

ISO27001驗證經驗分享

中原大學電算中心
2008.11

資安管理制度推動建置時程

- 96.3資訊安全教育訓練
- 96.3~96.11政策文件撰寫討論
- 96.4~96.12資訊資產風險評鑑作業
- 96.8~97.3營運持續管理作業
- 96.11~ 資訊安全管理實施
- 97.1內部稽核
- 97.2預評
- 97.3驗證通過
- 97.8內部稽核
- 97.9第一次追查驗證

驗證範圍

■ 實體範圍

- 電算中心辦公室(4間)
- 伺服器機房(3間)
- 電腦實習教室(9間)
- 校園資訊站

■ 系統範圍

- 電算中心所提供的校級應用系統及服務
-

電算中心關鍵業務簡介

- Itouch服務
 - Outlook服務
 - AD目錄服務
 - Agent flow
 - 公文線上簽核系統
 - 招生系統
 - 選課系統
-

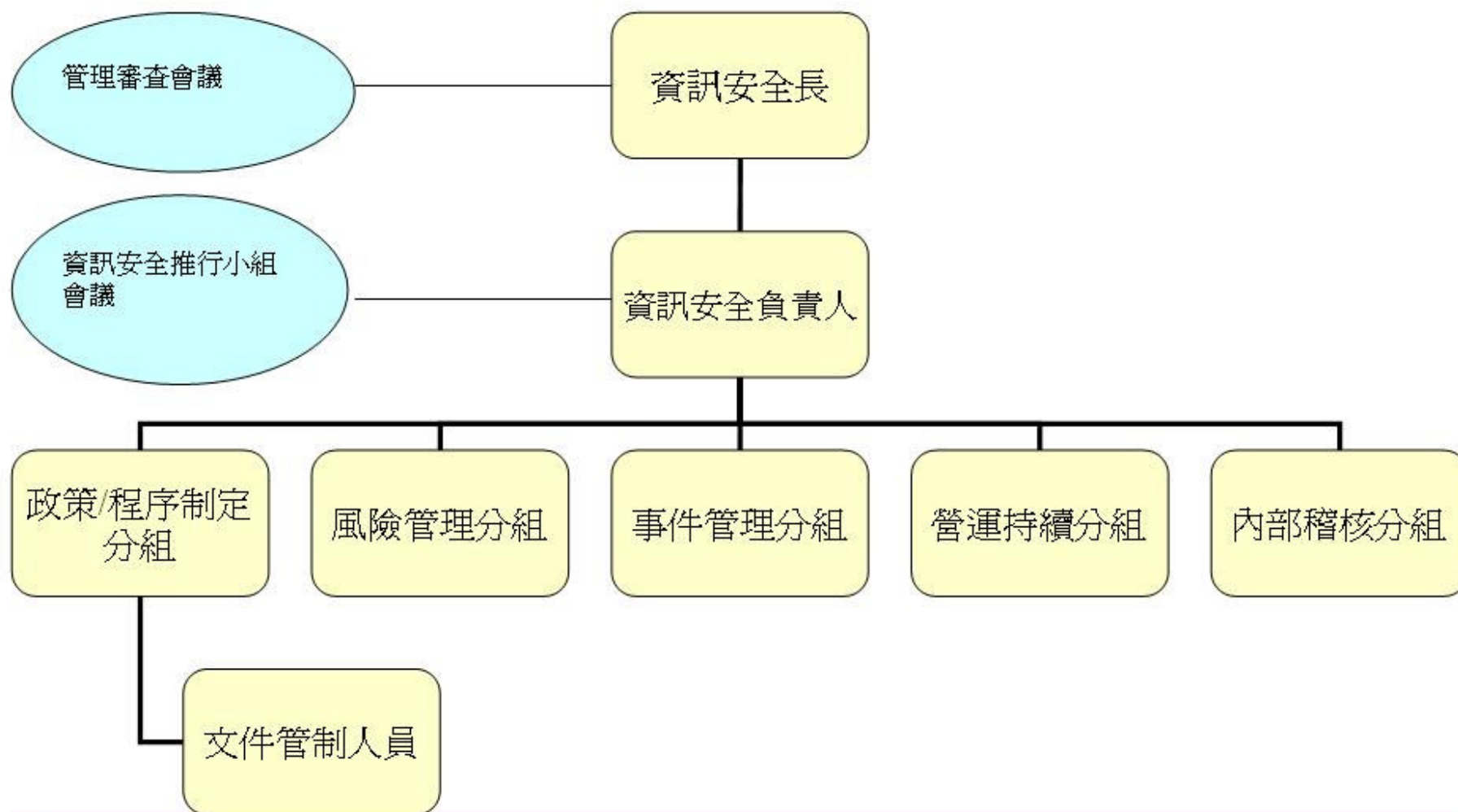
電算中心關鍵業務簡介(續)

- 校務資料庫Oracle DB
 - 單一簽入服務
 - DNS
 - e-Mail server
 - 網路主幹設備
 - 機電設備
 - 伺服器機房環境
-

組織/人員架構

- **CISO**資訊安全長：錢副校長建嵩
- 電算中心
 - 涂世雄(主任)、簡明美(助理)、江婕妤
 - 資訊服務組(資服組)
 - 張安平(組長)、葉平、孫茂哲、郭雅貞、魏新武、張冰珠、蔡佳玲、郭麗美、周素萍(育嬰假)、王得智、林麗桐、范植華、江俊傑、林文漢
 - 校務資訊組(校資組)
 - 鄭憲永(組長)、何武勳、蔡美惠、湯馨韻、徐文寅、項小龍、蔣旭政、魏玉玲、吳敏菁、林雅婷、王佳祥、張弘典、沈君鄉、陳怡靜、鄭昆發、陳婷婷
 - 共計：專職24人、約聘9人

資安管理制度推動組織架構



資訊安全教育訓練統計

類別	科目	時數
建置	資訊安全簡介與資訊安全政策	6
	風險管理及風險評鑑	4
	持續營運計畫與管理	2
	資訊安全內部稽核	6
宣導	全員認知宣導	12
稽核	ISO 27001主導稽核員訓練(每人)	40

1.自辦教育訓練：共15場，計30小時。

2.外訓：LA共四名(每人:8小時*5天)-張安平、蔡美惠、項小龍、林文漢，皆取得國際LA證照。

重要變革

ISMS控制項	重要變革
A.5 安全政策	資訊安全政策擬定 資訊安全聲明宣導 資訊安全政策定期審查
A.6 資訊安全組織	設置資訊安全推動組織
A.7 資產管理	資訊資產標示 資訊資產分類 資訊資產風險評鑑
A.8 人力資源安全	資訊安全教育宣導
A.9 實體與環境安全	安裝自動滅火系統 伺服器機房裝卸區規劃 建置IC門禁及監視錄影系統 建立設備定期檢查制度

重要變革(續)

ISMS控制項	重要變革
A.10 通訊與作業管理	擬定資訊委外管理程序 資訊系統定期備份
A.11 存取控制	帳號權限定期審查 螢幕保護設定及桌面淨空
A.12 資訊系統取得、開發及維護	建立應用系統資安控管表
A.13 資訊安全事故管理	資訊安全事件通報及處理
A.14 營運持續管理	營運持續計劃擬定 災害復原計畫及演練
A.15 遵循性	使用自行開發軟體版權稽核工具清查&稽核 請法律專家協助鑑別適用之法律、法規及辦法

順利驗證要素

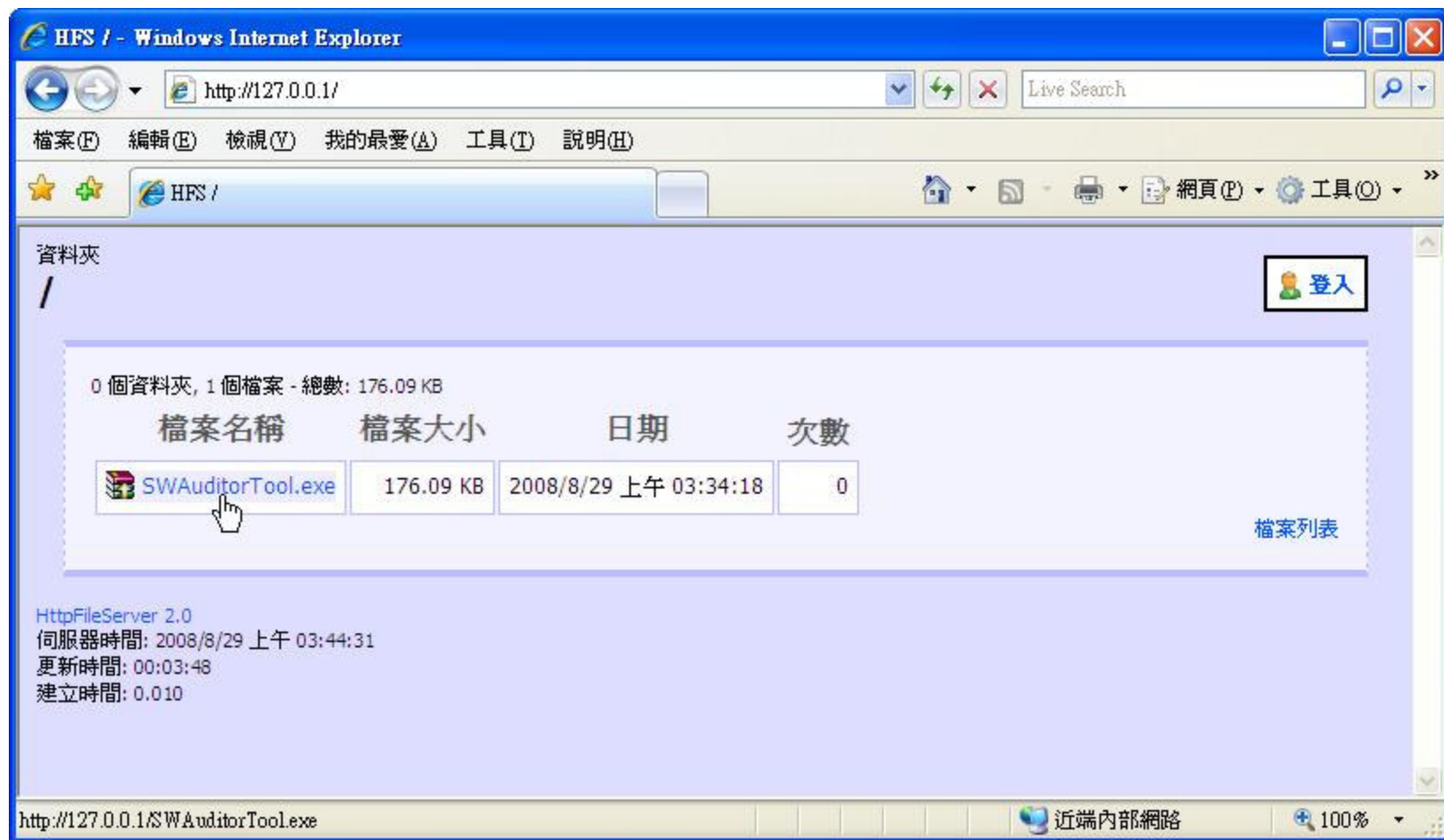
- 高層全力支持
 - 預算支援及跨單位協商
- 全員投入
 - Process Owner：8人
 - 內稽小組
 - 組長1員、組員4員、內稽觀察員4員
 - 藉由培養內稽觀察員方式，讓更多同仁熟悉相關程序書內容及規範
- 聘請專業顧問量身訂作ISMS及相關程序書
- 每週中心會議討論資安相關議題

已順利通過第一次追查驗證

- 內稽以全面實際稽核為主，找出待改善事項以強化**ISMS**，非虛應了事
 - 不符合及疑似不符合事項 **11** 項
 - 尚未提供之證據 **8**項
 - 建議事項 **4**項
- 內稽後彙整資安案例加強宣導
- 於今年**9月17**日以零主缺零次缺通過每半年一次外稽追查驗證

軟體版權稽核工具SWAuditor

- 本校自行開發之**ISO 27001 / CNS 27001**驗證與稽核的好幫手，只要**2 ~ 3分鐘**，立即挑出未授權軟體或禁裝的**P2P (點對點)**軟體，並可得知最近執行**Windows Update**更新作業系統的時間。
 - 可避免於**ISMS**驗證外稽時被查到有人使用非法軟體，而造成整個驗證失敗。
-



只須將本工具軟體置於網頁
伺服器，並將網址藉由
E-mail 提供給同仁下載。



下載時，直接選擇「執行」即可。



接著會開啟Excel軟體，在「安全性警告」視窗中，請按「啓用巨集」繼續即可。

A	B	C	D	E	F	G	H	I	J	K	L	M
標	項目名稱	產品名稱	廠商	版本	安裝日期	相關網址						
3	{0001B4F1	PDFCrea	Frank Hein	0.9.2	20060710	http://www.sf.net/projects/p						
3	{026A7A8	Acer Tablet PC Buttons										
	{0510E9B	Microsoft Reader										
	{0EFD2F9	Security Up	Microsoft	02.1.0.2	20080112							
3	{2908F0C	Internet 病	Symantec	11.0.2	20050908							
3	{29EC3BB	綜合所得	關貿網路		9 20080521	http://tax.nat.gov.tw						
3	{3248F0A	Java(TM)	Sun Micros	1.6.0.0	20080522	http://java.com						
	{350C97B	WebFldrs 2	Microsoft	09.50.6513	20030910							
	{44D02D8	ZSMC USE	ZSMC	2007.07.05	20080414							
	{44D4AF7	Microsoft I	Microsoft	08.0.50727.	20071007							
	{57D28E1	MSXML 6.	Microsoft	06.10.1200.	20080112							
	{625386A	Microsoft .	Microsoft	02.0.5238	20071007							
	{627ABB6	TTS	synthigenc	1.0.0.0	20080707							
	{63569CE	Windows C	Microsoft	1.3.0254.0	20050908	http://www.microsoft.com/genuine/downloads/whyValidate.aspx/about						
	{67C5EC1	Microsoft .	Microsoft	01.1.50727.	20071007							
	{68A3504	Microsoft V	Microsoft	02.0.50727	20071007							
	{6C53106	Microsoft .	Microsoft	01.0.4292	20071007							
3	{7148F0A	Java 2 Run	Sun Micros	1.4.2_01	20031006	http://www.java.com						
3	{7F14F68	EPSON Web-To-Page										
	{804835F	Microsoft V	Microsoft	02.0.50727	20071007							
3	{8A708DD	Intel(R) Extreme Graphics 2 Driver										
3	{8C2FA1E	Acer Noteb	Acer	2.0.12.21	20031011	http://www.acer.com						
	{9011040	Microsoft C	Microsoft	011.0.8173.	20080814	http://www.microsoft.com/taiwan/support						
	{9012000	Compatibil	Microsoft	012.0.6215.	20080814	http://www.microsoft.com/support						
	{9052040	Microsoft C	Microsoft	011.0.3709.	20060611	http://www.microsoft.com/support						
3	{91CA39B	i-Sync ME for S-Series		1.01.01								
	{A28E82A	Microsoft I	Microsoft	08.0.50727.	20071007							

接著會在Excel中進行軟體的分類及標示處理。

A57												
A	B	C	D	E	F	G	H	I	J	K	L	M
	3 {A7FCAC8	DVR Contr		2.00.0000	20080612							
	3 {AC76BA8	Adobe Rea	Adobe Sys	8.1.2	20080306	http://www.chinese-t.adobe.com/products/acrobat/main.html?c=tw						
	3 {B508B3F	Microsoft .	Microsoft	02.1.21022	20080221							
	3 {BC69DDI	EPSON Easy Photo Pri		1.2.3.0								
	3 {BED7385	Microsoft I	Microsoft	01.0.50727.4	20071007							
	3 {C0610404	Microsoft V	Microsoft	08.0.50727.4	20080112							
	3 {C47F1E78	Microsoft S	Microsoft	03.0.0.0	20071007							
	{CA0A1E5	Symantec I	Symantec	05.5.1.6	20050908							
	3 {CF8EA26	MSDN Lib	Microsoft	8.0.50727.4	20071007							
	{D327AFC	Symantec S	Symantec	11.0.2	20050908							
	3 {F2545484	O2Micro S	您的公司	1.00.0000	20030910	http://www.yourcompany.com						
	1 {FABFEAF	PAPAGO!	Maction	12.1.0	20080425	www.mactiontech.com						
	3 {FCE65C4	Microsoft V	Microsoft	01.1.1905.1	20050912							
	3 Acer English Online Help Creator											
	3 AddressBook											
	3 Adobe Flas	Adobe Flas	Adobe Sys	9.0.115.0		http://www.adobe.com/go/getflashplayer						
	3 Agere Syst	Agere Systems	AC'97 Modem									
	3 AutoItv3	AutoIt v3.2.10.0										
	3 avast!	avast! Anti	Alwil Softw	4.8		http://www.avast.com						
	3 Branding											
	3 Cdic 中英	Cdic 1.1	Lcc Wizard			http://cview.com.tw						
	3 Connection Manager											
	3 DIBDVBT	KWorld DVB-T	USB2 Drivers									
	3 DirectAnimation											
	3 DirectDrawEx											
	3 DXM_Runtime											
	3 EPSON Pri	EPSON印表機軟體										
	3 ESC79 灌	ESC79 灌階使用說明										

Microsoft Excel - SWList.xls				
檔案(F) 編輯(E) 格式(O) 插入(I) 工具(T) 資料(W) 視窗(W) 說明(H)				
A1 申原大學軟體版權稽核工具				
A	B	C	D	E
1	中原大學軟體版權稽核工具		機密等級：〈限閱〉	by 林文漢 Ver.2008.08.
2				
3	人事代碼：		姓名(列印後親簽)：	掃描時間：2008.08.29-0
4	財編後五碼：			
5	電腦說明： <input type="checkbox"/> PC <input type="checkbox"/> NB <input type="checkbox"/> 工讀生 <input type="checkbox"/> 會議PC <input type="checkbox"/> 其它：			作業系統更新日期：20X
6	IP位址：	0.0.0.0 (卡號：00-0A-E4-0B-74-9F)；		
7				
8	標 版權說明	項目名稱	產品名稱	廠商
9	1 (請選擇...)	{FABFEAFE-BCB4-4D99-8F6D-C2CB4AB2F313}	PAPAGO! R12 PC	Maction
10	1 P2P軟體(禁裝)	Peer*	Peer*	
11	2 (請選擇...)	{44D02D8B-FFB3-4245-8D26-68D10B4C4023}	ZSMC USB PC Camera (ZS211)	ZSMC
12	2 (請選擇...)	{627ABB6F-A158-49A1-9F9C-715D81769F0F}	TTS	synthigence
13	2 (請選擇...)	{CA0A1B54-CE0F-4366-B09C-A87B61DC5633}	Symantec Network Drivers Update	Symantec Corporation
14	2 (請選擇...)	{D327APC9-7BA4-473A-8319-6EB7A0D40138}	Symantec Script Blocking Installer	Symantec
15	2 (請選擇...)	WIC		
16	3 免費或全校授權	{0001B4FD-9E83-4D90-A792-FD14B838B01D}	PDFCreator	Frank Henninger, Philip C.
17	3 免費或全校授權	{026A7A88-C017-4DB2-83DC-8E4P6006D843}	Acer Tablet PC Buttons	
18	3 免費或全校授權	{0510E9B6-C		
19	3 免費或全校授權	{0EFD2F9-8		icrosoft Corporation
20	3 免費或全校授權	{2908F0CB-C		mantec Corp
21	3 免費或全校授權	{29EC3BB5-4		貿網路股份有限公司
22	3 免費或全校授權	{3248F0A8-6		n Microsystems, Inc.
23	3 免費或全校授權	{350C97B6-3		icrosoft Corporation
24	3 免費或全校授權	{44D4AF75-4		icrosoft Corporation
25	3 免費或全校授權	{57D28E19-8		icrosoft Corporation
26	3 免費或全校授權	{625386A4-E		icrosoft Corporation
27	3 免費或全校授權	{63569CE9-F		icrosoft
28	3 免費或全校授權	{6705E016-6		icrosoft Corporation

只要2~3分鐘就可完成稽核報表，標示「3」綠色字樣項目可略過不管，只須把重心放在標示「1」或「2」的未知軟體或禁裝的P2P軟體就好。這就是這套工具最迷人的地方，甚至連作業系統更新時間都有顯示喔!!

D3 姓名(列印後親簽):

列印 (筆記本便箋書寫器)

A	B	C	D	E
中原大學軟體版權稽核工具			機密等級:《限閱》	by 林文漢 Ver.2008.6
人事代碼: 11333			姓名(列印後親簽):	掃描時間: 2008.08.29
財編後五碼: 16888				
電腦說明: <input type="checkbox"/> PC <input type="checkbox"/> NB <input type="checkbox"/> 手提 <input type="checkbox"/> 會議PC <input type="checkbox"/> 其他				作業系統更新日期: 2
IP位址: 0.0.0.0 (卡號:)				

標	版權說明	項目名稱	產品名稱	廠商
1	已有版權證明	FABFEAFE-B	APAGO! R12 PC	Maction
1	P2P軟體(禁裝)	Peer+	zPeer+	
2	設備附加軟體或	4D8ED8B-FF	SMC USB PC Camera (ZS211)	ZSMC
2	免費軟體Freeware	27ABB6F-A1	TS	synthigence
2	我會自行移除	CA0A1E54-C1	ymantec Network Drivers Update	Symantec Corporation
2	我會自行移除	D327AFC9-7E	ymantec Script Blocking Installer	Symantec
2	全校授權軟體	IC		
3	免費或全校授權	0001B4FD-9E	DFCreator	Frank Heindricher, Philip
3	免費或全校授權	026A7A88-00	acer Tablet PC Buttons	
3	免費或全校授權	0510E9B6-C4	microsoft Reader	
3	免費或全校授權	0EFDF2F9-836D-4EB7-4		Microsoft Corporation
3	免費或全校授權	2908F0CB-C1D4-447F-9		Symantec Corp
3	免費或全校授權	29EC3BB5-EFE7-431D-8		關貿網路股份有限公司
3	免費或全校授權	3248F0A8-6813-11D6-A		Sun Microsystems, Inc.
3	免費或全校授權	350C97B6-3D7C-4EE8-1		Microsoft Corporation
3	免費或全校授權	44D4AF75-6870-41F5-9		Microsoft Corporation
3	免費或全校授權	57D28E19-EAAB-4381-1		Microsoft Corporation
3	免費或全校授權	625386A4-B6B6-4911-A		Microsoft Corporation
3	免費或全校授權	63569CE9-FA00-469C-AF3C-E3D4D99AC917	windows Genuine Advantage v1.5.0204.0	Microsoft
2	免費或全校授權	67C5EC16-0DC1-4045-A7EE-D7D0EEA4D54D	Microsoft .NET Framework 2.0 Language Pack - CHT	Microsoft Corporation

(請選擇...)

(請選擇...)

免費軟體Freeware

全校授權軟體

免費或全校授權軟體

已有版權證明

試用軟體(Shareware)

我會自行移除

我會請購不足版權

設備附加軟體或驅動

其他(請在備註欄說明)

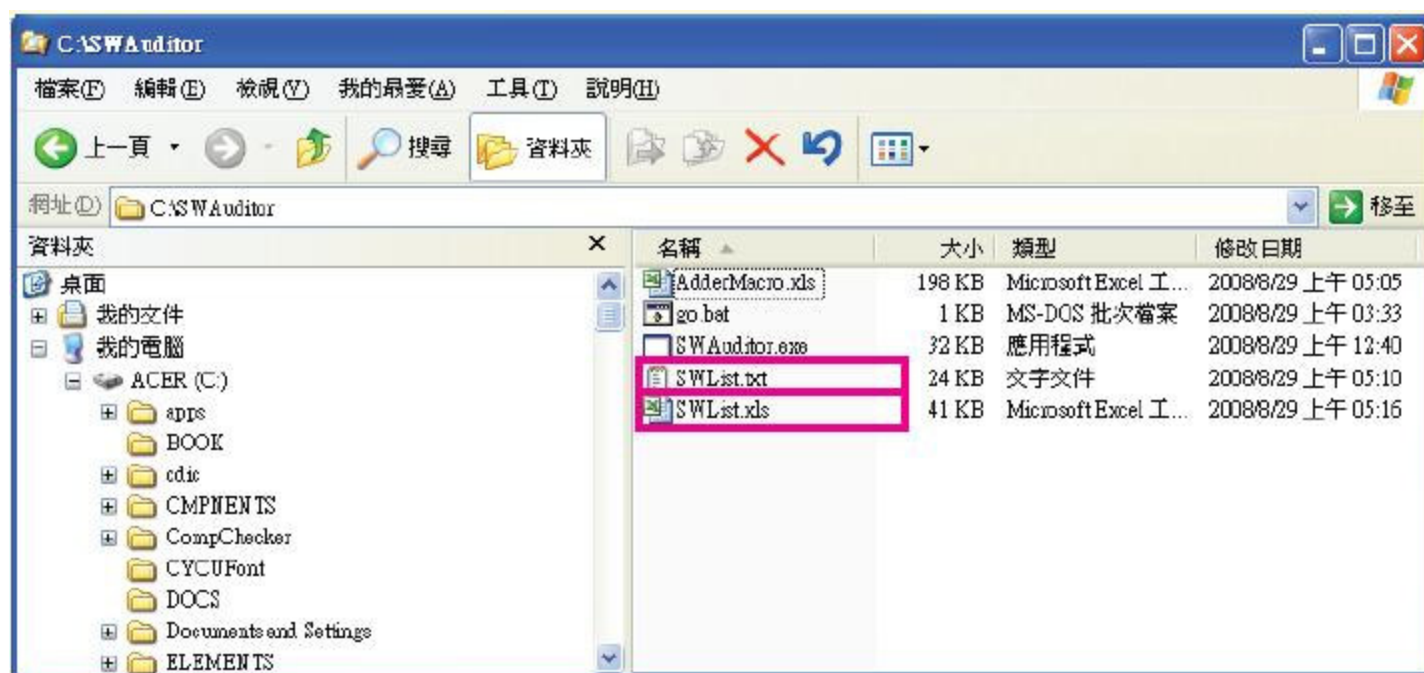
P2P軟體(禁裝)

輸入基本資料及針對標籤「1」及「2」一一由下拉選單中挑選版權說明，確認無誤後就可印出報表。

姓名(列印後親簽): 林文漢

中原大學軟體版權稽核工具		機密等級:《限》	by 林文漢 Ver.2008.08.29 04:59		
人事代碼:	11333	姓名(列印後親簽): 林文漢	掃描時間: 2008.08.29-05:16:17		
財編後五碼:	16888				
電腦說明:	<input checked="" type="checkbox"/> PC <input type="checkbox"/> NB <input type="checkbox"/> E 讀生 <input type="checkbox"/> 會議PC <input type="checkbox"/> 其它:		作業系統更新日期: 2008.08.14		
IP位址:	0.0.0.0 (卡號: 00-0A-E4-0B-74-9F):				
標	版權說明	項目名稱	產品名稱	廠商	版本
1	已有版權證明	(FABFEAFE-BCB4-4D99-8F6D-C2CB4AB2F3)	PAPAGO! R12 PC	Maction	12.1.0
1	P2P軟體(禁裝)	Peer	Peer		
2	設備附加軟體	(44D02D8B-FFB3-4245-8D26-68D10B4C4023)	ZSMC USB PC Camera (ZS211)	ZSMC	2007.07.05
2	免費軟體Free	(627ABB6F-A158-49A1-9F9C-715D81769F0F)	TTS	synthgence	1.0.0.0
2	我會自行移除	(CA0A1E54-CE0F-4366-B09C-A87B61DC5633)	Symantec Network Drivers Update	Symantec Corporation	5.5.1.6
2	我會自行移除	(D327AFC9-7BAA-473A-8319-6EB7A0D40138)	Symantec Script Blocking Installer	Symantec	11.0.2
2	全校授權軟體	WIC			
3	免費或全校授	(0001B4FD-9EA3-4D90-A79E-FD14BA3AB011)	PDFCreator	Frank Heindöffer, Philip C	0.9.2
3	免費或全校授	(026A7A88-0017-4DB2-83DC-8E4F6006D843)	Acer Tablet PC Buttons		
3	免費或全校授	(0510E9B6-C4C9-4C1D-8FE9-89EDDAA54958)	Microsoft Reader		

報表印出並親自簽名後再呈報給相關處理人員。



可請同仁回傳「SWList.txt」
及「SWList.xls」以進行工具
的改良。