風險評鑑報告、風險處理計畫、資安管理系統之各項程序與控制措施、執行各項表單紀錄等皆列爲稽核階段中書面審查之必備文件。

參、稽核依據及重點

現階段建置及稽核資安管理系統主要文獻爲「資訊安全管理作業要點」（Code of practice for information secuity management，標準編號爲ISO 17799：2000/BS7799-1：2000/CNS 17799）及「資訊安全管理系統要求」（Specification for information security management systems 標準編號爲BS7799－2:2000/CNS 17800），另有行政院頒布之「行政院及所屬各機關資訊安全管理要點」及「行政院及所屬各機關資訊安全管理規範」等，現行國內外將資訊安全管理系統要求作爲稽核標準；另ISO組織爲確保所訂之國際標準能持續改進並合乎世界潮流，於94年6月改版，內容修正爲11章39個控制目標133個控制措施。以下就行政院主計處電子處理資料中心推動資安稽核服務之稽核重點說明如下，俾讀者能一窺資安稽核工作內容及重點：

一、資訊安全政策

控制目標：提供管理階層對資訊安全的指示與支持。

控制措施：1.資訊安全政策文件

2.審查與評估

稽核重點：檢視資安政策內容之完整性、資安政策核准層級、發布途徑，是否定期審查及評估；並抽樣訪問人員對資安政策之了解程度。

二、安全組織

（一）內部組織

控制目標：在組織內管理資訊安全。

控制措施：1.管理階層對資訊安全的承諾

2.資訊安全協調工作

3.資訊安全責任配置

4.資訊處理設施授權作業

5.保密協議

6.跨機關合作與協調

7.資訊安全顧問及諮詢

8.獨立的資訊安全審查

（二）外部團體

控制目標：維持外部使用者存取資訊及使用設施之安全管理。

控制措施：1.鑑別來自外部使用者之風險

2.外部人員作業安全

3.第三方合約中之安全要求

稽核重點：檢視管理階層對資安工作的支持與承諾、資安推動組織、明訂資安責任、重要資訊處理之保密協議、鑑別外部組織存取風險及規範必要之安全處理措施、資安要求納入第三方合約；並抽樣訪問員工及外部人員對資安責任之了解程度。

三、資產管理

（一）資產責任

控制目標：爲維護組織資產適切的保護。

控制措施：1.資產清冊

2.資產擁有者

3.資產授與及使用

（二）資訊分類

控制目標：確保資訊資產獲得適當的保護層級。

控制措施：1.分類指引

2.資訊標示與處理

稽核重點：檢視資產分類及安全等級標準，資產安全標示處理，資產清冊之完整性，資產擁有者、管理者、使用者之責任區分；並抽樣訪問員工對資產安全等級及管理要求。

四、人力資源安全

（一）聘雇前

控制目標：確保受雇人員承包商及第三方使用者了解職務，降低設施遺失、詐欺或誤用之風險。

控制措施：1.角色與職務

2.篩選

3.聘用條件與限制

（二）聘雇期間

控制目標：確保受雇人員承包商及第三方使用者了解資訊安全的威脅與問題、本身責任與義務，且能執行組織安全政策，降低人爲錯誤的風險。

控制措施：1.管理責任

2.資訊安全認知教育與訓練

3.懲罰程序

（三）聘雇中止或變更

控制目標：確保受雇人員承包商及第三方使用者退出組織或變更聘雇關係的安全。

控制措施：1.聘雇終止

2.資產歸還

3.移除存取權限

稽核重點：檢視重要職務受雇人員安全評估方式，人員（含第三方使用者）異動其各項權限異動措施，員工之資安責任規定，資安認知教育與訓練紀錄，員工違反資安之處理程序規定，員工離職時資產歸還程序；並抽樣訪問員工對資安責任之了解程度及職務異動之權限處理程序。

五、實體與環境安全

（一）安全區域

控制目標：避免營運場所及資訊遭未經授權存取、損害與干擾。

控制措施：1.實體安全邊界

2.實體進入控制措施

3.辦公處所及設施之保護

4.不受外在及環境的威脅

5.在保全區域內工作

6.隔離的收發與裝卸區

（二）設備安全

控制目標：避免資產遺失、毀壞或受損，並避免營運活動中斷。

控制措施：1.設備安置及保護

2.電源供應

3.纜線的安全

4.設備維護

5.場外設備之安全

6.設備之安全報廢或再使用

7.財產攜出

稽核重點：檢視進入重要實體區域之管制措施，機房環境安全監控，資訊設備報廢之處理程序，設備攜出安全程序，場外資訊設備使用安全；並抽樣檢視機房門禁管理有效性、機房日誌記錄與管理、機房安全措施及緊急應變措施。

六、通訊與作業管理

（一）安全區域作業程序與責任

控制目標：確保正確與安全地操作資訊處理設備。

控制措施：1.書面作業程序

●稽核—書面審查場景

2.操作變更管制

3.職責區隔

4.分隔開發與作業設施

（二）第三方服務傳送管理

控制目標：實施與維護第三方服務與資訊傳遞安全。

控制措施：1.服務遞送

2.監控與審查第三方服務

3.第三方服務變更管理

（三）系統規劃與驗收

控制目標：降低系統失效的風險。

控制措施：1.容量規劃

2.系統驗收

（四）惡意軟體的防範

控制目標：保護軟體及資訊完整性免於受惡意軟體損害。

控制措施：1.對抗惡意軟體的控制措施

2.對抗行動碼的控制措施

（五）備份

控制目標：維護資訊及資訊處理設施之完整性及可用性。

控制措施：資訊備份

（六）網路管理

控制目標：確保網路內資訊安全。

控制措施：1.網路控制措施

2.網路服務安全

（七）儲存媒體的處理與安全

控制目標：避免資產未經授權的揭露、修改、破壞及營運活動中斷。

控制措施：1.可攜式電腦儲存媒體之管理

2.媒體之報廢

3.資訊處理程序

4.系統文件之安全

（八）資訊交換

控制目標：維護組織內與外部資訊交換之安全。

控制措施：1.資訊交換政策與程序

2.交換協議

3.儲存媒體運送過程之安全

4.電子訊息

5.營運資訊系統

（九）電子商務服務

控制目標：確保電子商務服務安全。

控制措施：1.電子商務

2.線上交易

3.公開可取得的資訊

（十）監控

控制目標：偵測未經授權的資訊處理活動。

控制措施：1.監視日誌

2.監控系統的使用程序

3.日誌資訊的保護

4.管理者與操作員日誌

5.系統錯誤記錄

6.時鐘同步

稽核重點：檢視資訊設備之操作程序及管理責任，第三方服務之安全監控與管理，系統驗收程序，惡意程式之偵測與預防，資料與系統之備份，網路服務安全，可攜式設備管理，系統文件安全管理，重要資訊交換安全，公開資訊或線上交易之保護措施，各項日誌監控管理；並抽樣訪問員工之防毒措施，系統漏洞修補程序，資訊交換處理，可攜式媒體之管理及資料備份作法。

七、存取控制

（一）存取控制之營運要求

控制目標：控制資訊之存取行為。

控制措施：存取控制政策

（二）使用者存取管理

控制目標：確保授權使用者之存取並防止未經授權存取。

控制措施：1.使用者註冊

2.特權管理

3.使用者通行碼管理

4.使用者存取權限審查

（三）使用者責任

控制目標：避免未經授權之使用者存取。

控制措施：1.通行碼之使用

2.無人看管之資訊設備

3.桌面淨空與螢幕淨空政策

（四）網路存取控制

控制目標：防止未經授權存取網路服務。

控制措施：1.網路服務使用政策

2.外部連線之使用者身分鑑別

3.網路設備識別

4.遠端診斷與通訊埠保護

5.網路區隔

6.網路連線控制

7.網路路由控制

（五）作業系統存取控制措施

控制目標：防止對作業系統之未經授權存取。

控制措施：1.安全登入程序

2.使用者識別與身分鑑別

3.通行碼管理系統

4.系統公用程式之使用

5.終端機自動關機時間

6.連線時間的限制

（六）應用系統之存取控制

控制目標：防止資訊系統中之資訊未經授權之存取。

控制措施：1.資訊存取限制

2.敏感性系統之隔離

（七）行動式電腦作業與遠距工作

控制目標：確保使用行動式電腦與遠距工作之資訊安全。

控制措施：1.行動式電腦作業

2.遠距工作

稽核重點：檢視資訊存取控制政策，使用者及第三方存取權限申請及審查程序，使用者通行碼使用管理，系統管理者通行碼使用管理，網路服務使用政策，外部連線使用者鑑別機制，網路區隔措施，敏感性系統隔離措施，行動式電腦管理措施；並抽樣訪問員工存取權限取得方式，密碼設定與管理，螢幕淨空政策及行動式電腦管理作法。

八、系統取得、開發及維護

（一）系統之安全要求

控制目標：確保資訊系統已建置安全機制。

控制措施：安全要求分析及規格

（二）應用系統之安全

控制目標：預防應用系統中使用者資料遺失、遭未授權修改或誤用。

控制措施：1.輸入資料之確認

2.內部處理之控制

3.訊息鑑別

4.輸出資料之確認

（三）密碼控制措施

控制目標：保護資訊之機密性、鑑別性及完整性。

控制措施：1.使用密碼控制措施之政策

2.金鑰管理

（四） 系統檔案安全

控制目標：確保系統檔案安全。

控制措施：1.系統軟體之控制

2.系統測試資料之保護

3.原始程式庫之存取控制

（五）開發及支援作業之安全

控制目標：維護應用系統軟體及資訊之安全。

控制措施：1.變更管制程序

2.作業系統變更之技術審查

3.套裝軟體變更之限制

4.資訊洩漏

5.軟體開發委外

（六）技術脆弱性管理

控制目標：降低利用已知技術性脆弱點攻擊之風險。

控制措施：技術脆弱性控制

稽核重點：檢視應用系統安全規格，應用系統安全設計，測試資料保護措施，程式原始碼存取管制措施、系統變更處理程序，系統委外開發安全管理，資訊系統技術脆弱性控制；並抽樣訪問程式庫、資料庫、系統文件及系統變更處理等管理措施。

九、資訊安全事件管理

（一）通報資訊安全事件與弱點

控制目標：確認資訊安全事件與弱點之傳達，以採取及時矯正措施。

控制措施：1.資安事件之通報

2.安全弱點之通報

（二） 資訊安全事件管理與改善

控制目標：確保資訊安全事件之有效管理。

控制措施：1.職務與程序

2.從資安事件中學習

3.蒐證

稽核重點：檢視資安事件通報程序，資安事件與系統弱點通報與管理，資安事件矯正資料；並抽樣訪問員工對資安事件通報程序及矯正實施情形。

十、營運持續管理

（一）營運持續管理之考量

控制目標：防治營運活動中斷，保護重要營運過程不受重大故障或災害影響。

控制措施：1.營運持續管理過程

2.營運持續及風險評鑑

3.持續計畫之撰寫及實施

4.營運持續規劃框架

5.營運持續計畫之測試、維護及重新評鑑

稽核重點：檢視關鍵性業務風險評估，營運持續管理計畫文件，營運持續管理計畫測試演練記錄；並抽樣訪問員工對營運持續管理計畫之了解程度。

十一、符合性

（一）遵守法規要求

控制目標：避免違反所有刑法、民法、行政命令、管理規定或合約義務及所有安全要求。

控制措施：1.適用法令之鑑別

2.智慧財產權

3.組織紀錄之保護

4.個人資訊的資料保護及隱私

5.預防資訊處理設施遭誤用

6.密碼控制措施規定

（二）遵守安全政策、標準與技術

控制目標：確保系統遵守組織安全政策與標準。

控制措施：1.遵守安全政策與標準

2.技術符合性之檢查

（三） 資訊系統稽核考量

控制目標：使系統稽核得到最大成效並將干擾降至最低。

控制措施：1.資訊系統稽核控制

2.系統稽核工具之保護

稽核重點：檢視組織重要紀錄保護措施，智慧財產權保護措施，合法軟體查核，實施資安稽核，並抽樣訪問使用合法軟體及資安內稽執行績效。

肆、結語

以上爲資安稽核項目及稽核重點，期望各單位藉著稽核之實施，可及早發現資安執行的死角，避免因人爲一時的疏忽，釀成重大的災難；雖然資通安全已爲大家所熟知，並且已爲各機關所重視，但是如果資安工作不落實，則資安事件之發生是不可避免，只在於其發生時間及影響的大小而已，不要心存僥倖；資安防護要能有效，誠如本中心萬主任於94年9月主計人員領導研究班資安報告中之結語：資安工作成功的關鍵因素在於有管理階層實際的支持、正確的風險評鑑與擬訂有效的控制措施、全體員工的認知與實踐、資安政策之定期審查與評估及不定期的實施稽核等。資安工作是永無止盡，應建立「維護資安，人人有責」的基本觀念，希望大家落實執行各項資安規定，才有安全無虞之資訊作業環境，以迎接資訊化社會之各項挑戰。❖