中山科學研究院委託合作研究

國防科技學術合作研究計畫成果報告

CSII 共通作業環境之資訊安全防護管理研析

A Study on Information Security Management of the CSII Common Operation Environment

計畫歸屬：電子與資訊系統

計劃編號：91-2623-7-009-018

執行期間：91 年 1 月 1 日至 91 年 6 月 30 日

計劃主持人：劉敦仁

協同主持人：羅濟群

執行單位：國立交通大學資訊管理研究所

中山科學研究院委託合作研究

國防科技學術合作研究計畫成果報告

CSII 共通作業環境之資訊安全防護管理研析(第二部分)

A Study on Information Security Management of the CSII Common Operation Environment (Part II)

計畫歸屬：電子與資訊系統

計劃編號：91-2623-7-009-018

執行期間：91 年 1 月 1 日至 91 年 6 月 30 日

計劃主持人：劉敦仁

協同主持人：羅濟群

執行單位：國立交通大學資訊管理研究所

目　錄

目　錄 I
表 目 錄 III
圖 目 錄 IV
第 1 章　業務持續性管理 1
1.1　業務持續性管理的特點 1
1.1.1　業務持續性管理程式 1
1.1.2　業務持續性和影響分析 2
1.1.3　編寫和實施持續性計劃 2
1.1.4　業務持續性計劃架構 2
1.1.5　業務持續性計劃的檢查、維護和重新分析 3
1.1.5.1　計劃的檢查 3
1.1.5.2　計劃的維護和重新分析 3
1.1.6　資通安全事件通報及應變作業流程 4
1.1.7　業務持續性計畫程序書(範例) 6
第 2 章　風險管理 8
2.1　術語和定義 8
2.2　風險評估 8
2.2.1　步驟一：系統特徵的描述 11
2.2.1.1　系統相關資訊 11
2.2.1.2　資訊取得的方法 12
2.2.2　步驟二：威脅的識別 12
2.2.2.1　識別威脅的來源 13
2.2.2.2　動機與威脅的行為 13
2.2.3　步驟三：弱點的識別 15
2.2.4　步驟四：現有控制措施的分析 16
2.2.4.1　控制措施的方法 16

2.2.4.2 控制措施的分類 16
2.2.4.3 控制措施分析的技巧 17
2.2.5 步驟五：可能性的決定 17
2.2.6 步驟六：衝擊的分析 17
2.2.7 步驟七：風險程度的決定 19
2.2.8 步驟八：控制措施的建議 21
2.2.9 步驟九 ：風險評估報告的撰寫 21
2.3 風險緩和(Risk Mitigation) 21
2.3.1 風險緩和的選擇方案 22
2.3.2 風險緩和的策略 22
2.3.3 控制措施實施的方法 23
2.3.4 成本效益的分析 26
參考文獻 28

表 目 錄

表 2-1：常見的威脅來源 13
表 2-2：常見的人為威脅、動機與可能的攻擊行動 14
表 2-3：弱點/威脅配對 15
表 2-4：可能性(機率)的定義(非制式，可自訂) 17
表 2-5：衝擊程度的定義(非制式，可自訂) 18
表 2-6：常用的風險評估係數 19
表 2-7：風險等級矩陣(RISK-LEVEL MATRIX) 20
表 2-8：風險等級與必須採取的行動 20

圖 目 錄

圖 1-1：資通安全事件通報及應變作業流程圖(參考*1) 4
圖 2-1：風險評估流程圖 10
圖 2-2：風險緩和的行動 22
圖 2-3：風險緩和流程圖 25

第 1 章　業務持續性管理

1.1　業務持續性管理的特點

目標：防止資管中心之業務活動中斷，保證重要業務流程不受重大故障和災難的影響。

應該實施業務持續性管理程式，預防和恢復控制相結合，將災難和安全故障（可能是由於自然災害、事故、設備故障和蓄意破壞等引起）造成的影響降低到可以接受的水平。

應該分析災難、安全故障和服務損失的後果。制定和實施應急計劃，確保能夠在要求的時間內恢復業務流程。應該維護和執行此類計劃，使之成爲其他所有管理程式的一部分。

業務持續性管理應該採用控制措施，確定和降低風險，限制破壞性事件造成的後果，確保重要操作及時恢復。

1.1.1　業務持續性管理程式

應該在整個組織內部制定培育和維護業務持續性的管理程式。還應該包括業務持續性管理的主要內容，如下所示：

a) 瞭解組織所面臨的風險，考慮其可能性和影響，包括確定重要業務流程及其優先順序別。

b) 瞭解中斷可能對業務造成的影響（必須找到適當的解決方案，正確處理較小事故以及可能威脅組織生存的大事故），並確定資訊處理設施的業務目標。

c) 適當考慮購買保險，可以將其作爲業務持續性程式的一部分。

d) 制定符合業務目標和優先級別的業務持續性戰略並記錄在案。

e) 制定符合戰略的業務持續性計劃並記錄在案。

f) 定期對計劃和程式進行檢查和更新。

g) 確保在組織的程式和結構中納入業務持續性管理。業務持續性管理程式的協調責任應該在組織內部某一級（如資訊安全管理會議）進行適當分配（參閱『資訊安全管理程序』第 4.1.1 節）。

1.1.2 業務持續性和影響分析

要確保業務持續性，應該首先確定可能引起業務流程中斷的事件，如設備故障、水災和火災。然後，應該進行風險評估(第 2 章)，確定中斷可能造成的影響（破壞程度和恢復時間）。這兩項活動都應讓業務資源和流程的所有者完全參與。此項評估涉及所有業務流程，不只局限於資訊處理設施。

應該根據風險評估結果制定相應的戰略計劃，確定業務持續性總體方案。計劃制定後應該由管理層進行批准。

1.1.3 編寫和實施持續性計劃

應該制定計劃維護業務運作，或在重要業務流程中斷或發生故障後在規定時間內恢復業務運作。業務持續性計劃程序應該考慮以下內容：

a) 確定並認可各項責任和應急程式。

b) 執行應急程式，以便在規定時間內進行恢復。要特別注意對有關外部業務和合約的評估。

c) 商定程式的備案。

d) 對員工進行適當的訓練，讓他們瞭解包括危機管理在內的商定應急程式；檢查並更新計劃。

計劃程式應著重強調要求的業務目標，如在可接受的時間內恢復向客戶提供的具體服務。爲此，應該考慮所需服務和資源，包括人員、非資訊處理資源以及資訊處理設施的低效運行安排。

1.1.4 業務持續性計劃架構

應該維護一個業務持續性計劃的架構，保證所有計劃前後一致，確定測試和維護的優先順序別。每個業務持續性計劃都應該詳細說明計劃執行的條件以及執行每一部分計劃的負責人員。確定新的要求時，應該對已制定的應急程式（如疏散計劃或現有的低效運行安排）相應進行修改。

業務持續性計劃架構應該考慮以下內容：

a) 計劃執行條件。在計劃執行前說明要採用的程式（情況評估辦法、參與人員等）。

b) 應急程式。說明在發生危及業務操作和/或生命的事故後要採取的措施。還應該包括公共關係管理方面的安排以及與相應政府機構（如警察、消防和當地政府）保持有效聯繫的安排。

c) 低效運行程式。說明應該採取哪些措施，以將重要業務活動或支援服務轉移到其他臨時地點並在規定時間內恢復業務流程。

d) 恢復程式。說明應該採取哪些措施，以恢復正常業務運作。

e) 說明計劃檢查方式和時間的維護計劃以及計劃維護程式。

f）宣傳訓練活動。旨在讓人們瞭解業務持續性程式，保證這些程式始終有效。

g）個人責任。說明由誰負責執行哪一部分計劃。根據要求應該指定備選方案。

每個計劃都應該有一個所有者。應急程式、採用人工進行的低效運行計劃以及恢復計劃都應該由擁有相應業務資源或程式的人負責。備用技術服務的低效運行安排（如資訊處理和通信設施）通常應該由服務提供商負責。

1.1.5 業務持續性計劃的檢查、維護和重新分析

1.1.5.1 計劃的檢查

業務持續性計劃常常由於錯誤估計、疏忽或者設備（人員）的變化可能無法通過檢查。因此，應該對計劃進行定期檢查，保證其新穎性和有效性。進行此類檢查時，還應該保證負責進行恢復的所有小組成員以及其他相關人員對計劃有一定的瞭解。

業務持續性計劃的檢查計劃應該說明各部分計劃的檢查方式和時間。建議對計劃各部分進行頻繁檢查。應該採用各種技術，確保計劃的實際運作。這些技術包括：

a）對各種情況進行公開檢查（利用中斷示例討論業務恢復方面的安排）。

b）類比（尤其用來對負責事故/危機發生後管理的人員進行訓練）

c）技術恢復的檢查（保證資訊系統能夠有效恢復）。

d）備用場地恢復的檢查（繼續業務流程，同時在主要場地外執行恢復操作）。

e）供應商提供的設施和服務的檢查（確保外部提供的服務和產品符合合約中的規定）。

f）全面演習（檢查組織、人員、設備、設施和程式是否能夠應付中斷情況）。技術可以由任何組織使用，應該反映具體恢復計劃的特點。

1.1.5.2 計劃的維護和重新分析

應該通過定期審議和更新對業務持續性計劃進行維護，確保其始終有效。應該在組織的變更管理計劃中採用適當程式，確保業務持續性問題得到適當處理。

應該分配各個業務持續性計劃的定期評審責任；業務持續性計劃更新後，應該檢查還有哪些業務安排變動尚未在該計劃中得以反映。該正式變更控制程式還應該確保把更新計劃分發下去，而且在對完整計劃進行定期審議後更新計劃更加完善。

需要更新計劃的情況的示例包括購買新設備或作業系統升級以及在以下方面發生的變動：

a）人員。

b）地址或電話號碼。

c）經營戰略。

d）場所、設施和資源。

e）法律法規。

f）承包商、供應商和主要客戶。

g）流程，或新的流程/廢止的流程。

h）風險（操作風險和金融風險）。

1.1.6 資通安全事件通報及應變作業流程

當安全故障或災難的發生時，需通報「資訊安全管理會議」。「資訊安全管理會議」應依照「資通安全事件通報及應變作業流程」(圖 1-1)評估可能的損失，並執行業務持續性計劃，將災難和安全故障（可能是由於自然災害、事故、設備故障和蓄意破壞等引起）造成的影響降低到可以接受的水平。

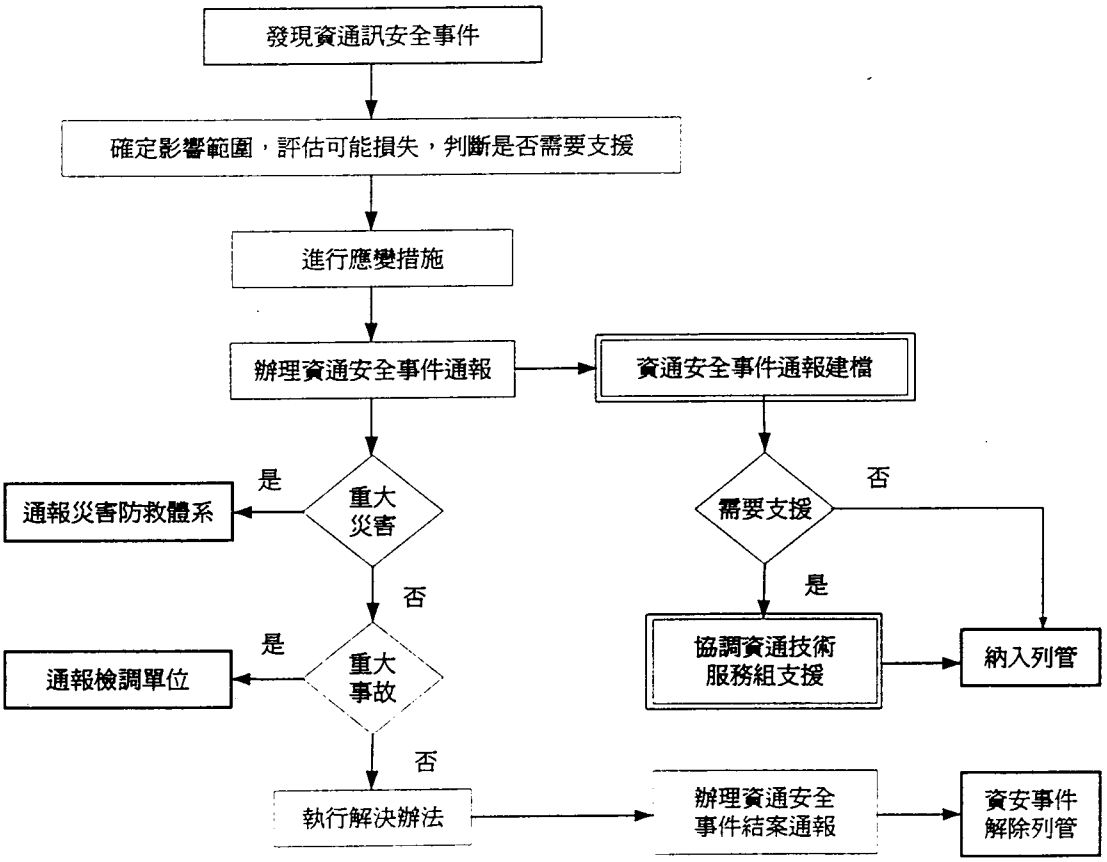


圖 1-1：資通安全事件通報及應變作業流程圖(參考*[1])

[1]行政院，「建立我國資通訊基礎建設安全機制計劃」，民國九十年一月十七日

資通安全事件之安全等級分為以下四級：

- 『A』級：影響公共安全、社會秩序、人民生命財產
- 『B』級：系統停頓，業務無法運作
- 『C』級：業務中斷、影響系統效率
- 『D』級：業務短暫停頓、可立即修復

影響等級在『B』級以下時，應由「資訊安全管理會議」負責處理，並且成立資通應變中心，處理全部狀況。「資訊安全管理會議」應考慮發生之資通安全事件之事實、可能影響之範圍等事項，適時回報「國家資通安全應變中心」及其主管機關。當系統恢復正常運作時，亦需回報之，以解除列管。

1.1.7 業務持續性計畫程序書(範例)

中山科學研究院 資訊管理中心

業務持續性計畫程序書

1. 目的：

MIS 系統主機是所有電腦使用者與生產線賴以作業之重要設備，為避免主機在遭受意外事故或不明原因造成主機癱瘓時，嚴重影響人員與資管中心任務，故建立此辦法，其目的在於主機意外當機或遭受破壞時，於最短之時間將主機復原，減少使用者等待之時間，進而減低資管中心之損失。

2. 計劃執行條件：

MIS 系統負責人經過初步觀察後，仍無法找出問題點，並且評估該意外無法在 3 個小時內恢復。

3. 範圍：資管中心各 MIS 電腦伺服器主機。

4. 應急程序：

採紙本作業替代原 MIS 業務，無法替代之業務，先暫時停止服務。

5. 權責：

5-1 系統工程師：負責 MIS 系統之開發與維護。

5-2 網管工程師：負責主機與網路管理，與備份作業。

5-3 主管：負責網路工程師各項作業之督導與查察。

6.定義：

6-1 伺服器主機：不同於一般個人電腦，其硬體配備等級較高，用以存放公用之重要檔案與程式。

6-2 當機：主機遭受人為疏失或硬體故障，造成主機無法啟動或資料遺失，以致使用者無法存取公用程式或資料。

6-3 系統復原：當伺服器當機時，將備份資料從磁帶中還原至原主機，或候補之主機上。

6-4 系統測試：為避免伺服器當機復原速度緩慢，故以備份機器模擬意外事故，將備份主機回復至原主機相同狀態。

7. 作業流程：

7-1 復原作業：

當機事故發生➔網路工程師通知相關使用部門採取其他候補作業➔相關網路與系統工程師對當機事故作判定➔設備替換與資料復原➔復原作業測試正常➔通知相關使用部門➔網路工程師填寫系統復原(測試)紀錄表➔列入年度測試重點機台。

7-2 測試作業：

主管模擬當機事件發生➔網路工程師當機事故判定➔設備替換與資料復原➔復原作業測試正常➔填寫 MIS 系統復原(測試)紀錄表➔作業檢討。

8. 作業內容：

8-1 各廠各伺服器備份作業需依照各廠備份作業辦法，由專人每日或定時備份重要資料。主管人員應確實做好督導與稽核之工作。

8-2 重大事故復原作業需列入工程師教育訓練重點，對人為產生之事故更需做好預防管制工作。

8-3 對重要作業主機應準備備份主機，再意外發生時，可先以接替作業，以避免原主機復原時機過長影響生產作業。

8-4 年度測試需針對重要主機每年模擬狀況測試一次，並針對測試缺失，列入教育訓練重點

8-5 各廠主機區域需嚴格人員進出管控，於主機上之操作皆需詳載於機房工作日誌。

第 2 章　風險管理

根據〔ISO/IEC 17799 資訊技術—資訊安全管理的實施要則〕，資訊中心應該確定自己的安全要求(需求)，而安全要求(需求)的第一個來源便是對組織所面臨的風險進行評估。通過風險評估，確定風險和安全漏洞對資產(或業務)的威脅，並估計風險發生的可能性以及潛在的影響。一旦確定了安全要求(需求)，就應該選擇並實施適宜的控制措施，確保將風險降低到一個可接受的程度。

風險管理包含三個程序：風險評估、風險緩和與持續評量改進的過程。2.2 節將描述一個可供參考使用的方法論，以進行風險評估。風險評估包含：風險的識別、評估風險所帶來的衝擊以及提出如何降低風險的建議方案；2.3 節將描述一個參考的程序，說明如何降低風險到一個可接受程度。這個風險緩和的程序包含：將風險評估過程中所產生的建議方案排出優先順序、執行與維護風險評估過程中所產生的建議方案。

形成風險的因素常受科技進步、政經情勢與社會人文環境之影響，由此可知形成風險的因素難以掌控，正因如此多數風險具有多變的性質。由於風險因素的多變性，風險管理必須是持續性的工作，今日的控制措施，明日不見得仍然有效，因此風險管理程序具有自我循環和重複之特性。是故，定時(或隨時)反覆識別風險，並依此調整控制措施是進行風險管理的基本原則。

2.1　術語和定義

資訊安全

資訊機密性、完整性和可用性的保護

機密性

確保只有獲得授權的人才能存取資訊。

完整性

確保資訊和處理方法的準確性和完整性。

可用性

確保獲得授權的用戶在需要時可以存取資訊並使用相關資訊資產。

2.2　風險評估

風險評估是風險管理的第一個步驟。組織利用風險評估來決定潛在威脅可能造成的衝擊程度。風險指的是某個特定的威脅來源行使某個潛在弱點的可能性(機率)，以及這個活動為組織所帶來的負面衝擊。

為了決定未來不利情況發生的機率，必須在考量潛在弱點與現有的反制措施下，分析資訊系統可能的威脅。而衝擊指的是威脅行使某個弱點所帶來的傷害的強度。

風險評估的方法論包含下列九個步驟，並將分別說明於 2.2.1 至 2.2.9：

- 步驟一：系統特徵的描述(2.2.1 節)
- 步驟二：威脅的識別(2.2.2 節)
- 步驟三：弱點的識別(2.2.3 節)
- 步驟四：現有控制(反制)措施的分析(2.2.4 節)
- 步驟五：可能性(機率)的決定(2.2.5 節)
- 步驟六：衝擊的分析(2.2.6 節)
- 步驟七：風險程度的決定(2.2.7 節)
- 步驟八：控制措施的建議(2.2.8 節)
- 步驟九：風險評估報告的撰寫(2.2.9 節)

步驟二、三、四與六可在步驟一完成後同時進行。圖 2-1 描述了這九個步驟，以及每個步驟的輸入與產出資訊。

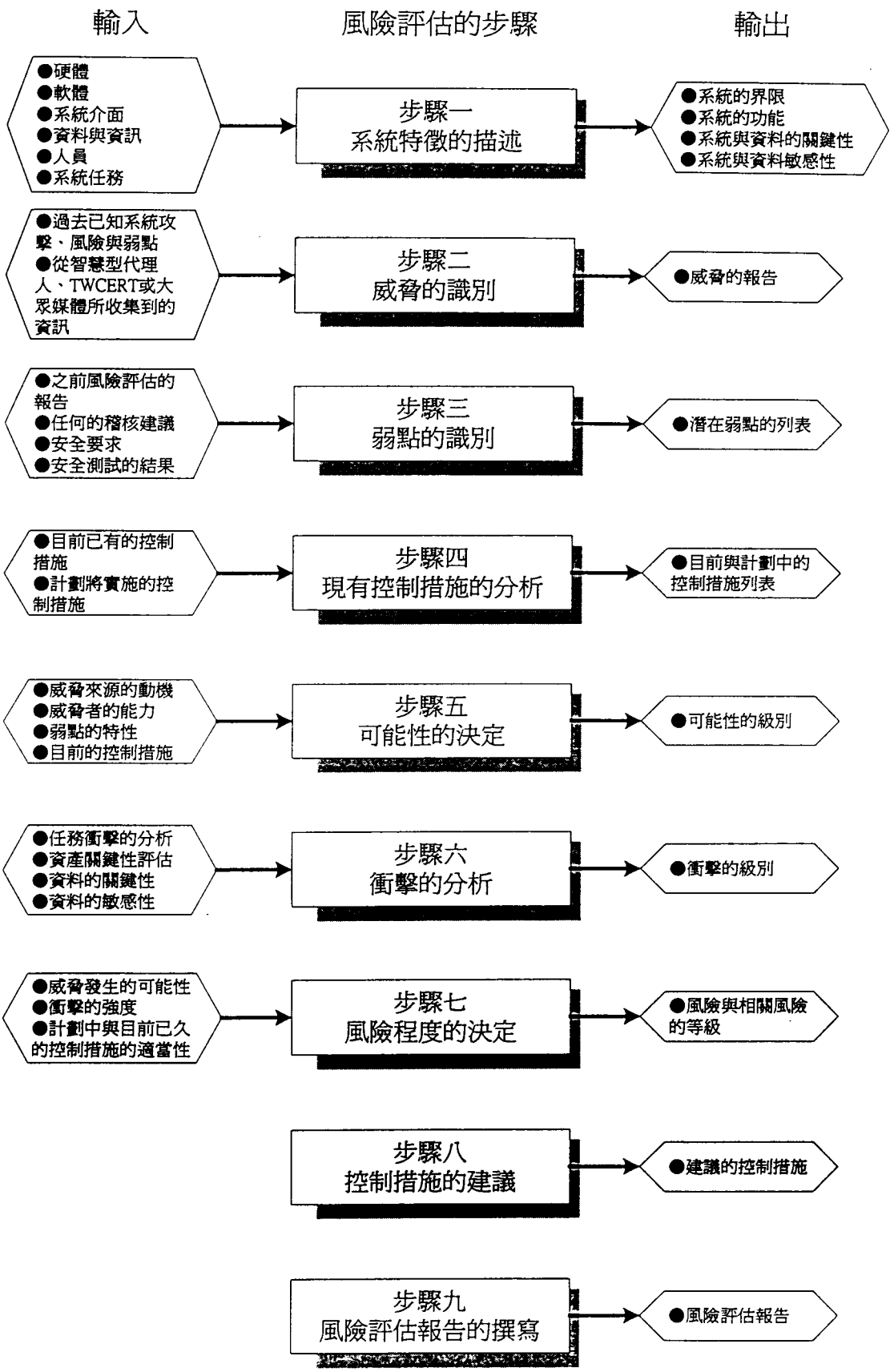

輸入
風險評估的步驟
輸出
●硬體
●軟體
●系統介面
●資料與資訊
●人員
●系統任務
步驟一
系統特徵的描述
●系統的界限
●系統的功能
●系統與資料的關鍵性
●系統與資料敏感性
●過去已知系統攻擊、風險與弱點
●從智慧型代理人、TWCERT或大眾媒體所收集到的資訊
步驟二
威脅的識別
●威脅的報告
●之前風險評估的報告
●任何的稽核建議
●安全要求
●安全測試的結果
步驟三
弱點的識別
●潛在弱點的列表
●目前已有的控制措施
●計劃將實施的控制措施
步驟四
現有控制措施的分析
●目前與計劃中的控制措施列表
●威脅來源的動機
●威脅者的能力
●弱點的特性
●目前的控制措施
步驟五
可能性的決定
●可能性的級別
●任務衝擊的分析
●資產關鍵性評估
●資料的關鍵性
●資料的敏感性
步驟六
衝擊的分析
●衝擊的級別
●威脅發生的可能性
●衝擊的強度
●計劃中與目前已久的控制措施的適當性
步驟七
風險程度的決定
●風險與相關風險的等級
步驟八
控制措施的建議
●建議的控制措施
步驟九
風險評估報告的撰寫
●風險評估報告

圖 2-1：風險評估流程圖

2.2.1 步驟一：系統特徵的描述

評估一個資訊系統的風險，第一步要先決定整個風險評估的範圍。在這個步驟中，資訊系統與組成這個系統的資源與資訊的範圍都必須被確定。透過系統特徵的描述可以決定風險評估的範圍，描繪操作授權的範圍，以及說明確定風險界限所必須的資訊(例如：硬體、軟體、系統介面、負責的部門或是支援的人員)。

2.2.1.1 節將說明用來描述資訊系統與其作業環境特徵的相關資訊來源。2.2.1.2 節則建議了一些的方法，用以取得關於資訊系統處理環境的資訊。

2.2.1.1 系統相關資訊

識別資訊系統的風險需要對整個資訊系統的處理環境有深刻的理解。因此，執行風險評估的人員首先必須收集系統相關資訊，這些資訊通來源常被分成下列幾類：

- 硬體
- 軟體
- 系統介面(例如內部與外部的連接)
- 資料與資訊
- 維護與使用該系統的人員
- 系統的任務
- 系統與資料的關鍵性
- 系統與資料的敏感性

其他與操作環境相關的資訊包含(但不僅限於)：

- 資訊系統的功能需求
- 該系統的使用者(例如：系統技術的提供者、利用該系統達成企業任務的使用者)
- 影響該系統的安全政策(例如：組織政策、政府法令、工業規範等)
- 系統的安全架構
- 目前網路的拓撲
- 維護系統與資料的可用性、完整性與機密性的資訊儲存媒體保護措施
- 與資訊系統相關的資訊流程(例如：系統介面、系統輸出與輸入流程圖)
- 資訊系統已使用的技術(Technical)控制措施(例如：內建或外掛的安全產品。這些安全的產品能提供識別、授權、強制或非強制的存取控制、稽核、殘餘資訊的保護以及資料加密等功能。)
- 資訊系統已使用的管理(Management)控制措施(例如：行為的規範與安全規劃)
- 資訊系統已使用的操作(Operational)控制措施(例如：人員安全、備份、意外事故的恢復、系統的維護、離線的儲存、使用者帳號建立與刪除的規範、不同使用者權限的劃分等)

- 資訊系統的實體安全環境(例如：設備安全、資料中心的政策)
- 資訊系統作業換環境上的安全(例如：溼度、水源、電源、污染、溫度等的控制)

如果評估的系統僅在設計階段，尚未完成，則系統資訊可由設計或需求文件中獲得。對於正在發展的系統，必須先定義好該系統未來需有的主要安全規則與特性。發展中系統的安全資訊，可由系統設計文件與系統安全計劃中找到有用的資料。

2.2.1.2 資訊取得的方法

可使用下列任一個方法(或其組合)取得與資訊系統相關的資訊：
問卷：此問卷必須給適當的技術或非技術的人員填寫。也可以用在面談的過程中使用。

- 面談：進行風險評估的人員可由面談的過程得到許多寶貴的資訊。評估人員可由面談過程中，取得資訊系統在實體環境上的資訊，以及資訊系統在操作安全上的資訊。附錄一提供了在面談過程中，經常詢問的問題，以供參考。這裡指的面談將會是面對面的活動，並且提供了評估人員實地的對資訊系統操作環境進行評估的機會。
- 檢視文件：檢視政策文件(例如：法律文件、指導方針)，與系統文件(例如：使用者說明、系統管理手冊、系統設計與需求文件、系統增補文件)。
- 使用自動化的掃描工具：例如使用網路掃描工具找出大部分站台所執行的服務，使用自動化的工具可以提昇資訊收集的效率。

資訊的取得不僅限於在風險評估的第一個步驟中進行，而是在整個風險評估程序(第一步到第九步)都可以執行。

第一步驟的產出是：受評估資訊系統的特性描述。包含資訊系統環境的描述，以及系統界限的輪廓。

2.2.2 步驟二：威脅的識別

威脅：一個特別的威脅來源成功的攻擊一個特定弱點的可能性。弱點是一個可能被意外觸發或是蓄意啟動的缺點。在沒有弱點可以攻擊的情況下，徒有威脅來源不代表一定會有風險產生。為了決定威脅發生的可能性，必須考慮威脅的來源(2.2.2)、潛在的弱點(2.2.3)與現有的控制措施(2.2.4)。

威脅：一個特別的威脅來源成功的攻擊一個特定弱點的可能性。

2.2.2.1 識別威脅的來源

這個步驟的目的是找出可能的威脅來源(Threat-Source)，並且將這些可能的威脅來源編輯成威脅報告書。

威脅的來源可能是：(1)其目標在於蓄意地啟動弱點的方法，或是(2)意外地觸發弱點的情況。

只要有可能傷害到資訊系統的任何清況或事件都是威脅的來源，常見的威脅來源可能來自於人、環境以及自然的情況。茲分述如下：

表 2-1：常見的威脅來源

常見的威脅來源	
自然的威脅	水災、地震、龍捲風、山崩、雪崩、雷暴或是其他的災害。
人為的威脅	人為所觸發的事件，包含蓄意行為(例如：網路攻擊、惡意的軟體或是非授權的情況下存取機密資料)，以及非蓄意的情況(例如：資料輸入時的誤值狀況)。
環境的威脅	長期的停電、作業環境的污染等。

在評估威脅的來源時，必須考慮所有可能傷害到資訊系統及其作業環境的所有威脅來源。舉例來說：雖然坐落於沙漠中的機房不太可能收到自然水災的侵害，因此威脅來源報告書中不會有自然水災的威脅，但是如果考慮到大量的水管漏水而造成電腦機房淹水的情況時，那麼這個水災的威脅也必須列入威脅的來源之一。

2.2.2.2 動機與威脅的行為

發動攻擊的動機與能力使得人成為非常危險的威脅來源。表 2-2 說明了目前常見的人為威脅、他們可能的動機以及所可能的攻擊行為。該表對於組織研究其人為威脅的環境有很大的幫助，也可以修改該表成為組織私人的人為威脅報告書。如此之外，檢視系統過去被非法入侵的狀況，回顧違反安全政策的行為報告與意外報告書，或是與系統管理者、使用者的面談過程等，都能夠有效地找出人為威脅的來源。

在潛在的威脅來源被找出來之後，還必須分析它們發動攻擊的動機以及發動攻擊的能力，這樣做的目的是要方便 2.2.5 節計算出威脅來源攻擊系統弱點的可能性(詳見 2.2.5 節)。

表 2-2：常見的人為威脅、動機與可能的攻擊行動

威脅來源	動機	可能的攻擊行動
駭客(Hacker) 破壞者(Cracker)	挑戰 自尊心 叛亂	系統入侵、破壞 非授權狀況下存取系統
電腦罪犯	破壞資訊 非法揭露資訊 獲得財物上的報酬 竄改資料	電腦犯罪(例如：電腦追蹤) 詐騙(例如：重送、偽造、攔截封包) 系統入侵 欺騙行為
恐怖份子	勒索 破壞 自肥 復仇	炸彈，或其他恐怖主義 資訊戰爭 系統攻擊(例如：DDoS) 系統滲透 系統竄改
工業間諜	取得競爭優勢 進行商業間諜活動	偷竊資訊 非法打探個人隱私 系統滲透 非經授權的存取系統(例如：存取機密的、私人的以及技術相關的資訊)
內部人員(訓練不佳的、心情不好的、惡意的、解僱的、粗心的、不誠實的員工)	好奇心 自尊心 收集情報 獲得財物上的報酬 復仇 非蓄意的錯誤(例如：資料輸入的錯誤、程式撰寫的錯誤)	譴責某位員工 勒索 瀏覽私人資訊 濫用電腦 愚弄或偷竊 輸入偽造、錯誤的資料 攔截 惡意的程式碼(例如：病毒、邏輯炸彈、特洛伊木馬) 販賣個人資訊 系統錯誤(bug) 系統入侵 系統破壞 非授權狀況下存取系統

除了表 2-2 中所列的威脅來源之外，有許多政府機構以及私人的安全企業也會公佈它們所發現威脅來源。政府及業界不斷的收集關於資訊安全方面的資訊，透過這些資訊可以提昇我們找出系統威脅來源的能力，這些資訊的來源包含下列的機構：

- 情報機構(例如：調查局的情報資料)。
- 電腦網路危機處理/協調中心(TW-Cert)
- 大眾媒體、特別是 Web-based 上的資源(例如：SecurityFocus.com, SeurityWatch.com, SecurityPortal.com 與 SANS.org)

第二步驟的產出是：可能會攻擊系統弱點的威脅來源列表(威脅報告書)。

2.2.3 步驟三：弱點的識別

資訊系統威脅分析的過程中，除了上一步驟的威脅來源分析以外，還包含弱點的分析。這個步驟的目的在於找出資訊系統中可能被威脅來源攻擊的弱點(瑕疵、缺點)。

弱點：系統安全的程序、設計、執行或是內部控制上的瑕疵或缺點。這個缺點可能意外的被啟動或是蓄意的被攻擊，進而導致系統安全受到侵害，或者違反系統的安全政策。

表 2-3 以表格的方式說明了弱點/威脅配對。

表 2-3：弱點/威脅配對

弱點	威脅來源	可能的威脅活動
被解僱員工的使用者代號(ID)並沒有即時的從系統中移除	被解僱的員工	撥號進入公司網路，並且存取公司私有的資料
公司的防火牆允許 inbound telnet，並且某台主機(X)上的 guest 帳號並沒有被取消	未經授權的使用者(例如：駭客、被解僱的員工、電腦罪犯、恐怖份子)	利用 telnet 連接至 X 主機，並且列用 guest 帳號瀏覽系統檔案
廠商已經找到系統在安全設計上的新瑕疵，但是新的 patch 尚未安裝到系統上	未經授權的使用者(例如：駭客、被解僱的員工、電腦罪犯、恐怖份子)	利用已知的系統弱點，未經授權地存取敏感的系統檔案
資訊中心使用自動灑水的消防系統。但是並沒有適當的覆蓋防水布以避免硬體因灑水受傷害	火災、疏忽的人員	資訊中心中的自動灑水消防系統被啟動

底下建議幾個能夠找出資訊系統在技術上與非技術上弱點的方法：(1)透過 2.2.1.2 節中資訊取得的方法找出系統弱點，或(2)從廠商官方的網頁中尋找已知的系統弱點，以及(3)從網際網路中尋找已經被發現的系統弱點。或者由下列已知弱點的出處取得參考文件：

- CERT(http://www.cert.org/)
- TWCERT(http://www.twcert.org.tw/)
- 先前風險評估的文件
- 資訊系統的稽核報告、系統異常報告書
- 系統測試報告
- 系統弱點資料庫(例如：NIST I-CAT, http://icat.nist.gov)
- 安全顧問
- 廠商
- 資訊安全公司
- 軍用系統所公佈的弱點報告

除了從既有文件內找尋弱點以外，亦可藉由對系統進行安全測試來找出可能的弱點。系統安全測試的方法包含：

- 自動化的弱點掃描工具
- 安全測試與評估(ST&E / 自行發展的測試程式或演練計劃)
- 從威脅來源的觀點所進行滲透測試(假扮駭客)

第三步驟的產出是：弱點/威脅配對(如表 2-3)。可能被威脅來源攻擊的系統弱點列表。

2.2.4 步驟四：現有控制措施的分析

這個步驟的目的是：分析組織現有的控制措施，或是計劃欲實施的控制措施是否能夠有效的用來降低或消除已經找到的威脅。為了方便步驟五能夠產生潛在弱點被威脅來源攻擊的可能性(機率)大小，必須先考慮現有的控制措施。舉例來說，如果威脅來源對於弱點的興趣不大，或沒有攻擊弱點的能力，或者已經存在有效率的安全措施可以消除、將低弱點被攻擊的時所帶來的傷害，那麼弱點就比較不會收到攻擊，或收到攻擊的可能性(機率)就會比較低。

接下來將在 2.2.4.1 到 2.2.4.3 分別討論控制措施的方法，控制措施的分類與控制措施分析的技巧。

2.2.4.1 控制措施的方法

安全控制措施包含技術與非技術性的方法。技術性的方法指的是整合在電腦系統軟體、硬體、韌體內的防衛方法。例如：存取控制的機制、識別與授權的機制、加密的方法以及入侵偵測軟體等。非技術性的方法則包含管理上的控制措施與操作上的控制措施。例如：資訊安全政策、作業程序、以及人員、實體、環境上的安全控管。

2.2.4.2 控制措施的分類

技術性或非技術性的控制措施，可以更進一步的分類成預防性的或是偵測性的兩類。

- 預防性的控制措施禁止任何違反安全政策的行為發生。包含了強制性的存取控制、加密與身分認證措施。
- 偵測性的控制措則是在違反安全政策的行為發生時，發出警告訊息。包含了稽核軌跡、入侵偵測方法、以及檢查核等措施。

2.2.4.3 控制措施分析的技巧

發展系統安全需求檢查表的方式可以有效率的分析控制措施。系統安全需求檢查表可以用來分析系統是否安全，因此檢查表有必要即時的更新，以反映組織環境的改變(例如：安全政策、方法、需求的改變)。

第四步驟的產出是：列出現有或即將採用來避免系統弱點遭受攻擊，或是降低攻擊所帶來的衝擊的控制措施。

2.2.5 步驟五：可能性的決定

為了產生潛在弱點被運用的可能性(機率)，必須考慮下列的因素：

- 威脅來源的動機與能力
- 弱點的特性
- 現有控制措施的效力

可以高(High)、中(Medium)、低(Low)的方式來描述弱點受威脅來源運用(攻擊)的可能性。表 2-4 說明了這三個可能性的等級。但這三個等級並非制式規定，可依需求增減之，例如增加極高(Very High)等級。

表 2-4：可能性(機率)的定義(非制式，可自訂)

等級	可能性的定義
高(High)	威脅來源有高度的動機與足夠的能力，且現有的控制措施並不足以預防弱點被攻擊或運用。
中(Medium)	威脅來源有高度的動機與足夠的能力，唯現有的控制措施已經能夠適當的阻止弱點被攻擊或運用。
低(Low)	威脅來源缺少動機與能力，或現有的控制措施已經能夠適當的預防，或者能夠有效的妨礙弱點被攻擊或運用。

第五步驟的產出是：可能性(機率)的列表(例如：高、中、低)。

2.2.6 步驟六：衝擊的分析

步驟五將危機發生的可能性區分為若干等級，並詳細定義之。步驟六則將危機發生後所帶來的衝擊也分成數個等級，並詳細說明每個等級所代表的意義。這個步驟需仰賴 2.2.1.1 所取得的下列資料：

- 系統的任務(系統所執行程序)
- 系統與資料的關鍵性(系統的價值與其對組織的重要性)
- 系統與資料的敏感性

衝擊分析便是將損失對組織資訊資產所造成損害的衝擊程度排列順序，分析的方法可根據受衝擊資產對組織的關鍵性與敏感性，進行質(Qualitative)的分析，或是量(Quantitative)的分析。如果之前沒有做過任何衝擊分析，可以根據為了維護系統與資料的可用性、完整性與機密性所需的保護程度，來決定系統與資料的敏感性。系統與資訊的擁有者都有責任協助分析其所屬系統或資訊衝擊的程度。

換言之，當任何一個安全事件發生，只要系統或資料的完整性、可用性與機密性等安全目標因此喪失或者降低，都可以當作是該事件造成了負面的衝擊。在衝擊分析時，可依據這三個安全目標進行衡量。底下簡略的敘述這三個安全目標，及未達成時的後果：

- 喪失完整性：系統與資料的完整性是指預防資訊被不正當的修改。假如資料或資訊系統在不經意或蓄意的狀況下，被未經授權的修改，即喪失了完整性。假如錯誤未被更正，利用錯誤的資訊將導致不正確或錯誤的決策。
- 喪失可用性：假如與組織任務相關的資訊系統無法被其使用者使用，則會影響組織的任務，因為不能使用該系統，將會影響使用者完成組織任務的效率。
- 喪失機密性：系統與資料的機密性指的是預防系統資訊被非經授權的揭露。機密性的資訊遭非授權的揭露所帶來的衝擊可能會危害到國家安全，或是造成機密行動曝光。

有形的衝擊可以利用量化(Quantitative)的方式來衡量衝擊的大小，例如衝擊所造成營業額的損失金額、修復該系統需花費的成本，或是更正該問題所需的努力等。但是有些衝擊難以進行進行量化的分析，例如組織公信力的損失。像這樣的衝擊便適合利用質(Qualitative)的分析，將其衝擊的程度區分成為高、中、低等類似的等級，如表 2-5。

表 2-5：衝擊程度的定義(非制式，可自訂)

衝擊程度	衝擊的定義
高(High)	弱點如果被啟動(攻擊)將造成(1)大量有形資產或資源的巨大損失；或 (2)嚴重的傷害或妨礙到組織任務的進行，組織的聲譽或是組織的利益；或(3)導致人員死亡或是嚴重的傷害。
中(Medium)	弱點如果被啟動(攻擊)將造成(1)有形資產或資源的損失；或(2)傷害或妨礙到組織任務的進行，組織的聲譽或是組織的利益；或(3)導致人員的傷害。
低(Low)	弱點如果被啟動(攻擊)將造成(1)少數有形資產或資源的損失；或(2)明顯的影響組織任務的進行，組織的聲譽或是組織的利益。

質的分析與量的分析

質(Qualitative)的分析的主要優點在於它可以將風險依照緊急程度排列順序，並且快速的針對重要的地方進行改進。其缺點是無法提供衝擊強度的量化指標，因此較難進行成本效益分析。

量(Quantitative)的分析的主要優點在於提供衝擊強度的量化指標，因此在推薦控制措施時，比較容易進行成本效益分析。其缺點是單純的根據數字大小進行衝擊的分析可能會相當的模糊，因為數字本身並無法看出衝擊的程度，除非事先以質的方法定義過某個程度的數字代表某個程度的衝擊(例如：受影響的人員大於 5 人，即為嚴重事件或是損失達 100000 萬元以上則為嚴重事件)。風險評估常用的係數如表 2-6 所示。

表 2-6：常用的風險評估係數

觀念	衍生的公式
暴露因子(Exposure Factor / EF)	該威脅導致特定資產損失的百分比
單一事件損失預期值 (Singel Losee Expectancy / SLE)	資產價值 *暴露因子(EF)
年度發生率 (Annualized Rate of Occurrence / ARO)	該事件每年發生的頻率
年度損失預期值 (Annualized Losee Expectancy / ALE)	單一事件損失預期值(SLE) *年度發生率(ARO)

第六步驟的產出是：衝擊強度的定義(例如：高、中、低)。

2.2.7 步驟七：風險程度的決定

步驟七將決定資訊系統特定風險的程度，這裡所指的特定風險即為步驟三所產生的每一個弱點/威脅配對。某弱點/威脅配對的風險可由下列因素決定：

- 某個威脅來源運作(攻擊)某個特定系統弱點的*可能性(機率)*(即第五步驟的產出)。
- 系統弱點被運作(攻擊)後，所造成*衝擊的強度*(即第六步驟的產出)。
- 針對用來減低或消除危機之*控制措施的適當性分析*(即第四步驟的產出)。

步驟七利用風險等級矩陣(Risk-Level Matrix)進行風險的評估，如表 2-7 所示。某個特定弱點/威脅配對的風險，便是將其發生可能性(機率)的評分乘以衝擊強度的評分。表 2-7 為一 3*3 矩陣，列出了在三種可能性(高、中、低)與三種衝擊強度(高、中、低)分類下所有的狀況。使用時可以需求，自訂風險等級矩陣，例如增加非常強烈(Very High)的可能性機率與非常強烈(Very High)衝擊程度等級，使風險等級矩陣成為一個 4*4 的矩陣。

風險大小的決定非常的主觀，但其基本的原理便是給予各個等級的可能性(機率)與衝擊強度一個數值，舉例來說：

- 發生的可能性(機率)為高(High)等級則給予數字 1.0，可能性(機率)為中(Medium)等級則給予數字 0.5，為低(Low)等級則給予數字 0.1。
- 衝擊程度為高(High)等級則給予數字 100，衝擊程度為中(Medium)等級則給予數字 50，為低(Low)等級則給予數字 10。

假設某一弱點/威脅配對發生的可能性(機率)等級為高(High)，而衝擊程度等級也為高(High)，該弱點/威脅配對的整體風險係數則為 100(1.0*100)，如表 2-7。若風險係數位於 50 與 100 之間可定義為高風險等級(High Risk Level)，風險係數位於 10 與 50 之間為中風險等級(High Risk Level)，係數小於 10 則為低風險等級(High Risk Level)，這便是最終的風險等級。

表 2-7：風險等級矩陣(Risk-Level Matrix)

衝擊的程度 / 發生的可能性	低 (10)	中 (50)	高 (100)
高 (1.0)	低(Low) 10 * 1.0 = 10	中(Medium) 50 * 1.0 = 50	高(High) 100 * 1.0 = 100
中 (0.5)	低(Low) 10 * 0.5 = 5	中(Medium) 50 * 0.5 = 25	中(Medium) 100 * 0.5 = 50
低 (0.1)	低(Low) 10 * 0.1 = 1	低(Low) 50 * 0.1 = 5	低(Low) 100 * 0.1 = 10

最終的風險等級代表系統、設備、程序的弱點遭到攻擊時其危機的等級。得到最終風險等級之後，可以詳細描述各個風險等級，以及其所必須採取的行動，如表 2-8。其中可以詳細描述當該等級的風險發生時，高階主管，該任務的負責人所必須採取的措施與行動。

表 2-8：風險等級與必須採取的行動

風險等級	描述與必要之行動
高(High)	如果風險等級被評定為為高，則有強烈的需要進行補救。現有的系統可以繼續運作，但是必須儘快採行更正或補救的措施。
中(Medium)	如果風險等級被評定為為中，則必須在一個合理的時間內發展補救措施。
低(Low)	如果風險等級被評定為為低，則該系統的責任歸屬者必須決定是否接受這個風險，或是著手進行補救。

第七步驟的產出是：風險等級(例如：高、中、低)。

2.2.8 步驟八：控制措施的建議

風險評估的程序除了瞭解風險的程度以外，最後還必須建議若干可用來消彌或降低風險到一定可接受程度的控制措施。可依下列的因素衡量可行的控制措施及其替代方案：

- 建議方案的效用(例如：系統的相容性)
- 合法性
- 組織的政策
- 對作業的衝擊程度
- 安全性與可靠性

控制措施的建議是整個風險評估程序的最終結果，這些被建議採行的控制措施將會成為風險緩和(2.3 節)階段的輸入。在風險緩和階段將會對本階段所提出的控制措施進行評估、排列優先順序並且執行。要注意的是，採用哪一種被建議的控制措施都可以降低損失，但是究竟要採用哪一種控制措施則需要考量其成本效益(Cost-Benefit)之後方能決定。

第八步驟的產出是：用來緩和風險的建議控制措施及其替代方案。

2.2.9 步驟九 ：風險評估報告的撰寫

風險評估的過程一但結束，必須將其結果文件化，寫成正規的報告或是簡報。風險評估報告是一份管理性質的報告，它可以幫助管理者與其該任務的責任歸屬者，在制定政策、程序、預算、系統操作與變更管理方式時的決策使用。

與稽核、調查報告不同的是，風險評估的報告不應該以"責備"的出發點來撰寫，風險評估報告必須有系統、有條理的撰寫，如此高階管理者才能夠瞭解風險的所在，並配置適當的資源，減少可能的損失。附錄二提供了一份可供參考的風險評估報告範本。

第九步驟的產出是：風險評估報告(描述威脅、弱點、風險大小評估與建議的控制措施)。

2.3 風險緩和(Risk Mitigation)

風險緩和是整個風險管理程序中的第二大步驟，它的目的是將風險評估程序最後所建議的控制措施加以排列優先順序，並且以可接受的成本，確認、控制、排除可能影響資訊系統安全的風險或將其危害最小化的過程。

欲將所有的風險全部消除是不切實際，也是不可能完成的任務，因此管理者的責任在於使用最少的成本，執行最適當的控制措施，使風險得以降到一個可以接受的程度，進而得到最小的衝擊。

以下各節將描述風險緩和的選擇方案(2.3.1 節)、風險緩和的策略(2.3.2 節)、控制措施實施的方法(2.3.3 節)，以及成本效益的分析(2.3.4 節)。

2.3.1 風險緩和的選擇方案

風險緩和是高階管理人員用來減少任務所承擔之風險的系統化方法。管理人員可由下列選項中，選擇其中一向來完成風險緩和：

- 風險承擔：接受可能發生的風險，並且使系統持續運作，或是執行某向控制措施來降低風險到可接受的程度。
- 風險規避：消除產生風險的原因或結果以避免風險(例如：停止系統運作，關閉將受波及的系統)
- 風險限制：執行控制措施，將風險限定在一定的程度之內。
- 研究與承認：承認某項弱點，並且開始研究控制措施來降低該弱點可能造成的損失。
- 風險轉移：將風險轉移，使所受的損失得到補償(例如：購買保險)。

2.3.2 風險緩和的策略

如 2.3.1 節所述，風險並不能完全克服，也不只有一種方式可以緩和風險，因此管理人員及系統責任歸屬者常會問：「在什麼情況下，我需要採取行動？」「什麼時候？應該採取哪些控制措施？」圖 2-2 敘述了這些問題。

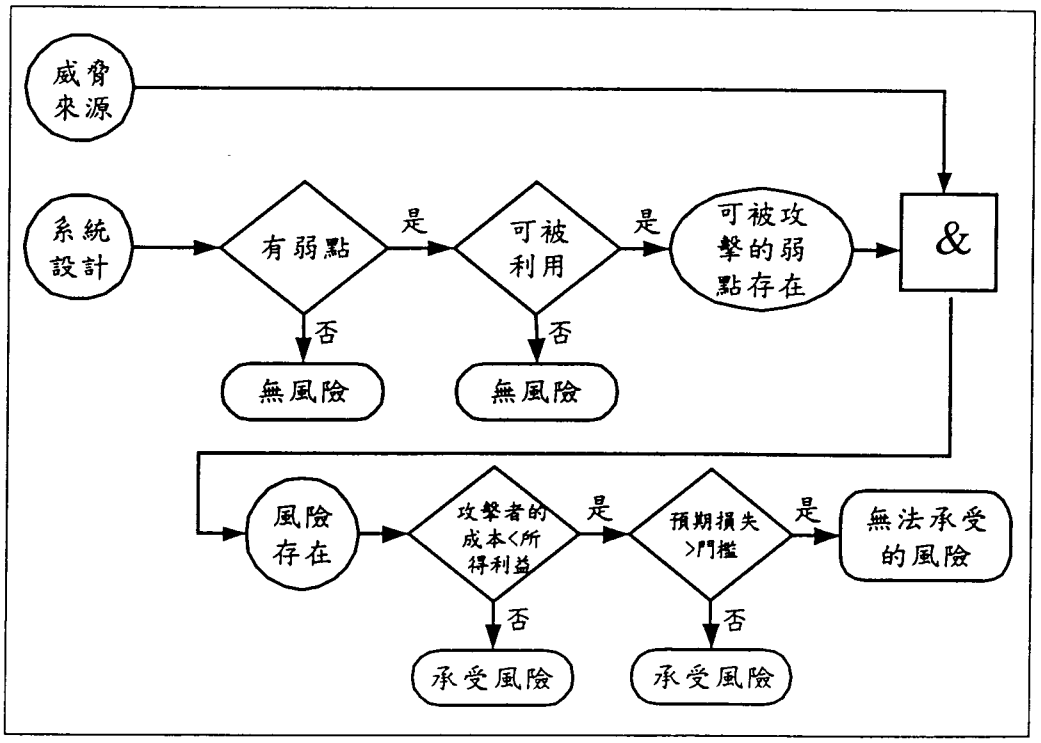


圖 2-2：風險緩和的行動

由圖 2-2 可以更進一步導出四個風險緩和的策略：

- 當弱點(缺陷或缺點)存在時→執行保全技術，減少弱點發生的機率。
- 當弱點可能被運作時→應用分層的保護，管理上的控制將事件的損失最小化，或避免該事件的發生。
- 當攻擊者的成本比其潛在收益小時→採用一些保護措施減少攻擊者的動機或是增加攻擊者的成本。
- 當損失極大時→採用設計的原則、架構的設計、技術與非技術上的保護來限制攻擊的程度，因此可以減低可能的損失。

2.3.3 控制措施實施的方法

當必須採用控制措施時，須謹記下列原則：

以最低成本，在最少的衝擊狀況下，將最大的風險，降低到可接收的程度。

底下將說明實施控制措施以緩和風險的方法論：

- 步驟一、排列優先順序：根據風險評估報告中的風險等級，將所有行動派列優先順序。在資源配置的時候，高的優先權應先給予那些無法接受的風險(被給予非常高(Very High)等級的風險)。因為這些弱點/威脅配對需要立即的補救，以保護組織。

  步驟一的產出為—優先權由高至低的行動列表。

- 步驟二、評估建議的控制措施：風險評估過程中所建議的控制措施並不一定是適合執行的。在這個步驟必須分析建議控制措施的可行性(例如：使用者的接受程度、相容性)，與效用(所提供的保護程度、風險降低的程度)。本步驟的目的是要選擇最適當的控制措施。

  步驟二的產出為—可行的控制措施列表。

- 步驟三、執行成本效益分析：為了協助管理者找出最有成本效益的控制措施，必須執行成本效益分析。2.3.4 節將詳述成本效益分析。

  步驟三的產出為—描述執行或不執行的控制措施的成本效益分析。

- 步驟四、選擇控制措施：根據成本效益分析的結果，管理者選擇最有成本效益的控制措施來降低風險。被選擇的控制措施可以結合技術的、操作的以及管理的控制因素，以確保組織的安全。

  步驟四的產出為—被選擇的控制措施。

- 步驟五、指定負責人：找出擁有適當的專業能力與足夠的能力集之適當人員(內部員工或是外部契約人員)負責執行已經選定的控制措施，並且為其負責。

  步驟五的產出為—責任人員列表。

- 步驟六、發展安全防護措施執行計劃：這個步驟必須產生安全措施執行計劃(行動計劃)，這個計劃最少需要包含下列資訊：
  - 風險(弱點/威脅配對)與其風險等級(由風險評估報告中取得)
  - 建議的控制措施(由風險評估報告中取得)
  - 行動的優先順序
  - 選擇的控制措施(根據可行性、效益、對組織帶來的好處與成本而決定)
  - 執行所選定的計劃所需的資源
  - 權責團隊或人員的列表
  - 開始執行日期
  - 預計完成日期
  - 維護的要求

  安全防護措施執行計劃可以協助並促進風險緩和的程序。附錄三提供了可供參考的安全防護措施執行計劃範本。

  步驟六的產出為—安全防護措施的執行計劃。

- 步驟七、執行所選定的控制措施：根據個別的情況，所執行的控制措施可能可以降低風險，但無法消彌風險，因此必須列出剩餘的風險。

  步驟七的產出為—剩餘的風險。

圖 2-3 說明了風險緩和的流程圖。

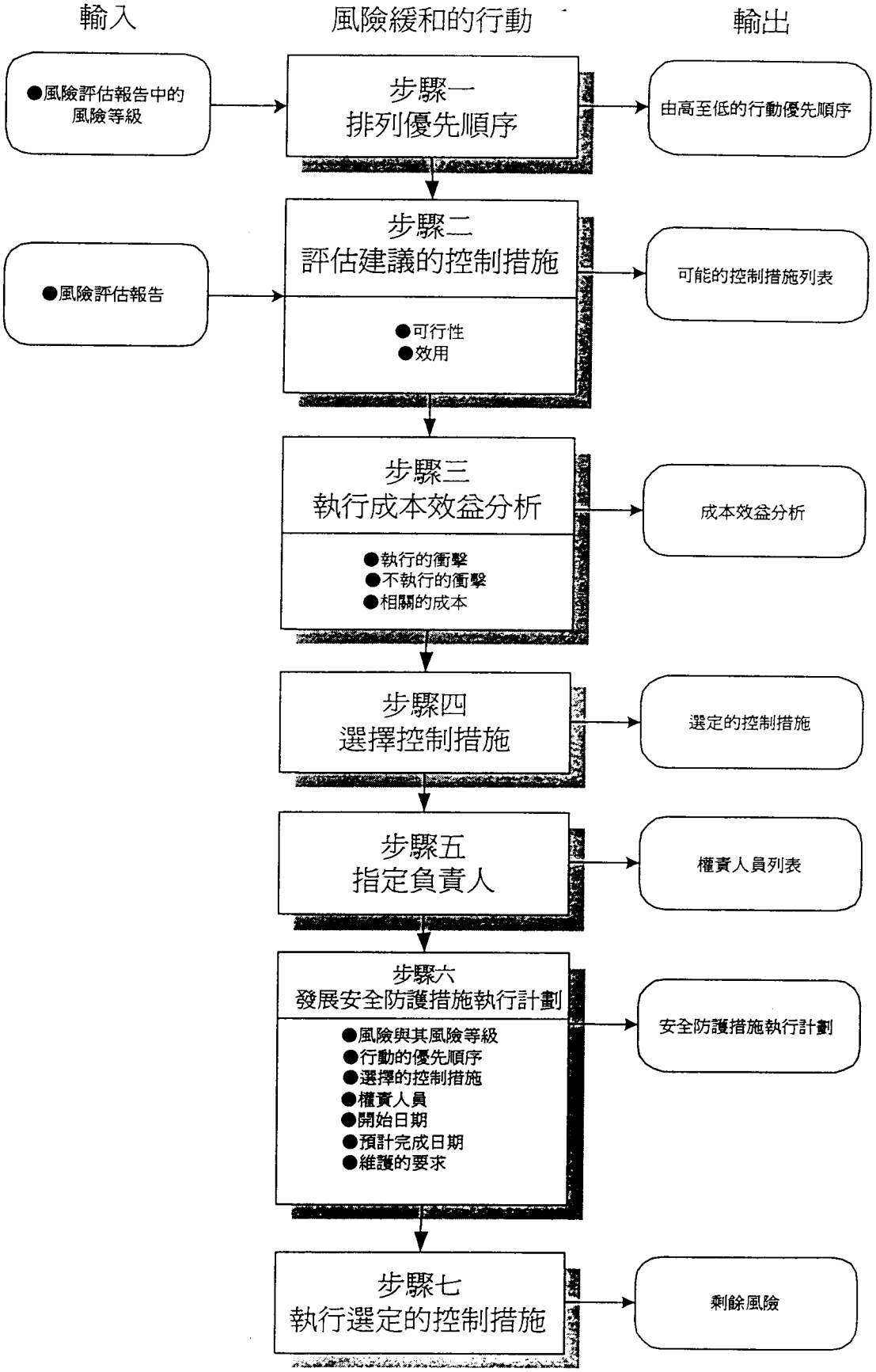

輸入
風險緩和的行動
輸出
●風險評估報告中的風險等級
步驟一
排列優先順序
由高至低的行動優先順序
步驟二
評估建議的控制措施
●可行性
●效用
●風險評估報告
可能的控制措施列表
步驟三
執行成本效益分析
●執行的衝擊
●不執行的衝擊
●相關的成本
成本效益分析
步驟四
選擇控制措施
選定的控制措施
步驟五
指定負責人
權責人員列表
步驟六
發展安全防護措施執行計劃
●風險與其風險等級
●行動的優先順序
●選擇的控制措施
●權責人員
●開始日期
●預計完成日期
●維護的要求
安全防護措施執行計劃
步驟七
執行選定的控制措施
剩餘風險

圖 2-3：風險緩和流程圖

2.3.4 成本效益的分析

為了有效的配置資源，並且執行具有成本效益的控制措施，在找出所有可行的控措施與評估它們的可行性與效益之後，必須對每一個被建議執行的控制措施進行成本效益的分析，以決定哪個控制措施是必要適當的。

成本效益的分析可以是質(Qualitative)或量(Quantitative)的分析。成本效益分析的目的是要顯示出執行某控制措施的成本對於所減低的風險而言是合理的。舉例來說，組織是不太可能實施一個需要耗費$1,000 萬，但卻只能減少$200 萬損失的控制措施。

成本效益分析包含：

- 確定執行某項控制措施的衝擊(做所帶來的衝擊)
- 確定不執行某項控制措施的衝擊(不做所帶來的衝擊)
- 估計執行的成本。包含：
  - 軟、硬體的採購成本
  - 若必須犧牲系統效率以增加安全性時所減少的作業效率
  - 實施額外的配套措施所需的成本
  - 增聘新進人員以執行所建議的政策、程序或服務的成本
  - 訓練成本
  - 維護成本
- 評估執行的成本，以及執行後為系統與資料關鍵性所帶來的效益，在考慮成本與相關的衝擊下，決定執行新的控制措施對組織的重要性。

組織必須考量執行某控制措施的成本，與不執行該控制措施所造成的損失成本，如果不符合成本效益，則可以考慮不要採行該控制措施。

成本效益分析範例：系統 X 儲存並且處理關鍵性且敏感性的員工私人資料，但是系統 X 卻尚未採行任何稽核的功能。底下將對於系統 X 是否該執行稽核功能，進行成本效益的分析。項目(1)與(2) 說明了執行與不執行稽核功能所帶來的無形衝擊(例如：妨礙因素)，項目(3)說明了有形的衝擊(例如：實際的成本)。

(1) 系統加入稽核功能的衝擊：系統稽核的功能可以使得管理者能監控使用者操作系統的活動，但是將會將低系統的效能，並使得使用者的生產力連帶的將低。此外，加入稽核功能續要額外的資源，如(3)所述。
(2) 不加入稽核功能的衝擊：沒有稽核功能，使用者操作系統的活動無法被監控、追蹤。因此無法增加安全性，保護組織的機密資料。
(3) 加入系統稽核功能的估計成本：

使系統具有稽核功能的成本—無成本，內建系統功能	$ 0
每年執行稽核檢查與文件建檔工作的額外人力	$XX,XXX
訓練(例如：系統稽核組態，產生報告)	$ X,XXX
另購的稽核報告產生軟體	$ X,XXX
每年稽核資料的維護(例如：儲存、建檔)	$ X,XXX
估計成本	$XX,XXX

瞭解成本與效益之後可以下列原則決定是否採用某控制措施：

- 假如執行控制措施所減少的風險比所需要的還要多，怎可以找看看是否有比較便宜的替代方案。
- 假如執行控制措施的成本比其所能降低的風險還要多，則乾脆尋找其他方案。
- 假如控制措施不能有效率的降低風險，則找尋其他的控制措施一起執行，或是換一個不同的控制措施。
- 假如控制措施能有效的降低風險，並且具有成本效益，則採用它。

通常執行控制措施的成本比較能具體衡量，而不執行的成本較難衡量，因此高階管理者在決定是否執行控制措施來保護組織時扮演了關鍵性的角色。

參考文獻

[1] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "*Risk Management Guide for Information Technology Systems*," National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, October 2001

[2] Kenneth N. Myers, "*Total Contingency Planning for disasters: Managing Risk... Minimizing Loss... Ensuring Business Continuity,*" Wiley, 1993

[3] Evan Marcus, Hal Stern, "*Blueprints for High Availability—Designing Resilient Distributed Systems,*" Wiley, 2000

[4] Ronald L. Krutz, Russell Dean Vines, "*The CISSP Prep Guide—Mastering the Ten Domins of Computer Security,*" Wiley, 2001

[5] ISO/IEC, "*ISO/IEC 17799 Information Technology — Code of Practice for Information Security Management,*" ISO, 2000/12/01

[6] 行政院，「建立我國資通訊基礎建設安全機制計劃」，民國九十年一月三十一日

[7] 行政院研考會（88）會訊字第 05787 號函頒，「行政院所屬各機關資訊安全管理規範」，民國八十八年十一月十六

[8] 編輯：黃芳川，「資訊安全手冊——第三版」，行政院主計處電子處理資料中心，民國九十年五月一日

[9] 主編：葉邵威，「電腦中心作業規範」，資訊工業策進會

[10] Bruce Schneier 著，吳箋玲譯，「秘密與謊言」，商周出版，民國九十年九月

[11] 國立嘉義大學，「國立嘉義大學資訊安全管理規範實施要點」(網頁資料)，來源：http://www.ncyu.edu.tw/cc/left/law/d7.htm

[12] 國立中正大學，「國立中正大學資訊安全管理規範實施要點」(網頁資料)，來源：http://www.ccu.edu.tw/center/other/security.htm

[13] 樊國楨，鐘乃業，方仁威，「國家資通訊基礎建設安全機制計畫記事（上）」（網頁資料），工研院電通所，來源：http://www.gss.com.tw/eis/25/p83.htm

附錄一：面談問卷範例

面談問卷的內容，可以根據被評估的資訊系統而有所不同。為了取得組織環境的資訊，在訪談過程中可能詢問的問題包含：

- 合法的使用者有哪些？
- 組織的任務為何？
- 用來完成組織任務之資訊系統的目的為何？
- 這個系統對於完成組織任務的重要性有多高？
- 資訊系統已知的要求為何？
- 組織需要哪些資訊(輸入與輸出)？
- 資訊系統所產生、使用、處理、儲存或檢索的資訊有哪些？
- 該資訊對組織任務的重要性有多大？
- 資訊流動的路徑為何？
- 資訊系統處理之資料的型態為何(財物、人事、研發、醫療或指揮命令)？
- 資訊的敏感程度為何？
- 系統資訊本身或系統所處理的資訊是否能被揭露，或是不應該項哪些對象揭露？
- 該資訊被處理及儲存的地點為何？
- 資訊儲存的型態為何？
- 假如資訊被非經授權的人取得，對組織的潛在衝擊為何？
- 對於資料完整性與可用性的要求為何？
- 假如系統或資訊不可靠，對組織任務的影響為何？
- 組織能夠容忍的系統停工期有多長？停工期與平均的系統修復或復原時間比起來有多大？其他使用者可以採用的系統替代方案為何？
- 系統發生故障或是無法使用，是否會造成人員健康上的傷害或死亡？

附錄二：風險評估報告範例

執行摘要：

I. 簡介

- 目的
- 風險評估的範圍

描述系統的組成元件、要素、使用者、系統位置，以及其他任何與被評估系統相關的細節。

II. 風險評估的方法

簡短的敘述風險評估所使用的方法，例如：

- 參與者(例如：風險評估團隊成員)
- 用來取得資訊的技術(例如：工具或問卷的使用)
- 風險規模的描述(例如：3 x 3、4 x 4 或 5 x 5 的風險等級矩陣)

III. 系統特性

描述系統的特性，包含硬體(例如：伺服器、路由器、閘道器)、軟體(例如：應用軟體、作業系統與協定)、系統介面(例如：通訊的線路)、資料與使用者。提供系統的連接圖、輸入與輸出的流程圖，以描述出風險評估的範圍。

IV. 威脅報告

收集並且列出潛在的威脅來源，以及任何可能發生在被評估系統上的相關威脅活動。

V. 風險評估的結果

列出所觀察到的現象 (所有的弱點/威脅配對)，每一項觀察到的現象必須包含：

- 每一個現象的編號，與該現象簡短的描述(例如：現象 I：使用者的系統密碼會被猜出或是破解)。
- 針對威脅來源與弱點之間關係的描述。
- 現有的用來降低風險的控制措施。

- 發生可能性的描述與評估(例如：高、中或低可能性)。
- 衝擊分析的描述與評估(例如：高、中或低衝擊)。
- 根據風險等級矩陣所決定的風險等級 (例如：高、中或低等級)。
- 能用來降低風險的建議控制措施及其他可能的選擇方案。

VI. 總結

合計所有現象的總計，利用表格的方式概述這些現象、與其相關的風險等級、建議的控制措施、以及任何的評論，以協助在風險緩和階段時，建議控制措施的執行。

中山科學研究院 資訊管理中心
安全防護措施執行計劃(範例)

(1) 風險 (弱點/威脅配對)	(2) 風險等級	(3) 建議的控制措施	(4) 優先順序	(5) 選用的控制措施	(6) 執行時所需的資源	(7) 負責人員/團隊	(8) 起始/終止執行日期	(9) 維護要求/評論
非經授權的使用者可以利用 guest 帳號，以 telnet 的方式連線到 XXX 伺服器，並且瀏覽敏感性的公司資料	高	● 不允許回撥(inbound)的 telnet 連線 ● 不允許企業網路外對公司敏感性資料的存取 ● 不開放 guest 帳號，或設定複雜的 guest 帳號密碼	高	● 不允許回撥(inbound)的 telnet 連線 ● 不允許企業網路外對公司敏感性資料的存取 ● 取消 guest 帳號	10 個小時的時間，以進行系統的組態設定與測試	王某某(XXX 伺服器的系統管理者)與羅某某(公司防火強的管理者)	2002/6/3~ 2002/6/4	週期性的執行系統安全檢視與測試，以確保 XXX 伺服器被適當地保護

(1) 風險(弱點/威脅配對)來自於風險評估程序的產出
(2) 針對每項風險(弱點/威脅配對)的相關風險等級來自於風險評估程序
(3) 建議的控制措施是風險評估程序的產出
(4) 優先順序是根據風險等級與可用的資源所決定(例如：資金、人員或技術)
(5) 由建議的控制措施中選擇某一個控制措施以執行
(6) 執行該選定的控制措施所需的資源
(7) 指定負責執行新控制措施的人員或團隊
(8) 執行控制措施的起始日期與專案的終止日期
(9) 新控制措施執行完畢後的維護要求

中山科學研究院 資訊管理中心
安全等級分類表(範例)

xx 年 xx 月 x 版

安全分類等級	複製原則
AA (極機密)	◎除備份外，禁止任何形式的複製
	儲存原則
	◎如為電子檔案，則需每月進行一次備份 ◎一般檔案需放置於安全的實體位置
	郵寄、傳真和電子郵件傳輸原則
	◎禁止使用電子郵件傳輸
	通過移動電話、語音郵件、應答機等交談方式進行傳輸
	◎禁止此類傳輸
	銷毀原則
	◎電子形式資料銷毀時，應將儲存媒體軌段皆填為 0 ◎一般文件銷毀時，應燒毀

本表根據 xx 年 xx 月第 x 次資訊安全管理會議通過實施

1. imi3-01 資訊安全管理作業程序
2. imi4.1.1-01 資訊安全會議作業程序
3. imi4.1.4-01 資訊處理設施異動作業程序
4. imi4.2-01 第三方存取管制程序
5. imi4.3-01 外包合約管制作業程序
6. imi5-01 資產分類管制程序
7. imi6.1-01 人員安全管理作業程序
8. imi6.1-02 用戶問題諮詢作業程序
9. imi6.2-01 員工資訊安全教育訓練作業程序
10. imi6.3-01 資訊安全事故矯正預防作業程序
11. imi7.1-01 資訊安全區管制作業程序
12. imi7.2.4-01 資訊處理設備管理作業程序
13. imi7.2n7.3-01 資訊環境安全管理程序
14. imi8.1-01 機房開關機作業程序
15. imi8.2-01 資訊處理系統驗收作業程序
16. imi8.3-01 病毒防制作業程序
17. imi8.4-01 備份及復原管理作業程序
18. imi8.5-01 網路連線管理作業程序
19. imi8.6-01 儲存媒體管理作業程序
20. imi8.7.4-01 安全電子郵件管理作業程序
21. imi9.1-01 個人工作職掌與資訊系統存取範圍作業程序
22. imi9.2-01 用戶存取管理作業程序
23. imi9.3-01 個人資訊安全作業程序
24. imi9.4-01 網路存取控制作業程序
25. imi9.5.1n9.5.2-01 作業系統安全作業程序
26. imi9.5.3n9.5.4-01 系統密碼申請作業程序
27. imi9.6-01 系統資源申請與原始碼型管作業程序
28. imi9.7-01 事件日誌管理作業程序
29. imi9.8-01 行動計算和遠端工作作業程序
30. imi10.2-01 應用軟體開發安全作業程序
31. imi11-01 業務永續運作管理作業程序
32. imi12.1-01 符合性管制作業程序
33. imi12.2n12.3-01 資訊安全內部稽核作業程序

中山科學研究院

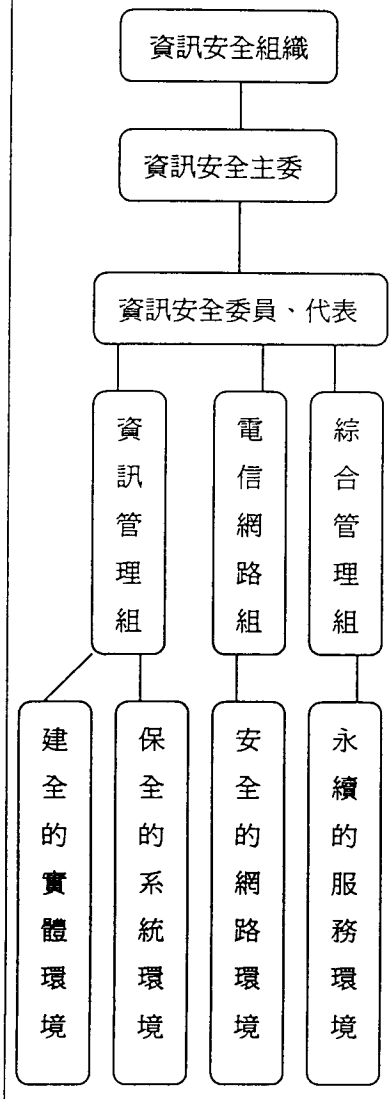
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全管理作業程序	imi3-01		

目的：管理階層承諾保証組織內資訊安全

範圍：本程序書所載資訊安全適用於中山科學研究院資訊管理中心

參考文件：中山科學研究院通信資訊安全推動執行委員會作業辦法

流程圖	權責	作業內容與步驟	表單
	主任 副主任、組長 資訊管理組組長 各組組長 資訊安全主委	1. 資訊安全組織架構 1.1 資管中心組織 1.2 資訊安全主委：主任(副主任爲代理人) 1.3 資訊安全委員：副主任、組長 1.4 資訊安全代表：資訊管理組組長 2. 資訊安全政策 建全的實體環境(委由資訊管理組負責) 安全的網路環境(委由電信網路組負責) 保全的系統環境(委由資訊管理組負責) 永續的服務環境(委由綜合管理組負責) 3. 資訊安全政策由本中心各組組長審查 4. 資訊安全政策由資訊安全主委核准 5. 前述審查應留下記錄	

中山科學研究院

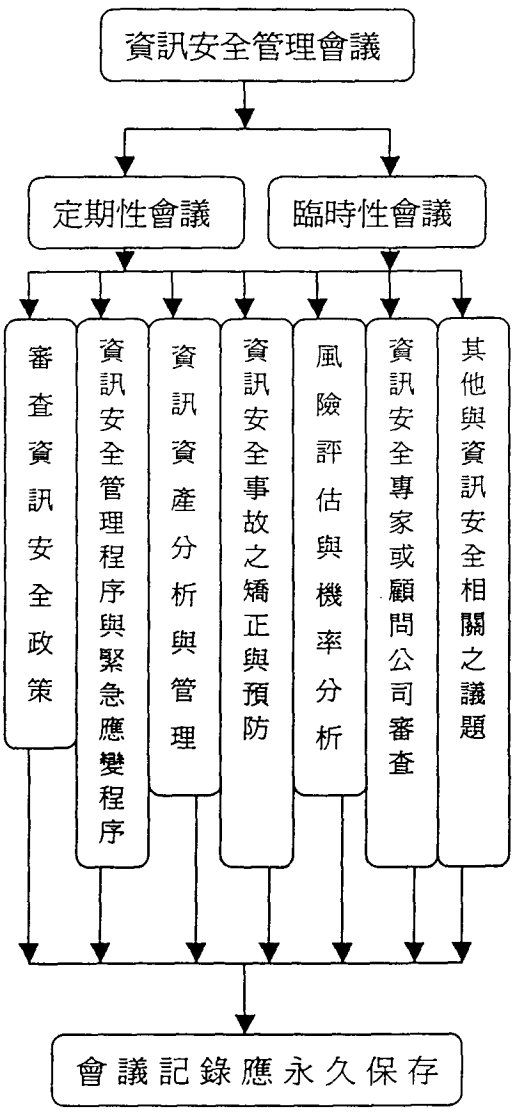
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全會議作業程序	imi4.1.1-01		

目的：管理組織內部資訊安全

範圍：中山科學研究院資訊管理中心

參考文件：

流程圖	權責	作業內容與步驟	表單
	資訊安全代表 資訊安全專家 顧問公司	1. 資訊安全管理會議 1.1 召集人：資訊安全代表 1.2 出席者：資訊安全委員，許可時應邀集外聘專家顧問公司與會。 1.3 定期性會議：每半年一次 1.4 臨時性會議：視須要舉行 1.5 會議內容 1.5.1 審查資訊安全政策。 1.5.2 資訊安全管理程序與緊急應變程序 1.5.3 資訊資產分析與管理：資訊資產權責分配表 1.5.4 資訊安全事故之矯正與預防 1.5.5 風險評估與機率分析 1.5.6 資訊安全專家或顧問公司審查 1.5.7 其他與資訊安全相關之議題 1.6 會議記錄應永久保存 2. 資訊安全稽核 2.1 必要時，本中心將邀請上級單位評審 2.2 必要時，本中心將邀請驗証公司評審	「矯正預防單」 「風險評估表」 「會議記錄」

中山科學研究院

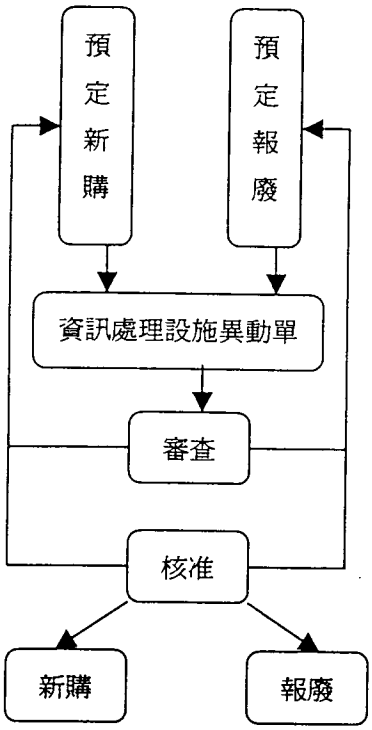
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊處理設施異動作業程序	imi4.1.4-01		

目的：資訊處理設施之新購(上線)、報廢下線之管制

範圍：凡本中心使用的資訊處理設施(硬體)均適用

參考文件：

流程圖	權責	作業內容與步驟	表單
	資訊安全代表 資訊安全代表	1. 新購上線應填寫「資訊處理設施異動單」 1.1 審查：資訊處理設施使用單位主管 1.2 核准：資訊安全代表 2. 報廢下線應填寫「資訊處理設施異動單」 2.1 審查：資訊處理設施使用單位主管 2.2 核准：資訊安全代表	「資訊處理設施異動單」 「資訊處理設施異動單」

中山科學研究院

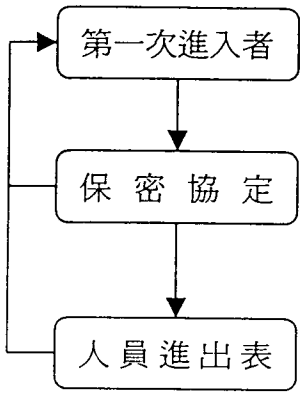
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	第三方存取管制作業程序	imi4.2-01		

目的：管控第三者存取組織資訊設施與資訊資產

範圍：非本中心聘顧之現場人員(組織)或經由網路連結進入本中心之人員(組織)

參考文件：

流程圖	權責	作業內容與步驟	表單
		1. 第一次進入者皆應簽署「保密協定」 2. 實際進入本中心之第三者應登錄於「人員進出表」 3. 透過網路連結，進入本中心維護各類資訊系統前，應提出申請表單	「保密協定」 「人員進出表」

中山科學研究院

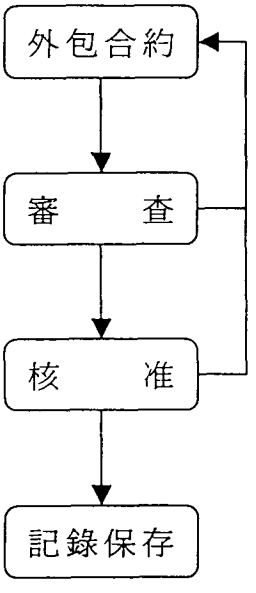
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	外包合約管制作業程序	imi4.3-01		

目的：管控本中心簽定外包合約之資訊安全事項。

範圍：硬體建置、軟體系統、研究計畫均屬之。

參考文件：

流程圖	權責	作業內容與步驟	表單
	資訊安全代表	1. 審查：由非合約執行單位 1. 1 審查內容： 符合法律、規章之要求、組織資訊安全風險評估、災難事故權責。 2. 核准:外包合約由資訊安全代表核准。 3. 記錄應永久保存	刻章 資訊安全－外包合約管制章 審查 | 核准 | 備註

中山科學研究院

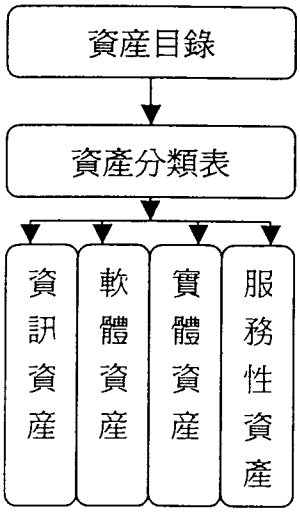
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資產分類管制作業程序	imi5-01		

目的：建立本中心資產目錄，並指定負責人，並對組織資產進行適當的保護

範圍：資訊資產、軟體資產、物質資產、服務

參考文件：行政院及所屬各機關資訊安全管理規範

流程圖	權責	作業內容與步驟	表單
	資訊安全代表 資訊安全主委	1. 資產目錄 資訊安全代表應負責建立「資產分類表」，以確保資產能被施以有效的保護。建立過程應確認每項資產及其所有權和安全分類，並據以施行不同級別的保護。 2. 資訊資產得有 2.1 資訊資產：資料庫和資料檔案、系統文件、使用者手冊、訓練教材、作業及支援程序、業務永續運作計劃、退守計劃、歸檔資訊； 2.2 軟體資產：應用程式軟體、系統軟體、開發工具以及公用程式； 2.3 實體資產：電腦設備（處理器、監視器、膝上型電腦、數據機）、通訊設備（路由器、PABX、傳真機、應答機）、磁媒體（磁帶和磁片）、其他技術設備（電源 、空調器）、家具、機房； 2.4 服務性資產：電腦及通訊服務、其他技術性服務（電源、空調）。	「資產分類表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資產分類管制程序	imi5-01		

目的：建立本中心資產目錄，並指定負責人，並對組織資產進行適當的保護

範圍：資訊資產、軟體資產、物質資產、服務

參考文件：行政院及所屬各機關資訊安全管理規範

流程圖	權責	作業內容與步驟	表單
	資訊安全代表 資訊安全主委	3.「資產分類表」應由資訊安全委員共同制定，資訊安全代表審查。 4.「資產分類表」結果應由資訊安全主委核准後實施。 5. 資訊資產安全等級：極機密性(AA)、機密性(A)、強敏感性(BB)、敏感性(B)及一般性(C)等三類。此分類每六個月定期檢視之，或依據存取控制政策進行更改 6. 資訊標識 根據「資產分類表」，每項資訊資產都應有明確的標記和處理資訊的妥善步驟 7. 資訊處理 說明該資產類別是否允許複製；儲存；通過郵寄、傳真和電子郵件、移動電話、語音郵件、應答機等交談方式進行傳輸進行傳輸；以及該類別的銷毀原則	「資產分類表」

中山科學研究院

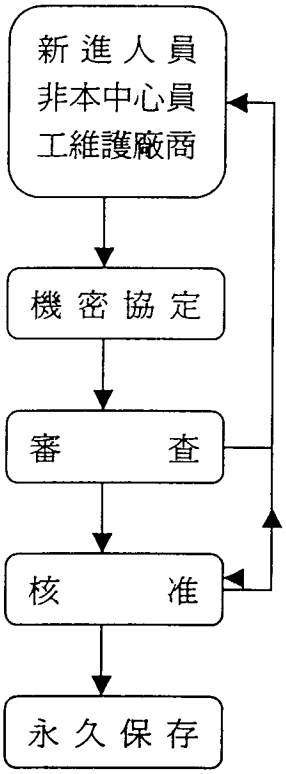
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	人員安全管理作業程序	imi6.1-01		

目的：防上操作錯誤、偷竊、詐騙或濫用設施等人為風險。

範圍：本中心聘人員、約雇人員；及凡第一次進入本中心具有安全顧慮(例如：承包商、工讀生、維修人員)者皆適用。

參考文件：

流程圖	權責	作業內容與步驟	表單
	新進人員	1. 本中心員工應依新進人員晉用辦法審查其資格，同時簽署「機密協定」留存。	「機密協定」
	非本中心員工	2. 非本中心員工，具有安全疑慮者，應要求簽署「機密協定」留存。	「機密協定」
	資訊安全代表	3.「機密協定」應由直屬主管審查及交資訊安全代表核准。	「機密協定」
	資管組	4.「機密協定」一式兩份，正本永久保存於資管組，影本交本人收執。	「機密協定」
	資訊安全代表	5. 本中心員工離職時，直屬主管應逐條審查該員工是否違反「機密協定」之規定，並提交資訊安全代表核准後方得離職。	「機密協定」
		6. 支援本中心資訊處理設備維運之維護廠商，必要時，應與本中心簽署「機密協定」，或在維護合約中加註機密條款。	「機密協定」
	資訊安全代表	7.「機密協定」應說明資訊安全責任，該責任由資管組制定，本中心各組組長審查，資訊安全代表核准，協定內容應每半年提交資訊安全會議討論內容修訂與增減。	「機密協定」

中山科學研究院

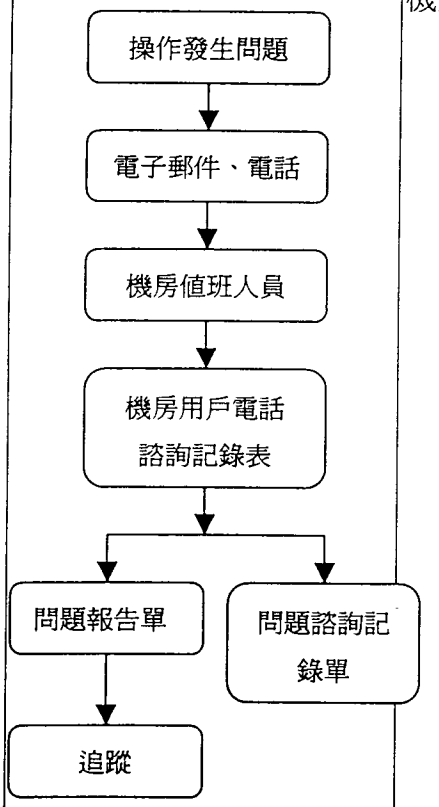
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	用戶問題諮詢作業程序	imi6.1-02		

目的：降低諮詢過程中的錯誤操作、詐騙與濫用等人為風險

範圍：本中心正職員工透過電子郵件或電話系統諮詢機房值班人員之過程。

參考文件：用戶問題諮詢作業程序

流程圖	權責	作業內容與步驟	表單
	機房值班人員	1、凡個人操作發生之無法解決問題，皆可以透過電子郵件或電話諮詢機房值班人員 2、機房值班人員應正確記錄諮詢日期時間、單位與姓名電話 3、諮詢之電話內容應分類填寫於「機房用戶電話諮詢記錄表」 4、該問題若能由值班人員協助解決，則應填寫解決方法與負責人於「機房用戶電話諮詢記錄表」內。同時登錄於「問題諮詢記錄單」 5、若該問題由值班人員無法解決，則應該另填於「問題報告單」繼續追蹤	「電子郵件」 「機房用戶電話諮詢記錄表」 「問題諮詢記錄單」 「問題報告單」

中山科學研究院

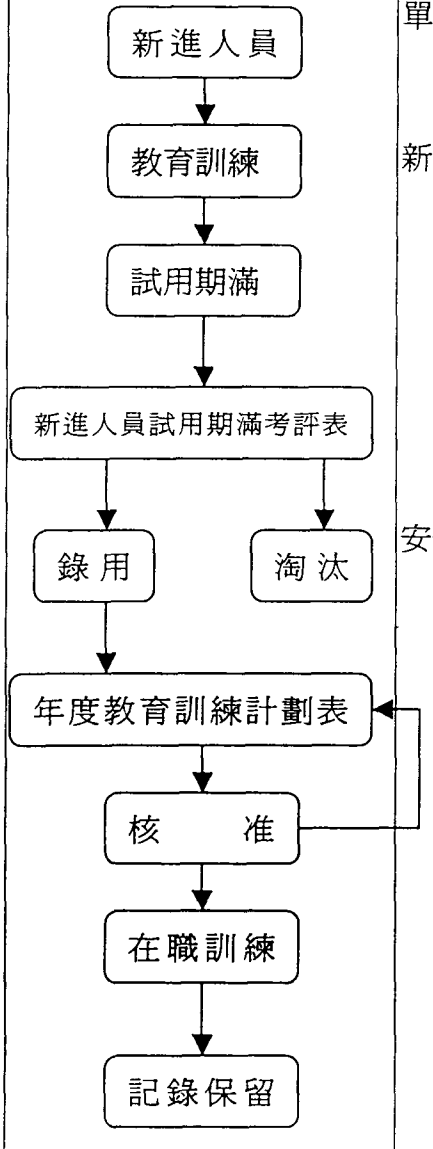
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	員工資訊安全教育訓練作業程序	imi6.2-01		

目的：爲保證員工瞭解資訊安全存在的威脅和問題，將可能風險降至最低

範圍：凡本中心全體同仁均適用之

參考文件：機房人員訓練程序與記錄

流程圖	權責	作業內容與步驟	表單
	單位主管 新進人員 安全主委	1. 各單位主管負有對所屬新進人員及在職員工之資訊安全教育訓練之義務。 2. 新進人員教育訓練：單位主管應指派資深人員指導，其內容包括、電腦設備之使用、作業標準、作業流程、作業安全。 3. 試用期滿呈報：主管於新進人員試用期滿後，填寫「新進人員試用期滿考評表」表示合格錄用。 4. 在職員工教育訓練： 4.1 資管組應於每年，擬定資訊安全教育訓練計畫，編成「年度教育訓練計劃表」，定案後呈安全主委核准，以爲內、外訓之依據。 4.2 受訓後之評核：在外受訓後應自結訓日起一週內連同（1）結訓証書或証明文件正本。（2）參考資料或教材。繳回行政組，以爲認可及記錄之依據。 4.3 單位主管應不定時主動觀察部屬受訓後之工作實際應用表現，作爲往後本中心資訊安全管理訓練是否可繼續執行之參考。	 「新進人員試用期滿考評表」 「年度教育訓練計劃表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	員工資訊安全教育訓練作業程序	imi6.2-01		

目的：爲保證員工瞭解資訊安全存在的威脅和問題，將可能風險降至最低

範圍：凡本中心全體同仁均適用之

參考文件：機房人員訓練程序與記錄

流程圖	權責	作業內容與步驟	表單
		4.4 內訓之執行：內訓爲內部開課，講師可分爲內聘講師、外聘講師及外訓回饋講師。受訓人員必須在「上課簽到表」上簽名，並將簽名單交至資管組備查。 5. 員工教育訓練記錄保留至員工離職爲止。	「上課簽到表」

中山科學研究院

資 訊 管 理 中 心

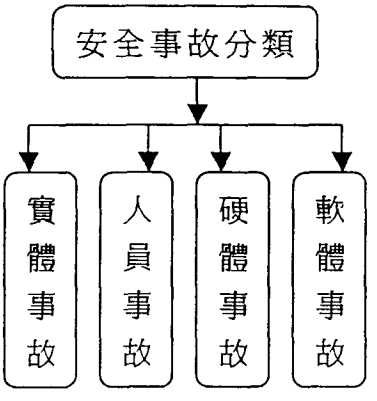
文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全事故矯正預防作業程序	imi6.3-01		

目的：降低資訊安全事故的再發率及增加資訊安全事故的預防率。

範圍：凡影響資訊安全事故事件者屬之。

參考文件：變更管理與問題管理程序。

流程圖	權責	作業內容與步驟	表單



1. 安全事故分類
   1.1 實體事故：建物、電力、環境(溫度、濕度、壓力)
   1.2 人員事故：破壞、竊盜、交接、代班
   1.3 硬體事故：主機、儲存媒體、網路設備、不斷電系統
   1.4 軟體事故：病毒、Bug、當機

2. 安全事故等級
   針對安全事故所牽連之資產分類等級劃分：
   (1)極嚴重、(2)嚴重、(3)重要、(4)一般。

3. 安全事故通報:通報層級如下表所示，

	上級	安全主委	安全代表	組長
極嚴重	通報	通報	通報	通報
嚴　重		通報	通報	通報
重　要			通報	通報
一　般				通報

4. 矯正措施
   4.1 任何安全事故發生後，應填寫「問題報告單」並應在 5 個工作天內完成矯正行動。

「問題報告單」

中山科學研究院

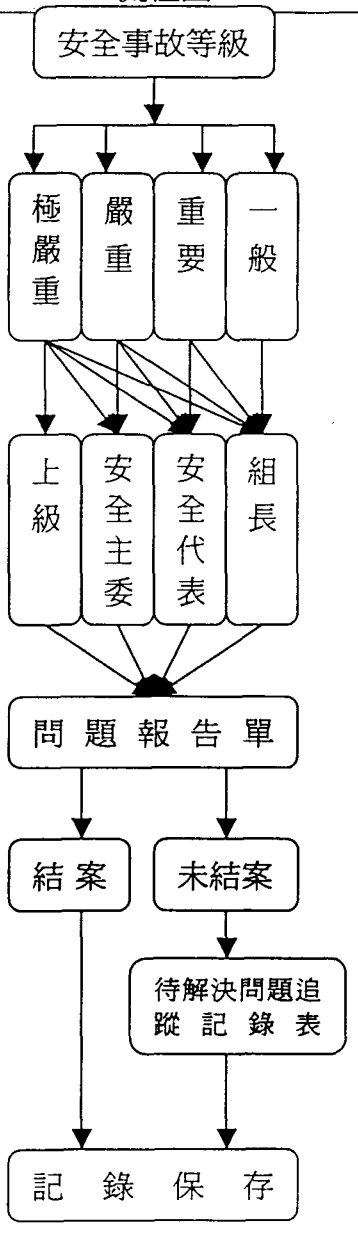
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全事故矯正預防作業程序	imi6.3-01		

目的：降低資訊安全事故的再發率及增加資訊安全事故的預防率。

範圍：凡影響資訊安全事故事件者屬之。

參考文件：變更管理與問題管理程序。

流程圖	權責	作業內容與步驟	表單
		4.2 問題無法在五個工作天內結案時，應繼續填寫「待解決問題追蹤記錄表」列管 . 預防措施 5.1 依資訊安全教育訓練辦法執行 5.2 不定期收集資訊安全相關報導傳閱 5.3 定期定點宣導資訊安全政策	「待解決問題追蹤記錄表」

中山科學研究院

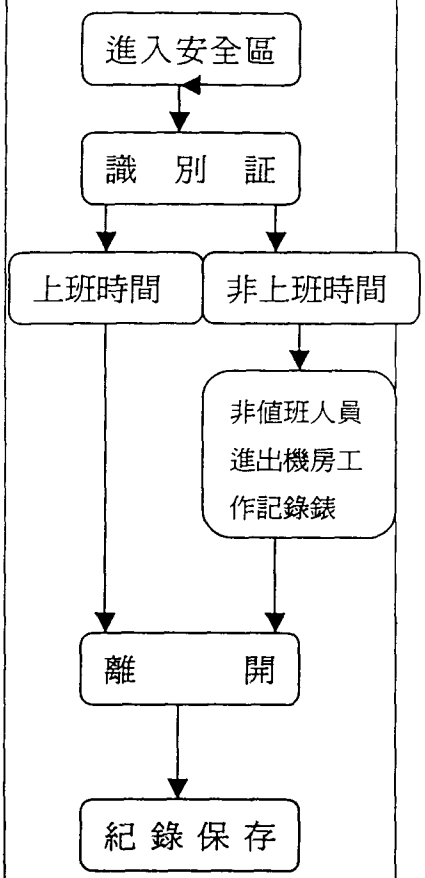
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全區管制作業程序	imi7.1-01		

目的：預防非法存取破壞干擾本中心資產

範圍：本院資訊管理中心安全隔離區

參考文件：廠商進出機房管理規定暨附件一廠商配合規定事項

流程圖	權責	作業內容與步驟	表單
		1. 安全區：主任辦公室，一樓機房，及所有資產存放位置。 2. 進入安全區 2.1 上班時間：應配掛識別証，訪客及維修廠商須有陪同人員，並應登記進入日期時間以及行程目的 2.2 非上班時間：應按規定配掛識別證外，並應登錄於「非值班人員進出機房工作記錄錶」 3. 離開安全區:訪客及維修廠商須有陪同人員在旁督導或學習，陪同人員應稽核其敏感資訊的存取和資訊設備的使用，並應登記離開日期時間，同時須把相關作業內容或解決方法詳載於工作日誌內 4. 安全保障 4.1 必要時，安全區內「資產配置圖」，應加以核准後方可放置相關設備 。	「非值班人員進出機房工作記錄錶」 「資產配置圖」

中山科學研究院

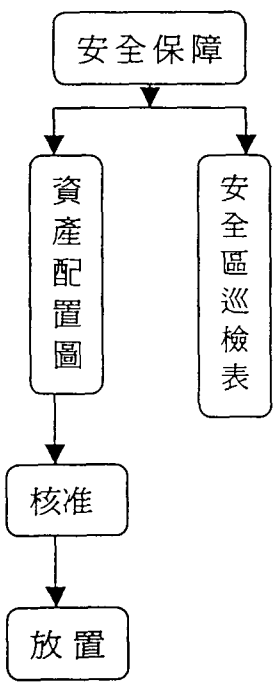
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全區管制作業程序	imi7.1-01		

目的：預防非法存取破壞干擾本中心資產

範圍：本院資訊管理中心安全隔離區

參考文件：廠商進出機房管理規定暨附件一廠商配合規定事項

流程圖	權責	作業內容與步驟	表單
		4.2 應不定時巡查安全區並填寫「安全區巡檢表」 4.2.1 辦公事務機（影印機、傳真機、長途國際電話）是否未經授權使用 4.2.2 門窗關開情形 4.2.3 監視系統 4.2.4 借測與借用設備 4.2.5 組織相關資訊(公告欄等) 4.2.6 發電機燃油等危險物品 1. 應急設備與備份媒體的位置 5.加班或假日之突發緊急作業，需進入安全區時，仍應規定填寫機房工作日誌並直接取用緊急應變鑰匙操作，但需事後補核備	「安全區巡檢表」

中山科學研究院

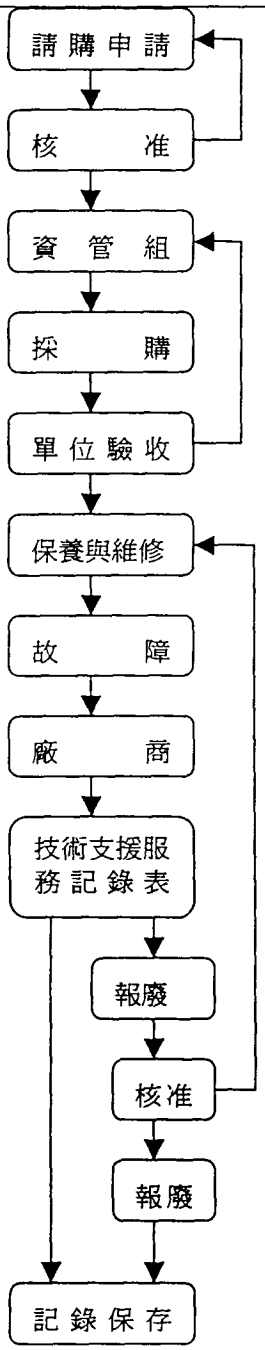
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊處理設備管理作業程序	imi7.2.4-01		

目的：爲確保資訊處理設備性能並符合操作使用

範圍：凡本中心所使用之電腦設備均屬之

參考文件：

流程圖	權責	作業內容與步驟	表單
	行政組 資管組 資管組	1. 行政組負責資訊設備之管理及保養維護。 2. 資管組負責資訊設備之採購及故障之送修。 3. 資訊設備 3.1 資訊設備之申購、驗收及管理 3.1.1 使用單位依需求提出申購，填寫「請購申請書」，由資管組負責採購。 3.1.2 使用單位依申購單規格書或合約書內容進行驗收，由資管組會同使用單位進行驗收，並將驗收結果寫於「請購申請書」上。 3.2 相關資訊設備應具有操作說明書或使用手冊。 3.3 資訊設備之保養與維修 3.3.1 資訊設備之保養項目及週期，依資訊設備檢查表進行保養。 3.3.2 資訊設備故障時，由資管組進行故障排除，如排除無效時即通知廠商進行維修，維修時應填寫「技術支援服務記錄表」。	 「請購申請書」 「技術支援服務記錄表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊處理設備管理作業程序	imi7.2.4-01		

目的：爲確保資訊處理設備性能並符合操作使用

範圍：凡本中心所使用之電腦設備均屬之

參考文件：

流程圖	權責	作業內容與步驟	表單
		3.4 資訊設備之報廢 3.4.1 資訊設備在維修無效或不堪使用時才可提出報廢 3.4.2 資訊設備報廢時需填寫「報廢單」說明報廢原因，資訊安全代表或代理人核准方可報廢 3.4.3 相關記錄需保存備查	「報廢單」

中山科學研究院

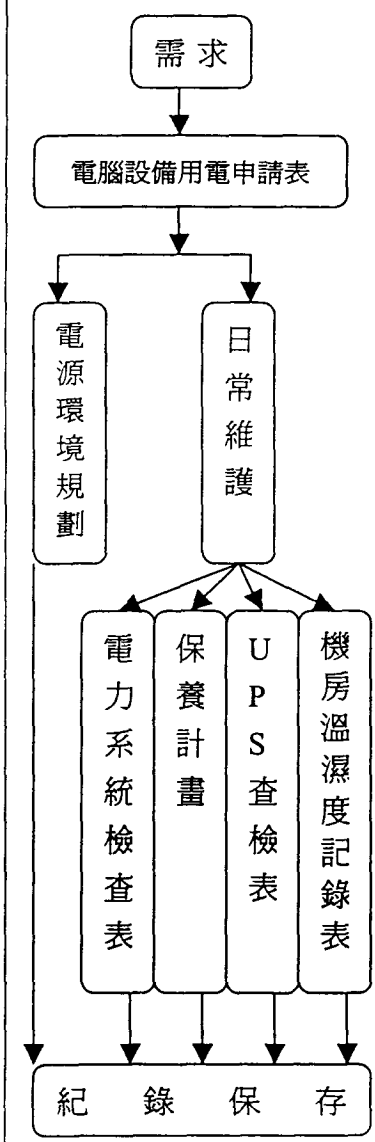
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊環境安全管理作業程序	imi7.2n7.3-01		

目的：維持資產儲放地點之穩定維運環境

範圍：電源、通訊、空調、給水、消防

參考文件：

流程圖	權責	作業內容與步驟	表單
		1、電源系統 1.1 電腦機房內各項設備安裝使用前，須先填妥「電腦設備用電申請表」 1.2 電源環境規劃 1.2.1 電腦設備用電應獨立迴路，並加裝不斷電系統，必要時應添購發電機。 1.2.2 資管中心應規劃獨立的接地系統與避雷針。 1.2.3 所有電腦主機與儲存媒體之機構外殼應有接地端，必要時應加裝漏電斷路器。 1.2.4 安全區內禁止吸煙，並應放置效期正常之滅火器數個。 1.3 日常維護 1.3.1 資管組應負責每日依「電力系統檢查表」查檢電力系統。 1.3.2 電力設備應與供應商簽定保養計畫：包括絕緣試驗、控制迴路、接地設施等。 1.3.3 資管組應負責每日依「UPS 查檢表」，查檢 UPS 系統。	「電腦設備用電申請表」 電力系統檢查表」 「UPS 查檢表」

中山科學研究院

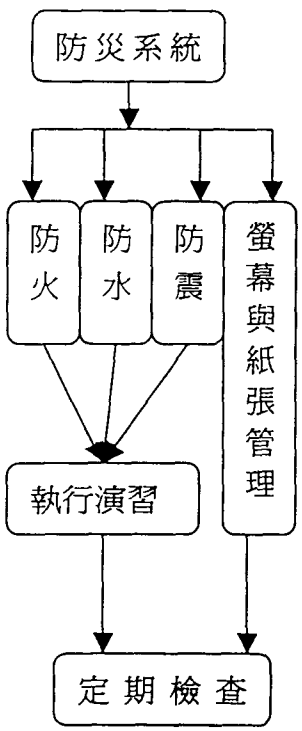
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊環境安全管理程序	imi7.2n7.3-01		

目的：維持資產儲放地點之穩定維運環境

範圍：電源、通訊、空調、給水、消防

參考文件：

流程圖	權責	作業內容與步驟	表單
		1.3.4 資管組應負責每日檢測填寫「機房溫濕度記錄表」。 2、防災系統 2.1 防火 2.1.1 必要時，電腦機房應使用防火建材、煙霧偵測警報器，並配備消防給水系統。 2.1.2 每一個電腦主機五公尺範圍內，應配備滅火器。 2.1.3 必要時，電腦機房應備有防火閘門與排煙出口。 2.1.4 所有逃生路線應備有緊急照明燈。 2.1.5 資訊安全代表應定期執行消防演習，其中消防水管與灑水管路應每三個月通水一次。 2.2 防水 2.2.1 必要時，高架地板下面與應佈建排水系統。 2.2.2 必要時，應添購緊急抽水設備。 2.2.3 資管中心建築外圍，應儲存足夠之防水砂包。	「機房溫濕度記錄表」

中山科學研究院

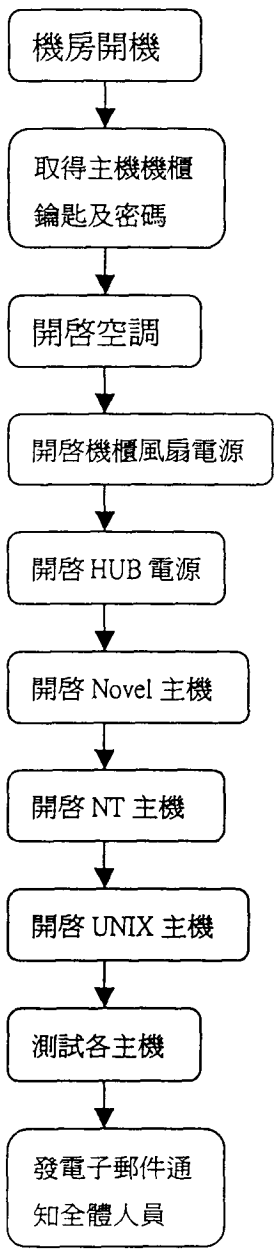
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	機房開關機作業程序	imi8.1-01		

目的：保證資訊處理系統的操作安全無誤

範圍：管制所有資訊處理設施之操作手冊制定，發行、保存與責任劃分

參考文件：

流程圖	權責	作業內容與步驟	表單
		1　機房開機 1.1 取得主機機櫃鑰匙及密碼 1.2 開啓空調 1.3 開啓機櫃風扇電源 1.4 開啓 HUB 電源 1.5 開啓 Novel 主機 1.6 開啓 NT 主機：PDC，BDC，獨立主機（file server, Exchange...） 1.7 開啓 UNIX 主機：請依照 UNIX 主機開機步驟 1.8 測試各主機是否可正常運作 1.9 發電子郵件通知全體人員	

中山科學研究院

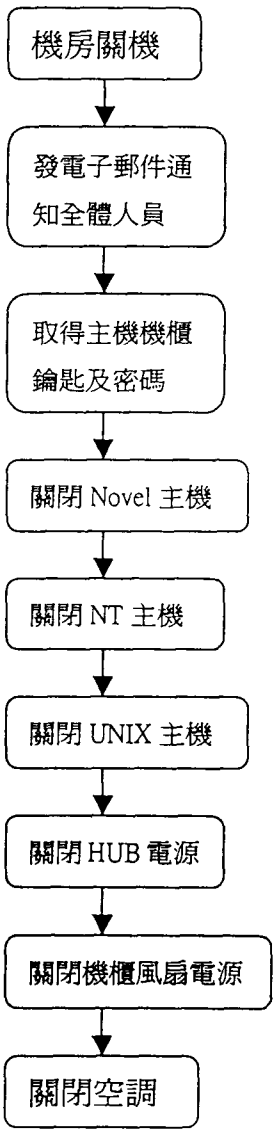
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	機房開關機作業程序	imi8.1-01		

目的：保證資訊處理系統的操作安全無誤

範圍：管制所有資訊處理設施之操作手冊制定，發行、保存與責任劃分

參考文件：

流程圖	權責	作業內容與步驟	表單
		2　機房開機 2.1　關機前發信通知全體人員 2.2　關機前，確信取得主機密碼機櫃鑰匙 2.3　關閉 Novel 主機 2.4　關閉 NT 主機：獨立主機（file server, Exchange...），BDC， PDC 2.5　關閉 UNIX 主機：請依照 UNIX 主機關機步驟 2.6　關掉 HUB 電源 2.7　關掉機櫃風扇電源 2.8　關掉空調	

中山科學研究院

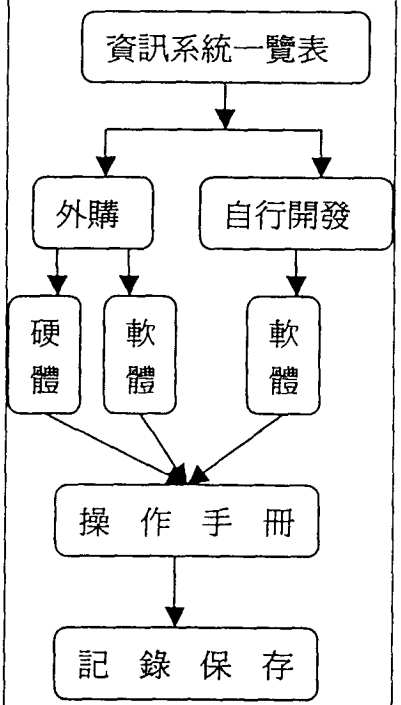
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊處理系統驗收作業程序	imi8.2-01		

目的：保證資訊處理系統的操作安全無誤

範圍：管制所有資訊處理設施之操作手冊制定，發行、保存與責任劃分

參考文件：

流程圖	權責	作業內容與步驟	表單
		1 本中心使用之資訊處理系統應載入「資訊系統一覽表」，並應管制其版本狀態 2 外購之硬體資訊處理系統應由廠商提供一般使用操作手冊與系統管理操作手冊 2.1 驗收程序依採購合約執行 2.2 合約表應載明系統升級方式與未來容量需求規劃 3 外購之軟體資訊處理系統應由廠商提供操作手冊 3.1 驗收程序依採購合約執行 3.2 合約表應載明系統升級方式與未來容量需求規劃 4 本中心自行開發設計之軟體系統，應撰寫操作手冊。 4.1 開發階段：應使用個人或組內電腦設備 4.2 測試階段：應使用專門測試用電腦設備 4.3 操作階段：應使用對（內/外）主機 4.4 階段轉移前應進行備份並應由資訊安全代表核准	「資訊系統一覽表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊處理系統操作手冊管理作業程序	imi8.1n8.2-01		

目的：保證資訊處理系統的操作安全無誤

範圍：管制所有資訊處理設施之操作手冊制定，發行、保存與責任劃分

參考文件：

流程圖	權責	作業內容與步驟	表單
		5　操作手冊應視爲組織資產的一部份，並納入交接 6　相關記錄應加以保存	

中山科學研究院

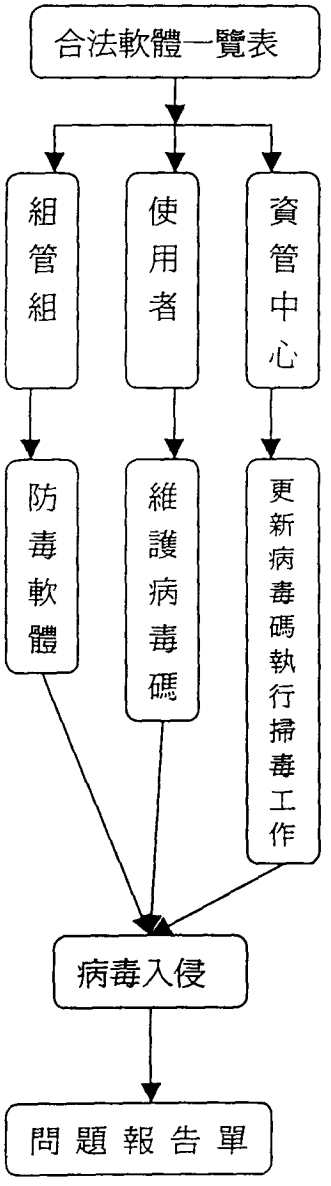
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	病毒防制作業程序	imi8.3-01		

目的：保護軟體和資訊的完整性

範圍：本中心所有桌上型暨攜帶型個人電腦與伺服器

參考文件：

流程圖	權責	作業內容與步驟	表單
	組管組 使用者 資管中心	1、本中心禁止使用非法軟體，中心應維持「合法軟體一覽表」 2、組管組負責本中心所有個人電腦防毒軟體之安裝與維護。 3、安裝於個人電腦之防毒軟體應由使用者維護病毒碼最新狀態。 4、伺服器防毒工作應由資管中心負責，除定期更新病毒碼資訊，應在每日下班後，執行一次掃毒工作。 5、資管中心應隨時注意最新病毒訊息，並公告週知。 6、遇有病毒入侵事件時，需要時，應填寫「問題報告單」。	「合法軟體一覽表」 「問題報告單」

中山科學研究院

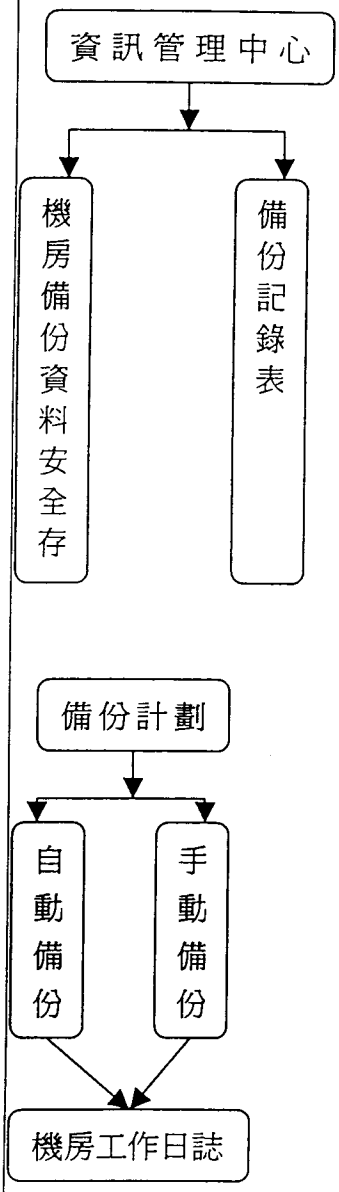
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	備份及復原管理作業程序	imi8.4-01		

目的：維持資訊系統的完整性和可用性

範圍：系統軟體、程序資料、工作日誌

參考文件：管理資訊系統檔案備份與回復作業程序

流程圖	權責	作業內容與步驟	表單
	資訊管理中心	1、資訊管理中心應維持「機房備份資料安全存放表單」以及「備份記錄表」，並定期更新。 2、備份計劃 2.1 自動備份：權責人員應負責自動化備份程式的穩定性，並記錄於「機房工作日誌」保存備查。 2.2 手動備份：權責人員應負責定期執行備份工作，並記錄於「機房工作日誌」保存備查。 3、備份等級 3.1 嚴格備份：異地備份，距離十公里以上，兩組備份以上。 3.2 中級備份：異地備份，距離一公里以上，備份一組。 3.3 基本備份：本地備份，備份一組。	「機房備份資料安全存放表單」 「備份記錄表」 「機房工作日誌」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	備份及復原管理作業程序	imi8.4-01		

目的：維持資訊系統的完整性和可用性

範圍：系統軟體、程序資料、工作日誌

參考文件：管理資訊系統檔案備份與回復作業程序

流程圖	權責	作業內容與步驟	表單
		4、復原備份演練 4.1 資管組應定期檢查備份資料的完整性。 4.2 資管組應定期檢查備份環境的穩定性。 4.3 資訊安全代表應不定期稽核備份復原能力，並比對工作日誌。 5、結束	

中山科學研究院

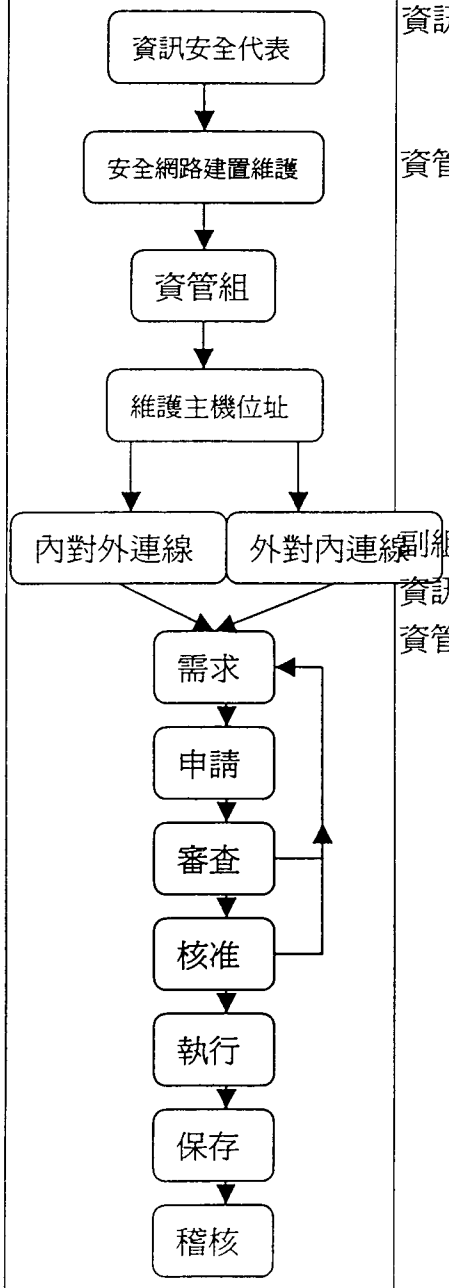
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	網路連線管理作業程序	imi8.5-01		

目的：提供透過網路存取資源時的安全性

範圍：由組織內到外之連網及從組織外到內之連網

參考文件：

流程圖	權責	作業內容與步驟	表單
	資訊安全代表 資管組 副組長 資訊安全代表 資管組	1. 資訊安全代表應負責安全網路環境之建置與維護。 2. 資管組應維護主機位址一覽表，並隨時保持最新狀態。 3. 由內對外連線 3.1 需求：電子郵件、應用程式、瀏覽特定網站等。 3.2 申請：由需求人員填寫申請表。 3.3 審查：副組長以上部門主管。 3.4 核准：資訊安全代表。 3.5 執行：資管組人員執行設定、核發帳號密碼、使用權限等工作，並通知需求者。 3.6 保存：資管組人員將申請表歸檔備查。 4. 由外對內連線 4.1 需求：凡可藉由網路簽入主機系統、應用軟體等需求。 4.2 申請：由需求人員填寫申請表。 4.3 審查：部門主管與資訊安全代表。 4.4 核准：資訊安全主委。	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	網路連線管理作業程序	imi8.5-01		

目的：提供透過網路存取資源時的安全性

範圍：由組織內到外之連網及從組織外到內之連網

參考文件：

流程圖	權責	作業內容與步驟	表單
		4.5 執行：資管組人員執行設定、核發帳號密碼、使用權限等工作，並通知需求者。 4.6 保存：資管組人員將申請表歸檔備查。 4.7 稽核：資管主人員應定期查核使用撞狀況。 5.應用服務連線政策 5.1Web Proxy 5.1.1 No access 5.1.2 Allow authenticated access from inside out. Deny all access from outside 5.1.3 Allow authenticated access from inside out. Allow authenticated access from outside to internal servers 5.1.4 Allow access from inside out. Deny all access from outside. 5.1.5 Allow access from inside out. Allow authenticated access from outside to internal servers. 5.2 FTP Proxy 5.2.1 For Inside Users: 5.2.1.1 No access 5.2.1.2 Allow authenticated "GETs" only 5.2.1.3 Allow authenticated "GETs" and authenticated "PUTs" 5.2.1.4 Allow "GETs" 5.2.1.5 Allow "GETs" and authenticated "PUTs"	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	網路連線管理作業程序	imi8.5-01		

目的：提供透過網路存取資源時的安全性

範圍：由組織內到外之連網及從組織外到內之連網

參考文件：

流程圖	權責	作業內容與步驟	表單
		5.2.1.6 Allow "GETs" and "PUTs" 5.2.2 For Outside Users: 5.2.2.1 No access 5.2.2.2 Allow authenticated "GETs" and "PUTs" 5.3 Telnet Proxy 5.3.1No access from inside or outside 5.3.2Allow authenticated access from inside out. Deny access from outside. 5.3.3 Allow authenticated access from inside out. Allow authenticated access from outside. 5.3.4Allow access from inside out. Deny access from outside. 5.3.5Allow access from inside out.Allowonly authenticated access from outside.	

中山科學研究院

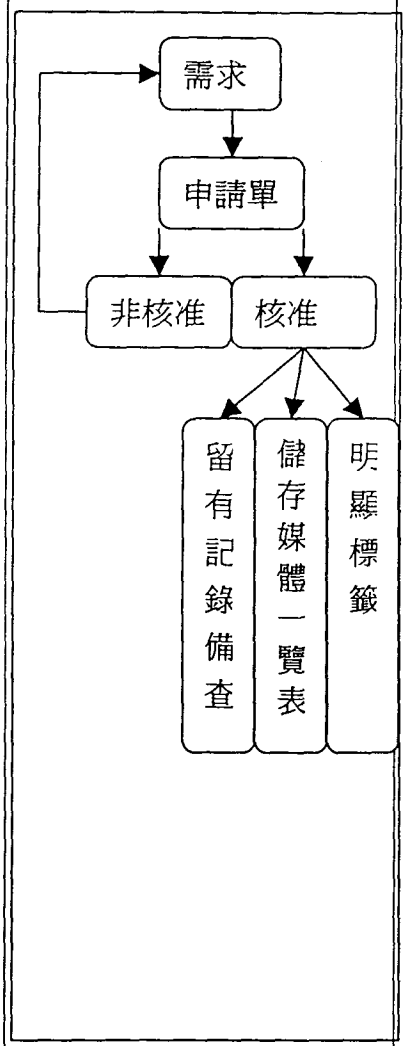
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	儲存媒體管理作業程序	imi8.6-01		

目的：有效掌握儲存媒體之使用記錄與管理

範圍：電子儲存媒體：磁碟機、燒錄機、光碟片、磁帶、軟磁片。

參考文件：電腦設備實體防護、存取控制與資料安全保密措施規定

流程圖	權責	作業內容與步驟	表單
		1、擁有儲存媒體之需求人員均應提出申請並填寫申請單 2、非本中心核發管制之儲存媒體禁止攜入安全範圍內 3、本中心核發儲存媒體應由資管組登錄於「儲存媒體一覽表」 4、本中心核發與使用中之儲存媒體應有明顯標籤以爲識別 5、人員異動時，儲存媒體列入交接 6、本中心核發儲存媒體非經副組長以上主管核准，並留有記錄備查，禁止攜出資管中心 7、儲存媒體維修、報廢應經副組長以上主管核准，並留有記錄備查 8、任何磁帶、磁片、光碟、硬碟等媒體進出資訊室，需向媒體管理人員提出申請 9、電腦使用者未經核准，不得裝置使用抽取式硬碟，原則上一台電腦一個內裝硬碟	「儲存媒體一覽表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	儲存媒體管理作業程序	imi8.6-01		

目的：有效掌握儲存媒體之使用記錄與管理

範圍：電子儲存媒體：磁碟機、燒錄機、光碟片、磁帶、軟磁片。

參考文件：電腦設備實體防護、存取控制與資料安全保密措施規定

流程圖	權責	作業內容與步驟	表單
		10、檔案訊息交換，應利用網路及電子郵件進行作業，本中心人員未經核准，不得經由媒體或其他網路傳輸方式攜出管制資料 11、所有電腦皆應裝置防毒軟體，並設定由硬碟開機，以避免病毒感染。郵件伺服器與檔案伺服器應安裝防毒軟體，以杜絕網路病毒侵入	「儲存媒體一覽表」

中山科學研究院

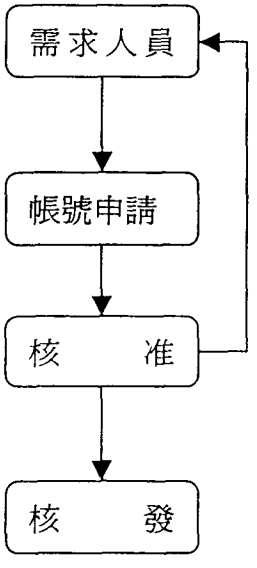
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	安全電子郵件管理作業程序	imi8.7.4-01		

目的：避免電子郵件產生資訊安全風險

範圍：本中心郵件主機所有登錄帳號均屬

參考文件：

流程圖	權責	作業內容與步驟	表單
	副組長	1. 帳號申請：需求人員填寫申請單，經副組長以上主管核准，交由資管組設定帳號、密碼與信箱空間容量。	
	資管組	2. 發送信件 2.1 非 WEBMAIL 系統：需要時，資管組應加以攔截存檔，以備事後追查之需。 2.2 WEBMAIL 系統：需要時，資管組應加以限制使用來發送郵件，僅允許可以收取郵件。	
		3. 禁止利用內部網路散發與工作內容無關之訊息。	
	資管組	4. 資管組應負責安裝郵件主機防毒軟體，並定期檢查病毒碼更新狀況。	
	資管組	5. 資管組應加強宣導，郵件附加檔之存取，避免危急電腦系統。	

中山科學研究院

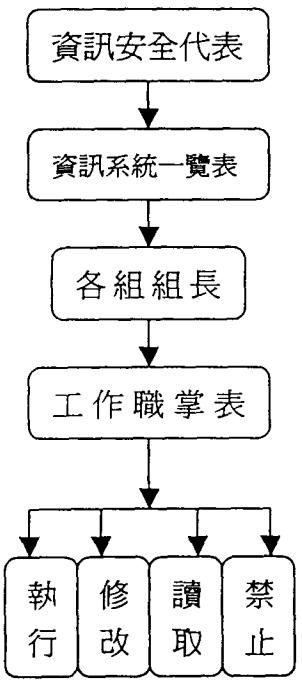
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	個人工作職掌與資訊系統存取範圍作業程序	imi9.1-01		

目的：控制對資訊系統的存取，應該根據既定的職掌範圍加以監控

範圍：本中心正職員工與本中心資訊系統

參考文件：

流程圖	權責	作業內容與步驟	表單
	組長	1. 各組組長應負責訂定組內正職員工之「工作職掌表」，並隨時保持最新狀態。	「工作職掌表」
		2.「工作職掌表」應在新人試用期滿後一個月內建立。	「工作職掌表」
	資訊安全代表	3. 資訊安全代表應負責訂定本中心在役之「資訊系統一覽表」，並隨時保持最新狀態	「資訊系統一覽表」
		4. 基本上，本中心資訊系統使用權限區分爲：執行、修改、讀取、禁止等四項權限	
		5. 個人工作內容涉及資訊系統使用與資料存取時，應在「個人工作職掌表」內載明	個人工作職掌表」
	資訊安全代表	6. 上述載明，應由資訊安全代表核准，同時註記於「資訊系統一覽表」內	「資訊系統一覽表」
		7. 結束	

中山科學研究院

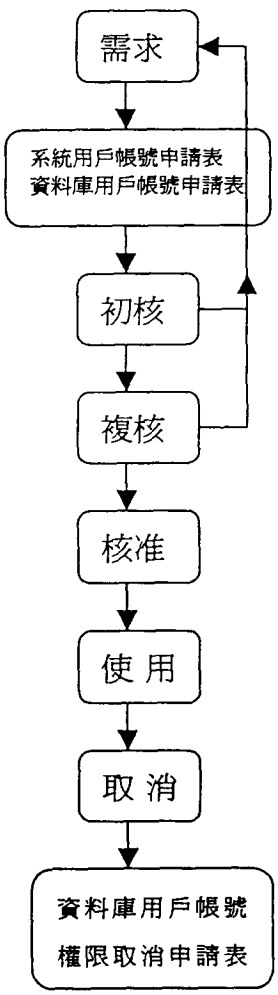
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	用戶存取管理作業程序	imi9.2-01		

目的：管理資訊系統存取許可權與服務

範圍：作業系統、資料庫系統、工作目錄、資訊處理系統等，應註冊方可取得授權使用者皆是。

參考文件：電腦設備實體防護、存取控制與資料安全保密措施規定

流程圖	權責	作業內容與步驟	表單
	系統發展小組 作業環境小組 系統管理者	1. 作業系統：申請 1.1 帳號申請應填寫「系統用戶帳號申請表」。 1.2 初核：系統發展小組負責。 1.3 複核：作業環境小組負責。 1.4 核准：系統管理者。 2. 資料庫系統：申請 2.1 帳號申請應填寫「資料庫用戶帳號申請表」。 2.2 初核：系統發展小組負責。 2.3 複核：作業環境小組負責。 2.4 核准:作業環境資料庫管理者。 3. 資料庫系統：取消 3.1 資料庫帳號取消應填寫「資料庫用戶帳號權限取消申請表」 3.2 查核：作業環境資料庫管理者 4. 工作目錄 4.1 工作目錄使用權限、名稱、容量，應填寫「工作目錄申請表」 4.2 初核：系統發展小組 4.3 複核：作業環境小組 4.4 核准：系統管理者 4.5 記錄：系統管理者應將使用者申請過程，填寫於「工作目錄申請處理記錄」	「系統用戶帳號申請表」 「資料庫用戶帳號申請表」 「 資料庫用戶帳號權限取消申請表」 「工作目錄申請表」 「工作目錄申請處理記錄」

中山科學研究院

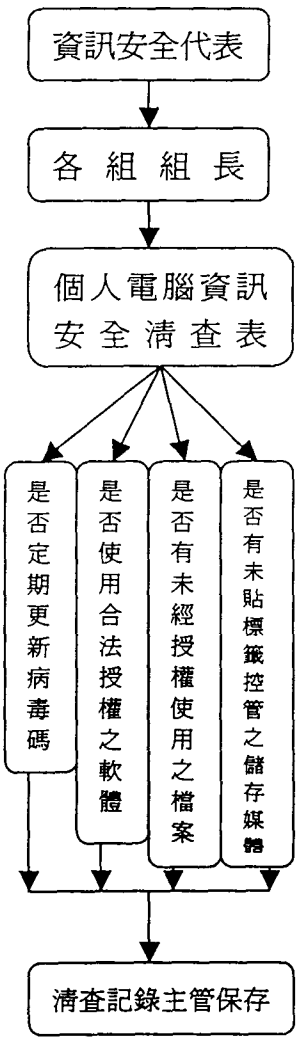
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	個人資訊安全作業程序	imi9.3-01		

目的：防止非法的存取本中心相關資訊資源

範圍：本中心正職員工

參考文件：

流程圖	權責	作業內容與步驟	表單
	資訊安全代表	1. 資訊安全代表應責成各組組長，每半年清查每一正職員工所使用之個人電腦，包括攜帶式電腦設備。 2. 清查內容包括： 2-1 是否定期更新病毒碼。 2-2 使否使用合法授權之軟體。 2-3 是否有未經授權使用之檔案資料(資訊系統產生者)。 2-4 是否有未貼標籤控管之儲存媒體。 3. 清查記錄應由組長以上主管保存半年以上。 4.結束	「個人電腦資訊安全清查表」

中山科學研究院

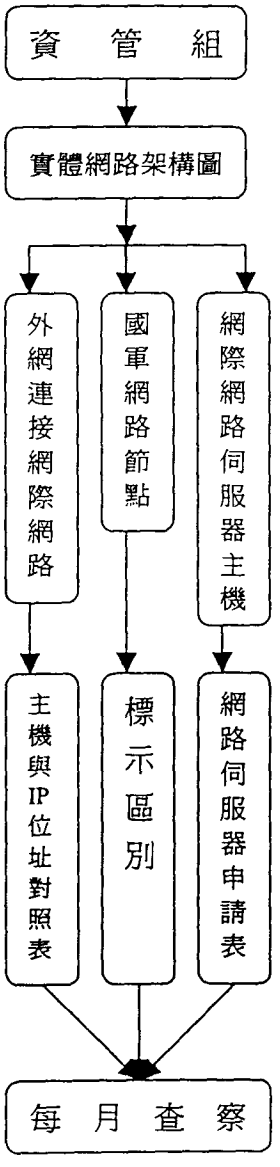
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	網路存取控制作業程序	imi9.4-01		

目的：保護網路化服務並控制對內外網路服務的存取。

範圍：本中心網路所轄之國軍網路(內網)與網際網路(外網)。

參考文件：

流程圖	權責	作業內容與步驟	表單
	資管組	1. 資管組應維護本中心「實體網路架構圖」，並隨時保持最新狀態備查。	「實體網路架構圖」
	資管組	2. 資管組應維護本中心外網連接網際網路之「主機與 IP 位址對照表」。	「主機與 IP 位址對照表」
		3. 連接國軍網路節點與網際網路節點之主機或個人電腦應明顯標示區別。	
		4. 網際網路伺服器主機，除 DNS 和 MAIL 外，皆須填寫「網路伺服器申請表」，經審查核准後方可建立。	「網路伺服器申請表」
	資管組	5. 資管組每月應查察中心電腦主機與個人電腦是否逾越內外網連線之使用範圍。	
	資管組	6. 資管組每月應查察中心伺服器主機是否逾越內外網服務之使用範圍。	
		7. 結束	

中山科學研究院

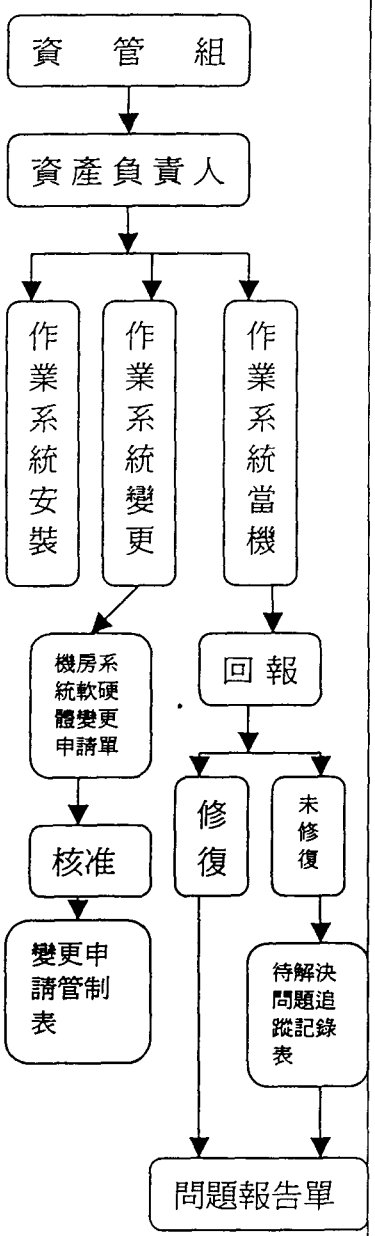
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	作業系統安全作業程序	imi9.5.1n9.5.2-01		

目的：維護本中心工作站電腦主機系統安全。

範圍：本中心個人電腦外之工作站級電腦主機系統。

參考文件：變更管理與問題管理程序。

流程圖	權責	作業內容與步驟	表單
	資管組 資產負責人	1. 資管組權責人員應負責工作站電腦主機作業系統安裝 1.1 作業系統安裝 資產負責人應確認作業系統安裝版本之正確及系統光碟儲放位置，內外網路連線是否依規定，電腦主機規格是否與合約所列相符 2. 作業系統變更 2.1 因需求要升級改版變更工作站電腦主機，應填寫「機房系統軟硬體變更申請單」，經權責人核准後執行 2.2 作業系統變更後，權責人員應填寫「變更申請管制表」 3. 作業系統當機 3.1 當機時，應依「資訊安全事故矯正預防作業程序」，回報管理階層 3.2 修復時，應由被授權的人員執行回復工作，並填寫「問題報告單」 3.3 當機問題無法解決時，應填寫「待解決問題追蹤記錄表」列管，直到系統恢復	 「機房系統軟硬體變更申請單」 「變更申請管制表」 「資訊安全事故矯正預防作業程序」 「問題報告單」 「待解決問題追蹤記錄表」

中山科學研究院

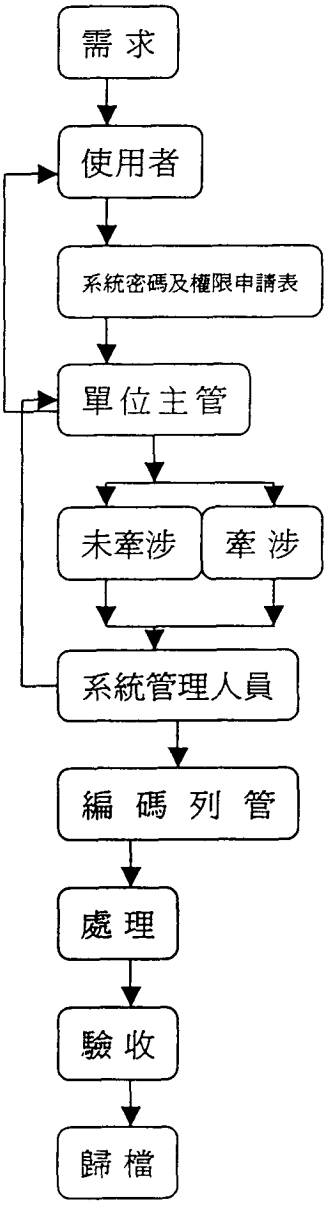
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	系統密碼申請作業程序	imi9.5.3n9.5.4-01		

1. 目的：登錄所有用戶於各類型多使者資訊系統之專用唯一識別字，以便操作者能夠追蹤具體的使用者責任。

範圍：本中心個人電腦外之工作站級電腦主機系統。

參考文件：變更管理與問題管理程序。

流程圖	權責	作業內容與步驟	表單
	使用者 資管組	1. 使用者於需求發生時，應填寫「系統密碼及權限申請表」；並詳述問題 (可以附件方式說明)，以利系統管理人員處理。 2. 申請表填寫完畢，應呈報其單位主管並請單位主管簽名 3. 若使用者之需求有牽涉到其他部門之業務範圍，使用者須要會簽該部門；經該部門會簽同意始可將申請表送達系統管理人員，若不同意則退回原申請人 4. 系統管理人員需視實際狀況，確認主管簽章或會簽部門主管簽章是否完整方可作業；否則應予以退件。並要求申請人完成步驟 2 及步驟 3 再行送件 5. 當系統管理人員確認該單據可收件後，應先行編碼列管 6. 資管組主管於接到使用者之需求，視其業務性質分配予系統管理人員處理	「系統密碼及權限申請表」

文件類別	名　稱	文件編號	發行日期	頁次
程序書	系統密碼申請作業程序	imi9.5.3n9.5.4-01		

2. 目的：登錄所有用戶於各類型多使者資訊系統之專用唯一識別字，以便操作者能夠追蹤具體的使用者責任。

範圍：本中心個人電腦外之工作站級電腦主機系統。

參考文件：變更管理與問題管理程序。

流程圖	權責	作業內容與步驟	表單
	使用者	7. 系統管理人員於受理後，立即確認該需求的起始及結束時間表，與申請人充份溝通；如無法達到申請者的需求時，應請求主管裁奪協調 8. 系統管理人員工程師處理完畢請使用者確認，若使用者確認無誤；則請使用者簽名確認。若使用者確認有問題，則退回系統管理人員重審處理。使用者簽名確認後，送交 MIS 部門主管審核；無誤即歸檔	
	資管組		

中山科學研究院

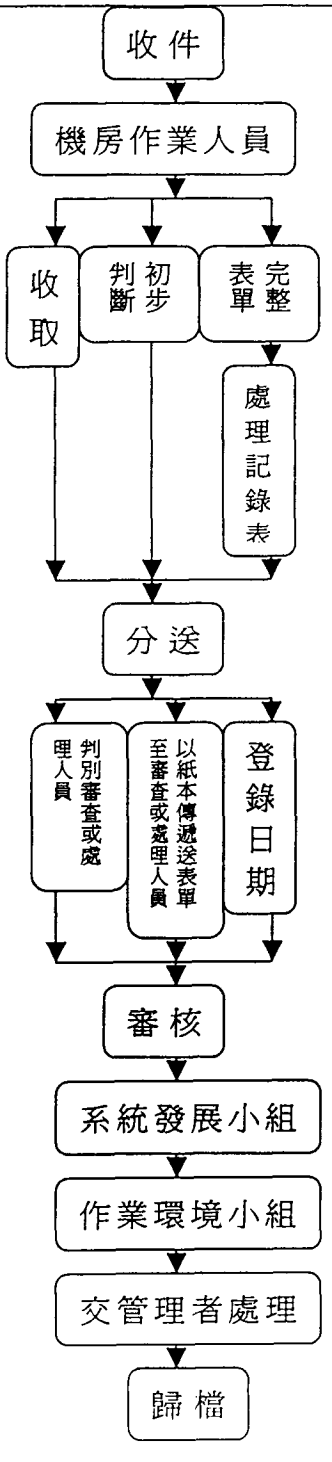
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	系統資源申請與原始碼型管作業程序	imi9.6-01		

目的：防止對資訊系統中資訊的非法存取

範圍：本中心系統資源與原始碼型

參考文件：

流程圖	權責	作業內容與步驟	表單
	機房作業人員 系統發展小組 作業環境小組	1. 收件：機房作業人員 1.1 收取紙本或Mail電子檔(印出紙本) 1.2 初步判斷填寫完整、正確否(如：主機名稱...)，若不完整則通知申請人改善。 1.3 完整表單則先登錄至「處理記錄表」，並賦與單號。 2. 分送：機房作業人員 2.1 判別審查或處理人員 2.2 以紙本傳遞送表單至審查或處理人員 2.3 登錄日期 3. 審核 3.1 審核人員 3.1.1 系統發展小組負責人審核 3.1.2 作業環境小組負責人審核 3.1.3 交管理者處理 3.2 型管員 3.2.1 查核所提附件資料與表單是否正確？若否，逕通知申請人補件。	「處理記錄表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	系統資源申請與原始碼型管作業程序	imi9.6-01		

目的：防止對資訊系統中資訊的非法存取

範圍：本中心系統資源與原始碼型

參考文件：

流程圖	權責	作業內容與步驟	表單
		4. 處理作業：資源管理者與型管員 4.1 依據表單填寫處理日期 4.2 處理完畢將紙本移交機房作業人員歸檔登錄 5. 結案：機房作業人員 5.1 表單歸檔登錄	

中山科學研究院

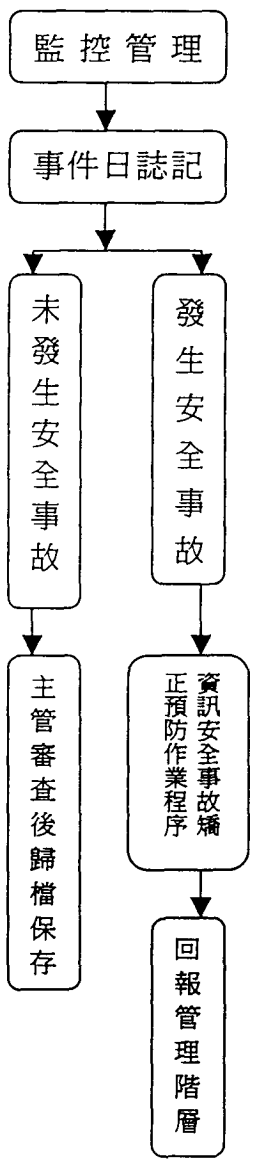
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	事件日誌管理作業程序	imi9.7-01		

目的：根據事件日誌對系統進行監控管理。

範圍：本中心安全區電腦主機。

參考文件：

流程圖	權責	作業內容與步驟	表單
		1. 事件日誌記錄 電腦主機的資產管理者應負責設定、儲定、列印、分析該主機事件的日誌。 2. 事件日誌審查 2.1 未發生安全事故時，事件日誌應經主管審查後歸檔保存。 2.2 若發生安全事故時，事件日誌應調閱分析其中原因，並依「資訊安全事故矯正預防作業程序」，回報管理階層。 3. 主機時鐘同步 3.1 資管組應負責調校本中心所有主機時鐘同步，至少每星期一次。	

中山科學研究院

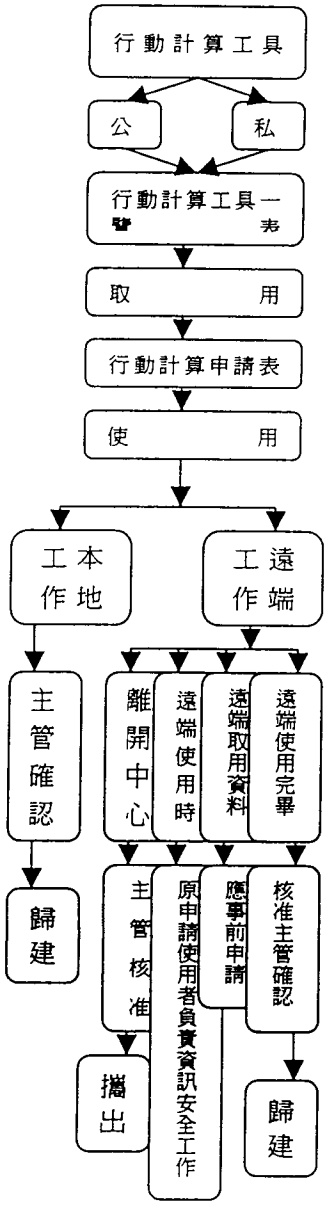
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	行動計算和遠端工作作業程序	imi9.8-01		

目的：確保在使用行動計算工具和遠端工作設施時資訊的安全。

範圍：筆記型電腦、掌上型電腦、膝上型電腦、行動電話、個人數位助理器。

參考文件：

流程圖	權責	作業內容與步驟	表單
		1. 登錄：本中心所有公用行動計算工具皆應造冊列管於「行動計算工具一覽表」；非公用行動計算工具於攜入時應先登記。 2. 取用：使用行動計算工具前應先填妥「行動計算申請表」獲得許可後，方可取用。 3. 使用： 3.1 本地工作：中心內使用完畢由原取用核准主管確認，未逾越申請使用之範圍，方可將設備歸建。 3.2 遠端工作 3.2.1 離開中心前應由原取用核准主管確認設備內未含任何機密性資料，方得攜出。 3.2.2 遠端使用時，由原申請使用者負責資訊安全工作。 3.2.3 遠端使用中，欲登入本中心主機取用資料、實施計算，應事前申請。 3.2.4 遠端使用完畢後，應由原取用核准主管確認，未逾越申請使用之範圍後，將設備歸建。	「行動計算工具一覽表」 「行動計算使用申請表」

中山科學研究院

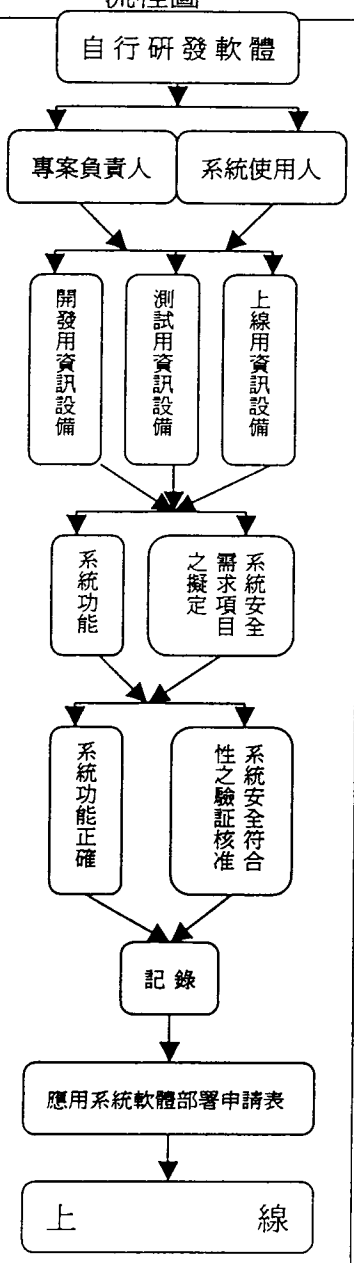
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	應用軟體開發安全作業程序	imi10.2-01		

目的：防止應用系統運算過程中資料的遺失、修改、誤用。

範圍：本中心自行研發設計之應用軟體

參考文件：

流程圖	權責	作業內容與步驟	表單
	專案負責人 系統使用人	1. 自行研發軟體，應指定(1)專案負責人與(2)系統使用人。	
		2. 資訊處理設備區隔，應指定(1)開發用資訊設備、(2)測試用資訊設備、(3)上線用資訊設備。	
		3. 軟體系統研發過程，依據「中山科學研究院軟體工程與資訊中心品質質手冊」，第四章設計管制所列各項程序書執行。	
	專案小組成員	4. 於設計輸入與設計輸出個階段應由專案小組之不同成員，執行原始碼、目的碼與執行檔間功能之比對。	
	專案負責人 系統使用人	5. 於設計審查階段，由專案負責人與系統使用人共同負責(1)系統功能與(2)系統安全需求項目之擬定。	
	專案負責人	6. 於設計驗証階段，由專案小組負責(1)系統功能正確性、(2)系統安全符合性之驗証，並經專案負責人核佳。	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	應用軟體開發安全作業程序	imi10.2-01		

目的：防止應用系統運算過程中資料的遺失、修改、誤用。

範圍：本中心自行研發設計之應用軟體

參考文件：

流程圖	權責	作業內容與步驟	表單
	系統使用小組	7. 於設計確認階段，由系統使用小組負責(1)系統功能正確性、(2)系統安全符合性之確認，並經系統使用人核准。	
	專案負責人 系統使用人	8. 若欲執行設計變更，應用專案負責人與系統使用人共同制定變更項目，並依序執行審查、驗証、確訒階段工作。	
		9. 審查、驗証、確認、變更皆應留有記錄。	
		10. 系統開發完成上線前，應填妥「應用系統軟體部署申請表」。	「應用系統軟體部署申請表」
		11. 需要時，系統安全符合性，可考慮下列事項。 11.1 上線前 11.1.1 系統執行電腦容量是否足備？ 11.1.2 是否有撰寫系統重新啓動作業程序。 11.1.3 是否有測試報告或記錄？ 11.1.4 新系統是否影響現行系統？ 11.1.5 是否辦理新系統教育訓練？	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	應用軟體開發安全作業程序	imi10.2-01		

目的：防止應用系統運算過程中資料的遺失、修改、誤用。

範圍：本中心自行研發設計之應用軟體

參考文件：

流程圖	權責	作業內容與步驟	表單
		11.2 資訊存取控制 11.2.1 使用者是否能接觸原始碼？ 11.2.2 是否具備使用者手冊？ 11.2.3 是否控制使用者存取權限？ 11.3 輸入輸出資料的正確範圍是否由程式管控？ 11.4 程式庫、執行碼之存放與改版是否經過授權並留有記錄？ 11.5 舊版原始碼是否安全存放保護？ 11.6 系統文件 11.6.1 是否存放於安全區內？ 11.6.2 分發及回收是否有簽收記錄？ 11.6.3 版本是否管控？ 11.6.4 電子檔和紙本檔是否取得一致性？ 11.7 系統變更後，相關文件是否更新？	

中山科學研究院

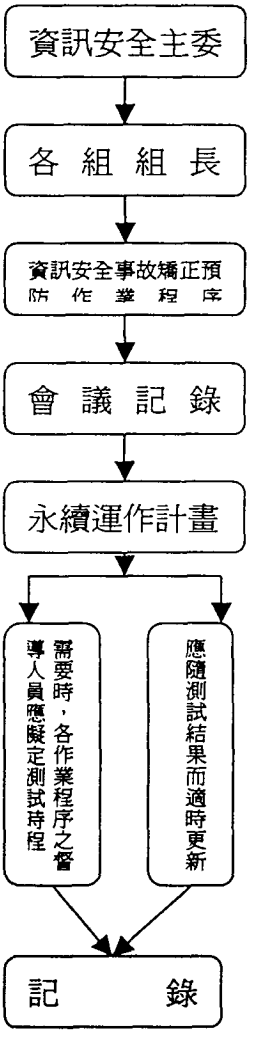
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	業務永續運作管理作業程序	imi11-01		

目的：防止業務活動中斷，確保重要工作流程不因重大故障或災難影響。

範圍：本中心所轄資訊管理組、電信網路組、綜合管理組。

參考文件：

流程圖	權責	作業內容與步驟	表單
		1.資訊安全主委應督導各組組長定期(每學年擇期)召開業務永續運作會議，同時討論『資訊安全事故矯正預防作業程序』，執行成效 2. 業務永續運作會議應討論 2.1 半年期(或年度)跨組及各組業務優先順序與負責人 2.2 假想各類災害發生之影響 2.3 需要時，對關鍵性業務應提供永續運作計畫 2.4 需要時，應測試永續運作計畫並更新不足之處 2.5 需要時，應協調原支援廠商或服務提供者支援 3.需要時，業務永續運作計畫應產出 3.1 關鍵性業務之應變作業程序，及督導人員 3.2 關鍵性業務之回復作業程序，及督導人員 3.3 關鍵性業務之測試作業程序，及督導人員 3.4 關鍵性業務之技術服務提供廠商，及督導人員 4.永續運作計畫之測試 4.1 需要時，各作業程序之督導人員應擬定測試時程 4.2 永續運作計畫應隨測試結果而適時更新，包括	「會議記錄」 「業務永續運作計畫」 「應變作業程序」 「回復作業程序」 「測試作業程序」

中山科學研究院

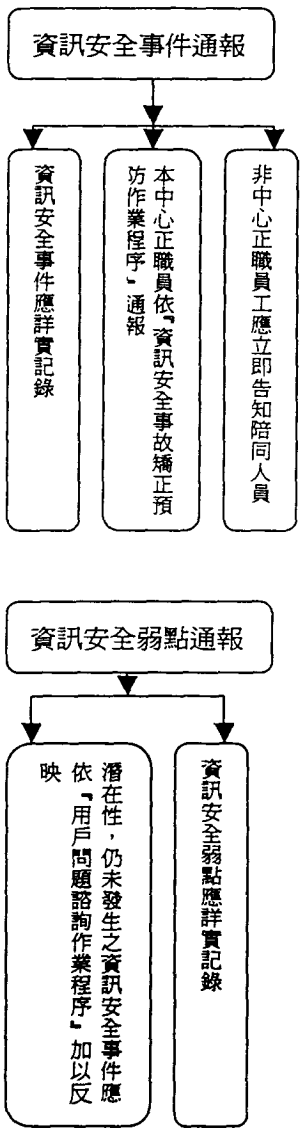
資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	業務永續運作管理作業程序	imi11-01		

目的：防止業務活動中斷，確保重要工作流程不因重大故障或災難影響。

範圍：本中心所轄資訊管理組、電信網路組、綜合管理組。

參考文件：

流程圖	權責	作業內容與步驟	表單
		4.2.1 新軟硬體設備添購 4.2.2 新技術的引進 4.2.3 教育訓練的需求 4.2.4 組織結構調整與人員調動 4.2.5 新的連結方式(人員地址電話更新) 4.2.6 新舊合約變動 4.2.7 業務流程的異動 4.2.8 法規條例的異動 5.資訊安全事件通報 5.1 資訊安全事件應詳實記錄 5.2 本中心正職員依『資訊安全事故矯正預防作業程序』通報 5.3 非中心正職員工應立即告知陪同人員 6.資訊安全弱點通報 6.1 潛在性，仍未發生之資訊安全事件應依『用戶問題諮詢作業程序』加以反映 6.2 上述資訊安全弱點應詳實記錄	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	符合性管制作業程序	imi12.1-01		

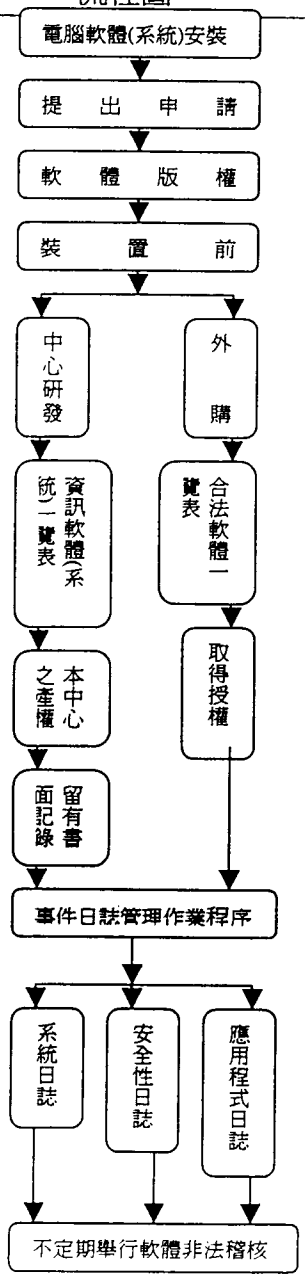
目的：規範資訊系統的使用以及資訊安全的措施，不違反刑法、民法、成文法、法規或合約義務以及任何安全要求。

範圍：資訊系統的設計、操作、使用和管理；資訊安全管理相關的作業程序。

參考文件：

1.智慧財產權保護法

2.電腦個人資料保護法

流程圖	權責	作業內容與步驟	表單
	綜合管理組 資訊管理組	1. 軟體版權 1.1 本中心研發設計之資訊軟體(系統)，其智慧財產權歸中山科學研究院擁有，版本聲明應在資訊軟體(系統未正式上線前確認並留有書面記錄 1.2 因行政業務或研發工作，需要安裝於本中心硬體設備上之資訊軟體(系統)，除共享軟體外，皆應於使用前取得授權 1.3 非本中心硬體設備上安裝之資訊軟體(系統)，不在管轄範圍 1.4 綜合管理組應維護外購之合法軟體與安裝使用位置(硬體設備)間的一致性，並填寫「合法軟體一覽表」以及妥善保存授權證明文件 1.5 資訊管理組應維護本中心研發設計之「資訊軟體(系統)一覽表」，詳細填寫設計者(單位)、維護者(單位)、使用者(單位)，並隨時保持最新狀態 2. 組織記錄 2.1 電腦運作所產生之系統日誌、安全性日誌、應用程式日誌，依照『事件日誌管理作業程序』處理	「合法軟體一覽表」 「資訊軟體(系統)一覽表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	符合性管制作業程序	Imi12.2n12.3-01		

目的：爲貫徹資訊安全政策，確立資訊安全內部稽核程序，以驗證資訊安全活動是否合乎規劃及確保資訊安全管理程序的有效性。

範圍：資訊安全管理程序所轄之本中心綜合管理組、資訊管理組、電信網路組。

參考文件：

1.資訊安全會議作業程序

2.資訊安全事故矯正預防作業程序

流程圖	權責	作業內容與步驟	表單
		2.2 非電腦運作過程產生之相關記路，依照中山科學研究院軟體工程與資訊中心品質手冊規定之『開發專案文件與品質記錄管制作業程序』和『品保專案文件與品質記錄管制作業程序』處理	
	綜合管理組	2.3 行政作業過程產生之表單、表格等紙張(本)記錄，依保存年限儲存；電子檔記錄應採離線儲存，需要備份儲存的對象與過程由綜合管理組規定	
	副組長	3. 本中心因業務需要取得之資料，不得違反電腦個人資料保護法之規定	
		4.資訊處理設施外借時，應取得資產管理者和副組長以上主管書面同意，方得放行	
	綜合管理組	5.本中心所有電腦軟體(系統)安裝，皆須向資管組提出申請，並由資訊人員安裝並列入管理，否則視同非法軟體，綜合管理組每季都會不定期舉行軟體非法稽核，請使用者不要輕易嘗試自行安裝，以免破財（使用者與一二級主管皆會受罰）	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全內部稽核作業程序	imi12.2n12.3-01		

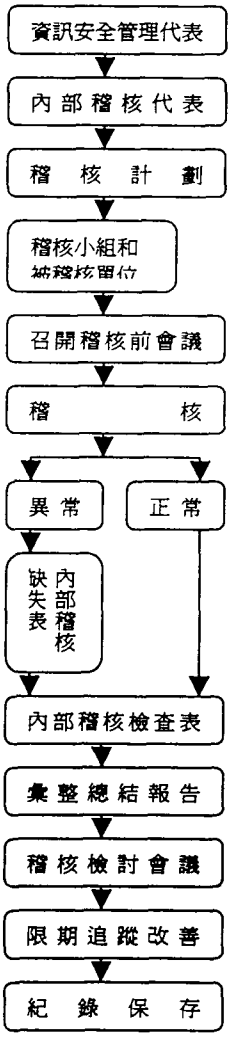
目的：為貫徹資訊安全政策，確立資訊安全內部稽核程序，以驗證資訊安全活動是否合乎規劃及確保資訊安全管理程序的有效性。

範圍：資訊安全管理程序所轄之本中心綜合管理組、資訊管理組、電信網路組。

參考文件：

1.資訊安全會議作業程序

2.資訊安全事故矯正預防作業程序

流程圖	權責	作業內容與步驟	表單
	資訊管理組組長 組長 組長 資訊安全代表 組長	1. 資訊安全管理代表應指定內部稽核代表，負責統籌資訊安全內部稽核活動 1.1 稽核代表需訂定半年度稽核計劃，並以書面或電子郵件方式通知相關組別 1.2 各組主管應負責追查資訊安全內部稽核工作的執行結果 1.3 各組主管依據稽核的結論與建議，迅速採取問題的改善與矯正措施 2. 資訊安全代表由資管組主管擔任，負責稽核工作推廣與督導改善 3. 各組主管輪流擔任稽核代表，負責統籌資訊安全內部稽核活動，訂定年度「稽核計劃表」 4. 稽核小組：經相關資訊安全訓練合格的人員，符合對稽核範圍工作熟悉者，或受過 ISO9001 內部品質稽核訓練課程者 4.1 稽核小組的任用，由資訊安全管理代表審定 4.2 稽核小組成員，須依資訊安全內部稽核步驟進行稽核工作	「稽核計劃表」

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全內部稽核作業程序	Imi12.2n12.3-01		

目的：爲貫徹資訊安全政策，確立資訊安全內部稽核程序，以驗證資訊安全活動是否合乎規劃及確保資訊安全管理程序的有效性。

範圍：資訊安全管理程序所轄之本中心綜合管理組、資訊管理組、電信網路組。

參考文件：

1.資訊安全會議作業程序

2.資訊安全事故矯正預防作業程序

流程圖	權責	作業內容與步驟	表單
		4.3 稽核工作分組並至各組別稽核，稽核人員不稽核自身工作 4.4 稽核頻率至少每半年一次，視執行狀況調整稽核頻率	
		5. 稽核步驟	
	稽核小組	5.1 召開稽核前會議，由稽核小組和被稽核單位會商，並決定各單位參與人員及稽核時間 5.2 稽核小組依稽核計劃並由合格人員擔任 5.3 稽核作業由品質稽核小組建立各項稽核書面報告與記錄	「內部稽核檢查表」
	稽核小組	5.4 稽核中,發現相關作業程序異常時，應提出「內部稽核缺失表」,交被稽核者，由被稽核主管提出矯正對策與完成期限	「內部稽核缺失表」
	稽核小組	5.5 稽核人員須彙整「內部稽核缺失表」,於稽核檢討會議中討論報告	
	稽核小組	5.6 稽核人員應依據「內部稽核缺失表」,所登錄的矯正行動與期限進行追蹤管制工作，並回報稽核代表	

中山科學研究院

資 訊 管 理 中 心

文件類別	名　稱	文件編號	發行日期	頁次
程序書	資訊安全內部稽核作業程序	Imi12.2n12.3-01		

目的：爲貫徹資訊安全政策，確立資訊安全內部稽核程序，以驗證資訊安全活動是否合乎規劃及確保資訊安全管理程序的有效性。

範圍：資訊安全管理程序所轄之本中心綜合管理組、資訊管理組、電信網路組。

參考文件：

1.資訊安全會議作業程序

2.資訊安全事故矯正預防作業程序

流程圖	權責	作業內容與步驟	表單
		5.7 稽核人員所提報改善作業無法落實執行時，由稽核代表呈報資訊安全管理代表，督導改善 6 彙整總結報告：稽核代表於稽核完成後，需彙整總結報告呈交資訊安全代表	
	資訊安全主委	7 資訊安全管理審查 7.1 各項稽核結果應於稽核檢討會議中檢討，以確保資訊安全程序持續運作適切性與有效性 7.2 稽核作業所產生的各項記錄於會議後，由資訊安全代表依『符合性管制作業』保存	