談 ISO 27001 管理實務－以試務整合通過三年重審換證為例

◎ 倪惠真

壹｜導入 ISO 27001 對考選部之重要性

「國家考試試務整合性管理系統」為考選部試務 e 化核心系統，支援國家考試作業流程各項作業。為使應考人儘速獲得考試結果，試務作業處理時程安排緊湊，且每項考試需處理大量應考人個人資料及成績資料（以 101 年為例，國家考試報考人數即突破 79 萬人次大關），囿於榜示前成績及應考人個人資料係機敏資訊，且各項作業於各工作場所投入眾多人力進行資料掃描、建檔、調閱、列印及應用，可能衍生相關作業風險。

為因應前揭系統兼具時程急迫、資料量大且機敏等運作特性，極需導入資訊安全管理機制（Information Security Management System，簡稱 ISMS），以國際化資訊安全規範標準（「國際資訊安全認證 ISO 27001」）檢視前揭系統控制措施之符合性，期能降低資安風險、強化國家考試試務作業資訊安全。

爰從技術面及管理面全方位進行規劃，在管理方面，首先進行風險評鑑，並訂定符合 ISO 27001 標準、個人資料保護法及相關法規要求之各項作業規範，以為部內同仁依循之準則。在技術方面，依循控制措施之規範，建置試務整合 e 化運作平臺，將伺服主機、資料庫及重要設備建置為高可用性架構，以防火牆依功能區隔成不同網段，運用防火牆政策設定，規範各網段安全性。並自 100 年 1 月導入資安防護及監控服務，進行全年無休之設備、防駭、防毒監控作業，以預警機制，及早發現異常問題或可能資安事件，事先防範與處理，提供安全、可靠、穩定的優質環境，以達機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）之資訊安全要求，確保考試作業運作順利。

貳｜推動與導入 ISO 27001 國際資訊安全標準

一、推動目標

推動試務整合性管理系統在開發、日常操作及維運等過程，能具備符合國際資訊安全管理認證標準之驗證要求，並經外部稽核第三方驗證程序，取得「國家資訊安全認證 CNS 27001」及「國際資訊安全認證 ISO 27001」為目標，另期藉由反覆執行 PDCA（Plan-Do-

Check-Act）過程及定期查驗各項作業之資安防護工作，促進試務整合資訊安全持續改善。

二、導入範圍

驗證範圍為系統開發、操作及維運過程；實體作業範圍為系統相關資訊資產及所屬機房，包括試務電腦機房、操作室、列表室、印表操作中心等工作場所，行政大樓辦公場所及第1、2試務大樓工作場所的試務專用PC使用端，均納入安全稽核區域。

三、導入過程

自98年元月啟動，歷經16個月，完成國際資訊安全ISO 27001認證所需各項作業，於導入過程中，逐步依該標準規範建立試務整合資訊安全管理制度（ISMS），並落實執行。

（一）成立資訊安全組織：

由高普考試司、專技考試司、特種考試司、資訊管理處、題庫管理處、統計室、政風室、人事室等單位共同組成「試務整合資訊安全處理小組」，定期執行資訊安全管理審查。

（二）進行風險評鑑及風險處理：

藉由資訊資產盤點建立資產清冊、評估資產之脆弱性、可能威脅及衝擊、確認現行控制措施、評估風險程度、訂定可接受風險等級、研提可行控制方法等步驟，評鑑風險，採取適當控制目標及控制措施以處理風險。

（三）建置資安四階管理文件：

擬訂資訊安全政策、資訊安全目標、適用性聲明書SOA等資安管理文件計70餘種，據以執行相關管控作業，並透過電子郵件及入口網資安專區宣導相關政策及訊息。

（四）落實管理措施：

依ISO 27001本文及試務整合適用性聲明書SOA之要求，實ISMS之建 、監督、審查、維持、改善措施等過程，包括落實執行資安四階文件要求、辦理資訊安全訓練、內部稽核作業、業務持續營運演練、資訊安全管理審查等事宜。

四、取得認證

由英國標準協會BSI臺灣分公司擔任第三方驗證機構，於99年3月31日通過預先評核的稽核，4月21日通過正式評核第1階段書面審核，4月29、30日通過正式評核第2階段現場審核，5月14日取得國家資訊安全CNS 27001及國際資訊安全ISO 27001雙認證。

參｜ISO 27001 三年重審換證執行歷程

國家考試試務整合性管理系統自 99 年 5 月取得 ISO / CNS 27001 雙認證已屆 3 年，必需通過重審換證稽核始得延續證書之有效性。其資訊安全管理制度係依 ISO 27001 標準中有關本文及附錄 A 之 11 項安全領域（如圖 1）為指引，擬訂資安四階管理文件，運用 PDCA（Plan-Do-Check-Active） 管理循環來建立、執行與管理（執行架構示意圖如圖 2），並適度運用資訊科技，落實執行管理規範。本章節茲分為「建立、實作及操作 ISMS」、「監控及審查」、「維護及改進」等三方面，說明考選部自取得認證至重審換證此三年期間落實執行 ISMS 之歷程。

<table>
<tr><td colspan="4">A5. 安全政策</td></tr>
<tr><td colspan="4">A6. 組織資訊安全</td></tr>
<tr><td colspan="4">A7. 資產管理</td></tr>
<tr><td>A8. 人力資源安全</td><td>A9. 實體與環境安全</td><td>A10. 通訊與作業管理</td><td rowspan="2">A12. 資訊系統取得、開發及維護</td></tr>
<tr><td colspan="3">A11. 存取控制</td></tr>
<tr><td colspan="4">A13. 資訊安全事故管理</td></tr>
<tr><td colspan="4">A14. 營運持續管理</td></tr>
<tr><td colspan="4">A15. 遵循性</td></tr>
</table>

▲ 圖 1　ISO 27001 標準附錄 A 之 11 項安全領域

▲ 圖 2　考選部試務整合 ISO 27001 訊安全管理制度執行架構示意圖

一、在「建立、實作及操作 ISMS」方面

考選部依 ISO 27001 附錄 A 之 11 項安全領域規範，在管理面及技術面之實作重點如下：

（一）在「附錄 A5. 安全政策」方面

1. 擬訂資訊安全目標如下，並定期審查，以確保持續的適當性、充分性、有效性：
   （1）本系統整體系統可用度應維持 98％以上，亦即平均每月非計畫性系統中斷服務之時間應低於 14.4 小時，每次可容忍最大中斷時間為 8 小時。
   （2）確保每年發生資安事件次數低於 2 次。

（二）在「附錄 A6. 組織資訊安全」方面

1. 維護試務整合資訊安全處理小組名單。
2. 每半年至少辦理一次資訊安全教育訓練，以建立正確使用觀念與習慣，內容涵蓋 ISMS 基礎、ISO 27001 標準規範、內部稽核員培訓課程、受稽人員須知等。
3. 要求新到職員工簽署「員工資訊安全須知」及「資訊安全聲明書」，委外廠商則簽署「資訊安全保密切結書」及「電腦機房作業安全守則」，使其瞭解資訊安全之責任。

（三）在「附錄 A7. 資產管理」方面

1. 建立及維護資訊資產清冊，並進行適當分類、分級及標示。

（四）在「附錄 A8. 人力資源安全」方面

1. 對於調動、離職之人員，其帳號及使用權限立即停用。
2. 每人每年至少 3 小時資訊安全教育訓練及社交工程演練。
3. 定期內部稽核抽查落實情形。

（五）在「附錄 A9. 實體與環境安全」方面

1. 設置消防、UPS 及發電機等設備，並定期檢查、維護與演練；機房內設備及網路線路皆明顯標示，並使用電流顯示機櫃電源排插；環控系統隨時監視機房溫度、空調狀況，有異常即刻通知管理者；機房內活動影像隨時透過監視錄影設備存錄。
2. 重要設備均建置成高可用性架構（High Availability），且將正式運作機組與測試機組分別建置於行政大樓 2 樓試務機房與第 1 試務大樓 2 樓

網報機房，使具異地備援機制，並定期執行業務持續營運演練。

3. 每日進行各項設備燈號巡檢、資料庫備份巡檢等日常安全檢視，發現異常即刻通知管理者。

4. 訂定機房作業相關資安規定；並以門禁系統管制與紀錄人員進出機房之情形，非授權人員進出機房應填寫「電腦機房出入管制表」且應有授權人員陪同，每月定期彙整機房門禁進出狀況，呈核主管；資訊設備攜出機房應填寫「電腦機房設備攜出申請表」，經核准後始得攜出。

（六）在「**附錄 A10. 通訊與作業管理**」方面

1. 建置試務整合專用網路環境，規劃縱深防禦機制，以防火牆形成隔離網段、部署網路型及主機型入侵偵測防禦系統等資訊安全防護設備，以偵測及阻隔外部惡意碼入侵；部署防毒中控主機、Patch 管理主機，作為各伺服主機及個人電腦有關作業系統 Patch、防毒程式、病毒碼之更新管理，以防護非法行動碼及降低系統弱點造成的風險；並透過 SOC 監控，有異常即刻通知管理者處理。

2. 資安防護及監控服務自 100 年 1 月啟用，透過自動化資安管理平臺，進行 24 小時全年無休之主機運作狀況、防駭、防毒等監控作業，以預警機制，及早發現系統、設備、網路、服務之異常問題或可能資安事件，事先加以防範及處理；透過 SOC 機制即時監控、分析及收集各主機系統事件，相關記錄保存 1 年，每月並綜整各主機系統日誌及運作記錄，呈核主管。

3. 備份策略為每日執行一次完整備份，每 2 小時執行一次交易備份，備份資料透過光纖網路異地存放於第 1 試務大樓 2 樓網路報名機房，且採 1 式 2 份的 D2D2T 模式，同時備份到磁碟及磁帶櫃，並定期執行資料回覆演練。若使用者需要回覆磁帶備份資料，則需填寫「資料備份（回存）申請單」，經核准後執行。

4. 將開發、測試及正式運作之環境，分別建置於不同主機上，以降低測試過程對正式運作系統的風險；在時差管控部分，以防火牆設定校時功能，各設備統一向防火牆校時；資訊處理設施及系統異動時，應填寫「異動申請單」，經核准後始得異動；系統管理者並定期檢查重要設備之資安相關設定。

5. ISMS 文件及重要系統操作手冊均文件化，置於適當儲存裝置，俾利具權限者隨時取得。

（七）在「附錄 A11. 存取控制」方面

1. 建置試務整合專用網路環境，以防火牆形成隔離網段，存取限制為僅特殊管理用途（如病毒碼更新、系統 patch 更新等）可對外連線之外，其餘均不得對外連線，亦不允許由外對內連線；防火牆另依功能區隔為試務主機環境區（含應用服務區、資料儲存區、系統支援區）、資安服務區、測試環境區等Zone區，並善用防火牆政策設定，規範各 Zone 區安全性，以提供更安全之環境；防火牆規則異動應填寫「異動申請單」，經核准後執行。
2. 帳號控管部分，規範每位使用者皆需有獨立帳號，不可共用；帳號新增、註銷及權限異動應填寫「帳號申請單」，經核准後執行；對於調動、離職人員之帳號及使用權限立即停用；每月彙整異動資料呈核主管，並每年定期盤點帳號。
3. 作業系統、資料庫及應用系統均設定密碼原則，由系統每 6 個月自動通知使用者變更密碼，並要求密碼長度為 6 碼以上、具複雜度之字元組合；另設定螢幕保護裝置啟動時間為 10 分鐘，並啟動密碼保護。
4. 公用電腦均安裝還原卡，當電腦關機後，存放於硬碟之資料即清空，以適當保護使用者端未授權資料之存取。
5. 建立文件存取控制政策，並定期內部稽核及抽查存取控制政策落實情形。

（八）在「附錄 A12. 資訊系統取得、開發及維護」方面

1. 不安全的系統設計及程式設計，將造成網站漏洞及資安風險，國家考試試務整合性管理系統之開發與建置訂有「應用系統資訊安全設計規格」，作為系統開發的安全規範，將資安設計納入系統功能，如身分認證、帳號管理、群組管理、權限管制、稽核紀錄、資料加解密等，以強化應用系統安全性。
2. 在資料庫安全性設計部分，針對姓名、身分證字號、行動電話、電子郵件等機敏性資料項採加密機制，對於機敏資料項相關報表或檔案，

進行模糊化處理，並留下存取紀錄，以為事後稽核之用。

3. 程式異動需填寫「異動申請單」，經核准後始得異動，並先於測試機組完成測試後，再更新到正式運行機組，且利用版本更新機制進行程式版本控管。

4. 在技術脆弱性管理部分，每半年進行網頁弱點掃瞄一次，每年進行滲透測試一次，藉以檢視系統建置或程式設計安全之盲點，加強防護網站應用程式安全，降低被植入木馬、竄改網頁、竊取機敏資 等風險，並針對檢測結果執行弱點修補，以降低脆弱性，確保系統安全。

（九）在「附錄 A13. 資訊安全事故管理」方面

1. 訂定「資訊安全事件處置作業綱要」，並依程序進行資安事故通報、後續預防矯正措施處理與改善，自 99 年至 102 年 8 月止計發生事件等級 1 級之資安事件 3 件、事件等級 2 級之資安事件 1 件。

（十）在「附錄 A14. 營運持續管理」方面

1. 為因應災難或意外發生後，儘速回復系統運作，以降低資料損害之衝擊，使業務持續營運，除了完成備份機制及異地備援機制之建置外，並訂定「業務持續營運作業綱要」、「業務持續營運計畫」、「業務持續營運演練計畫」等管理規範，定期進行關鍵業務回復演練，加強人員操作熟稔度，並藉由經驗累積，不斷改善演練計畫，確保考試業務持續運作。自 99 年至 101 年計執行演練 4 次，99 年之 2 次計畫著重於資料庫回復演練，100 年至 101 年則著重於系統異地回復演練，模擬當行政大樓試務機房發生災難或大部分設備損毀、故障時，將試務整合系統於異地（即網路報名機房）重啟服務到最低可用性。最後將執行結果及檢討提出「業務持續營運演練報告」呈核主管，並記錄改善項目作為下次演練計畫之改善。

2. 每年執行風險再評鑑，針對評鑑結果，風險等級大於 3 之資訊資產，研擬風險處理計畫，透過適當控制措施之執行，降低風險。

（十一）在「附錄 A15. 遵循性」方面

1. 每年定期檢討相關法規異動對本 ISMS 規範之影響，

並適時調整 ISMS 規範，以達法規遵循性。

2. 每年至少辦理一次內部稽核，以確認各項規範被正確執行，並對於稽核結果執行適切預防矯正措施以改善缺失。
3. 在技術遵循性部分，每半年進行木馬檢測、主機弱點掃瞄、網頁弱點掃瞄等資安檢測各一次，每年進行滲透測試一次，並針對檢測結果執行弱點修補。
4. 資訊系統稽核工具及資料保護部分，除了建置日誌伺服器儲存系統日誌之外，並導入資料庫監控稽核產品（Database Activity Monitoring，DAM）Imperva，以存錄使用者存取資料庫之軌跡，供資安事件數位鑑識用。日誌及軌跡資料至少保留 6 個月，對於存取權限並嚴格管控。

二、在「監控及審查」方面

（一）在「本文 6.內部稽核」方面

藉由內部稽核瞭解 ISMS 控制目標、控制措施是否有效實施並如預期執行，考選部訂定「資訊安全內部稽核計畫」，稽核範圍包括第三方服務、政策與標準的遵循等，定期依計畫執行，於 99 年及 100 年每半年執行一次，101 年起每年執行一次，並將執行結果及檢討提出「資訊安全內部稽核報告」呈核主管，且就缺失項目執行預防矯正措施，以防再發生。

（二）在「本文 7. 管理審查」方面

定期召開管理審查會議，審查及追蹤 ISMS 管理審查 9 項輸入與 5 項輸出是否適當、是否完整有效執行，並研訂控制措施，自 99 年至 102 年計召開管理審查會議 9 次。

三、在「維護及改進」方面

（一）在「本文 8. 持續改進」方面

藉由每年定期之內、外部稽核、監督事件分析、管理階層審查結果所發現之缺失項目，執行預防矯正措施，以持續改進資訊安全管理系統之有效性。

肆｜三年重審換證驗證結果

三年重審換證稽核由英國標準協會 BSI 臺灣分公司擔任第三方驗證機構，考選部於 102 年 4 月 11、12 日通過現場稽核，取得 3 年效期的國家資訊安全 CNS 27001 及國際資訊安全

ISO 27001 雙認證。稽核內容主要就系統之開發、運作、管理及維護等相關活動範圍及場所，進行 ISO 27001 標準的符合性稽核，稽核結果未發現主、次要缺失，惟抽樣發現 3 項觀察事項及 1 項改善機會，僅需內部執行預防矯正措施即可，說明如表 1：

伍｜具體成果及效益

「國家考試試務整合性管理系統」導入 ISO 27001 業已三年，投入相當多之人力及時間，擬定作業規範、落實執行規範、定期內稽、檢討與改善，並建置資安防護措施、進行資安監控與異常事件處理。通過三年重審換證，展現之具體成果及效益如下：

一、有效降低資安風險，提高系統可用性，確保業務持續營運

在管理方面，首先進行風險評鑑，訂定符合 ISO 27001 標準、個人資料保護法及相關法規要求之各項作業規範，作為部內同仁依循之準則，並落實執行與持續改善。在技術方面，依循控制措施之規範，建置試務整合 e 化運作平臺及資安防護體系，並以遠端監控之即時預警機制、每月資安彙整報告及資安弱點管理等作為，及早發現可能的入侵行為、病毒事件或系統潛

表 1　重審換證稽核結果及內部預防矯正措施

類別	追蹤項目	改善措施
觀察事項：A.11.5.3	請組織再行考量通行碼原則實施的完整性與有效性	1. 伺服器系統管理者帳號取消「密碼永久有效」之設定。 2. 資料庫帳號設定「強制執行密碼逾期」。 3. 操作室個人電腦「本機安全性原則」設定密碼原則為效期 6 個月及密碼長度 6 個字。
觀察事項：A.11.3.3	組織請再行審查螢幕淨空政策實施的有效性	檢查所有伺服器螢幕保護程式是否有漏設啟用者，將其設為啟用。
觀察事項：A.15.1.4	請組織再行考量機敏資料管理的適切性	以加密方式處理機敏資料報表檔案，承辦人若需下載開啟，應向系統管理員取得密碼方可開啟，並留下存取紀錄。
改善機會：A.7.1.1	組織請再行審查資訊資產清冊的完整性，如：SVN 版控軟體	於資訊資產清冊增列「公用元件及軟體」項目，並列入本年風險評鑑一併評鑑。

在弱點等，以掌握系統整體狀況，預為因應處理。整體而言，有效降低資安事件發生的機率、影響範圍及影響程度，提高系統可用性，以確保考試業務持續營運。

二、證明試務整合資訊安全符合國際標準要求

三年重審換證稽核由英國標準協會 BSI 臺灣分公司擔任第三方驗證機構，就系統之開發、運作、管理及維護等相關活動範圍及場所，進行 ISO 27001 標準的符合性稽核，稽核結果未發現主、次要缺失。經由外部公正第三方驗證機之專業稽核，驗證本系統相關控制措施之符合性，即證明「國家考試試務整合性管理系統」之維運達到一定的資安水準，符合國際資訊安全標準之要求。

陸｜結語

試務整合資訊安全導入 ISO 27001 歷經三年多之努力，業已步入穩定運作階段，未來應持續努力及改善的方向如下：

一、在管理面落實執行 ISMS 管控措施與持續改進

配合 ISO 27001 認證定期外部稽核之需要，以及依循管理循環 PDCA（Plan-Do-Check-Active）的精神，持續落實執行 ISMS 安全管控作業、辦理內部稽核與改善、風險評鑑與風險處理、預防矯正措施、業務持續營運演練、管理審查會議、資安宣導及外部稽核等作業項目，並藉由經驗累積，持續精進 ISMS 四階管理文件，以改善各項管控措施，強化整體資訊安全管控機制。

二、在技術面賡續加強 e 化平臺運作機能及資安防護

藉由資安防護體系之即時監控預警機制、每月資安彙整報告及資安弱點管理等作為，及早發現可能的入侵行為、病毒事件或系統潛在弱點，以掌握系統整體狀況，預為因應、處理及改善各種突發狀況，維護平臺運作順利，另配合法規要求及防護需要，適時編列預算引進設備，以加強資安防護能力。

◎作者：倪惠真　資訊管理處分析師