導入教育機構資訊安全管理制度

種子學校成果經驗分享說明會

正修科技大學

計算機中心 網路規劃組

何俊輝

98年3月20日

Agenda

一、正修科大計算機中心簡介

二、導入過程摘要說明

三、導入建置效益

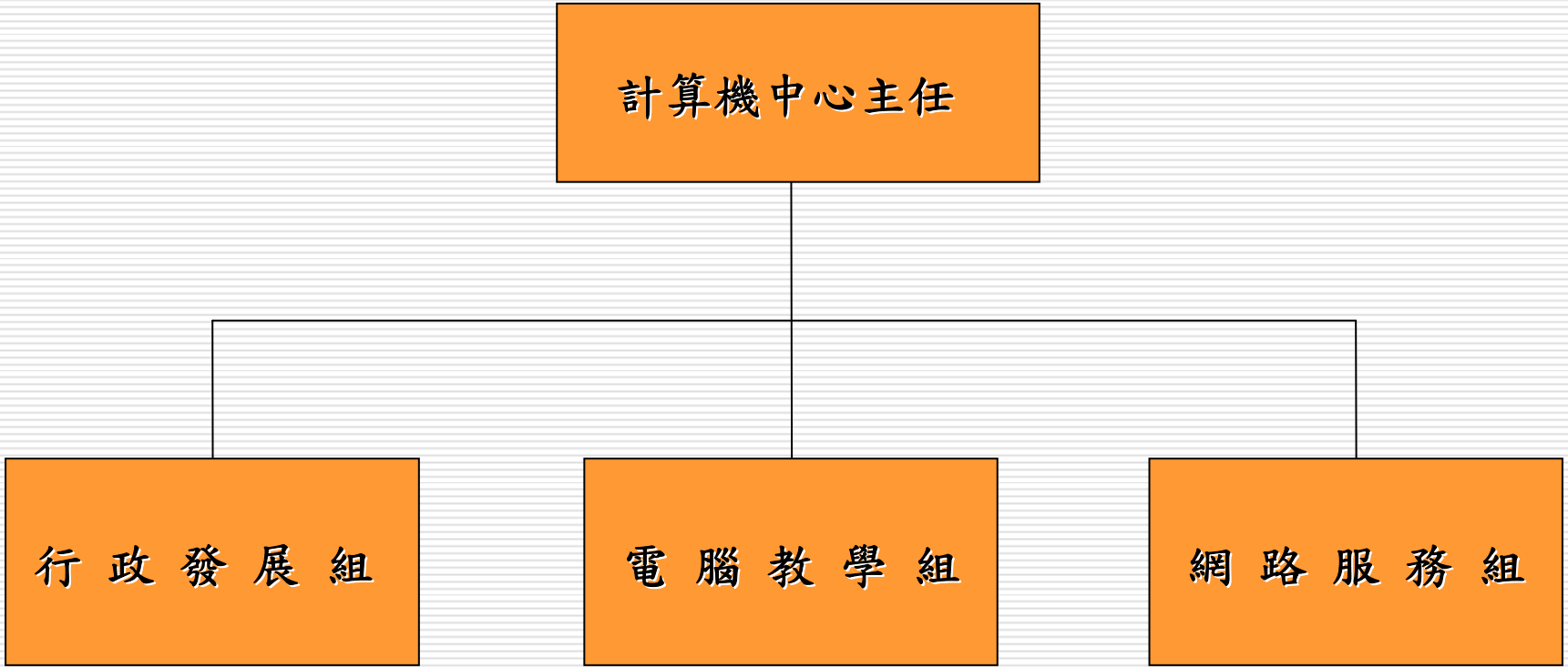
四、給予未來導入學校之建議

五、實例範本摘要說明

- 「業務永續運作管理與相關表單範例」

正修科大計算機中心簡介

計算機中心組織



重要核心業務

- 行政系統開發及維護
- 校務資料庫管理維護
- 規劃、建置及維運全校有線及無線網路環境
- 伺服器管理建置
- 網路服務維運管理
- 網路教學服務
- 負責全校非資訊及電子系所之電腦課程

導入過程摘要說明

ISMS導入過程

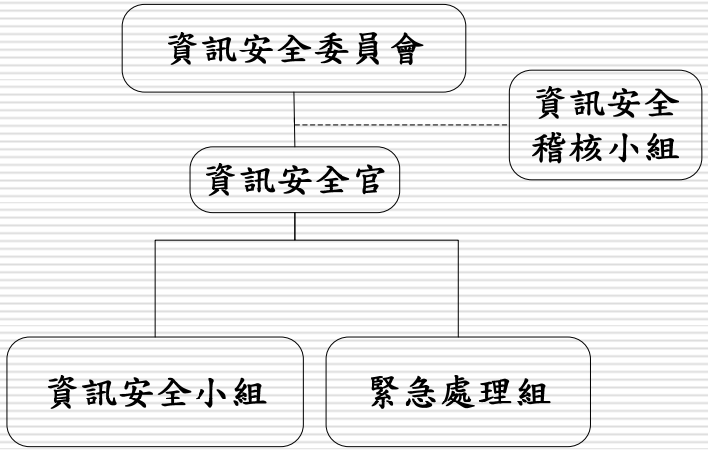
- 背景：
  - 承辦97年大專校院電算中心主任會議，籌備期與開會日期與ISMS導入期程嚴重重疊
- 人力：
  - 校內-網路規劃組2人、行政發展組2人
  - 校外-輔導顧問1人
- 資安文件公告方式：
  - 電子郵件發佈
  - 紙本傳閱簽名
- 宣導方式
  - 透過中心會議、電子郵件宣導

ISMS導入過程(續)

- 首先決定ISMS施作範圍及驗證範圍
  - 「資訊機房維運管理」
  - 「學籍管理系統維護管理」
- 選定理由
  - 資訊機房為本校網路、資訊服務最核心關鍵的區域，也是本單位的重要核心業務，為維持資訊機房正常運作，故選擇「資訊機房維運管理」為本次ISMS施作範圍與教育體系資通安全管理規範之驗證範圍
  - 學籍管理系統為本單位的重要核心業務之一，該系統含括本校所有學生之基本資料，為保護學生個人資料安全，並使該系統得以正常運作，故選擇「學籍管理系統維護管理」為本次ISMS施作範圍與教育體系資通安全管理規範之驗證範圍

ISMS導入過程(續)

- 擬定資訊安全政策
  - 資訊安全管理涵蓋11項管理事項
  - 資訊安全政策應至少**每年審查乙次**，以反映政府法令、技術及業務等最新發展現況
- 建立資訊安全組織



ISMS導入過程(續)

階段	階段一：規劃資訊安全政策	階段二：執行風險管理與評鑑
時程	97/08/18 ~ 97/09/11	97/09/12 ~ 97/9/26
	教育訓練/技術移轉	
執行作業	1. 組織業務分析 2. 成立資訊安全組織 3. 建立資訊安全政策 4. 建立文件管理機制	1. 資產分類及管理 2. 風險評鑑 3. 風險管理與產出適用性聲明
產出	1.專案推動執行計畫書 2.啟動會議簡報及會議紀錄 3.業務風險分析報告 4.資訊安全組織程序書 5.資訊安全政策 6.文件管理程序書 7.教育訓練教材	1.資訊資產管理程序書 2.風險評鑑與管理程序書 3.風險評鑑報告 4.資訊資產清單 5.風險改善計畫 6.適用性聲明 7.教育訓練教材

ISMS導入過程(續)

階段三：規劃資訊安全管理系統實施	階段四：制度落實與實施稽核作業
97/09/27 ~ 97/12/10	97/12/11 ~ 97/12/25
教　育　訓　練 / 技　術　移　轉	
1.建立資安文件體系與整合文件管理架構 2.建立ISMS四階文件 3.建立安全事件管理程序及業務永續運作計畫 4.業務永續運作計畫演練	1.資安內部稽核計畫 2.資訊安全稽核教育訓練活動 3.執行資安內部稽核
1.資訊安全管理ISMS四階文件 2.資訊安全事件應變處理程序 3.業務永續運作計畫 4.業務永續運作計畫演練報告	1.稽核計畫 2.稽核報告 3.管理審查會議紀錄

導入建置效益

導入建置效益

- 制度化、文件化
  - 規範業務與作業流程
  - 建立災害評估、檢測方式與復原計畫
- 定期檢視與習慣養成
  - 定期檢測認證範圍內資產
  - 養成遵守資安要求的習慣
- 紀錄保留
  - 重視紙本文件與電子資料
  - 強化Log server與log分析功能
- 更新資安設備
- 提升同仁資安意識

瞭解資訊安全弱點

- 資訊安全稽核結果及建議改善事項，提供具體改善內容
- 矯正及預防措施檢討
- 資訊安全組織成員提出之改善建議
- 相關團體的回饋與建議
- 透過審查使資安產品或技術的導入更有效
- 參加資安課程後，補強工作上需注意的地方

透過稽核結果及建議事項進行改善

評分「D」：相關資訊安全管理制度規範未建立，且未實施替代性資安控管措施			
稽核項目	稽核發現	建議事項	附註
無	無	無	無
評分「C」：相關資訊安全管理制度規範已建立，但未落實執行			
稽核項目	稽核發現	建議事項	附註
1. 玖、七文件要求：關於ISMS文件化（電子檔案或紙本），必須包含安全政策、安全目標、ISMS範圍、適用性聲明、資安事件記錄，以及其他有助於提升ISMS成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過期文件需保留或銷毀，應予以適當的鑑別。	未發現第一批發行文件之審核紀錄； 「資訊安全管理文件列表」中IS-D-025及IS-D-033與「文件修訂建議表」之發行日期不一致建議加強資訊安全管理文件列表鑑別管控	建議加強資訊安全管理文件列表鑑別管控	
2. A.15.1.2適用法規之遵循	ISMS文件負責人葉先生未列「資訊安全組織成員表」之資訊安全小組成員中	建議修訂「資訊安全組織成員表」	
3. A.8.1.1所屬角色與責任	於個人電腦中發現WinRAR壓縮軟體	建議移除該非授權之軟體	
評分「B」：相關資訊安全管理制度規範未建立，但已實施替代性資安控管措施			
稽核項目	稽核發現	建議事項	附註
無	無	無	無

透過稽核結果及建議事項進行改善(續)

其他建議事項
1. 適用性聲明書之其驗證範圍描述，建議考量其適切性。
2. 「資訊安全組織程序書」第5.1.2點，由本中心各單位主管及本校具資安專長之教師組成...，建議資訊安全委員會成員，可再加上非中心之具資安專長人員。
3. 「資訊安全管理文件列表」，建議可加上『版本』欄位以加強文件之鑑別管控。
4. 建議可再重新檢閱ISMS文件之表單『紀錄編號』，以確保是否還有遺漏編碼之表單。
5. 「外單位聯絡清單」，建議可加上環安組、電工或警衛等聯絡資訊。
6. 「資訊安全政策」，建議可採用e-mail方式向委外服務廠商或工讀生宣達。
7. 「資訊資產清冊」中發現『ISMS維運紀錄表單』其機密性為1，與「保密切結書」之機密等級不符，建議修訂其機密性價值；另學籍系統之備份CD可加列入該清冊中。
8. 「業務流程衝擊分析表」，建議可依據重要性的資產規劃其業務流程之RTO、RPO。
9. 「風險改善計畫」，建議可將已完成作業之日期加上，並將相關處理動作紀錄保存。
10. 「業務永續運作演練活動紀錄」，建議可將規劃演練成果的檢討時程日期、時間述明，另若有相關業務單位配合演練，建議可加於協辦單位欄位。
11. 建議追蹤豪勉科技及瑞協電機之「合約商保密切結書」。
12. 建議可於機房中加設CCTV，以加強機房區域的安全性。
13. CCTV監控系統，建議以帳號密碼加以管控，另注意時間矯正。
14. 學籍系統備份媒體(CD)，建議可考量異地備份作業。
15. 建議可於機房中增設手提式滅火器。
16. 「網路設備設定檔」其機密性資產價值為4，建議加強相對應之管控機制。
17. Junniper防火牆，建議加強管理者帳號分權管控機制。
18. 建議針對UPS進行充放電測試，以確保不斷電系統之有效性。

矯正及預防措施檢討

項次	問題或缺失說明	原因分析	矯正與預防措施評估	預計完成日期
1	未發現第一批發行文件之審核紀錄； 「資訊安全管理文件列表」中IS-D-025及IS-D-033與「文件修訂建議表」之發行日期不一致建議加強資訊安全管理文件列表鑑別管控	第一批發行文件於發佈前已經謝主任審核核示公告，但未留下任何書面審核記錄。 「資訊安全管理文件列表」中IS-D-025及IS-D-033與「文件修訂建議表」之發行日期不一致是導因於同仁對文件列表之發行日期認知不同所致。	於資訊安全管理審查會議中，提報討論事項，並請會議追認通過。 修訂「資訊安全管理文件列表」，使之更符合文件控管之目的。	97/12/25
2	ISMS文件負責人葉先生未列「資訊安全組織成員表」之資訊安全小組成員中	由於IS-B-001資訊安全組織程序書，未明確載明文管人員需列入資訊安全小組成員，因此未予已列入。	修訂「資訊安全組織成員表」，將文管人員列入資訊安全小組。	97/12/20
3	於個人電腦中發現WinRAR壓縮軟體	作業人原因疏忽未依規定要求移除非授權使用軟體。	已請相關人員依規定辦理，將授權軟體移除。	97/12/20

資訊安全組織成員提出之改善建議

資訊安全委員會
☐無
資訊安全官
☐建議擴大資安管理委員會之參與人員，以廣納多方意見。 ☐為增加稽核能力，建議於本中心開辦主導稽核員認證課程。
資訊安全小組
☐為提升緊急應變能力，建議增加異地備援機制
資訊安全稽核小組
☐無

相關團體的回饋與建議

單位	回饋與建議
上級機關	☐教育部： 教育部97年12月17日箋函告知，本校於97年7至11月在校園網路疑似侵犯智慧財產之案件共計57件。要求加強督導校園網路管理並建立更嚴謹之網路館管機制。 ☐教育部：針對P2P使用，來函要求行政人員禁止使用P2P軟體，以防止資料外洩的情事發生，近日更要求大專校院針對使用P2P軟體非法下載網路資源之情形希望採『原則管制、例外開放』。
輔導單位(KPMG)	☐擬定教育訓練與宣導計畫來持續強化本中心同仁對於資通安全之完整認知 ■排定年度教育訓練計畫(包含委外人員)以符合行政院對於B級單位人員教育訓練時數要求 ■透過電子報或內部網站來宣導人員應遵守之資通安全相關規定 ■選擇適當之測驗方式來檢驗教育訓練與宣導之效果與人員是否擁有足夠之相關知識，並從中找出後續改善之道

透過審查使資安產品或技術導入更有效

- 97年第2或3季導入流量分類管控設備
  - 預估使用預算2,200,000元
  - 設備將建置於校園網路出入口端、，管控校園進出網際網路之流量
  - 預期之效益為針對P2P下載量及頻寬可加以管制，達到總量管制，長期監控之目的
- 建立校園網路管理系統
  - 有鑑於近幾年正修校園網路架構與設備不斷升級與改善，也使得校園網路架構也日趨複雜，為了有效管理，並在網路出現問題時能夠迅速找出問題，排除狀況，因此需要一套具效率的網路管理系統。
  - 預計完成時程為97年第四季
  - 預期成本為350,000
  - 預期效益

導入前後學籍管理系統維護管理比較

	Before	After	影響
使用者帳戶	1.未全面清查,資料庫留有一些已不使用之帳號 2.填寫請辦單	1. 清查資料庫使用者名單與IP,是否由user已調離不該有權限,或權限已變動,..整理後存檔 2. 申請者需填IS-D-025表單	更清楚全校那些單位工作人員確實可使用系統與其權限
系統密碼管理	未限制密碼長度 與強迫更新密碼	程式修改 a. 限制密碼6~10碼 b. 三個月需更新密碼否則無法進入系統 c. 超過6個月未使用者帳號將無法使用需表重新申請帳號	程式修改花很多時間,但也著實有些成效..新程式上線後三個月便陸續接到電話密碼進不去... 這一輪後再也沒少於6碼的密碼,半年未登入者也發現他的密碼非萬年密碼.. 程式控管比宣導更改密碼成效好太多
程式改版版本EXE	BY Mail寄給user	加密後再寄給user	沒密碼的人無法安裝程式

導入前後學籍管理系統維護管理比較(續)

	Before	After	影響
程式改版版本異動紀錄	紀錄不全 寄MAIL(程式EXE)會簡單紀錄此次版本異動內容	每次版本更動詳細紀錄修改內容(IS-D-032)	以前靠MAIL寄件備份留存,但有過電腦重灌MAIL全掛紀錄也跟著掛 雖然需花時間紀錄 不過需要回頭查時可很清楚從紀錄查到那個版本修改過甚麼內容
備份	不定期	程式修改前一定被份,並定時備份	以前小修改沒備份直接修改,但若有閃失須回想那邊更改過, 費時,現強迫養成習慣,修改測試比較不擔心.因有備份
資料轉檔	EXCEL檔 Email寄出	為安全加密處理 需求者收到mail後需來電詢問密碼才能打開檔案	加密後需求單位更加緊慎,會詢問資料安全性可否給.比較不敢隨便給資料

給予未來導入學校之建議

- 導入的時機
- Budget
  - 編列適當的預算
  - 尋求口碑好的顧問公司輔導
- 資安組織與層級
  - 決定資安組織範圍的大小
  - 避免過多審查層級
- 人力資源
  - 以團隊工作取代單打獨鬥
- 主動積極作為化解抗拒心態

實例範本摘要說明

學籍系統障礙偵測與復原之作業程序

當學籍管理系統出現錯誤，無法執行時，應先通知本中心程式負責人，並依下列程序執行障礙偵測與復原：

1. 程式負責人確認程式否正常運作:

檢查方式:程式負責人於程式開發電腦，啟動程式，檢查是否能正常執行，

檢查結果:若程式能正常執行，則可判斷資料庫 仍正常運作，請繼續下一步驟。

檢查結果：程式無法執行，或其它情況造成無法正常使用請依**內部網路障礙偵測與復原，資料庫伺服器障礙偵測與復原，防火牆障礙偵測與復原**程進行處理。

2. 程式負責人確認使用者端學籍管理系統程式本身是否錯誤:

檢查方法：詢問操作人員錯誤訊息與障礙狀況。

檢查結果一： 無相關錯誤訊息，請至第下一步驟。

檢查結果二：無法連線至資料庫，檢查內部網路是否能正常連線，若內部網路無法正常運作，請依通知網路管理人員依**內部網路障礙偵測與復原**處理程序處理，若內部網路可正常連線，請通知防火牆管理人員檢查防火牆規則是否正確，同時依**防火牆障礙偵測與復原**程序進行處理。

檢查結果三：帳號或密碼錯誤，確認使用者帳號密碼是否正確，密碼是否過期，檢查密碼修改記錄，檢查密碼是否被竄改，填寫[資訊安全事件報告單]，同時請使用者填寫[IS-D-025-資訊服務申請表]申請重置密碼。

檢查結果四：其它錯誤訊息，檢查是否安裝最新版程式，是否已安裝相關設定檔，若有必要時重新安裝學籍管理系統程式

3.程式負責人確認使用者電腦是否能正常使用:

檢查方式:詢問使用者電腦是否能正常上網，與開啟其它應用程式。

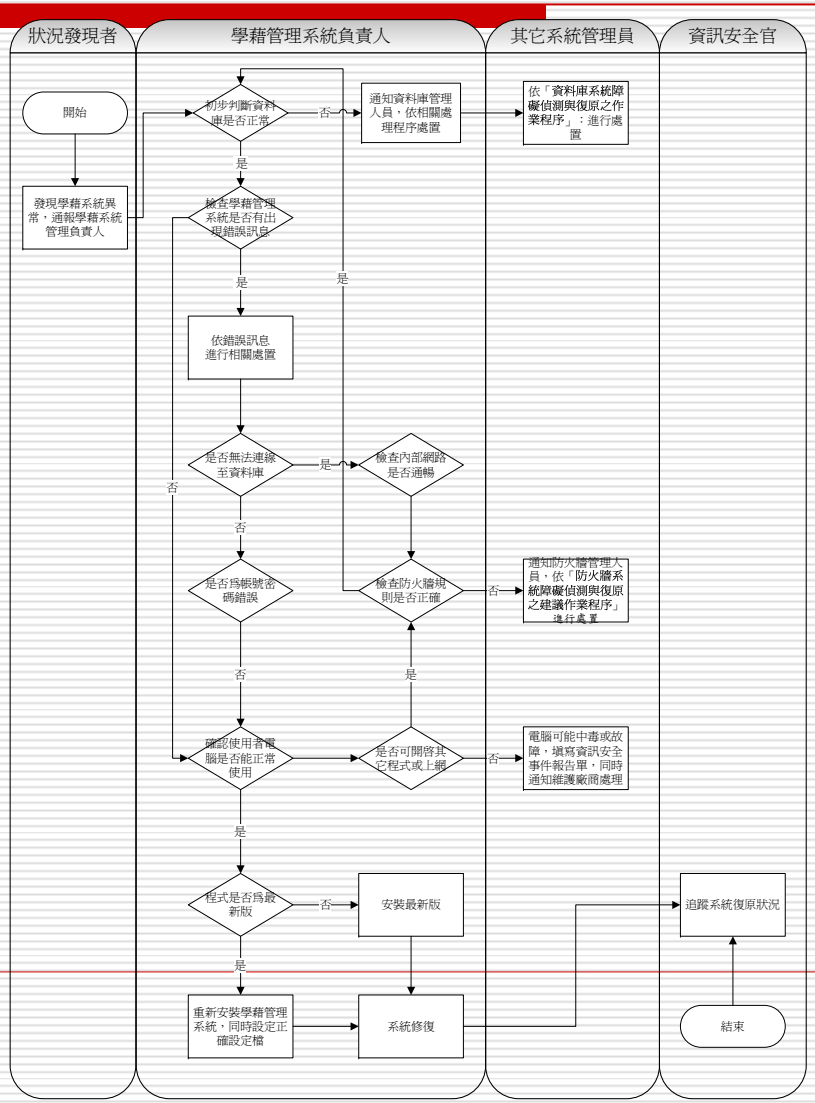
檢查結果一:無法正常上網或無法開啟其它應用程式，判斷使用者電腦可能中毒或故障，填寫[資訊安全事件報告單]與執行安全　　事件通報與應變作業流程。

檢查結果二:可正常使用網路或開啟其它應用程式，判斷可能被防火牆阻檔，請通知防火牆管理人員檢查防火牆規則是否正確，同時依**防火牆障礙偵測與復原**程序進行處理。

通報處理狀況與檢討。進行**學籍系統障礙事件處理檢討。**

- 復原狀況檢討:向資訊安全官報告處理進度與狀況
- 事件處理檢討:依據「**學籍系統障礙偵測與復原之建議作業程序**」處理程序中有窒礙難行或可改進的步驟來進行討論與回饋。

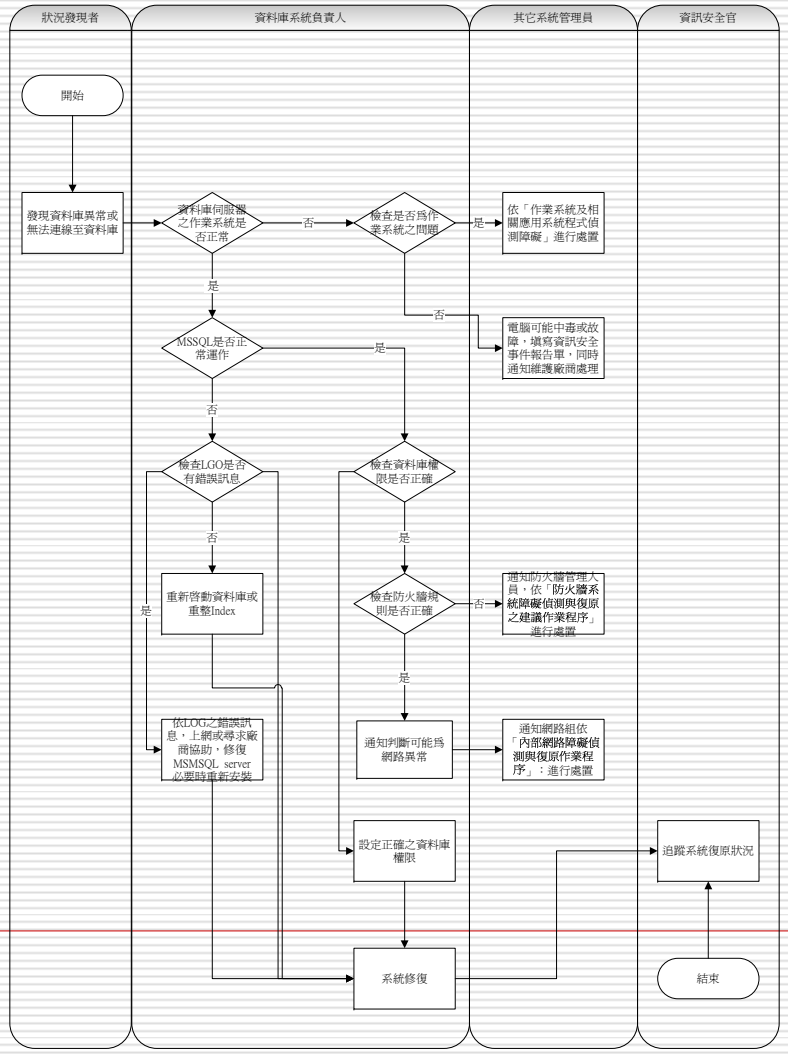
學籍管理系統障礙偵測與復原流程圖



資料庫系統障礙偵測與復原之作業程序

- **資料庫系統障礙偵測與復原之建議作業程序**
- 當資料庫系統出現異常，應先通知本中心資料庫管理負責人，依下列程序執行障礙偵測與復原：
  - 確認SQL是否正常運作：
- 檢查方法：使用SQL管理工具檢視資料庫是否正常運作。
- 檢查結果：
  - 如不正常，請繼續以下步驟
    - 資料庫應用程式系統無法正常運作，請依下列程序執行障礙偵測與復原：
    - 確認資料庫伺服器之作業系統是否正常運作
- 檢查方法：連線至資料庫伺服器檢測。
- 檢查結果：
  - 若發現遠端無法登入資料庫伺服器，請先判斷是否為網路中斷，若為網路中斷請依「網路障礙偵測與復原流程圖」處理。
  - 否則，請繼續以下步驟。
    - 資料庫管理人員至機房檢測伺服器，排除伺服器主機之故障
- 檢查方法：至機房伺服器主機檢測。
- 檢查結果：
  - 若作業系統可正常使用，但MSSQL 無法運作正常，請繼續以下步驟。
  - 若作業系統出現異常，請先檢查LOG檔是否判斷異常原因，同依「作業系統及相關應用系統程式偵測障礙」處理，同時由資料庫管理員，將備份之資料移至備援之伺服器先行上線，同時通知伺服器維護廠商進行維修。
    - 資料庫權限問題
- 檢查方法：檢查資料庫執行時所需目錄或檔案的相關權限。
- 檢查結果：
  - 若權限設定不對，則修改權限至正確。
  - 否則，請繼續以下步驟。
    - MSSQL程式錯誤
- 檢查方法：以資料庫管理界面，開啟資料庫，檢查LOG檔判斷誤錯之原因。
- 檢查結果：
  - 資料庫回應時間過長，可能為伺服器過於忙碌，請檢查資源是否耗盡，移除不必要之連線，同時檢查是否中毒或遭受駭客入侵。
  - 資料庫正常運作，但部份資料表無回應，判斷可能為Index錯誤，可重建Index修復錯誤，或依備份資料重新建立資料表。
  - 若LOG有相關之錯誤記錄，請依記錄之錯誤尋找相關解決方案。
- MSSQL服務停止，重新啟動MSSQL，若無法啟動，資料庫管理員，將備份之資料移至備援之伺服器先行上線，再進行錯誤排除，必要時重新安裝軟體。

資料庫障礙偵測與復原流程圖



演練規劃表

演練規劃表		
承辦人：薛甘霖 協辦單位：無 規劃日期：97/12/10		
演練規劃項目		規劃內容
1	規劃演練目標與範圍	規劃演練目標：確保關鍵業務流程遭受重大故障和災難事件而中斷時，能以迅速、有效的方法回復正常運作。 範圍：正修科技大學學籍管理系統
2	規劃演練腳本	請詳附件—97年度業務永續運作計畫演練腳本
3	規劃演練所需設備	備用伺服器一台
4	規劃演練所需系統	Server2003 ,MSSQL 2005

演練規劃表

5	規劃演練所需參與人員	資料庫管理人員 學籍系統負責人
6	規劃演練時程及完成時限	4小時
7	規劃演練測試方式與測試資源	測試備份資料復原於備援伺服器上狀況， 僅行政組相關人員參與測試
8	規劃演練成果的檢討時程	演練結束後

演練規劃表

演練暨處理執行表				
承辦人：薛甘霖 協辦單位：無 演練日期：97/12/10				
計畫開始時間	13:40	計畫需要時間	45分鐘	
計畫結束時間	14:00	實際作業時間	20分鐘	
演練執行項目		執行程序 （實際演練過程之執行紀錄）	負責人	執行結果
1	業務負責人通報	註冊組發現學籍管理系統無法使用，通知學籍管理系統負責人進行瞭解，經檢查後發覺為資料庫無回應，判定為資訊安全事件，無法於短時間內回復，立即通知資訊安全官及緊急處理組召集人，並報告狀況	莊培荃	填寫IS-D-036資訊安全事件報告單

問題與討論