德國ITBPM資安風險檢查表

中華民國資訊軟體協會
Information Service Industry Association of R.O.C.
台北市103承德路二段239號6樓
電話：(02)2553-3988
傳真：(02)2553-1319

中華民國資訊軟體協會
Information Service Industry Association of R.O.C.

中華民國96年5月

前　言

國際標準組織（ISO）於2005年發表ISO/IEC 27001，此一標準已成爲國際間資訊安全管理系統（ISMS）的共同語言。台灣在2001年起開始推動ISMS的認證，至今已經有127家政府機關、公民營單位通過了ISO/IEC 27001或BS7799的認證，在全球排名第4位。

儘管政府機關以及業界對資訊安全重要性，已經有相當程度的認同與投入。但是根據本會資安促進會會員表示，在輔導過程中，比較困難的一個項目是對「資安風險」的鑑別。因爲風險是未來的、無形的也是難以衡量的。但是在所有「資訊安全管理系統」的建置，都必須建立在組織資訊資產所面臨的安全風險大小與深淺之上。一方面組織可以投注在資訊安全的資源有限，另一方面資訊安全無限上綱又會影響到組織的運作效率。因此要落實資訊安全管理系統的功效，必須透過高度邏輯化的風險鑑別方法，以有效的識別並評估出風險的高低，再依據組織的風險接受準則，決定風險處理的作法，才能將有限資源做最有效的運用，達到「資訊安全管理系統」的建置目標。

執行風險鑑別時需針對不同的資訊資產，評定其面臨威脅的程度，方能規劃出相應而適當的防護措施。但實務上，都是由組織內的基層人員，運用腦力激盪法（窮舉法）以列舉組織內某資訊資產的所有可能威脅。這樣的作法，因爲從事風險評鑑人員個人的知識、歷練以及對組織營運深度洞察力的不同，可以產生迥然不同的風險鑑別結果。如果以少數個人的認知窮舉所認定的風險，作爲該組織投入龐大資源建置「資訊安全管理系統」，並全面在組織中實施，這種作法本身就是一個極大的風險管控漏洞。

有鑑於此，我們參考了由德國資訊安全局召集資安專家所編撰的「IT基準安全防護手冊」（IT Baseline Protection Manual, ITBPM）。分門別類的整理出共7大類、61個模組、375項組織資訊資產經常面臨的威脅項目的檢查表（Check List）。讀者在風險評鑑過程中可以參考這些完整列舉的風險項目，用以對照組織內部所面臨的風險，不但避免窮舉與討論時間的浪費，更能善用國際資安專家的智慧，確保組織風險識別無所遺漏。

本檢查表之編印成輯，承德國評測及驗證機構TUV NORD台灣分支機構陳盈顯經理，將上述檢查表翻譯成中文，以及資訊工業策進會技術服務中心諸位專家之指導，特致謝意。

中華民國資訊軟體協會理事長　王忠正　敬上
中華民國資訊軟體協會資安促進會會長　陳振楠

2007.5

目錄 CONTENTS

共通元件的IT基準保護模組之威脅列表

模組	威脅類型	威脅項目
IT安全管理	組織缺陷之威脅	・IT安全管理不當或缺乏
組織	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・資源不當或缺乏相容性 ・缺乏維護或維護不當 ・未經授權進入保護區域 ・未經授權使用 ・資源使用不受管制
人員	不可抗力之威脅	・人員傷亡
	組織缺陷之威脅	・對規則與程序認知不足
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・IT系統的使用不當
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・社交工程 ・間諜行爲
應變規劃觀念	不可抗力之威脅	・IT系統故障
資料備份政策	技術故障之威脅	・儲存資料遺失
電腦病毒保護觀念	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・資源不當或缺乏相容性 ・IT安全措施缺乏監控 ・資源使用不受管制 ・IT使用者異動未適當調整 ・測試程序不當或缺乏
	人爲錯誤之威脅	・違反IT安全措施

模組	威脅類型	威脅項目
電腦病毒保護觀念	故意行爲之威脅	・資料或軟體不當運用 ・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒 ・惡作劇
密碼觀念	組織缺陷之威脅	・管理規定缺乏或不足 ・相關規定與程序認知不足 ・IT安全措施缺乏監控 ・金鑰管理不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・違反法律或規定使用加密程序 ・加密模組使用不當
	技術故障之威脅	・軟體的脆弱性或錯誤 ・無效的鑑別 ・加密模組失效 ・不安全的加密演算法 ・加密資料錯誤
	故意行爲之威脅	・否認接收到訊息 ・資料喪失機密性 ・未經授權使用加密模組 ・竄改加密模組參數 ・洩漏加密金鑰 ・僞造憑證 ・資訊喪失完整性
資安事故處理	組織缺陷之威脅	・資安事故處理不當
硬體與軟體管理	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・IT使用者異動未適當調整 ・資料可用性不足 ・稽核資料缺乏評估 ・存取權限管理不當

模組	威脅類型	威脅項目
硬體與軟體管理	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・資訊管理不當
	技術故障之威脅	・軟體的脆弱性或錯誤 ・功能未書面化
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・特洛伊木馬病毒
委外	不可抗力之威脅	・廣域網路故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權使用 ・測試程序不當或缺乏 ・檔案和儲存媒體的傳送不安全 ・IT安全管理不當或缺乏 ・存取權限管理不當 ・委外策略的缺陷 ・外部服務供應商合約不符要求

模組	威脅類型	威脅項目
委外	組織缺陷之威脅	・委外專案終止條款不當 ・對委外服務供應商的依賴性 ・委外專案對組織的負面影響 ・委外實施階段IT 安全管控不當 ・與委外服務供應商聯繫不足 ・委外的事故處理規劃不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失
	技術故障之威脅	・無效的鑑別 ・加密模組失效 ・委外供應商系統故障
	故意行爲之威脅	・透過連接埠進行遠端維護 ・系統管理員權限的濫用 ・社交工程 ・資料喪失機密性 ・資訊喪失完整性 ・委外服務供應商不當揭露資料給第三方

基礎建設模組之威脅列表

模組	威脅類型	威脅項目
建築物	不可抗力之威脅	・閃電 ・火 ・水
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域
	技術故障之威脅	・電源供應中斷 ・內部網路故障 ・安全設備故障
	故意行爲之威脅	・未經授權進入建築內 ・盜竊 ・破壞 ・攻擊

模組	威脅類型	威脅項目
佈纜	不可抗力之威脅	・電（纜）線走火
	組織缺陷之威脅	・路由切割不當 ・佈線文件欠缺 ・配線箱保護不當 ・頻寬規劃不當
	人爲錯誤之威脅	・不允許的線路連接 ・人爲疏忽造成線路損毀
	技術故障之威脅	・環境因素導致線路損傷 ・串音 ・瞬間電流保護不足

模組	威脅類型	威脅項目
佈纜	故意行爲之威脅	・線路的分接 ・線路的運用不當
作業區域－辦公室	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域 ・不當的工作環境損害IT的使用
	人爲錯誤之威脅	・清潔或外來人員導致的危害
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・破壞
作業區域－伺服器房間	不可抗力之威脅	・火 ・水 ・工作溫度和濕度不當
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域
	技術故障之威脅	・電源供應中斷 ・內部網路故障 ・電壓不穩定
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・未經授權進入建築內 ・盜竊 ・破壞
作業區域－資料媒體歸檔	不可抗力之威脅	・火 ・水 ・工作溫度和濕度不當 ・灰塵與髒污
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域
	故意行爲之威脅	・未經授權進入建築內 ・盜竊 ・破壞
作業區域－機電室	不可抗力之威脅	・火 ・水 ・工作溫度和濕度不當
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域

模組	威脅類型	威脅項目
作業區域－機電室	技術故障之威脅	・電源供應中斷 ・內部網路故障 ・電壓不穩定
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・未經授權進入建築內 ・盜竊 ・破壞
保護櫃	不可抗力之威脅	・火 ・水 ・工作溫度和濕度不當 ・灰塵與髒污
	組織缺陷之威脅	・IT安全措施缺乏監控
	人爲錯誤之威脅	・code keys使用不當
	技術故障之威脅	・電源供應中斷 ・內部網路故障 ・安全設備故障 ・環境因素導致線路損傷
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・盜竊 ・破壞 ・內部員工導致的威脅 ・外部人員導致的威脅 ・以方便爲理由降低保護措施
在家辦公	不可抗力之威脅	・火 ・水
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域 ・不當的工作環境損害IT的使用 ・檔案和儲存媒體的傳送不安全 ・遠端工作環境中儲存媒體和文件的處置不當
	人爲錯誤之威脅	・清潔或外來人員導致的危害

模組	威脅類型	威脅項目
在家辦公	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・未經授權進入建築內 ・遠端工作導致較高竊盜風險 ・遠端工作易導致其他人誤用 ・資料喪失機密性
電腦機房	不可抗力之威脅	・IT系統故障 ・閃電 ・火 ・水 ・電（纜）線走火 ・工作溫度和濕度不當 ・灰塵與髒污 ・自然災害之影響 ・重大公衆事件所造成之問題 ・颱風
	組織缺陷之威脅組	・管理規定缺乏或不足 ・對規則與程序認知不足

模組	威脅類型	威脅項目
電腦機房	組織缺陷之威脅	・IT安全措施缺乏監控 ・未經授權進入保護區域 ・路由切割不當 ・佈線文件欠缺 ・消耗品供應不當或不正確
	技術故障之威脅	・電源供應中斷 ・內部網路故障 ・安全設備故障
	故意行爲之威脅	・未經授權進入建築內 ・盜竊 ・破壞 ・攻擊 ・內部員工導致的威脅 ・外部人員導致的威脅 ・未經授權存取動態網路組件 ・破壞行爲

非網路系統模組之威脅列表

模組	威脅類型	威脅項目
DOS 系統個人電腦（單一使用者）	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當
	技術故障之威脅	・電源供應中斷 ・儲存媒體受損

模組	威脅類型	威脅項目
DOS 系統個人電腦（單一使用者）	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・電腦病毒 ・巨集病毒
UNIX 系統	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污

模組	威脅類型	威脅項目
UNIX系統	組織缺陷之威脅	・未經授權使用 ・IT使用者異動未適當調整 ・UNIX系統之敏感資料喪失機密性
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・人爲疏忽造成線路損毀 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・IT系統管理不當
	技術故障之威脅	・電源供應中斷 ・電壓不穩定 ・儲存媒體受損 ・軟體脆弱性被揭露 ・NIS伺服器和NIS用戶端缺乏鑑別 ・X伺服器和X用戶端缺乏鑑別
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・線路的分接 ・線路的運用不當 ・未授權使用IT系統 ・有系統的猜測通行碼 ・使用者權限的濫用 ・系統管理員權限的濫用 ・特洛伊木馬病毒 ・電腦病毒 ・利用監聽設備監聽 ・UUCP軟體遠端指令的濫用 ・巨集病毒 ・網路連線遭劫持
膝上型個人電腦	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污

模組	威脅類型	威脅項目
膝上型個人電腦	組織缺陷之威脅	・未經授權使用 ・資源使用不受管制 ・筆記型電腦使用者變更欠缺管理規章
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當
	技術故障之威脅	・儲存媒體受損 ・內部電源供應中斷
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・特洛伊木馬病毒 ・可攜式設備遭竊 ・電腦病毒 ・巨集病毒
DOS系統個人電腦（多使用者）	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權使用 ・IT使用者異動未適當調整 ・使用者交接缺乏管理 ・稽核資料缺乏評估
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・場域資料存取權限管理不當 ・個人電腦使用者的異動不正確

模組	威脅類型	威脅項目
DOS 系統個人電腦（多使用者）	技術故障之威脅	・電源供應中斷 ・儲存媒體受損
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・有系統的猜測通行碼 ・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒
WIN NT 系統個人電腦	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	組織缺陷之威脅	・未經授權使用 ・IT使用者異動未適當調整 ・Windows系統保護不當
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・IT系統管理不當
	技術故障之威脅	・電源供應中斷 ・儲存媒體受損 ・軟體脆弱性被揭露 ・自動開啓光碟
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・有系統的猜測通行碼 ・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒 ・在Windows NT系統之管理權限遭濫用 ・未經授權取得Windows NT管理權限

模組	威脅類型	威脅項目
WIN 95 系統個人電腦	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權使用 ・IT使用者異動未適當調整 ・使用者交接缺乏管理 ・稽核資料缺乏評估 ・使用者環境的不當限制
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・場域資料存取權限管理不當 ・個人電腦使用者的異動不正確 ・登錄檔修改不當
	技術故障之威脅	・電源供應中斷 ・儲存媒體受損 ・自動開啓光碟 ・Windows95資料備份不支援長檔名
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒 ・未遵循系統操作說明
WIN 2000 系統個人電腦	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	組織缺陷之威脅	・未經授權使用 ・IT使用者異動未適當調整

模組	威脅類型	威脅項目
WIN 2000 系統個人電腦	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・IT系統管理不當
	技術故障之威脅	・電源供應中斷 ・儲存媒體受損 ・軟體脆弱性被揭露 ・自動開啓光碟
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・有系統的猜測通行碼 ・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒 ・在Windows NT系統之管理權限遭濫用 ・未經授權取得Windows NT管理權限
連接網際網路之個人電腦	不可抗力之威脅	・IT系統故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・使用者交接缺乏管理
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・IT系統管理不當 ・無效率的網路搜尋 ・錯誤的組態設定和操作
	技術故障之威脅	・軟體的脆弱性或錯誤
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・特洛伊木馬病毒 ・電腦病毒

模組	威脅類型	威脅項目
連接網際網路之個人電腦	故意行爲之威脅	・巨集病毒 ・IP冒用 ・DNS冒用 ・Web冒用 ・動態網頁內容遭濫用 ・webmail遭濫用
一般非網路IT系統	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權使用 ・IT使用者異動未適當調整 ・使用者交接缺乏管理 ・稽核資料缺乏評估
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・IT系統管理不當 ・場域資料存取權限管理不當 ・個人電腦使用者的異動不正確
	技術故障之威脅	・電源供應中斷 ・儲存媒體受損
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・有系統的猜測通行碼 ・使用者權限的濫用 ・系統管理員權限的濫用 ・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒

網路系統模組之威脅列表

模組	威脅類型	威脅項目
以伺服器為基礎的個人電腦網路	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・火 ・水 ・灰塵與髒污
	組織缺陷之威脅	・未經授權使用 ・IT使用者異動未適當調整 ・頻寬規劃不當
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・人爲疏忽造成線路損毀 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・IT系統管理不當 ・缺乏結構化資料管理
	技術故障之威脅	・電源供應中斷 ・電壓不穩定 ・儲存媒體受損 ・軟體脆弱性被揭露 ・網路IT系統存取機制過於複雜
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・線路的分接 ・線路的運用不當 ・未授權使用IT系統 ・有系統的猜測通行碼 ・使用者權限的濫用 ・系統管理員權限的濫用 ・特洛伊木馬病毒 ・電腦病毒

模組	威脅類型	威脅項目
以伺服器為基礎的個人電腦網路	故意行爲之威脅	・訊息重送攻擊 ・僞裝 ・訊息內容分析 ・否認接收到訊息 ・阻絕服務攻擊 ・巨集病毒
UNIX伺服器	組織缺陷之威脅	・UNIX系統之敏感資料喪失機密性 ・連線至伺服器的網路存在安全缺陷 ・SAMBA組態的複雜性
	人爲錯誤之威脅	・UNIX檔案系統輸出不正確 ・sendmail的組態設定不當
	技術故障之威脅	・電源供應中斷 ・NIS伺服器和NIS用戶端缺乏鑑別 ・X伺服器和X用戶端缺乏鑑別
	故意行爲之威脅	・利用監聽設備監聽 ・UUCP軟體遠端指令的濫用 ・網路連線遭劫持
peer-to-peer網路	組織缺陷之威脅	・點對點功能導致網路效能降低 ・SAMBA組態的複雜性
	人爲錯誤之威脅	・IT系統管理不當 ・資源分享未保護 ・Windows 95通行碼儲存未保護 ・非故意取得Schedule+讀取權限
	故意行爲之威脅	・猜測WfW和Windows95之通行碼 ・僞裝WfW的識別名稱 ・刪除他人郵件

模組	威脅類型	威脅項目
WIN NT系統網路	組織缺陷之威脅	・連線至伺服器的網路存在安全缺陷 ・點對點功能導致網路效能降低 ・網域規劃不當 ・Windows系統保護不當
	技術故障之威脅	・網路IT系統存取機制過於複雜 ・自動開啓光碟
	故意行爲之威脅	・電腦病毒 ・利用監聽設備監聽 ・巨集病毒 ・在Windows NT系統之管理權限遭濫用 ・未經授權取得Windows NT管理權限
Novell Netware 3.x	不可抗力之威脅	・IT系統故障
	組織缺陷之威脅	・伺服器工作環境不安全 ・網路伺服器安全機制不當或缺乏 ・千禧年日期轉換
	技術故障之威脅	・電源供應中斷
	故意行爲之威脅	・電腦病毒 ・巨集病毒 ・蓄意造成系統不正常結束 ・繞過登入程序 ・臨時的存取帳號 ・網路分析工具 ・駭客攻擊Novell Netware ・Novell Netware 3.x 網路之管理權限遭濫用
Novell Netware 4.x	不可抗力之威脅	・IT系統故障
	組織缺陷之威脅	・伺服器工作環境不安全 ・網路伺服器安全機制不當或缺乏 ・NDS的複雜性

模組	威脅類型	威脅項目
Novell Netware 4.x	組織缺陷之威脅	・Novell Netware 版本從3.x升級到4 ・千禧年日期轉換
	人爲錯誤之威脅	・IT系統的使用不當 ・物件不愼遭刪除 ・檔案系統不愼設爲共享 ・時間不同步 ・錯誤的組態設定和操作
	技術故障之威脅	・電源供應中斷
	故意行爲之威脅	・電腦病毒 ・巨集病毒 ・繞過登入程序 ・臨時的存取帳號 ・網路分析工具 ・駭客攻擊Novell Netware ・Novell Netware 3.x 網路之管理權限遭濫用
異質網路	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・閃電 ・火 ・水 ・工作溫度和濕度不當 ・灰塵與髒污
	組織缺陷之威脅	・未經授權使用 ・IT使用者異動未適當調整 ・稽核資料缺乏評估 ・文件不當或缺乏 ・頻寬規劃不當 ・網路組件不相容 ・網路概念缺乏 ・纜線長度超過允許的最大值
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・人爲疏忽造成線路損毀 ・清潔或外來人員導致的危

模組	威脅類型	威脅項目
異質網路	人爲錯誤之威脅	害 ・IT系統的使用不當 ・IT系統管理不當 ・動態網路組件組態設定不當 ・網路分割不當
	技術故障之威脅	・電源供應中斷 ・電壓不穩定 ・軟體脆弱性被揭露 ・網路組件失效
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・破壞 ・攻擊 ・線路的分接 ・線路的運用不當 ・未授權使用IT系統 ・有系統的猜測通行碼 ・阻絕服務攻擊 ・未經授權連接IT系統 ・未經授權執行網路管理功能 ・未經授權存取動態網路組件
網路和系統管理	不可抗力之威脅	・人員傷亡 ・IT系統故障
	組織缺陷之威脅	・未註冊組件的操作 ・網路和管理系統的策略執行不當或缺乏 ・未經授權蒐集個人資料
	人爲錯誤之威脅	・管理系統組態設定不當 ・伺服器當機 ・事件誤判
	技術故障之威脅	・網路或系統管理組件失效
	故意行爲之威脅	・竄改管理參數
Windows 2000 伺服器	不可抗力之威脅	・人員傷亡 ・IT系統故障

模組	威脅類型	威脅項目
Windows 2000 伺服器	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用 ・儲存媒體交付不當 ・Active Directory規劃不當或缺乏
	人爲錯誤之威脅	・IT系統管理不當 ・Windows 2000組態設定錯誤 ・Active Directory組態設定錯誤
	技術故障之威脅	・網路IT系統存取機制過於複雜 ・自動開啓光碟 ・不安全的加密演算法
	故意行爲之威脅	・線路的分接 ・電腦病毒 ・在Windows NT系統之管理權限遭濫用 ・資料喪失機密性 ・洩漏加密金鑰 ・僞造憑證 ・資訊喪失完整性
S/390 and zSeries 大型主機	組織缺陷之威脅	・IT安全措施缺乏監控 ・文件不當或缺乏 ・因資料殘留而喪失機密性 ・zSeries系統環境之組態設定不當或錯誤
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・IT系統管理不當 ・錯誤的組態設定和操作 ・z/OS使用之字元轉換錯誤 ・z/OS之組態設定不當或錯誤 ・z/OS Web伺服器之組態設定不當或錯誤

模組	威脅類型	威脅項目
S/390 and zSeries 大型主機	人爲錯誤之威脅	・z/OS中Unix服務之組態設定不當或錯誤 ・z/OS檔案存取之管理不當 ・z/OS之系統時間錯誤 ・z/OS之資源存取功能之組態設定錯誤 ・z/OS系統功能使用錯誤 ・z/OS中系統設定之保護不當導致可動態變更參數 ・z/OS中整批工件之控制不當
	技術故障之威脅	・網路IT系統存取機制過於複雜 ・軟體的脆弱性或錯誤 ・z/OS作業系統超載

模組	威脅類型	威脅項目
S/390 and zSeries 大型主機	故意行爲之威脅	・資料或軟體不當運用 ・透過連接埠進行遠端維護 ・有系統的猜測通行碼 ・使用者權限的濫用 ・特洛伊木馬病毒 ・阻絕服務攻擊 ・網路分析工具 ・z/OS系統組態設定被竄改 ・z/OS日誌檔被竄改 ・使用者提升z/OS資料存取權限 ・z/OS中使用他人帳號 ・Linux/zSeries系統組態設定被竄改 ・利用TCP/IP協定攻擊z/OS系統 ・z/OS中資源存取之屬性使用不當

資料傳輸系統模組之威脅列表

模組	威脅類型	威脅項目
資料媒體交換	不可抗力之威脅	・工作溫度和濕度不當 ・灰塵與髒污 ・強力磁場導致資料損失
	組織缺陷之威脅	・資源不當或缺乏相容性 ・資料可用性不足 ・儲存媒體標示不當 ・儲存媒體交付不當 ・金鑰管理不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・違反IT安全措施 ・傳送過程中資料的遺失 ・傳送不正確的或不預期的資料紀錄
	技術故障之威脅	・儲存媒體受損
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・盜竊 ・未授權使用IT系統 ・電腦病毒

模組	威脅類型	威脅項目
資料媒體交換	故意行爲之威脅	・未經授權拷貝資料 ・巨集病毒
數據機	不可抗力之威脅	・IT系統故障
	人爲錯誤之威脅	・人爲疏忽導致設備或資料損壞 ・違反IT安全措施 ・人爲疏忽造成線路損毀
	技術故障之威脅	・電壓不穩定
	故意行爲之威脅	・資料或軟體不當運用 ・線路的分接 ・線路的運用不當 ・未授權使用IT系統 ・透過連接埠進行遠端維護 ・電話交談及資料傳送遭竊取 ・有系統的猜測通行碼 ・電腦病毒 ・僞裝 ・利用通行卡侵入電腦系統 ・巨集病毒

模組	威脅類型	威脅項目
防火牆	組織缺陷之威脅	・網路之敏感資料喪失機密性 ・安全閘道之營運持續不當
	人爲錯誤之威脅	・違反IT安全措施 ・IT系統管理不當 ・錯誤的組態設定和操作
	技術故障之威脅	・軟體脆弱性被揭露 ・網路IT系統存取機制過於複雜 ・NIS伺服器和NIS用戶端缺乏鑑別 ・X伺服器和X用戶端缺乏鑑別 ・儲存空間不足導致資料遺失 ・軟體的脆弱性或錯誤 ・軟體概念錯誤
	故意行爲之威脅	・資料或軟體不當運用 ・未授權使用IT系統 ・有系統的猜測通行碼 ・訊息重送攻擊 ・僞裝 ・阻絕服務攻擊 ・利用通行卡侵入電腦系統 ・IP冒用 ・來源路由濫用 ・ICMP協定濫用 ・路由協定濫用 ・DNS冒用
電子郵件	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權使用 ・IT使用者異動未適當調整 ・金鑰管理不當 ・因資料殘留而喪失機密性 ・E-Mail的使用不受管制 ・檔案描述不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・違反IT安全措施 ・IT系統的使用不當

模組	威脅類型	威脅項目
電子郵件	人爲錯誤之威脅	・傳送不正確的或不預期的資料紀錄
	技術故障之威脅	・儲存資料遺失 ・儲存空間不足導致資料遺失 ・訊息發送失效 ・E-Mail缺乏對可信賴性及機密性之鑑別
	故意行爲之威脅	・資料或軟體不當運用 ・線路的分接 ・未授權使用IT系統 ・特洛伊木馬病毒 ・電腦病毒 ・訊息重送攻擊 ・僞裝 ・訊息內容分析 ・否認接收到訊息 ・阻絕服務攻擊 ・巨集病毒 ・資料喪失機密性 ・E-Mail服務的濫用 ・假扮發送者 ・竄改電子郵件傳送清單 ・E-Mail超載 ・郵件炸彈 ・未經授權監控E-Mail ・資訊喪失完整性 ・Web應用程式的錯誤 ・HTML格式的電子郵件使用不當
網際網路伺服器	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用 ・IT使用者異動未適當調整 ・侵犯版權 ・頻寬規劃不當 ・通信線路使用不受管制 ・網站過時或資訊錯誤

模組	威脅類型	威脅項目
網際網路伺服器	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・無效率的網路搜尋 ・錯誤的組態設定和操作
	技術故障之威脅	・網路IT系統存取機制過於複雜 ・軟體的脆弱性或錯誤 ・軟體概念錯誤
	故意行爲之威脅	・資料或軟體不當運用 ・使用者權限的濫用 ・系統管理員權限的濫用 ・特洛伊木馬病毒 ・電腦病毒 ・阻絕服務攻擊 ・巨集病毒 ・IP冒用 ・DNS冒用 ・Web冒用 ・動態網頁內容遭濫用
遠程接取	不可抗力之威脅	・人員傷亡 ・IT系統故障 ・廣域網路故障
	組織缺陷之威脅	・對規則與程序認知不足 ・筆記型電腦使用者變更欠缺管理規章 ・金鑰管理不當 ・通信線路使用不受管制 ・網路組件不相容 ・遠端工作人員訓練不當或缺乏 ・RAS系統規則不當或缺乏
	人爲錯誤之威脅	・未經授權私自使用遠端工作站 ・遠端存取服務系統管理不當 ・遠程接取鑑別使用不當 ・遠程接取服務使用不當 ・遠端存取服務使用者端的組態設定不當 ・通行碼管理不當 ・資訊管理不當

模組	威脅類型	威脅項目
遠程接取	技術故障之威脅	・不安全的加密演算法 ・遠端存取服務用戶端操作環境的配置不當
	故意行爲之威脅	・線路的分接 ・線路的運用不當 ・可攜式設備遭竊 ・利用通行卡侵入電腦系統 ・資料喪失機密性 ・洩漏加密金鑰 ・關閉遠端存取服務之安全機制 ・將遠端存取服務用戶端當作伺服器使用 ・開放使用遠端存取服務組件
Lotus Notes	不可抗力之威脅	・人員傷亡 ・IT系統故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用 ・筆記型電腦使用者變更欠缺管理規章 ・儲存媒體交付不當 ・金鑰管理不當 ・通信線路使用不受管制 ・資料庫存取的複雜性 ・遠端工作人員訓練不當或缺乏
	人爲錯誤之威脅	・IT系統管理不當 ・通行碼管理不當 ・資訊管理不當 ・Lotus Notes伺服器組態設定錯誤 ・瀏覽器存取Lotus Notes組態設定錯誤
	技術故障之威脅	・資料庫故障 ・資料庫的資料遺失 ・不安全的加密演算法

模組	威脅類型	威脅項目
Lotus Notes	故意行爲之威脅	・線路的分接 ・線路的運用不當 ・可攜式設備遭竊 ・資料喪失機密性 ・未經授權監控E-Mail ・洩漏加密金鑰 ・僞造憑證 ・資訊喪失完整性 ・Lotus Notes的動態內容遭濫用 ・Lotus Notes遭駭客攻擊
網際網路資訊伺服器	不可抗力之威脅	・人員傷亡 ・IT系統故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用 ・IT使用者異動未適當調整 ・侵犯版權 ・頻寬規劃不當 ・通信線路使用不受管制 ・IIS的規劃不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・IT系統管理不當 ・無效率的網路搜尋 ・錯誤的組態設定和操作 ・通行碼管理不當 ・IIS規劃不當 ・支援IIS之作業系統組態設定不當 ・IIS的組態設定不當 ・IIS安全漏洞與測試工具的專業不足
	技術故障之威脅	・軟體脆弱性被揭露 ・網路IT系統存取機制過於複雜 ・軟體的脆弱性或錯誤 ・軟體概念錯誤 ・不安全的加密演算法

模組	威脅類型	威脅項目
網際網路資訊伺服器	故意行爲之威脅	・資料或軟體不當運用 ・線路的分接 ・使用者權限的濫用 ・系統管理員權限的濫用 ・特洛伊木馬病毒 ・電腦病毒 ・阻絕服務攻擊 ・巨集病毒 ・IP冒用 ・資料喪失機密性 ・未經授權監控E-Mail ・DNS冒用 ・洩漏加密金鑰 ・僞造憑證 ・資訊喪失完整性 ・Web冒用 ・動態網頁內容遭濫用 ・試探IIS系統的脆弱性
Apache Web伺服器	組織缺陷之威脅	・Apache伺服器的事故處理規劃不當
	人爲錯誤之威脅	・支援Apache之作業系統組態設定不當 ・Apache伺服器組態設定不當
	技術故障之威脅	・軟體的脆弱性或錯誤
	故意行爲之威脅	・試探Apache系統的脆弱性
Exchange /Outlook 2000	不可抗力之威脅	・IT系統故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・未經授權使用 ・通信線路使用不受管制 ・E-Mail的使用不受管制 ・Exchange Server規劃不當 ・外部存取Exchange e-mail管制不當 ・電子郵件系統連結至Exchange/Outlook不當

模組	威脅類型	威脅項目
Exchange /Outlook 2000	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・IT系統管理不當 ・場域資料存取權限管理不當 ・錯誤的組態設定和操作 ・Exchange 2000伺服器組態設定不當 ・Outlook 2000用戶端組態設定不當
	技術故障之威脅	・軟體的脆弱性或錯誤 ・訊息發送失效
	故意行爲之威脅	・未授權使用IT系統 ・使用者權限的濫用 ・電腦病毒 ・未經授權監控E-Mail

模組	威脅類型	威脅項目
Exchange /Outlook 2000	故意行爲之威脅	・洩漏加密金鑰 ・僞造憑證 ・資訊喪失完整性
路由器及交換器	組織缺陷之威脅	・路由器及交換器之規劃設計不當
	人爲錯誤之威脅	・路由器及交換器之組態設定錯誤 ・路由器及交換器之管理錯誤
	技術故障之威脅	・路由器及交換器預設值不當
	故意行爲之威脅	・ARP表被竄改 ・MAC位址僞冒 ・展開樹使用錯誤 ・虛擬區域網路安全性不足

電信模組之威脅列表

模組	威脅類型	威脅項目
電信系統	不可抗力之威脅	・火 ・工作溫度和濕度不當
	組織缺陷之威脅	・未經授權進入保護區域
	人爲錯誤之威脅	・清潔或外來人員導致的危害 ・操作錯誤導致電話交換機失效
	技術故障之威脅	・電壓不穩定
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・電話交換機之儲存資料喪失機密性 ・電話交談及資料傳送遭竊取 ・房間遭竊聽 ・取得電話帳單資料 ・員工的好奇心

模組	威脅類型	威脅項目
電信系統	故意行爲之威脅	・內部員工導致的威脅 ・外部人員導致的威脅 ・電話交換機之遠端連接埠遭濫用
傳真機	組織缺陷之威脅	・消耗品供應不當或不正確
	人爲錯誤之威脅	・誤判傳眞文件的法律效力
	技術故障之威脅	・感熱式傳眞紙褪色 ・傳眞傳送錯誤
	故意行爲之威脅	・線路的分接 ・未經授權使用傳眞機或傳眞伺服器 ・未經授權讀取傳眞資料 ・傳眞機及傳眞伺服器殘留資訊遭竊取之風險 ・僞冒傳眞 ・更改傳眞機上之傳送號碼 ・傳眞超載

模組	威脅類型	威脅項目
答錄機	不可抗力之威脅	・灰塵與髒污
	組織缺陷之威脅	・管理規定缺乏或不足 ・缺乏維護或維護不當 ・未經授權進入保護區域
	人爲錯誤之威脅	・答錄機使用不當
	技術故障之威脅	・電源供應中斷 ・答錄機內部電源失效 ・儲存空間不足導致資訊遺失
	故意行爲之威脅	・答錄機超載 ・判讀存取碼 ・遠端詢問的誤用
經由ISDN的LAN連接	不可抗力之威脅	・IT系統故障 ・廣域網路故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・未經授權進入保護區域 ・未經授權使用 ・IT使用者異動未適當調整 ・金鑰管理不當 ・稽核資料缺乏評估 ・網路之敏感資料喪失機密性 ・頻寬規劃不當 ・通信線路使用不受管制
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・清潔或外來人員導致的危害 ・IT系統的使用不當 ・IT系統管理不當 ・傳送不正確的或不預期的資料紀錄 ・場域資料存取權限管理不當
	技術故障之威脅	・軟體脆弱性被揭露 ・非營運期間網路仍持續連線

模組	威脅類型	威脅項目
經由ISDN的LAN連接	故意行爲之威脅	・資料或軟體不當運用 ・線路的分接 ・線路的運用不當 ・未授權使用IT系統 ・透過連接埠進行遠端維護 ・取得電話帳單資料 ・內部員工導致的威脅 ・外部人員導致的威脅 ・有系統的猜測通行碼 ・僞裝 ・訊息內容分析 ・利用通行卡侵入電腦系統 ・IP冒用 ・路由器之管理功能遭濫用 ・經由遠端IT系統濫用資源 ・竄改ISDN資料
傳真伺服器(Fax Servers)	組織缺陷之威脅	・未經授權使用 ・IT使用者異動未適當調整 ・稽核資料缺乏評估 ・傳眞使用不受管制
	人爲錯誤之威脅	・違反IT安全措施 ・誤判傳眞文件的法律效力
	技術故障之威脅	・傳眞傳送錯誤 ・儲存空間不足導致資料遺失
	故意行爲之威脅	・資料或軟體不當運用 ・線路的分接 ・未授權使用IT系統 ・訊息重送攻擊 ・僞裝 ・否認接收到訊息 ・未經授權使用傳眞機或傳眞伺服器 ・未經授權讀取傳眞資料 ・傳眞機及傳眞伺服器殘留資訊遭竊取之風險 ・僞冒傳眞 ・傳眞超載 ・利用通行卡侵入電腦系統 ・竄改網路位址清單

模組	威脅類型	威脅項目
行動電話	組織缺陷之威脅	・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用
	人爲錯誤之威脅	・違反IT安全措施 ・通行碼管理不當 ・資訊管理不當 ・通信雙方識別不當
	技術故障之威脅	・移動式通信網路失效 ・行動電話或PDA失效
	故意行爲之威脅	・資料或軟體不當運用 ・盜竊 ・惡作劇 ・SIM卡遭冒用 ・透過行動電話竊聽 ・竄改行動電話韌體 ・未經授權利用行動電話傳送資料 ・截聽行動電話 ・行動電話使用紀錄的分析
PDAs	不可抗力之威脅	・應用環境的改變導致安全等級降低
	組織缺陷之威脅	・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用

模組	威脅類型	威脅項目
PDAs	人爲錯誤之威脅	・違反IT安全措施 ・通行碼管理不當 ・資訊管理不當 ・通信雙方識別不當 ・z/OS中行動設備同步時發生錯誤
	技術故障之威脅	・行動電話或PDA失效 ・PDA安全機制不當 ・可攜式設備的資料遺失
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・未授權使用IT系統 ・可攜式設備遭竊 ・電腦病毒 ・透過可攜式設備竊聽 ・可攜式設備之資料使用不當 ・未經授權透過可攜式設備傳送資料 ・未經授權透過可攜式設備拍照或錄影

其他IT元件模組之威脅列表

模組	威脅類型	威脅項目
標準軟體	組織缺陷之威脅	・管理規定缺乏或不足 ・資源不當或缺乏相容性 ・測試程序不當或缺乏 ・文件不當或缺乏 ・侵犯版權 ・軟體測試使用實際資料
	人爲錯誤之威脅	・違反IT安全措施 ・錯誤的組態設定和操作
	技術故障之威脅	・軟體脆弱性被揭露 ・軟體的脆弱性或錯誤
	故意行爲之威脅	・特洛伊木馬病毒 ・電腦病毒 ・巨集病毒

模組	威脅類型	威脅項目
資料庫	不可抗力之威脅	・人員傷亡
	組織缺陷之威脅	・資源不當或缺乏相容性 ・稽核資料缺乏評估 ・測試程序不當或缺乏 ・資料庫安全機制不當或缺乏 ・DBMS的複雜性 ・資料庫存取的複雜性 ・資料庫使用者交接缺乏管理 ・緊急情況下媒體的儲存不當

模組	威脅類型	威脅項目
資料庫	人爲錯誤之威脅	・清潔或外來人員導致的危害 ・場域資料存取權限管理不當 ・DBMS管理不當 ・資料操作不愼遭修改
	技術故障之威脅	・資料庫故障 ・透過ODBC規避存取控制 ・資料庫的資料遺失 ・儲存空間不足導致資料庫的資料遺失 ・資料庫完整性/一致性的喪失
	故意行爲之威脅	・未授權使用IT系統 ・透過連接埠進行遠端維護 ・有系統的猜測通行碼 ・竄改資料庫 ・資料庫系統的阻絕服務
通訊	不可抗力之威脅	・人員傷亡
	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・缺乏維護或維護不當 ・未經授權使用 ・資源使用不受管制 ・稽核資料缺乏評估 ・網路之敏感資料喪失機密性 ・遠端工作人員訓練不當或缺乏 ・遠端工作人員作業限制導致的延遲 ・缺乏將遠端工作人員整合於資訊流中 ・IT系統故障反應時間過長 ・遠端工作人員的職務代理規定不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・違反IT安全措施 ・IT系統管理不當 ・傳送不正確的或不預期的資料紀錄

模組	威脅類型	威脅項目
通訊	人爲錯誤之威脅	・場域資料存取權限管理不當 ・未經授權私自使用遠端工作站
	技術故障之威脅	・儲存資料遺失
	故意行爲之威脅	・IT設備或配件不當運用或破壞 ・資料或軟體不當運用 ・線路的分接 ・線路的運用不當 ・未授權使用IT系統 ・透過連接埠進行遠端維護 ・有系統的猜測通行碼 ・使用者權限的濫用 ・系統管理員權限的濫用 ・特洛伊木馬病毒 ・電腦病毒 ・訊息重送攻擊 ・巨集病毒 ・僞裝 ・資料喪失機密性
Novell eDi–rectory	不可抗力之威脅	・人員傷亡 ・IT系統故障
	組織缺陷之威脅	・管理規定缺乏或不足 ・對規則與程序認知不足 ・IT安全措施缺乏監控 ・未經授權使用 ・金鑰管理不當 ・資料庫安全機制不當或缺乏 ・資料庫存取的複雜性 ・Novell eDirectory規劃不當或缺乏 ・Novell eDirectory分割和複製規劃不當或缺乏 ・LDAP存取Novell eDirectory規劃不當或缺乏
	人爲錯誤之威脅	・IT系統管理不當 ・傳送不正確的或不預期的資料紀錄 ・場域資料存取權限管理不當 ・加密模組使用不當 ・管理系統組態設定不當

模組	威脅類型	威脅項目
Novell eDirectory	人爲錯誤之威脅	・伺服器當機 ・事件誤判 ・錯誤的組態設定和操作 ・通行碼管理不當 ・Novell eDirectory組態設定錯誤 ・Novell eDirectory 存取權限設定錯誤 ・使用者存取Novell eDirectory組態設定錯誤 ・LDAP存取Novell eDirectory組態設定錯誤
	技術故障之威脅	・軟體脆弱性被揭露 ・網路IT系統存取機制過於複雜 ・儲存資料遺失 ・無效的鑑別 ・加密模組失效 ・不安全的加密演算法 ・軟體概念錯誤 ・Novell eDirectory失效
	故意行爲之威脅	・內部員工導致的威脅 ・外部人員導致的威脅 ・有系統的猜測通行碼 ・使用者權限的濫用 ・系統管理員權限的濫用 ・竄改資料庫 ・資料庫系統的阻絕服務 ・DNS冒用 ・未經授權使用加密模組 ・竄改加密模組參數 ・洩漏加密金鑰
歸檔	不可抗力之威脅	・IT系統故障 ・工作溫度和濕度不當 ・強力磁場導致資料損失 ・強光導致資料損失
	組織缺陷之威脅	・未經授權使用 ・檔案系統的升級不當 ・檔案系統的稽核軌跡不當

模組	威脅類型	威脅項目
歸檔	組織缺陷之威脅	・存檔的索引鍵不當 ・存檔儲存媒體的容量不當 ・存檔存取的文件不當 ・紙本資料轉成電子檔案無效 ・存檔期間重新建立的資料無效 ・存檔期間重新簽章無效 ・存檔程序的稽核無效 ・儲存媒體銷毀無效 ・檔案系統位置規劃不當
	人爲錯誤之威脅	・操作錯誤導致資料的機密性/完整性喪失 ・場域資料存取權限管理不當 ・伺服器當機 ・使用不當的儲存媒體 ・使用不符法令或規定的檔案系統
	技術故障之威脅	・儲存媒體受損 ・儲存資料遺失 ・儲存空間不足導致資料遺失 ・資料庫故障 ・資料庫完整性/一致性的喪失 ・網路組件失效 ・存檔資訊存取延遲 ・索引資料缺乏同步機制 ・加密方法過時
	故意行爲之威脅	・資料或軟體不當運用 ・攻擊 ・未經授權拷貝資料 ・竄改加密模組參數 ・洩漏加密金鑰 ・資訊喪失完整性 ・破壞行爲 ・檔案系統遭破壞 ・未經授權覆寫或刪除檔案

中華軟協資安促進會簡介

爲了保護消費者的隱私權、政府與企業的營運安全，重建全民與企業對電子商務機制的信賴，提升台灣的資訊安全水準，因此在業界先進鼓勵之下，於九十三年五月五日成立「中華民國資訊軟體協會資訊安全促進委員會」簡稱「中華軟協資安促進會」，集結業界的力量與有志推動資訊安全之各界菁英，以整合的力量，統一的訴求，籲請政府制定更積極的政策，投入更多的資源推動各項資訊安全機制，讓企業以實際的行動保護自己的數位化資產，保持營運的正常與穩定。

中華軟協資安促進會成立的主要目標爲：

一、推動各界重視組織內部之資訊資產價值，呼籲政府與企業投入資源，保障資訊資產之安全。
二、推動政府制訂有效資訊安全政策，並健全資訊安全相關法規。
三、結合民間產業力量，發展資訊安全相關產品與服務，達到先進國家之水準。
四、結合產、官、學與研究機構研商建立全國性之資訊安全防護機制。
五、建立與各國資訊安全推動組織之聯繫管道，促進台灣與國際資訊安全社群之合作關係。

中華軟協資安促進會會員名錄

中華數位科技股份有限公司

中華龍網股份有限公司

台衆電腦股份有限公司

台灣國際商業機器股份有限公司

台灣微軟股份有限公司

台灣網路認證股份有限公司

宏碁股份有限公司

宏瞻資訊股份有限公司

定興實業有限公司

岱昇科技股份有限公司

東捷資訊服務股份有限公司

威播科技股份有限公司

英國標準協會（BSI）

香港商漢德技術監督服務亞太有限公司台灣分公司

桓基科技股份有限公司

紐奧良文化事業股份有限公司

財金資訊股份有限公司

財團法人資訊工業策進會

國興資訊股份有限公司

康大資訊股份有限公司

組合國際電腦股份有限公司

翊利得資訊科技有限公司

惠普科技股份有限公司

精誠資訊股份有限公司

網擎資訊軟體股份有限公司

臺華科技股份有限公司

寬華網路科技股份有限公司

數位聯合電信股份有限公司

諮安科技股份有限公司

趨勢科技股份有限公司

關貿網路股份有限公司

（依筆劃順序排列）

MEMO