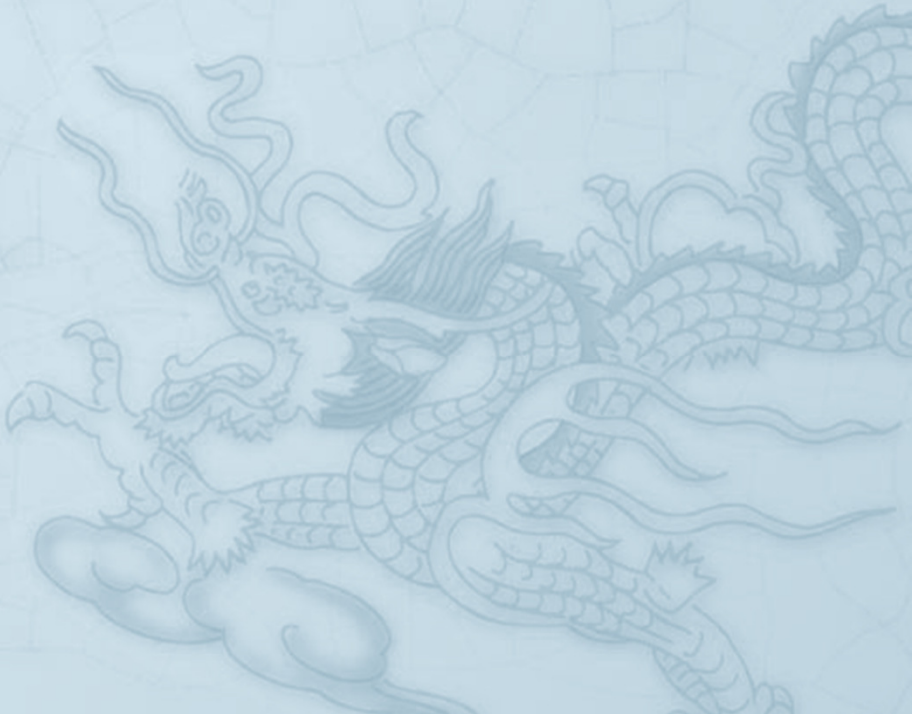
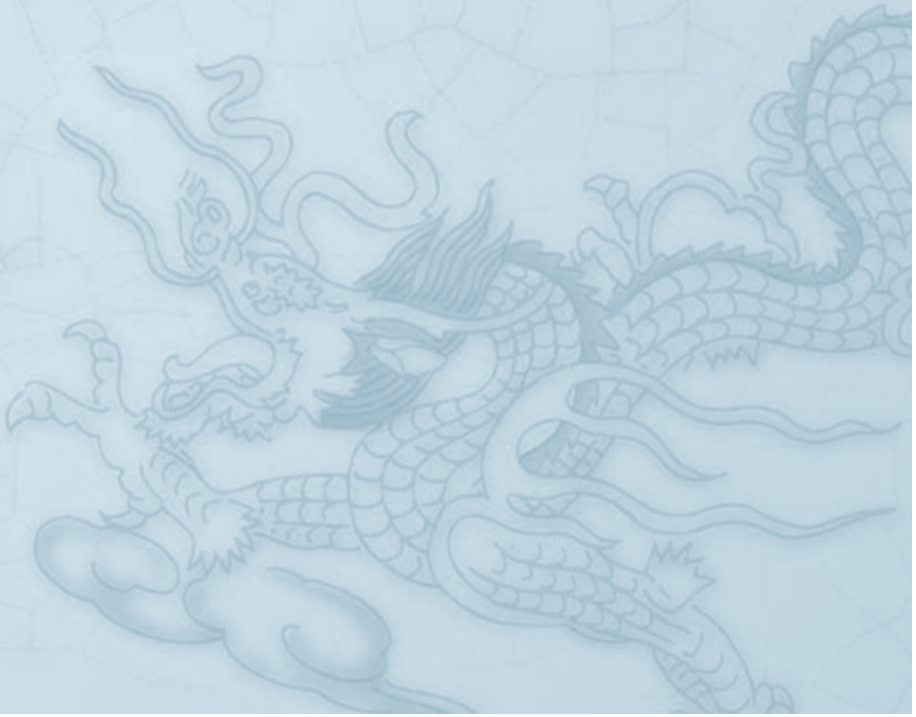
ISMS 資訊安全管理系統

Information Security Management System



資訊安全管理



何謂資訊

- 資訊是一種資產，就像其他的重要企業資產一樣，對組織具有價值，因此需要受到適當的保護。
- 資訊可以許多的形式存在，可以書寫或列印於紙上，儲存在電子儲存媒體上，以郵寄或電子儲存傳輸，顯示於影片上或在對話中說出。
- 不管資訊的形式是什麼，或者共用或儲存的方式是什麼，都應該受到適當的保護。

何謂資訊安全

- 保障組織資訊資產免於「不可承受的風險」
- 資訊安全特性
  - CIA
    - C： **機密性**(Confidentiality)：資訊不得被未經授權之個人、實體或程序所取得或揭露的性質。
    - I：**完整性**(Integrity)：對資訊之精確與完整安全保證的性質。
    - A：**可用性**(Availability)：已授權實體在需要時可存取與使用資訊之性質。
  - 3A
    - Authentication **認證**：確認身份
    - Authorization **授權**：授予應得之權限
    - Accounting **稽查**：記錄其行為
  - 其他性質
    - **可鑑別性**(Authenticity)：可證明一主體或資源之識別就是其所聲明者的特性。鑑別性適用於如使用者、程序、系統與資訊等實體。
    - **可歸責性**(Accountability)：確保實體之行為可唯一追溯到該實體的性質。
    - **不可否認性**(Non-repudiation)：對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。
    - **可靠性**(Reliability)：始終如一預期之行為與結果的性質。

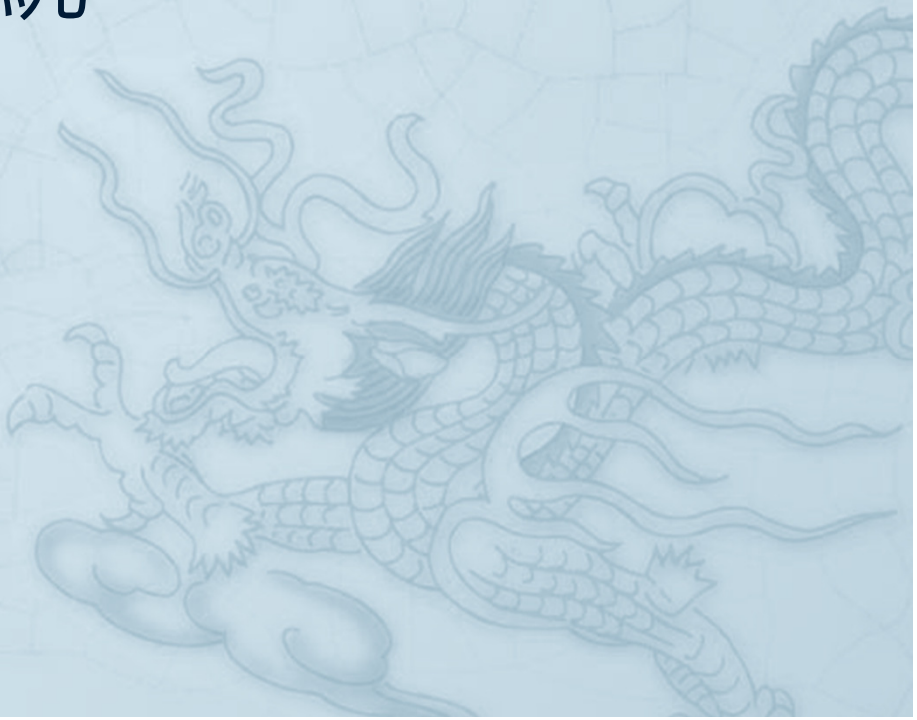
應保護的資訊資產類別–範例

- 資訊紀錄
  - 資料庫、資料檔、系統規劃與設計文件、使用與操作手冊、業務流程、合約、教育訓練教材、制度文件、內部控制管理辦法、其他相關典章制度等
- 電腦系統
  - 電腦作業系統、應用系統、開發工具、套裝軟體、公用程式等
- 人員
  - 組織內部人員：應用系統開發與維護人員、系統管理人員、資訊與設備擁有者及保管人員、資訊 / 文件製作人員以及一般使用者，包括正式人員與非正式人員。
  - 外部人員：承包商與業務合作夥伴。
- 基礎設施服務
  - 電力服務、空調服務、網路服務、電信服務
- 實體區域
  - 員工辦公區、主機控制室、管制區與門禁機房
- 實體設備
  - 主機、通訊設備、儲存媒體、水電設備

資訊安全的迷思

- 資訊安全是資訊人員的事?
- 資訊安全是資訊技術的事?
- 資訊安全只要做好保密工作?
- 使用或部署防護設備或軟體就高枕無憂?
- 我的單位已經百分之百的安全?
- 單位資訊沒價值,不用保護?

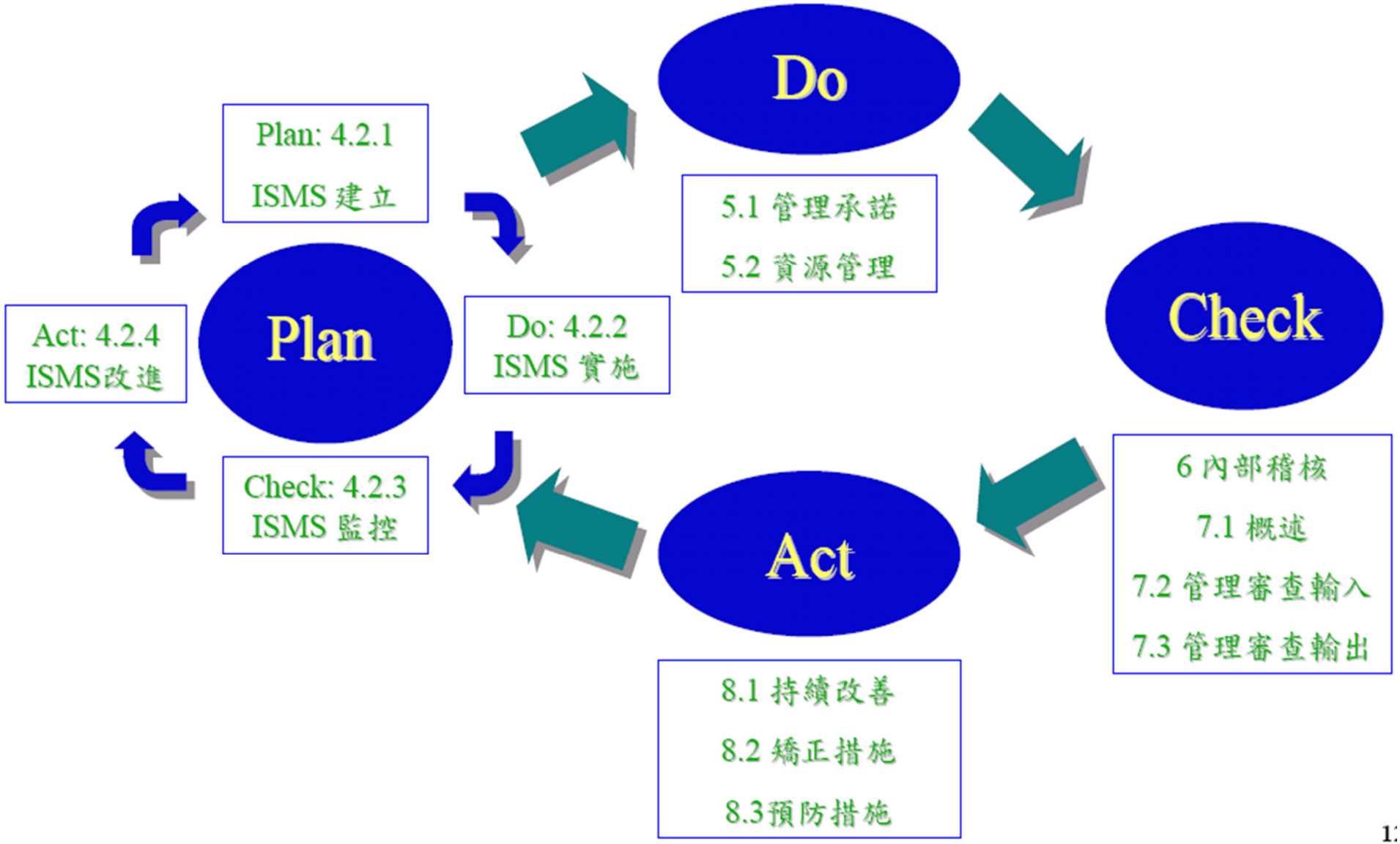
資訊安全管理系統



資訊安全管理系統

- ISMS(Information Security Management System)是一套有系統地分析和管理資訊安全風險的方法。
- 要達到100% 的資訊安全是一種過高的期望，資訊安全管理的目標是透過控制方法，把資訊風險降低到可接受的程度內。

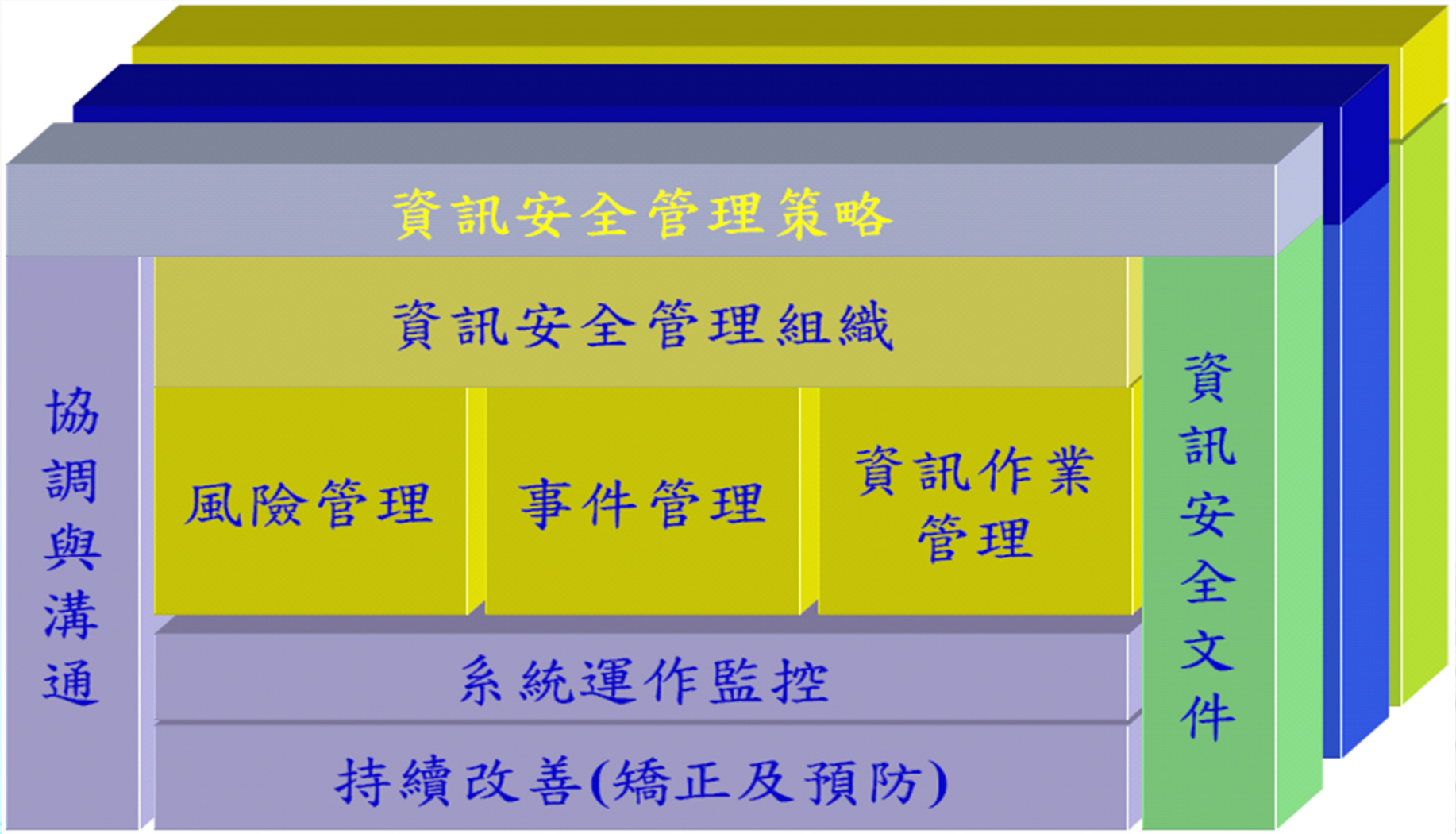
PDCA與ISMS


Plan: 4.2.1
ISMS 建立
Do
5.1 管理承諾
5.2 資源管理
Check
6 內部稽核
7.1 概述
7.2 管理審查輸入
7.3 管理審查輸出
Act
8.1 持續改善
8.2 矯正措施
8.3預防措施
Plan
Act: 4.2.4
ISMS改進
Do: 4.2.2
ISMS 實施
Check: 4.2.3
ISMS 監控

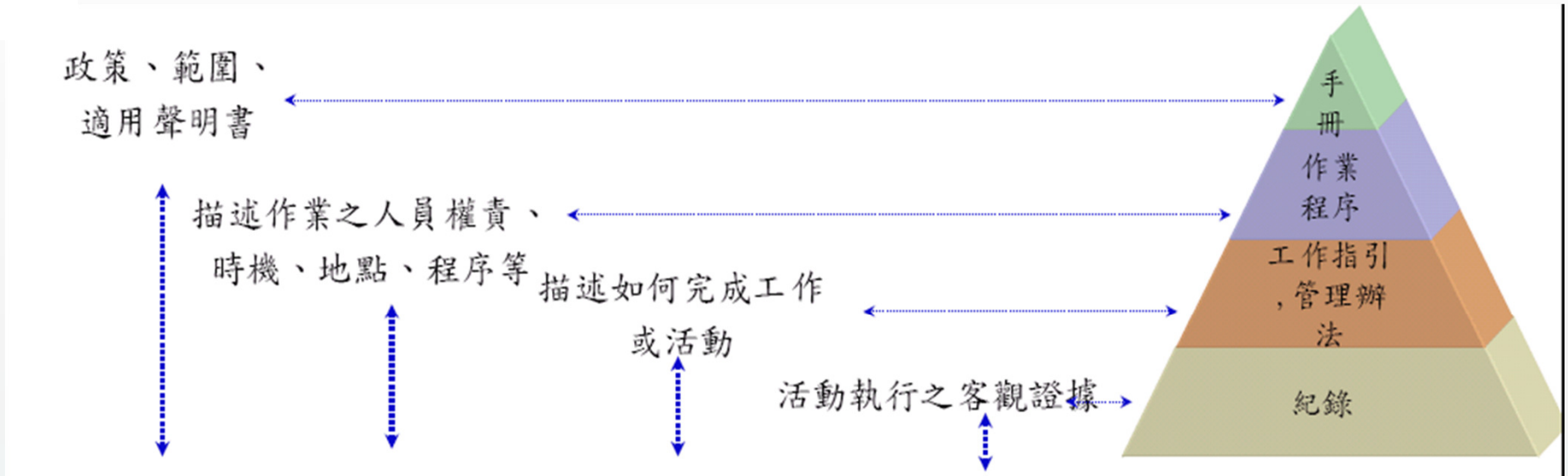
資安管理制度的成功要素

- 全面管理階層的承諾與支援
- 提供資訊安全管理活動適切經費
- 資訊安全政策/目標/活動與業務結合
- 資訊安全管理方法與架構需與企業文化契合
- 對風險審查、管理與資訊安全需求的充分了解
- 有效推廣資訊安全觀念(內部人員、主管與合作夥伴)
- 資訊安全相關文件容易取閱(內部人員、主管與合作夥伴)
- 提供適切的教育訓練
- 建置適切資訊安全事件管理機制
- 具有完整的衡量與回饋機制

資訊安全管理制度架構

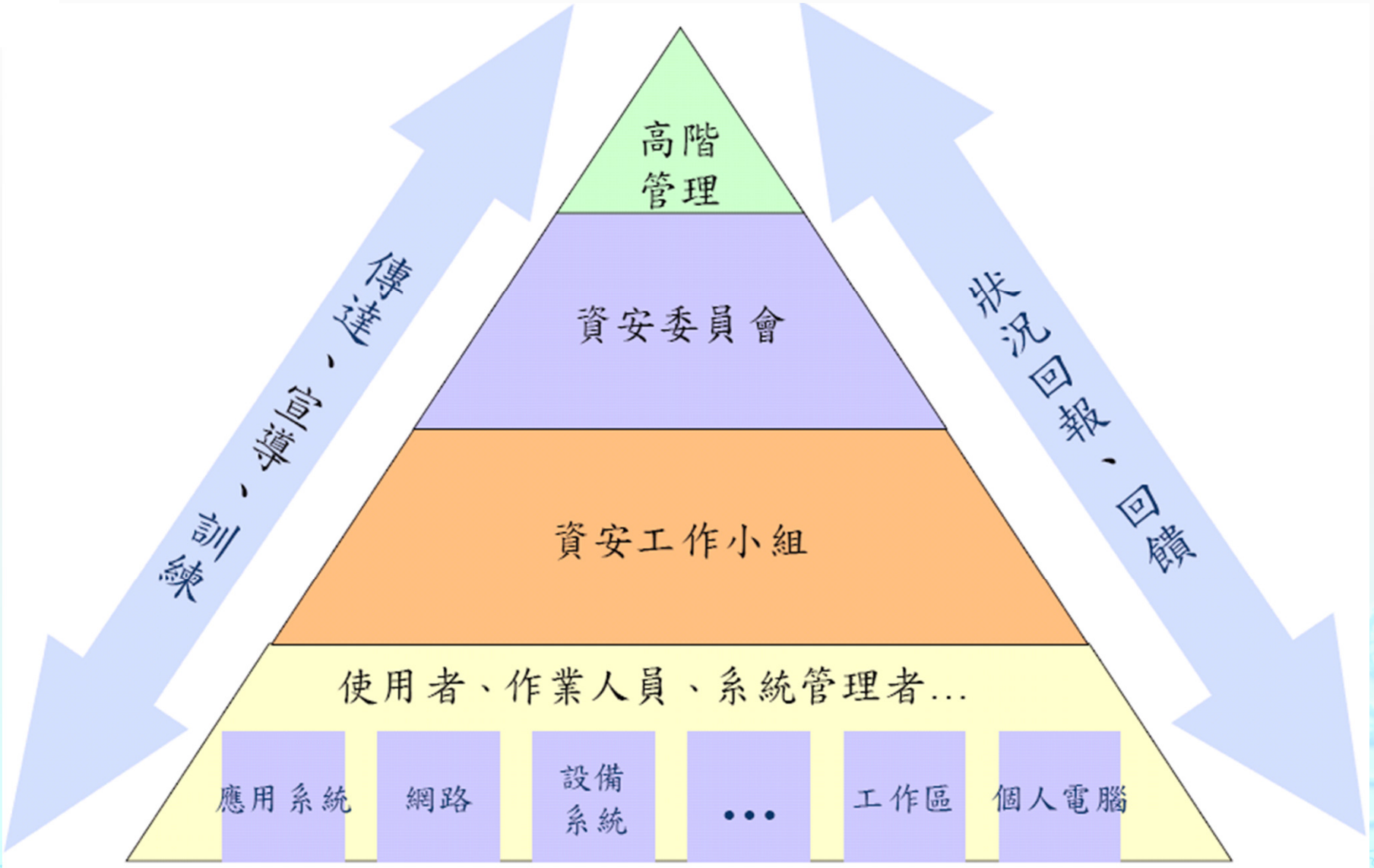

資訊安全管理策略
資訊安全管理組織
協調與溝通
風險管理
事件管理
資訊作業管理
資訊安全文件
系統運作監控
持續改善(矯正及預防)

資安管理系統與文件體系



階層	第一階	第二階	第三階	第四階
文件類別	手冊	程序	管理辦法	紀錄
名稱	資訊安全政策	風險管理	資訊資產風險評鑑辦法	訓練計劃與評核
	資訊安全政策細則	文件與紀錄管理	內部稽核辦法	風險評鑑報告
	適用聲明書	資安事件管理	資訊處理辦法	保密協議書
	資訊安全手冊	系統監控程序	資安事件管理辦法	資安事件紀錄
		管理審查	使用者註冊管理	固定資產移動單
		預防與改善程序	電腦資源管理辦法	-軟體借用 登錄表
		營運持續管理	網站管理辦法	…
			系統開發管理辦法	
			營運持續管理	

資安階層關係


高階管理
資安委員會
資安工作小組
使用者、作業人員、系統管理者...
應用系統
網路
設備系統
...
工作區
個人電腦
傳達、宣導、訓練
狀況回報、回饋

ISMS之建置與規劃

確認目標與範圍

- 確認ISMS的目標 – 範例
  - 改善本組織整體資訊安全管理制度能力，並建立與落實資訊安全管理相關作業及程序。
  - 提昇本組織資訊安全管理與技術專業能力，進而有效管理本組織業務風險。
  - 協助本組織XX業務通過最新版ISO27001:2005標準之驗證。
- 確認ISMS導入範圍 – 範例
  - 本組織之整體業務及服務
- 確認資安認證範圍 – 範例
  - 本組織之資訊系統業務，包含網際網路服務、資料儲存系統等等。
    - 實體位置：機房
    - 硬體設備：包含高效能磁碟儲存設備、高效能計算主機、磁帶儲存設備、遠程光纖網路交換器、數位內容儲存設備等系統。
    - 服務項目：各資訊系統、異地資料備援、備份、保存、災害救援、資料庫鏡射解決方案等相關應用服務。

導入資訊安全管理

- 依據ISO27001:2005進行資訊安全管理PDCA
- 實施基本控管措施
  - 法令需求
    - 智慧財產權
    - 資料及個人隱私權保護
    - 組織紀錄保全
  - 共通之安全管控
    - 建立資訊安全政策
    - 分配資訊安全責任
    - 通報安全事件
    - 業務持續運作管理
- 依據企業安全需求實施控管措施
  - 透過風險評鑑訂定安全需求
  - 選擇ISO27001附錄適用項目

通過驗證必須進行之活動

- 必須於驗證範圍內進行下列活動:
  - 建立資訊安全政策及管理目標作為指導方針
  - 成立資訊安全管理組織進行各項管理工作
  - 建立並實施風險管理機制
  - 風險評鑑
  - 風險處理
  - 實施資訊安全教育訓練
  - 建立資訊安全文件與紀錄管理機制
  - 建立資訊安全管理文件並實施資訊安全管控機制
  - 建立並實施各項資訊安全監控作業
  - 建立並實施資訊安全事件管理機制
  - 建立並實施業務持續運作管理機制
  - 建立並實施持續改善(預防及矯正)機制
  - 建立並實施資訊安全內部稽核機制檢核有效性
  - 建立並實施管理審查評量各項資安管理作業
  - 進行外部評審(預評及兩階段之正式評審)

資訊安全管理制度之建置規劃

階段	內容	產出
安全需求分析	•專案執行計畫書 •專案啟始會議簡報資料 •資安需求 •現況分析	•工作計畫書與簡報資料 •現況改善建議書
資安/流程教育	•ISMS建置課程教材 •ISO27001介紹 •資訊安全管理系統介紹及建置	•ISO27001訓練教材
安全政策與架構	•資訊安全政策一、二階文件 •資安組織建議報告	•資訊安全政策範本 •資訊安全政策教材
風險評鑑	•風險評鑑工具 •風險評鑑報告 •風險處理計畫書	•風險管理工具 •風險評估報告 •風險管理教材
風險處理	•資訊安全政策三、四階文件 •適用聲明書 •資安管理四階文件 •資安文件管理工具	•ISMS一~四階文件
施行與檢核	•內部稽核矯正建議 •外部稽核矯正建議 •ISO27001預評與正式評鑑報告 •版本提昇之輔導作業	•矯正或預防措施報告 •內部稽核教材

安全需求與現況分析目的

- 分析資訊安全管理實施現況與ISO27001:2005標準規範的差距，並初步評估立即改善作業。
- 了解現行作業，規劃資訊安全管理架構之重要依據
- 建議應執行之立即改善作業
- 調整專案工作項目及計畫

現況分析進行方式

- 收集安全管理資訊
  - 安全要求的期望
  - 安全組織運作
  - 安全管理措施（管理面）
  - 系統安全措施（系統面）系統架構及運作說明
- 現有文件及管理辦法檢視
- 現場觀察
- 訪談
- 工具
  - 業務流程分析表
  - 差異分析表

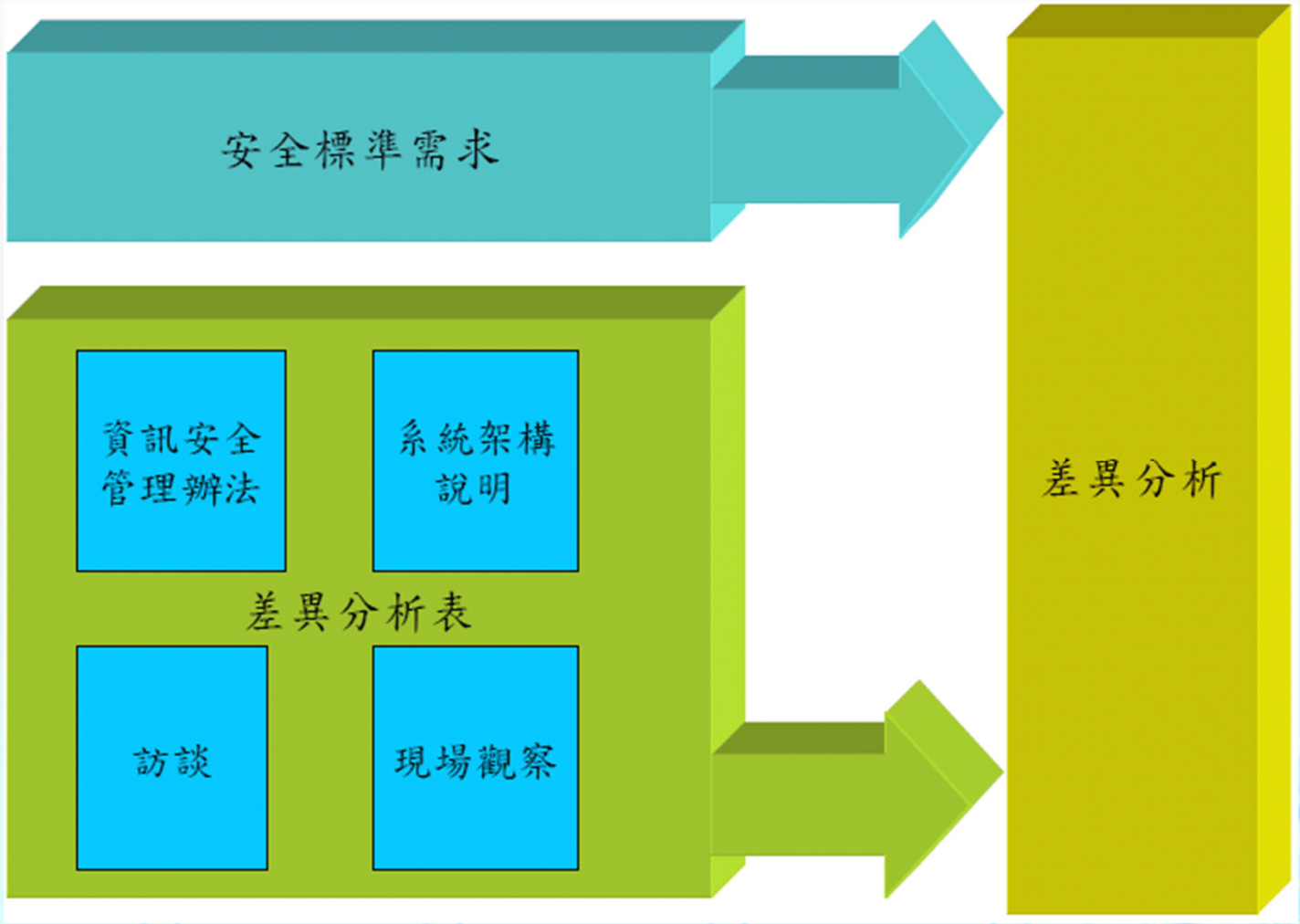
業務流程分析表

應用系統暨設備對照總表

業務/計畫/系統名稱	1	2	3	4
	WWW	電子郵件系統	公文系統	
負責組別	系統組	網路技術組	行政管理組	
MTD : 最大允許中斷時間	4hr	1hr	1hr	
RTO : 復原時間目標	8hr	8hr	8hr	
ROP : 資料回復時點目標	4hr	1hr	4hr	
程式語言/軟體	PHP	sendmail	ASP	
資料庫 →	MySQL		Oracle	

編號	主機/設備名稱	製造商+機型	作業系統	用途說明				
	WWW	HP DL380G3	Windos 2003	Web		v		
	WEBDB	HP DL380G4	Linux	資料庫伺服器		v		
	MAILSVR	HP DL380G5	RedHat 8.0	郵件伺服器			v	
	XXXServer	HP DL380G5	Windos 2003	公文系統				v

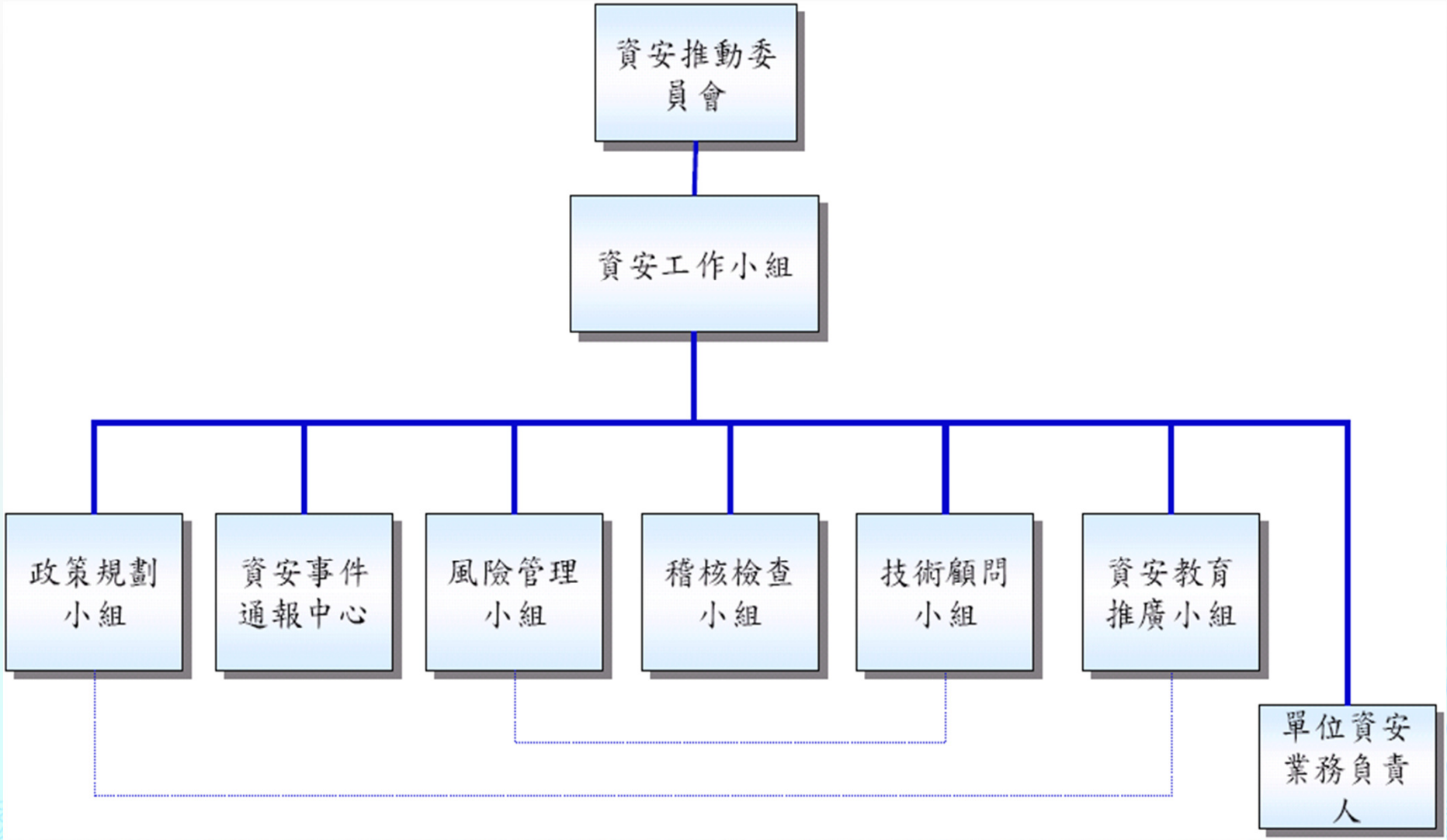
差異分析



資訊安全文件體系範例

階層	第一階	第二階	第三階	第四階
文件類別	資訊安全手冊	資訊安全程序書	管理辦法	紀錄
名稱	資訊安全政策 資訊安全手冊 適用聲明書	風險管理 文件與紀錄管理 事件管理 資安內部稽核 矯正與預防管理	資訊資產風險評鑑辦法 文件與紀錄管理辦法 資訊分級處理辦法 資安事件管理辦法 辦公室安全管理規則 電腦資源管理 網站管理辦法 人事管理規則 營運持續管理 電腦化資訊系統管理制度 …	例如 -訓練計劃與評核 -風險評鑑報告 -智慧財產權與保密協議書 -資安事件紀錄 -固定資產移動單 -軟體借用登錄表 …

資安組織規劃建議


資安推動委員會
資安工作小組
政策規劃小組
資安事件通報中心
風險管理小組
稽核檢查小組
技術顧問小組
資安教育推廣小組
單位資安業務負責人

資安組織任務職掌

工作小組	任務職掌
政策規劃小組	◆建立與維護檢討中心的資安政策 ◆建立維護檢討中心的資安標準以及程序 ◆界定與檢討資訊安全管理系統的範圍與控制措施 ◆建立與維護業務持續運作計劃
資安教育推廣小組	◆指導各單位資訊安全活動，以確認符合資訊安全政策與程序 ◆辦理安全認知與教育訓練計劃 ◆執行資訊安全管理系統及所有控制措施
風險管理小組	◆負責與推動資訊資產風險評鑑 ◆負責與推動資訊資產風險管理 ◆確認資訊資產的所有權與控制皆有適當的管理，同時符合資安風險管理政策與程序
稽核檢查小組	◆檢查資訊安全管理系統及所有控制措施之管理 ◆規劃執行資安稽核計劃，提出稽核報告，追蹤改善情形 ◆稽核檢查小組可採任務編組
技術顧問小組	◆發展資訊安全架構、標準及解決方案，包括了伺服器、工作站、網路、資料庫、應用程式等。 ◆發展與維護系統、資料庫、網路與應用程式的存取控制規則 ◆協助資訊安全事件管理中心執行第一線資訊安全事件回應與監測。
資安事件通報中心	◆監控記錄檔與回報資訊安全事件，以及向適當的管理階層報告類似的狀況 ◆第一線的資訊安全事件回應中心與監測中心

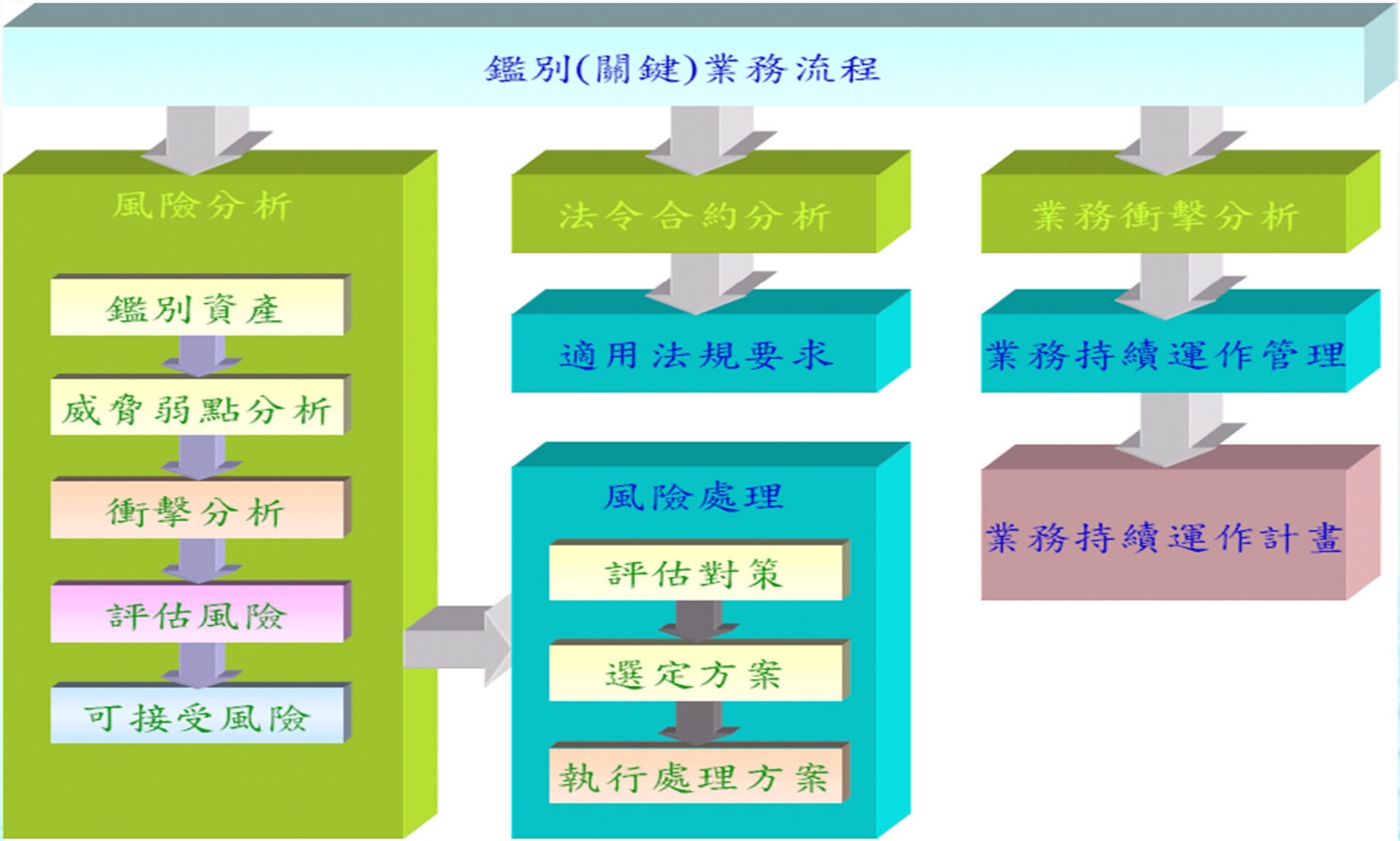
資安組織之運作會議

會議	資訊安全定期會議	資訊安全管理審查會議	年度計劃與預算會議
頻率	每季及必要時	每半年舉行	每年於第四季舉行
期間	依需要	依需要	依需要
出席者	資安工作小組成員	資安工作小組召集人與資安推動委員會	資安工作召集人與資安推動委員會
主題	◆審查與核准重要的資訊安全需求 ◆審查與解決重大的資訊安全議題 ◆檢視資訊安全管理的成效和回饋意見 ◆維護風險管理計劃 ◆風險評鑑審查會議	◆檢視年報、專案里程碑、獎勵相關人員 ◆審核業務持續營運計劃 ◆審核資訊安全政策 ◆執行管理階層審查工作	◆規劃下一年度的資訊安全計劃與預算

資安認知教育訓練規劃–因人而異

	高階主管	經理/單位主管	資訊技術人員	員工
需要或偏好	◆簡短 ◆底線(bottom line)訊息 ◆需要時提供支援事實 ◆與現在的業務優先順序或業務環境的關連性	◆清楚簡單、直接 ◆授權的來源 ◆與現在的營運、經濟與技術優先順係的關連性 ◆清楚的範圍 ◆逐步的指示 ◆重點的摘要 ◆供散佈的參考資料	◆清楚 ◆授權的來源 ◆技術原理 ◆指導性 ◆技術性的完全與精確	◆清楚 ◆授權的來源 ◆非技術性、簡單、快速
訊息	◆資訊安全政策的公告 ·一般政策 ·技術政策 ◆政策存放位置 ◆提供資安委員會未來方向 ◆決定相關資安流程 ◆高階主管的責任– ·給予支持 ·年度檢討資訊安全政策，及參加每季的資訊安全會議	◆資訊安全政策的公告 ·一般政策 ·技術政策 ◆政策存放位置 ◆提供建議給資安委員會 ◆執行資安委員會決議事項 ◆執行資安政策及相關流程 ◆經理的責任– ·執行資訊安全政策 ·確保員工遵守 ·提供員工常見問答集	◆資訊安全政策的公告 ·一般政策 ·技術政策 ◆政策存放位置 ◆提供建議給資安委員會 ◆實施資安委員會的指示 ◆支援資安政策，與履行相關流程 ◆資訊技術人員的責任– ·提供使用者的操作支援 ·了解相關政策	◆資訊安全政策的公告 ·一般政策 ·技術政策 ◆政策存放位置 ◆提供建議給資安委員會 ◆遵守資安委員會決議事項 ◆服從資訊安全政策及相關政策 ◆員工的責任– ·了解資訊安全責任 ·遵守相關責任

風險評鑑及管理


鑑別(關鍵)業務流程
風險分析
鑑別資產
威脅弱點分析
衝擊分析
評估風險
可接受風險
法令合約分析
適用法規要求
風險處理
評估對策
選定方案
執行處理方案
業務衝擊分析
業務持續運作管理
業務持續運作計畫

資產風險評鑑表-單筆內容範例

資產名稱	FTP伺服器(ftp.twaren.net)
部門	網路服務組
保管人	梁明章
資產類別	實體設備
數量	1
機密性	4 說明
完整性	4 說明
可用性	4 說明
資產價值	12 (機密性+完整性+可用性)
機敏性項目	N 符合「機密」及「敏感」性的資訊資產 (詳細說明)
備註	Linux-Gentoo-2.6
防護類別	
威脅	技術失效
脆弱點	缺少備份備援設施或流程
威脅等級(安控前)	2 說明
脆弱等級(安控前)	1 說明
衝擊等級(安控前)	2 說明
破壞事件的嚴重性(安控前)	4 (威脅等級*脆弱等級*衝擊等級)
風險值	48 (資產價值*破壞事件的嚴重程度)
風險等級	D 說明
建議安控機制	
風險降低原因說明	
威脅等級(安控後)	1 說明
脆弱等級(安控後)	1 說明
衝擊等級(安控後)	0 說明
破壞事件的嚴重性(安控後)	0 (威脅等級*脆弱等級*衝擊等級)

資訊資產評等範例-機密性

	確保只有經授權的人，方能允許存取資訊。			
分數	4	3	2	1
資訊紀錄	敏感性之資訊紀錄，僅開放給極少數必要知道的人使用。	敏感性之資訊紀錄，僅開放給必要知道的人使用。	非公開使用之非敏感性資訊紀錄	不限制使用之資訊紀錄。
電腦系統(AP,軟體)	敏感性之資訊處理設施與系統資源，僅開放給極少數必要知道的人使用。	敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。	非公開使用之非敏感性資訊處理設施與系統資源為者。	不限制使用之資訊處理設施與系統資源等。
設備	敏感性之資訊處理設施與系統資源，僅開放給極少數必要知道的人使用。	敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。	非公開使用之非敏感性資訊處理設施與系統資源為者。	不限制使用之資訊處理設施與系統資源等。
工作區	須要保密之實體資產，僅開放極少數有權限的人存取。	須要保密之實體資產，僅開放有權限的人存取。	內部可存取之實體資產，但不對外公開。	實體資產不限制使用，不會造成損失。
人員	僅限極少數有權限的人可以知道人員執行工作時所產生的知識。	僅限有權限的人可以知道人員執行工作時所產生的知識。	人員執行工作所產生的知識，內部可存取，但非公告週知。	人員執行工作所產生的知識，公開給大家知道，不會造成損失。

資訊資產評等範例-完整性

	確保資訊內容及資訊處理方法為正確而且完整。			
分數	4	3	2	1
資訊紀錄	不當的破壞或竄改資訊紀錄，會對業務應用造成很大的衝擊，甚至會造成業務失敗。	不當的損失、破壞或竄改資訊紀錄會對業務應用造成顯著的衝擊。	不當的損失、破壞或竄改資訊紀錄，會對業務應用造成輕微的衝擊。	不當的破壞或竄改資訊紀錄，所造成的業務衝擊可以忽略者。
電腦系統(AP,軟體)	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成很大的衝擊，甚至會造成業務失敗。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。	不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。
設備	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成很大的衝擊，甚至會造成業務失敗。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。	不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。
工作區	不當操作或破壞，會造成嚴重的傷害。	不當操作或破壞，會造成相當的傷害者。	不當操作或破壞，會造成輕微的傷害。	不當操作或破壞，所造成業務的傷害很少可忽略。
人員	人員執行工作所產生的知識，不當行為竄改，會造成嚴重的傷害者。	人員執行工作所產生的知識，不當行為竄改，會造成相當的傷害者。	人員執行工作所產生的知識，不當行為竄改，會造成輕微的傷害。	人員執行工作所產生的知識，不當行為竄改，不會對造成傷害。

資訊資產評等範例-可用性

	確保經授權的使用者當需要時，能存取資訊及使用相關的資產。			
分數	4	3	2	1
資訊紀錄	工作日(24小時)，至少95%的時間有權限的人可存取資訊紀錄。	工作日之上班時間，有權限的人都可存取資訊紀錄。	工作日之上班時間，至少50%的時間有權限的人可存取資訊紀錄。	工作日之上班時間，至少25%的時間有權限的人可存取資訊紀錄。
電腦系統(AP,軟體)	工作日(24小時)，至少95%的時間有權限的人可存取資訊系統與資源者。	工作日之上班時間，有權限的人都可存取資訊系統與資源。	工作日之上班時間，至少50%的時間有權限的人可存取資訊系統與資源。	工作日之上班時間，至少25%的時間有權限的人可存取資訊系統與資源。
設備	工作日(24小時)，至少95%的時間有權限的人可存取資訊系統與資源者。	工作日之上班時間，有權限的人都可存取資訊系統與資源。	工作日之上班時間，至少50%的時間有權限的人可存取資訊系統與資源。	工作日之上班時間，至少25%的時間有權限的人可存取資訊系統與資源。
工作區	工作日(24小時)，至少95%的時間可使用此實體資產者。	工作日之上班時間，都可使用此實體資產。	工作日之上班時間，至少50%的時間可使用此實體資產。	工作日之上班時間，至少25%的時間可使用此實體資產。
人員	人員執行工作所產生的知識，於工作日之上班時間(24小時)，至少95%的時間有權限的人都可取得者。	人員執行工作所產生的知識，於工作日之上班時間，有權限的人都可取得。	執行工作所產生的知識，於工作日之上班時間，至少50%的時間有權限的人可取得。	人員執行工作所產生的知識，於工作日之上班時間，至少25%的時間有權限的人可取得。

資訊資產評等範例-威脅等級

威脅/事件發生可能性	評等	說明	威脅頻率
極低	1	• 威脅來源缺乏動機或能力不足 • 防制脆弱性被利用的安全對策有效 • 不太可能發生	• 威脅事件雖然沒發生過,但有可能發生之 • 平均幾年才可能發生次數一次
低	2	• 防制脆弱性被利用的安全對策有效 • 威脅來源缺乏動機或能力不足 • 發生頻率低	• 平均每年發生次數一次以上
中	3	• 威脅來源有動機也有能力 • 防制脆弱性被利用的安全對策有效 • 有可能發生	• 平均每季都可能發生一次以上
高	4	• 威脅來源有強烈的動機與足夠的能力 • 防制脆弱性被利用的安全對策無效 • 時常發生	• 平均每月都可能發生一次以上
極高	5	• 威脅來源有強烈的動機與足夠的能力 • 防制脆弱性被利用的安全對策無效 • 發生頻率非常高	• 平均每周可能發生一次以上

資訊資產評等範例-弱點等級

難易度	評等	說明	一般分級原則
低	1	脆弱點很難被利用	● 僅限深入瞭解脆弱點技術，並於特定條件或環境下方能利用脆弱點 ● 不會損害資訊資產價值，或是受到損害後能立即回復 ● 必需運用特殊的方法才能利用脆弱點進行攻擊 ● 威脅來源必須花費長時間(可能需一個月以上)的資料收集，突破各層防護，才能接觸到關鍵資訊 ● 攻擊成功:可能要1~數個月以上
中	2	脆弱點被利用的難度適中	● 具備瞭解脆弱點技術知識，方能利用脆弱點 ● 資訊資產價值受到損害，且無法立即回復 ● 不需用特殊的方法就能利用脆弱點進行攻擊 ● 已實施保護的機制，威脅來源必須花費一段時間(可能是數天)進行資料收集即能接觸到關鍵資訊 ● 攻擊成功：可能是數天以上
高	3	脆弱點很容易被利用	● 任何人不需具備任何能力均有可有意或無意的利用脆弱點 ● 資訊資產價值受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊資產消失無法復原 ● 利用簡易的方法就能利用脆弱點進行攻擊或 ● 未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功或 ● 攻擊成功：可能是一天內到數天

資訊資產評等範例-衝擊等級

衝擊等級	評等	說明	
可忽略	0	可忽略	1.對於業務執行沒有影響; 2.可以立即完成復原
輕度	1	衝擊程度小	1.對於業務執行沒有影響; 2.可以立即完成復原 3.若持續發生且次數頻繁,對業務執行可能帶來潛在風險
中度	2	衝擊程度輕微	1.對於中心整體業務執行影響不大; 2.造成的損失可能僅影響單一業務或系統; 3.損失可能影響僅個人或少數幾人; 4.可以由個人進行復原; 5.修復或進行復原的措施可以在很短時間(1 小時)內完成
嚴重	3	衝擊程度重	1.對於中心整體業務執行造成損害; 2.造成的損失可能影響多種業務或數個系統; 3.損失可能影響多個部門或合作夥伴; 4.復原的措施必須由專業人員才能進行; 5.復原可能要數個小時~到一天才能完成"
癱瘓	4	衝擊程度很嚴重	1.中心整體業務執行造成損害; 2.事件處理不當可能對中心形象造成損害; 3.造成的損害可能影響全中心; 4.系統或相關服務停頓或癱瘓,業務無法運作; 5.合作夥伴或客戶失去信心; 6.復原的措施僅能由特定專業人員才能進行或修復人員不易取得; 7.復原無法於一天才能完成; 8.可能造成人員傷亡

資訊資產評等範例-風險等級

等級	說明
A	可能影響全中心或整體業務的營運，得視需要緊急處理。
B	可能會影響中心部分系統或部門業務的運作，需要及時處理。
C	可能影響局部系統、部門業務運作或個人工作進行，需在既定時間以內處理完成。
D	對系統或業務運作之影響有限，在既定時間以內處理即可。

決定可接受風險-管理審查會議

- 決定可接受風險
  - 衝擊影響程度
  - 預算
  - 時間
  - 安全需求
- 範例:
  - 風險等級為1 ~ 9
  - 風險值為6 以下為可接受風險

選定與評估風險處理對策

- 降低
  - 採取措施消除或者減少風險發生的因素。例如為了防止水災導致倉庫進水，採取增加防洪門、加高防洪堤等，可大大減少因水災導致的損失。
- 接受
  - 接受此風險發生的結果，但前提是「該風險之接受」需符合其安全政策與風險接受評估標準
- 避免
  - 消極躲避風險。譬如避免火災可將房屋出售，避免航空事故可改用陸路運輸等。因為存在以下問題，所以一般不採用。
    - 可能會帶來另外的風險。比如航空運輸改用陸路運輸，雖然避免了航空事故，但是卻面臨著陸路運輸工具事故的風險。
    - 會影響企業經營目標的實現。比如為避免生產事故而停止生產，則企業的收益目標無法實現。
- 轉嫁
  - 在危險發生前，通過採取出售、轉讓、保險等方法，將風險轉移出去

風險處理計劃

- 導入適當的控制措施, 以期風險完全地滿足組織政策及可接受風險之標準，並在掌握狀況下客觀地接受該等風險。

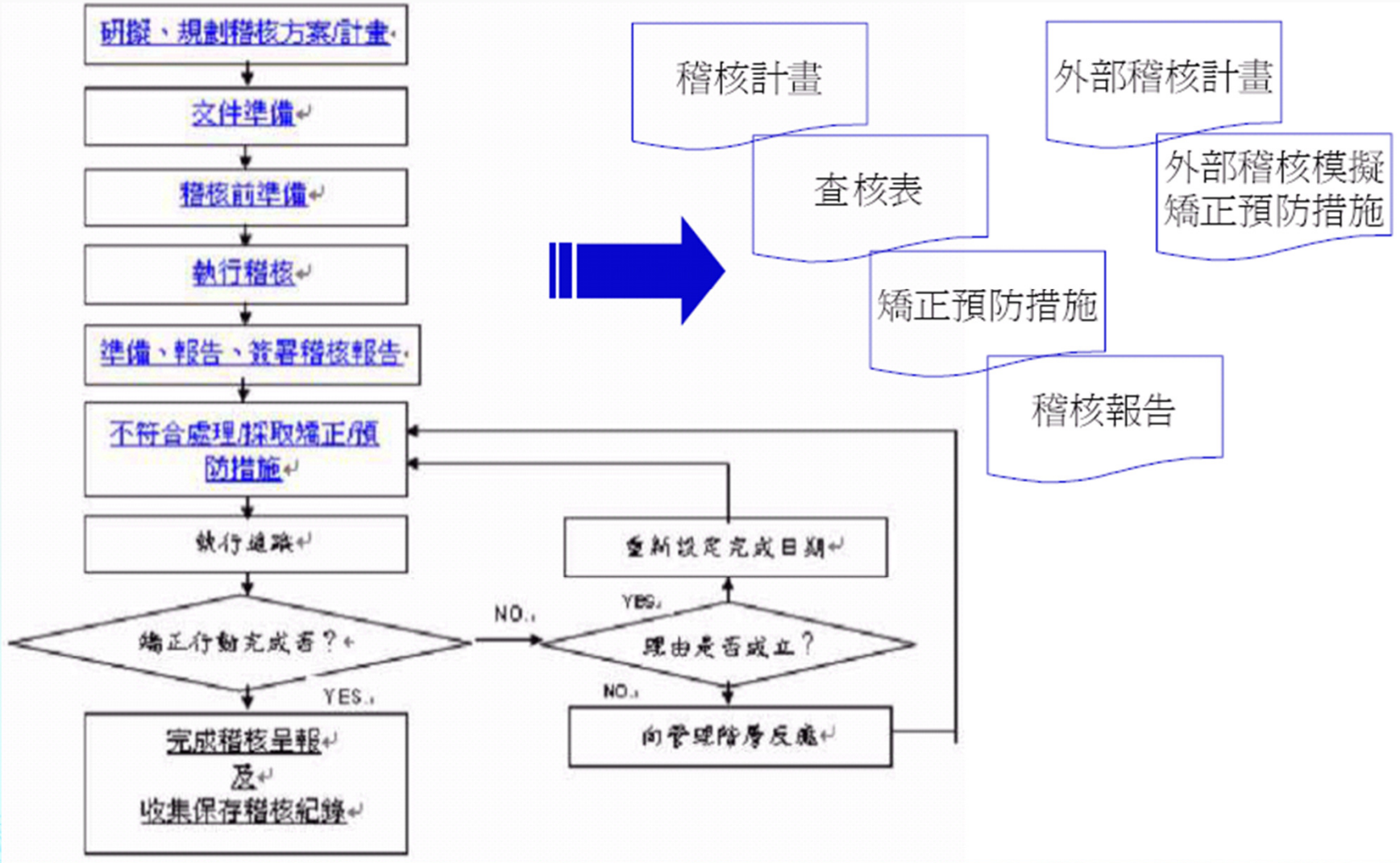
風險處理計劃-範例

編號	風險處理	負責單位	預計完成時間
1	建立應用系統測試環境	資訊技術組	2004/09/30
2	採用雙層防火牆	資訊技術組	2004/08/31
3	增訂門禁出入管理辦法	資訊技術組	2004/06/30
4	部署入侵偵測 (HIDS, NIDS)	資訊技術組	2004/08/31
5	數據機連線回撥	資訊技術組	2004/09/30
6	落實機房進出登記	資訊技術組	2004/06/30
7	宣導資安認知教育訓練	人事室	2004/07/31

內部稽核

- 稽核之6個階段
  - 稽核計劃表
  - 計劃與準備
  - 實施稽核
  - 報告稽核結果
  - 商定矯正措施
  - 跟進矯正措施

稽核作業規劃


研擬、規劃稽核方案/計畫
文件準備
稽核前準備
執行稽核
準備、報告、簽署稽核報告
不符合處理/採取矯正/預防措施
執行追蹤
矯正行動完成否？
NO
YES
重新設定完成日期
YES
理由是否成立？
NO
向管理階層反應
完成稽核呈報
及
收集保存稽核紀錄
稽核計畫
查核表
矯正預防措施
稽核報告
外部稽核計畫
外部稽核模擬
矯正預防措施

ISMS之改善

- 持續改善
  - 組織應藉由使用資訊安全政策、資訊安全目標、稽核結果、監視事件之分析、矯正與預防措施以及管理階層審查，以持續改進ISMS之有效性。
- 矯正措施
  - 為了防止再發生，組織應決定措施，以消除與ISMS要求不符合之原因。
- 預防措施
  - 組織應決定措施，以消除與ISMS要求潛在不符合之原因，並防止其發生。所採取之預防措施應與潛在問題之衝擊相稱。