電子檔案資訊安全

檔案管理局

檔案資訊組

課程大綱

- 電子檔案概念介紹
- 電子檔案安全技術
- 資訊安全管理系統

電子檔案概念介紹

- 電子檔案定義介紹
- 電子檔案安全威脅
- 電子檔案安全需求
- 檔案管理資訊系統
- 電子檔案管理要求
- 電子檔案管理目標

電子檔案定義介紹

- 電子文件(電子簽章法)

  指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

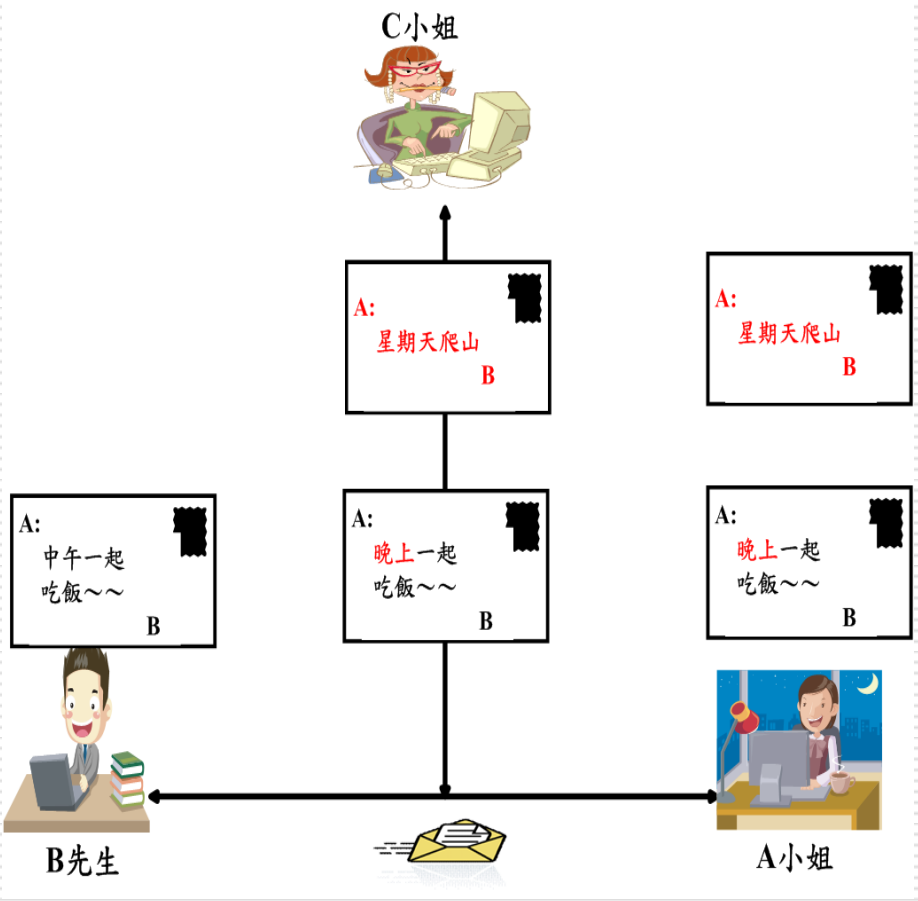
- 數位內容檔案(機關檔案管理資訊化作業要點)

  指將圖像、文字、影像、語音及動畫等資料運用資訊科技加以數位化後之電子影音檔案、電子檔案等。

- 電子檔案
  - 完成線上簽核之非機密電子文件(機關電子檔案管理作業要點)
  - 電腦可處理之文字或非文字資料(文書及檔案管理電腦化作業規範)

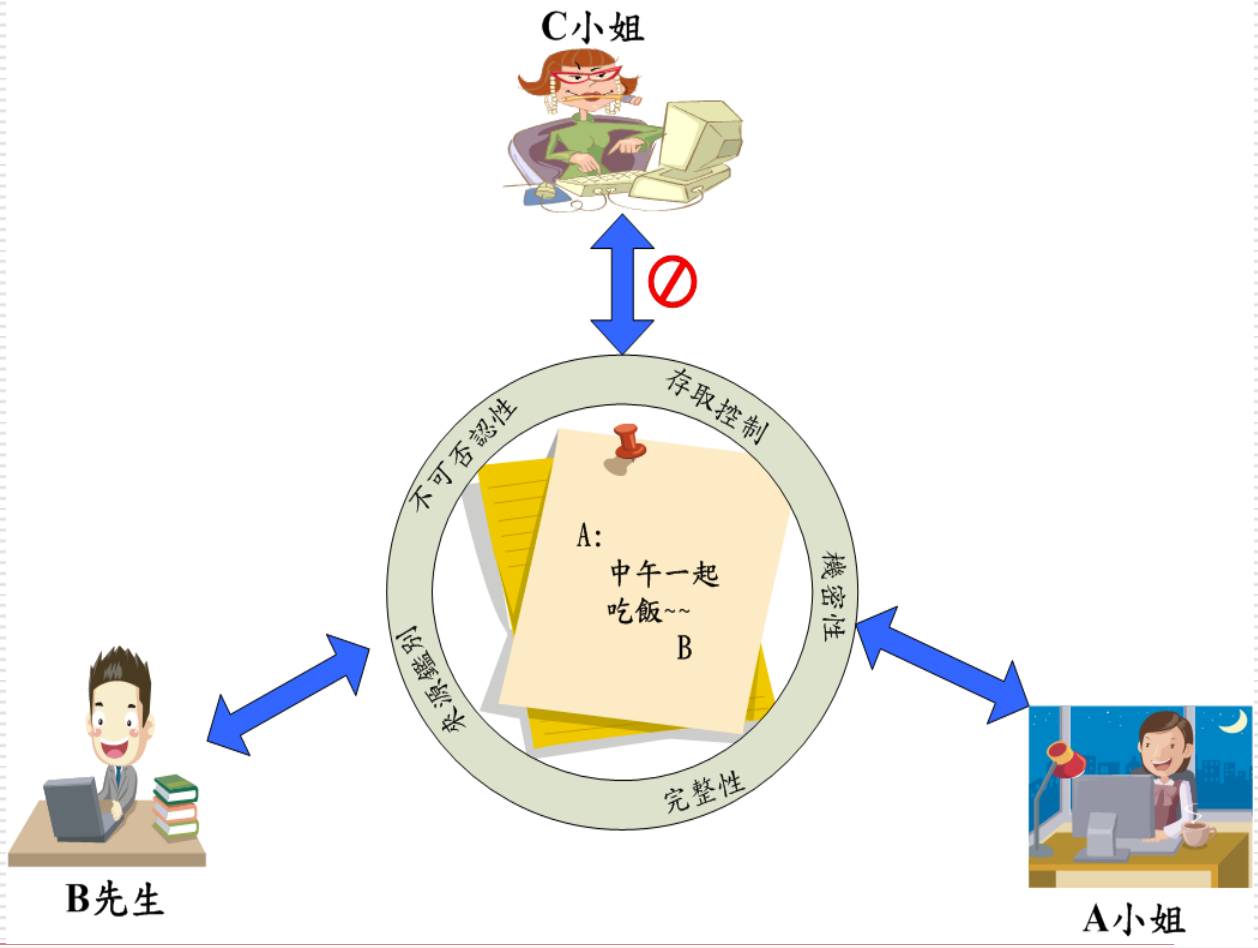
電子檔案安全威脅

- 內容竊知
- 內容偽造
- 內容竄改
- 冒名發文
- 駭客侵入
- 否認傳送或否認接收

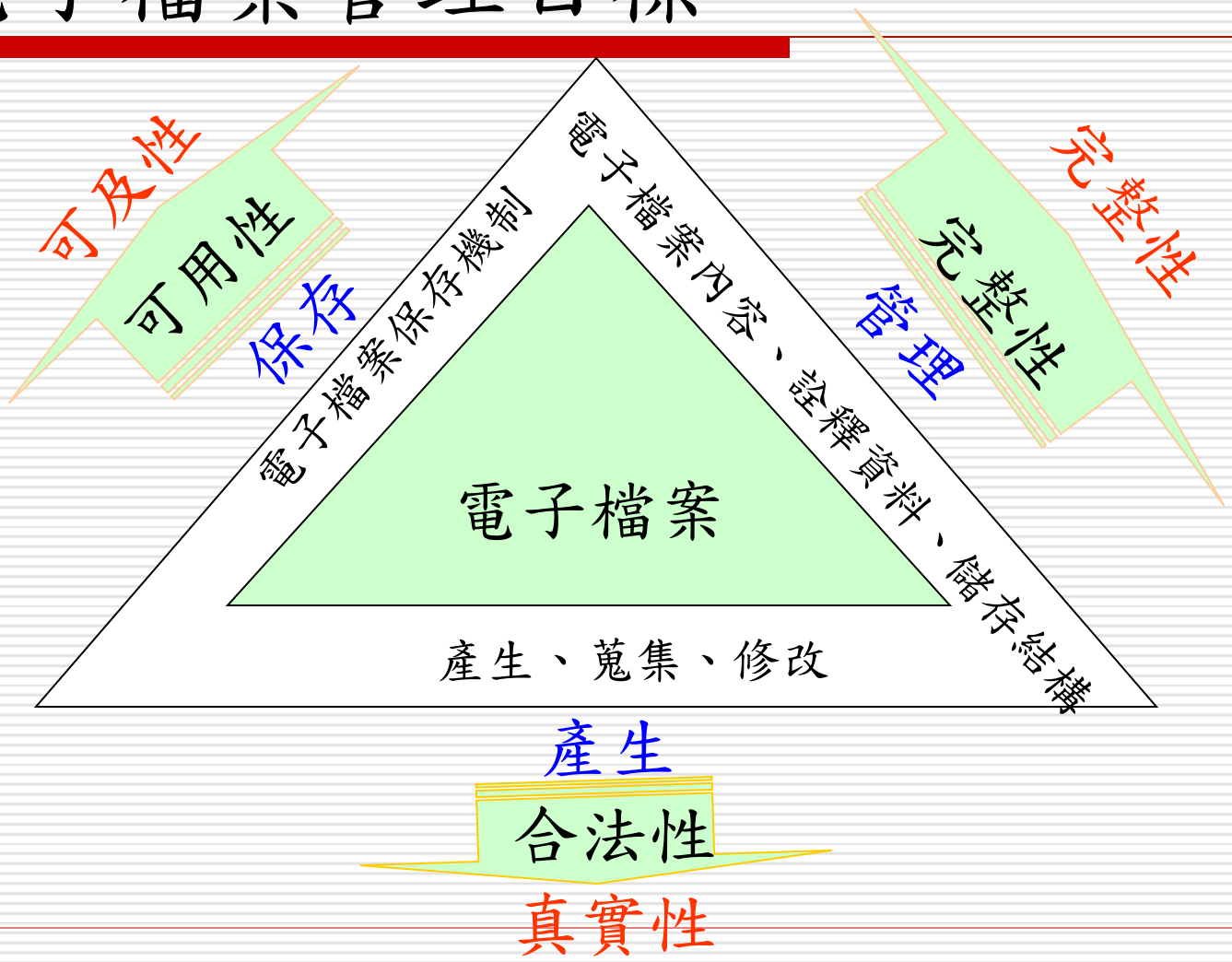


電子檔案安全需求

- 來源鑑別
- 機密性
- 存取控制
- 完整性
- 不可否認性



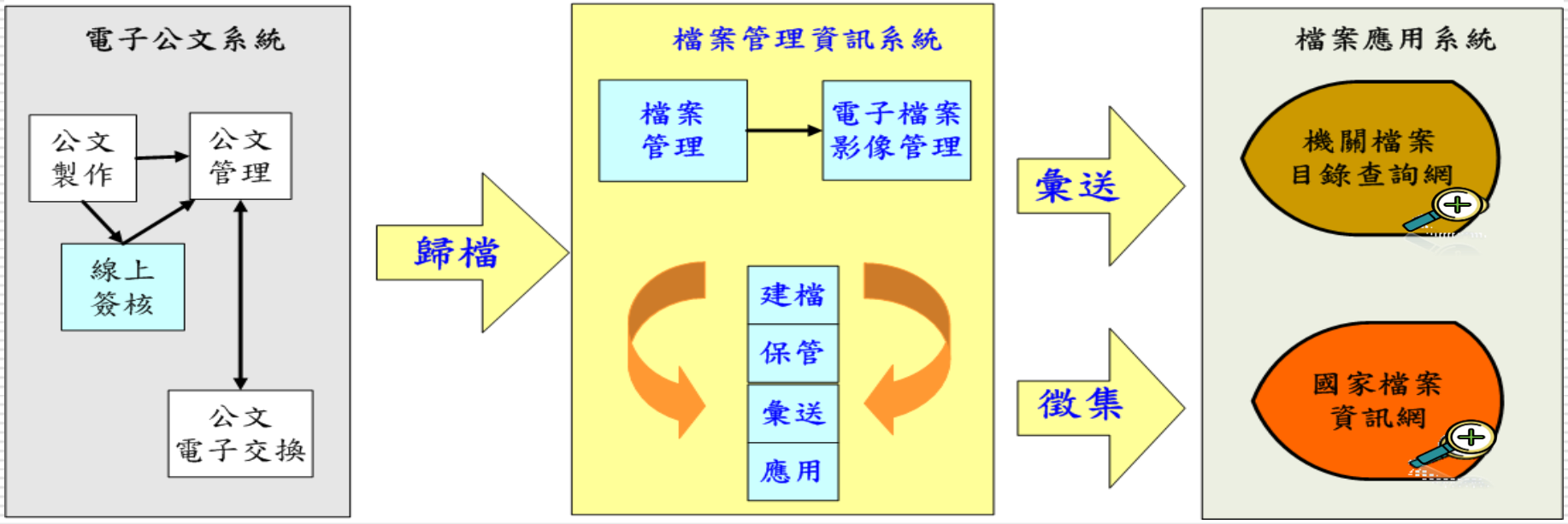
電子檔案管理目標


可及性
可用性
保存
電子檔案保存機制
電子檔案內容、詮釋資料、儲存結構
完整性
完整性
管理
電子檔案
產生、蒐集、修改
產生
合法性
真實性

檔案管理資訊系統

流程資訊化

公文管理 — 檔案管理 — 檔案應用



電子檔案管理要求（線上簽核）

- 點收➔確認電子檔案(檔案內容+電子簽章)
- 分編➔電子檔案不得任意刪除或修改
- 著錄➔電子檔案銓釋資料(附件2)
- 儲存➔電子檔案(附件8、附件9)
- 保存年限➔電子檔案轉置、更新、模擬及封裝
- 保存➔軟硬體設施維護、轉置、更新、模擬及封裝
- 稽核➔電子檔案(每年)
- 清查、技術鑑定、銷毀、移轉及稽核➔檔管人員會同資訊人員辦理

電子檔案安全技術

- 電子簽章法介紹
- 公務電子識別證
- ＰＫＩ基礎建設
- 電子檔案加解密
- 數位簽章之程序
- 安全儲存與傳輸
- 系統控管之機制

電子簽章法介紹

透過賦予電子文件和電子簽章的法律效力，建立可信賴的網路交易環境，確保能夠掌握某一資訊在網路傳輸過程中，是否遭到偽造、竄改或竊取，以保障資訊完整與安全性，並透過識別交易雙方身份，防止事後否認已完成交易的事實。

- 數位簽章效力
- 電子文件效力
- 收發文時間與地點之認定
- 憑證機構設立與管理
- 憑證機構罰則

電子簽章法介紹

- 電子簽章

  指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。

- 數位簽章

  指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成簽體，並得以公開金鑰加以驗證者。

電子簽章法介紹

- 憑證

  指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

- 憑證機構

  指簽發憑證之機關、法人。

- 資訊系統

  指產生、送出、收受、儲存或其他處理電子形式訊息資料之系統。

公務電子識別證

- 行政院及所屬各機關公務人員電子識別證管理作業要點
- 各機關應自行選用下列經濟部核定之憑證機構依法簽發之憑證，據以製作電子識別證：（第5條）

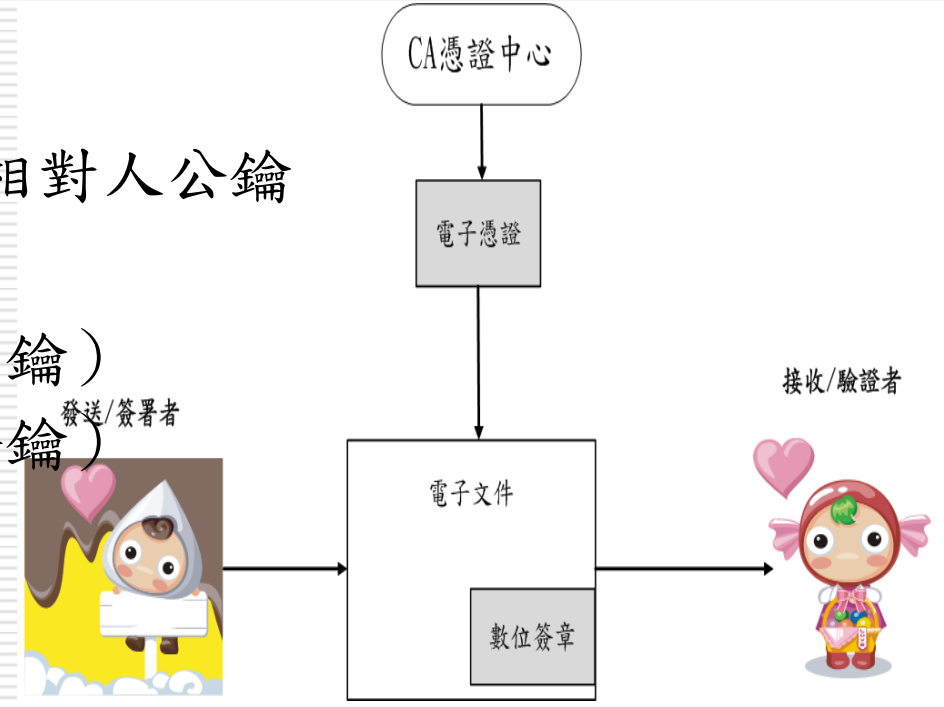
  (一)內政部核發供自然人使用之自然人憑證。

  (二)各機關自建之憑證機構簽發之憑證。

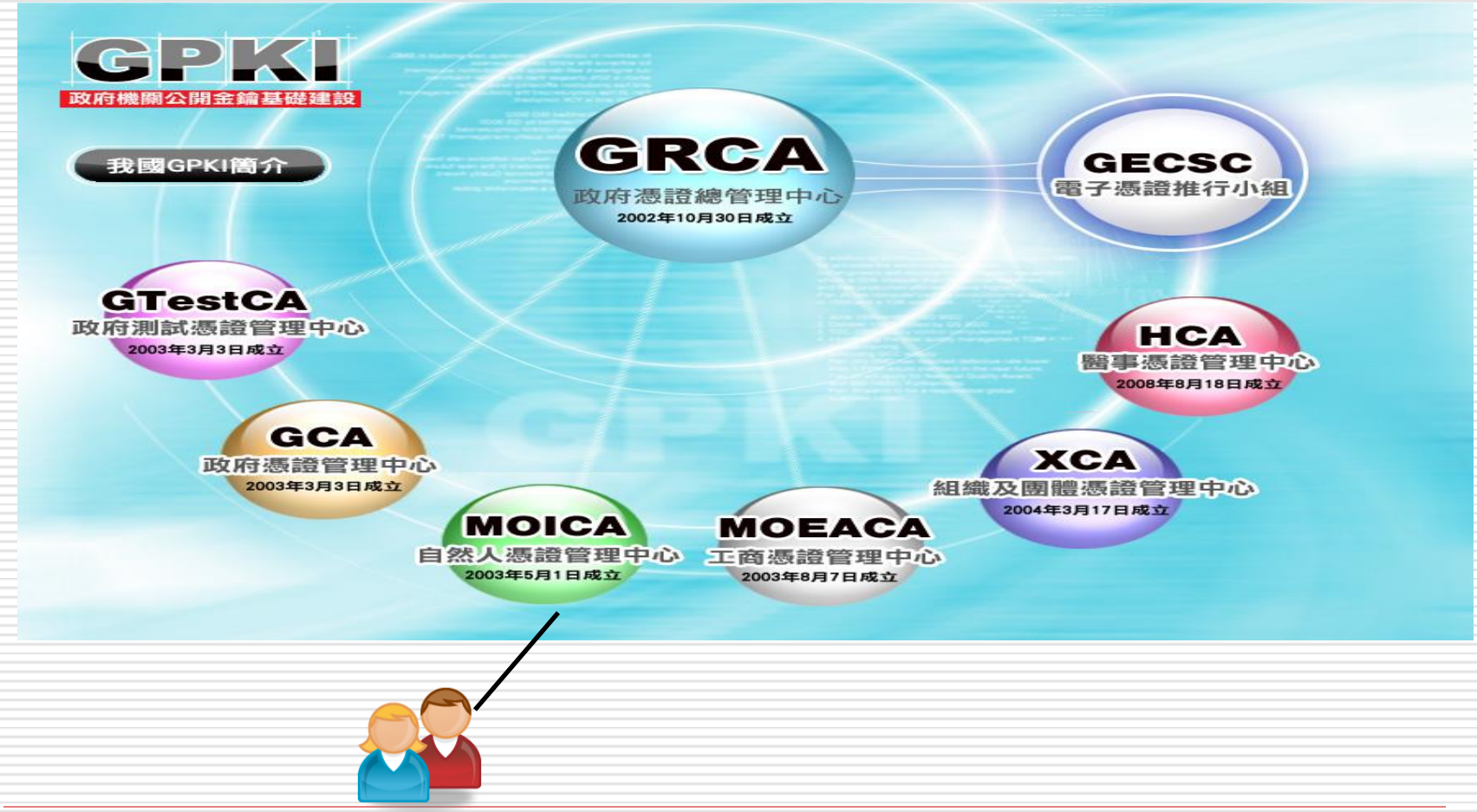
  (三)前二款以外憑證機構簽發之憑證。

公開金鑰(PKI)基礎建設

- PKI架構
  - 公鑰集中保管於公正第3人(憑證機構Certificate Authority, CA)
  - 私鑰由持有人保管
  - 向憑證機構(CA)查詢相對人公鑰
- 運作程序
  - 電子文件＋發送端(私鑰)
  - 電子文件＋接收端(公鑰)



政府憑證總管理中心

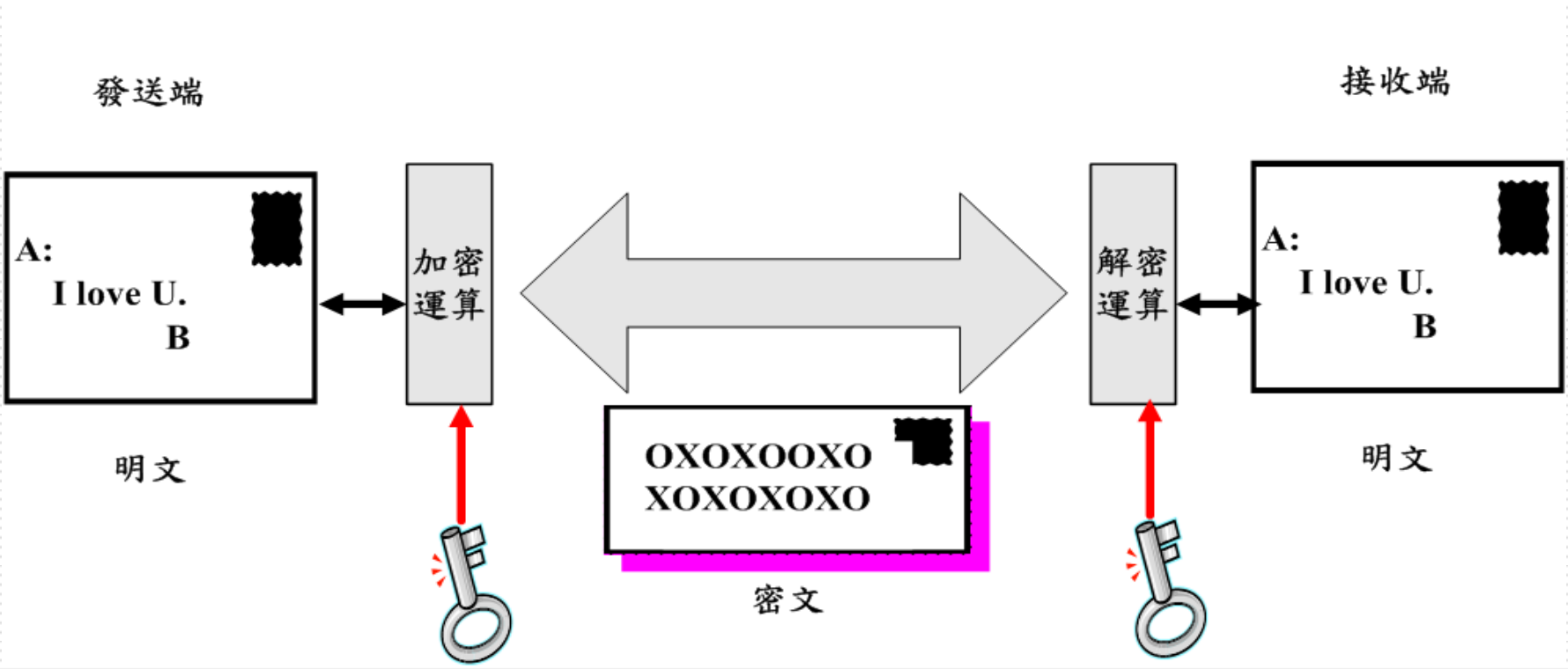

GPKI
政府機關公開金鑰基礎建設
我國GPKI簡介
GRCA
政府憑證總管理中心
2002年10月30日成立
GECSC
電子憑證推行小組
GTestCA
政府測試憑證管理中心
2003年3月3日成立
HCA
醫事憑證管理中心
2008年8月18日成立
GCA
政府憑證管理中心
2003年3月3日成立
XCA
組織及團體憑證管理中心
2004年3月17日成立
MOICA
自然人憑證管理中心
2003年5月1日成立
MOEACA
工商憑證管理中心
2003年8月7日成立

電子化政府電子認證服務分工

憑證名稱	簽發之憑證	註冊窗口	主管機關
GCA政府憑證管理中心	政府機關(構)及單位	行政院研究發展考核委員會	行政院研究發展考核委員會
MOEACA工商憑證管理中心	公司、分公司及商號	經濟部商業司 、各縣市政府公司及商號登記機關	經濟部
MOICA自然人憑證管理中心	一般民眾	內政部資訊中心及各縣市戶政事務所	內政部
XCA組織及團體憑證管理中心	學校、財團法人、社團法人、行政法人、自由職業事務所、其他組織或團體	各類憑證用戶之主管機關	行政院研究發展考核委員會
HCA醫事憑證管理中心	醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體	全國衛生局所	行政院衛生署

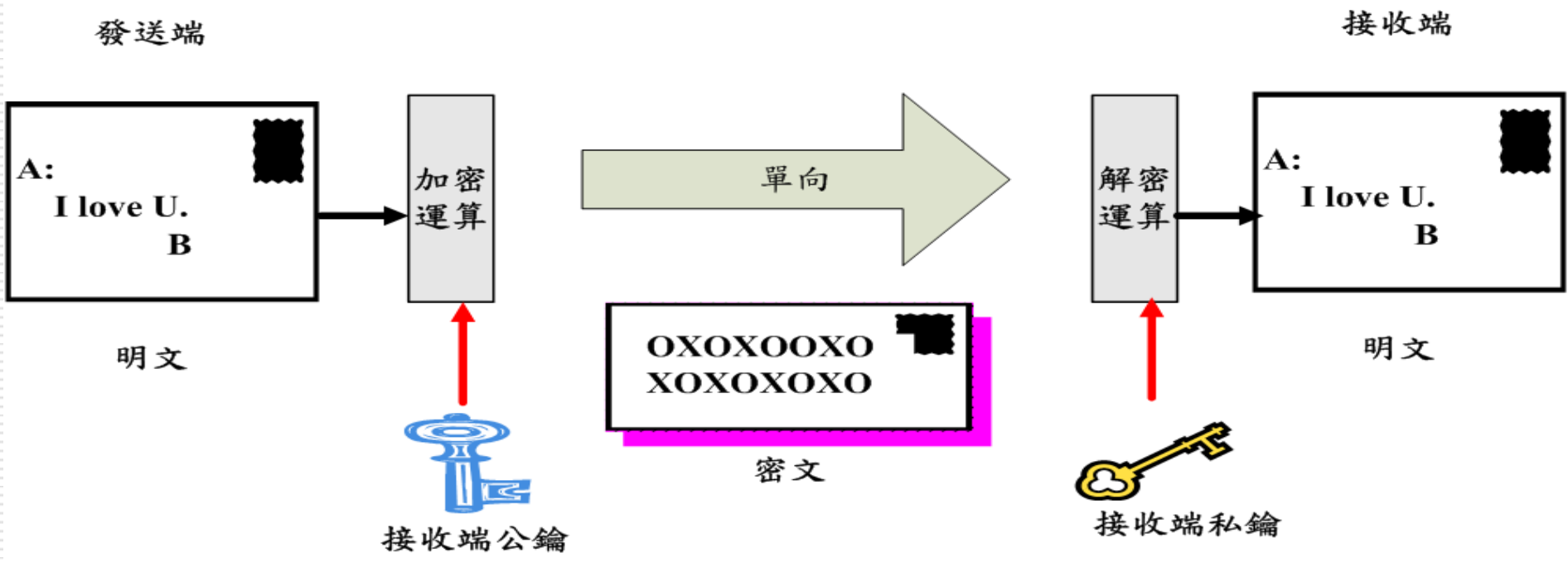
電子檔案加解密

- 對稱加密系統

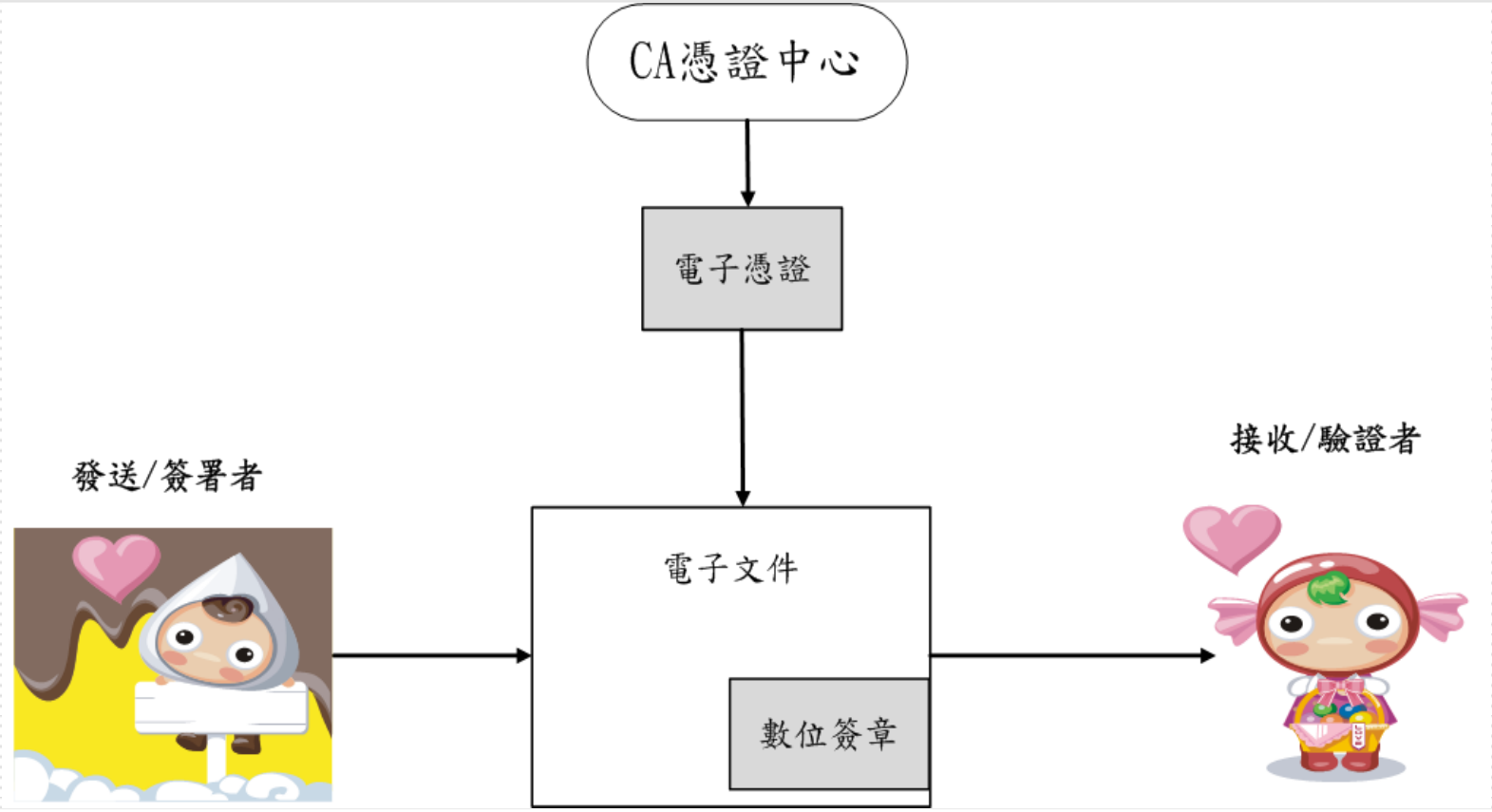


電子檔案加解密

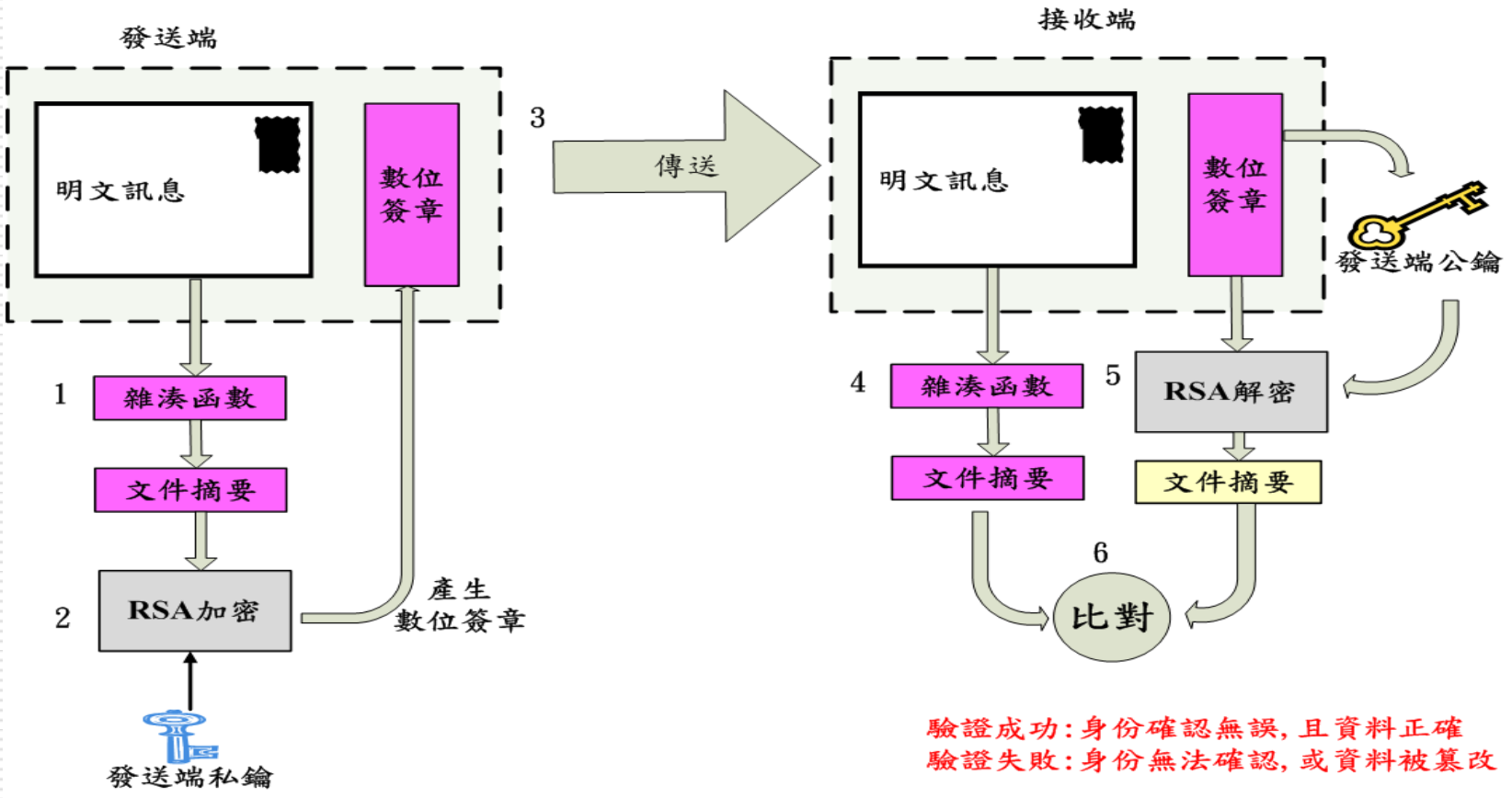
- 非對稱加密系統



數位簽章之程序



數位簽章之程序


發送端
明文訊息
數位簽章
3
傳送
接收端
明文訊息
數位簽章
發送端公鑰
1
雜湊函數
文件摘要
2
RSA加密
產生數位簽章
發送端私鑰
4
雜湊函數
文件摘要
5
RSA解密
文件摘要
6
比對
驗證成功：身份確認無誤，且資料正確
驗證失敗：身份無法確認，或資料被篡改

電子公文檔案管理系統安全控管機制

- 創稿或來文登錄
  - 產生【封裝檔】
  - 產生【密鑰】－為公文流程【簽註意見】加密使用
  - 產生【數位信封】

  以GCA應用軟體伺服器專屬憑證對【密鑰】加密，將其加至封裝檔。
- 簽核流程
  - 簽核者以【自然人憑證】進行公文資料加簽
  - 【簽註意見】由GCA應用軟體伺服器專屬憑證私鑰取出加密【密鑰】後，進行【簽註意見】加密。
- 公文辦畢歸檔
  - 檔管人員【自然人憑證】及【機關憑證】辦理加簽點收。

電子公文檔案管理系統安全控管機制

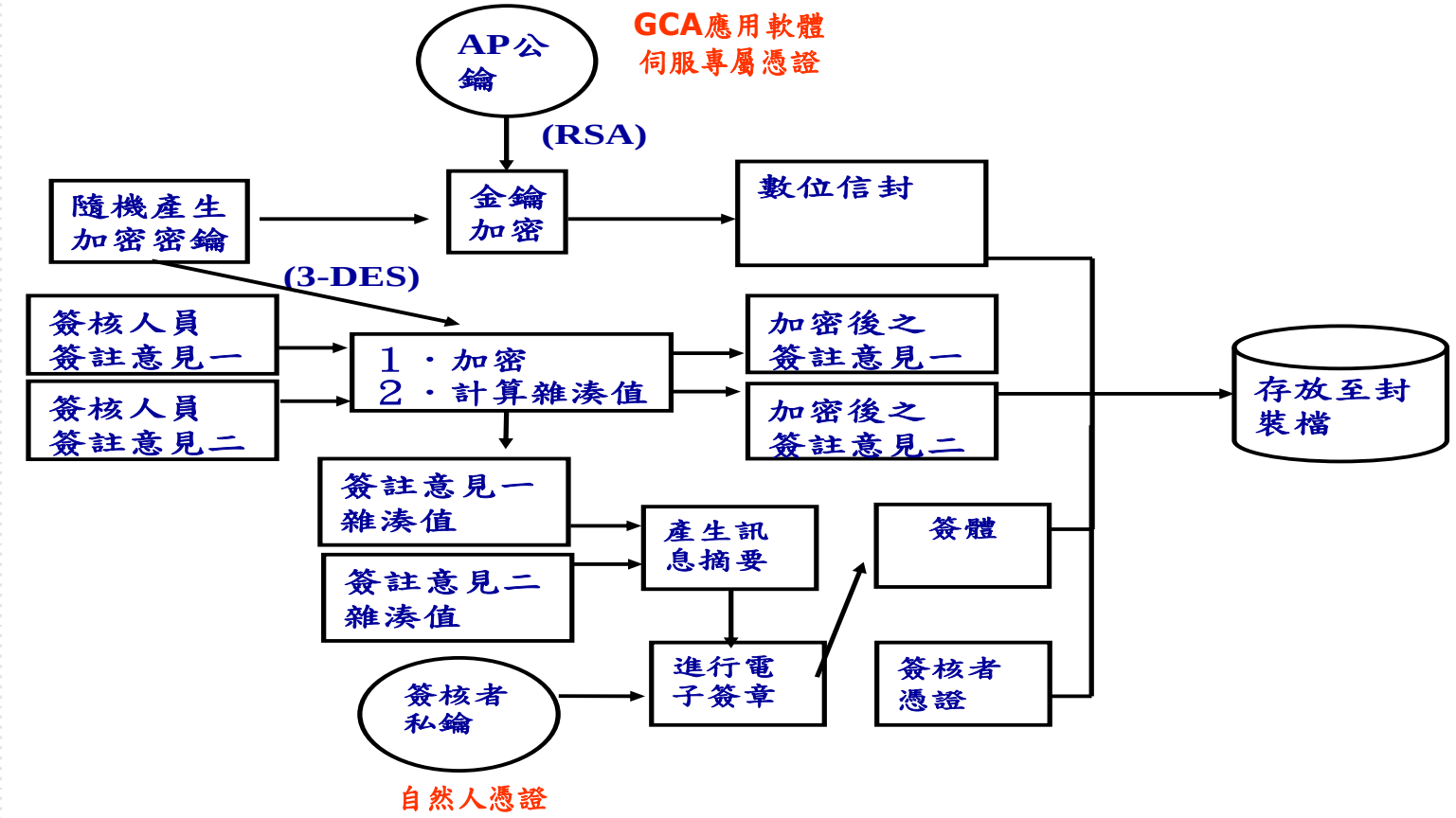
- 線上簽核電子公文檔案
  - 符合國際規範XML Signature技術
  - 將簽核者憑證、簽核時戳、簽核意見等資料封裝儲存。
- 臨時憑證管理
  - 簽核者未帶自然人憑證時，以【臨時憑證】辦理加簽。
  - 但公文歸檔點收前，須以【自然人憑證】辦理補簽。
- 可依使用者角色設定權限。
- 提供媒體有效性檢查。

電子公文檔案管理系統安全控管機制

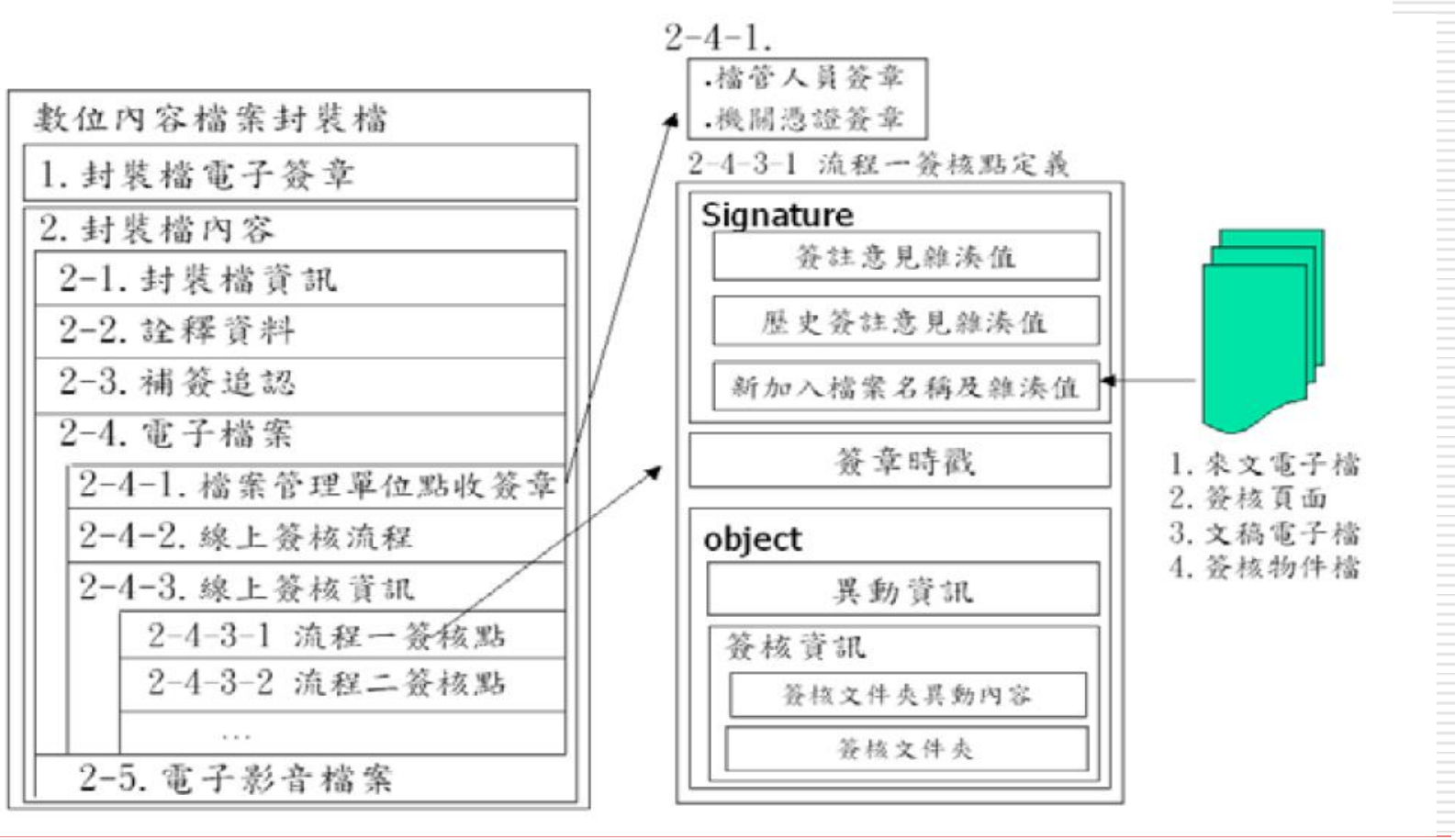
- 電子檔案儲存機制邏輯概念
  - 正式檔案區
    - 點收後，附加檔管人員【自然人憑證】及【機關憑證】之封裝檔。
    - 承辦人提出調卷申請後，可提供線上瀏覽。
  - 檢調應用區

    經核准調卷申請之檔案暫存區。
  - 原始文稿區
    - 承辦人之原始文稿電子檔，承辦人無須申請，即可瀏覽公文，預定保留2年，由系統定期清理。
    - 辦理中公文目錄資料，僅提供該件公文承辦人查詢。

電子公文檔案加簽及加密作法



線上簽核電子公文檔案封裝檔



安全儲存傳輸機制

- 電子檔案格式規範(附件八)

檔案型態	格式	檔案型態	格式
文字檔	XML、PDF、ODF	工程圖檔	IGES、DXF、STEP
圖片檔	JPEG、SVG	數位墨水	ISF
聲音檔	MP3、WAV	文字影像	JEPG、TIFF、PDF、WDL、PNG
視訊檔	MPEG-2、AVI、H.264		

安全儲存傳輸機制

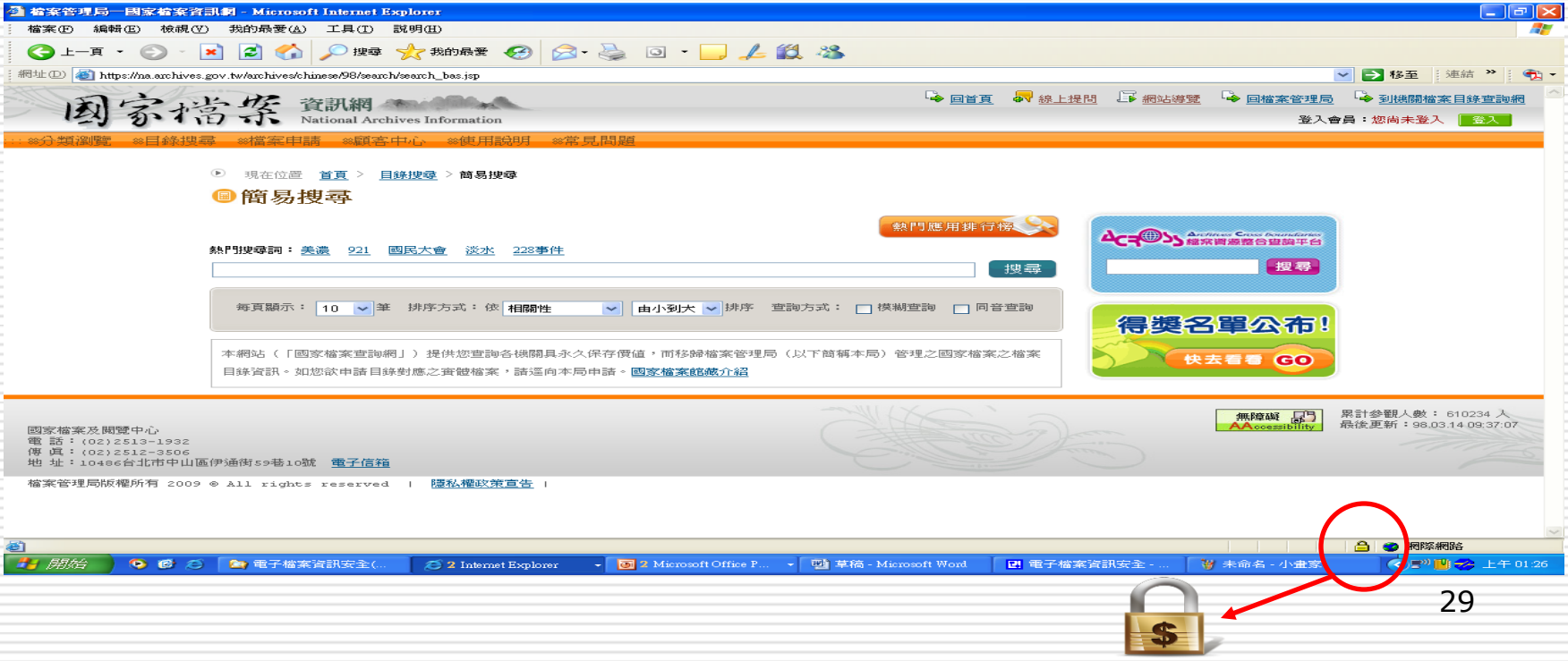
- 電子媒體格式規範(附件九)

媒體	規格	說明
CD-ROM	採黃皮書標準，檔案結構為ISO9660 Level 3或UDF資料規格為Mode 1。	國際標準
DVD-ROM	採單面單層(DVD-5)或單面雙層(DVD-9)儲存結構。	開放性標準
磁帶	採LVD或Ultra_wide SCSI介面，以DDS、DAT或DLT格式儲存。	
硬碟	採FAT32或NTFS硬碟檔案格式，且可支援USB1.1/2.0之傳輸介面	開放性標準

安全儲存傳輸機制

- SSL(Secure Socket Layer)

  Handshake連線程序、非對稱性密碼系統身份辨識、通訊是可信賴的



資訊安全管理系統

- 資訊安全法令規範
- 資訊安全定義介紹
- 資訊安全管理系統
- 風險管理活動情形
- ＩＳＭＳ認證標準

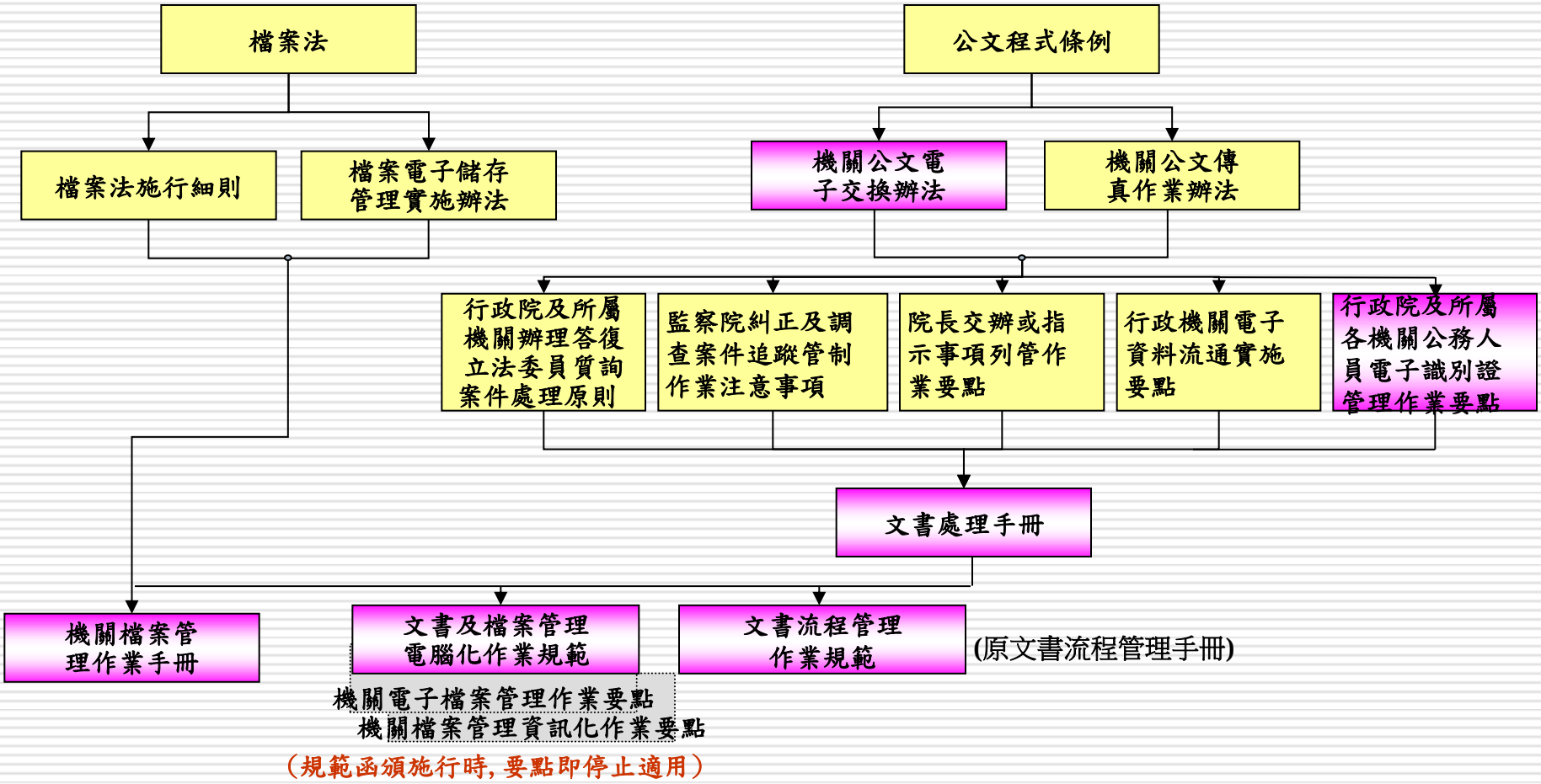
資訊安全法令規範

- 智慧財產權、資料保護法、電子監聽法、國家機密保護法、電腦處理個人資料保護法、通訊保障及監察法
- 電子簽章法
- 行政院及所屬各機關資訊安全管理規範
- 文書及檔案相關法規
  - 檔案電子儲存管理實施辦法
  - 機關電子檔案管理作業要點
  - 機關管理資訊化作業要點
  - 文書及檔案管理電腦化作業要點

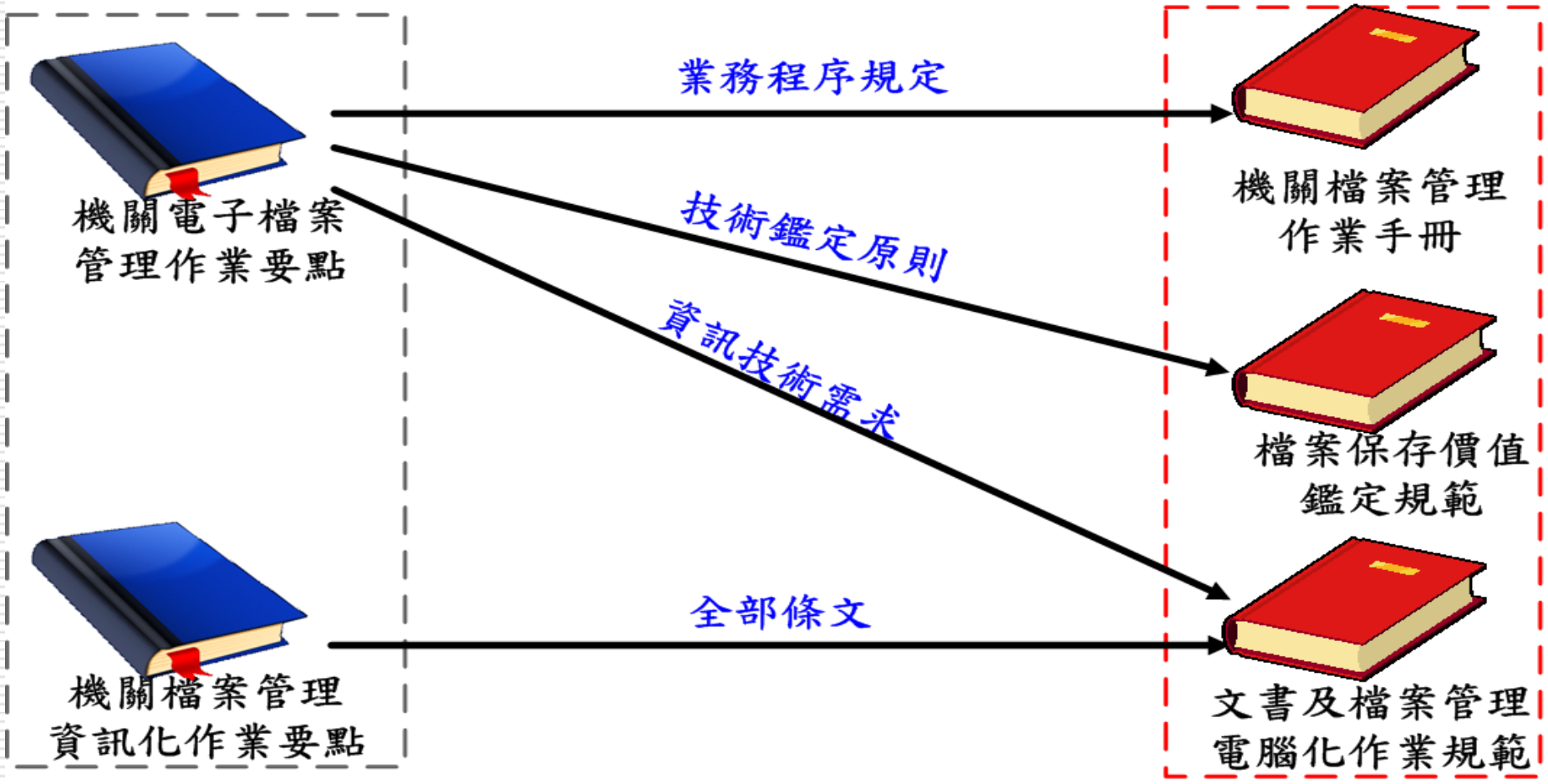
行政院及所屬各機關資訊安全管理規範

- 資訊安全政策制定及評估
- 資訊安全組織及權責
- 人員安全管理及教育訓練
- 電腦系統安全管理
- 網路安全管理
- 系統存取控制
- 系統發展及維護之安全管理
- 資訊資產之安全管理
- 實體及環境安全管理
- 業務永續運作計畫之規劃及管理

文書及檔案相關法規概況

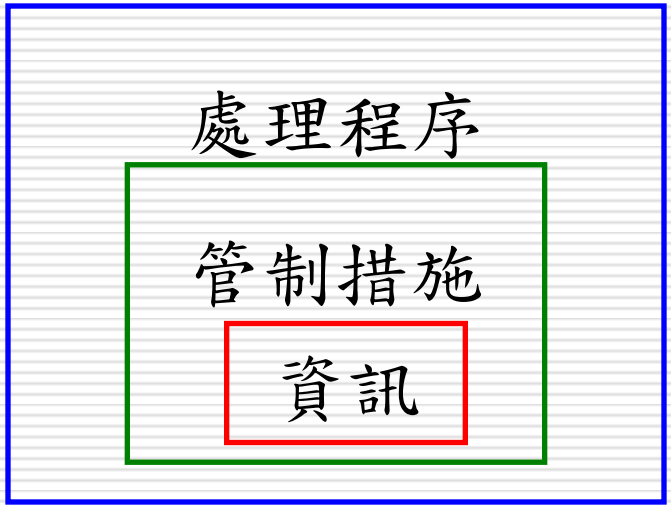


檔案相關法規要點整併情形



資訊安全定義介紹

- 資產
- 資訊
- 資訊安全



保護

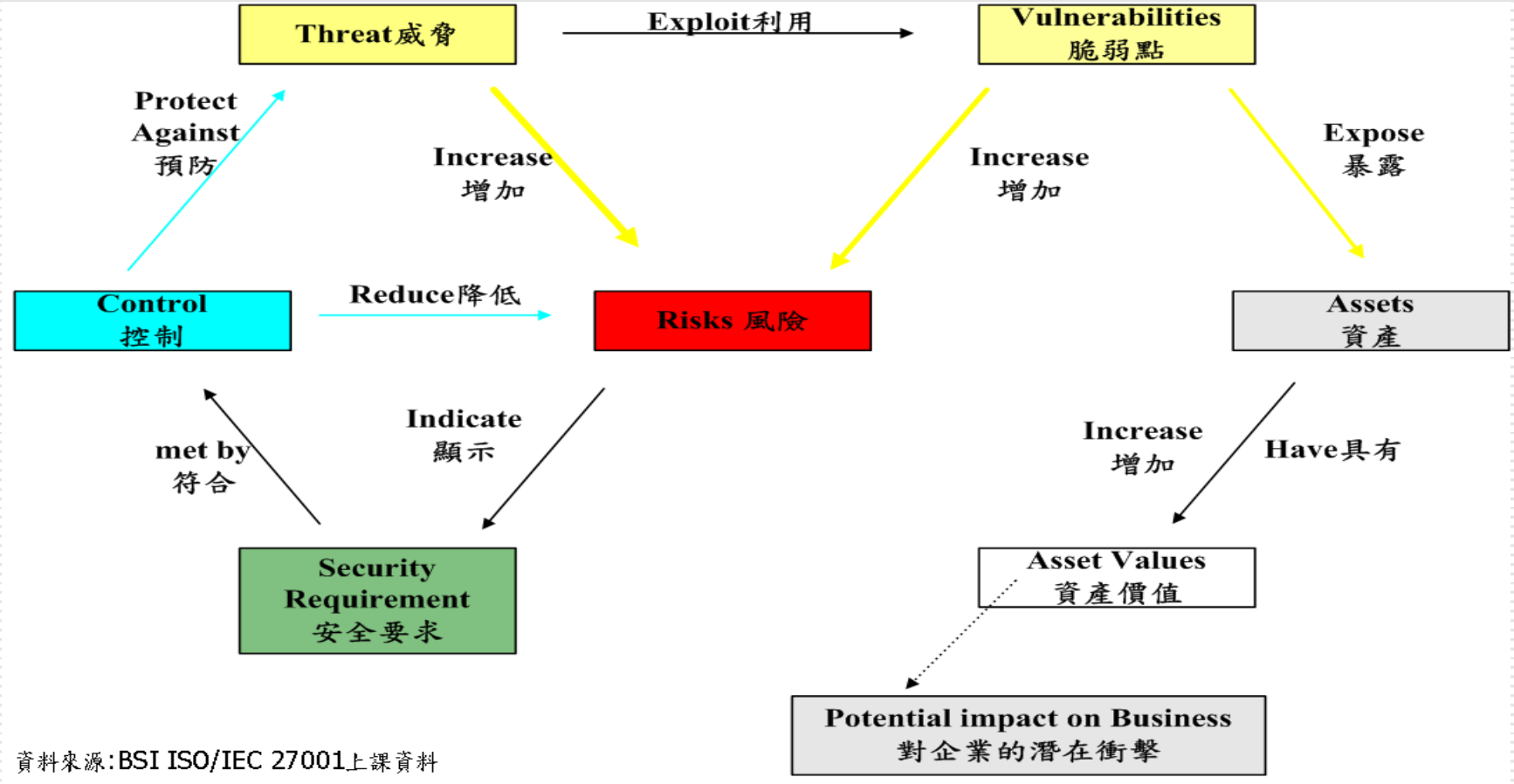
資訊安全管理系統

- 資訊安全管理系統(Information Security Management System；簡稱ISMS)

  整體管理系統的一部分，乃根據企業風險管理的辦法所制訂，用來建立、執行、操作、監控、審查、維護與改進資訊安全。

- 資訊安全管理系統國際認證標準
  - ISO 27001資訊安全管理系統實務規範
  - ISO 27002資訊安全管理實務準則

風險管理活動情形



資料來源:BSI ISO/IEC 27001上課資料

ＩＳＭＳ認證標準

- ISO 27001資訊安全管理系統實務規範
- ISO 27002資訊安全管理實務準則
- ISO 27001相關管理規範
- ISO 27001 PDCA模式
- 資訊安全系統文件規範
- 資訊安全系統控制措施

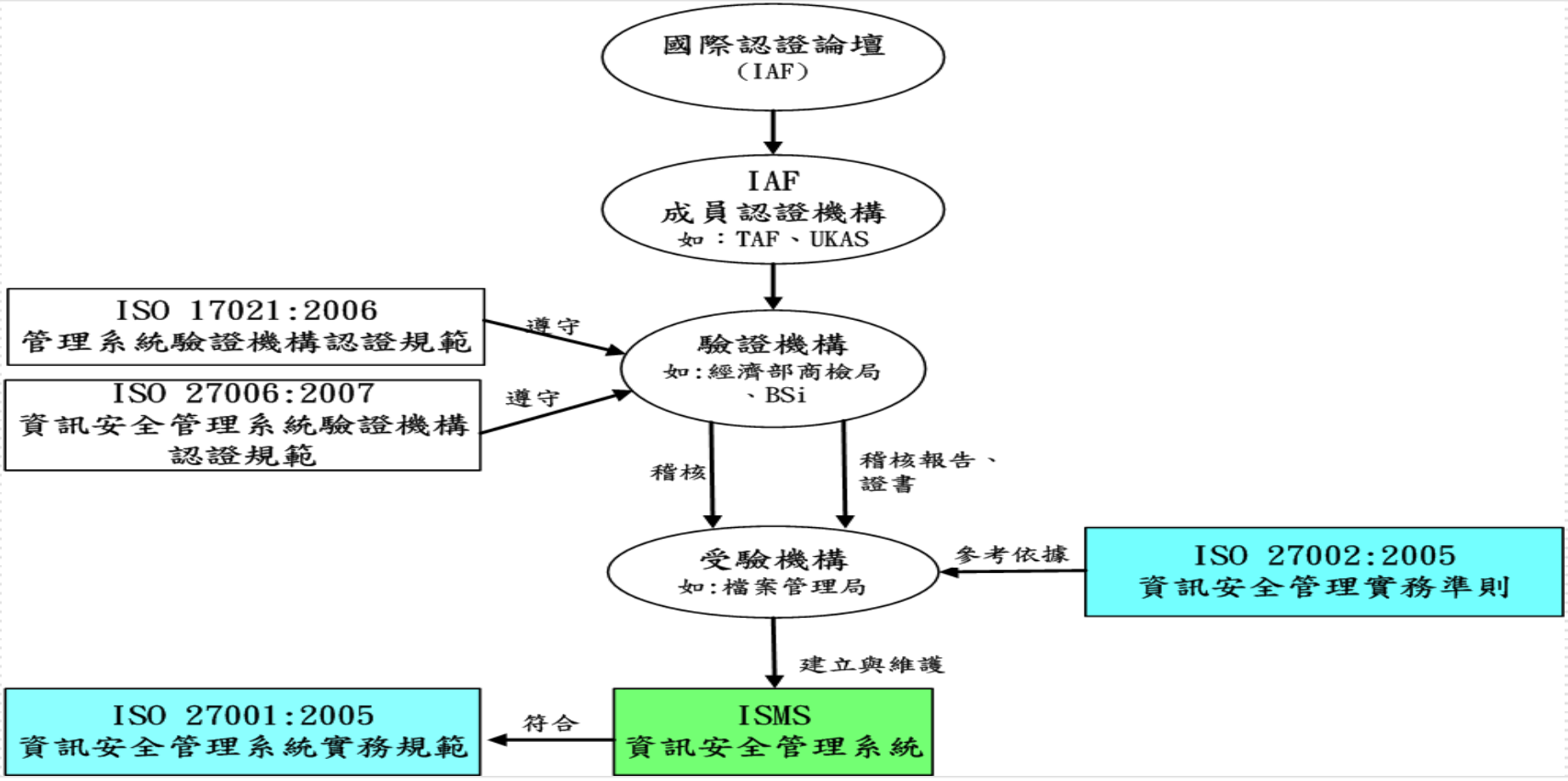
ISO 27001 ISMS實務規範

以PDCA（Plan-Do-Check-Act）過程導向模式管理已文件化的資訊安全管理系統，藉由國際符合性評鑑程序及週期性稽核作業，審查組織資訊安全管理系統，驗證資訊安全管理系統有效性。

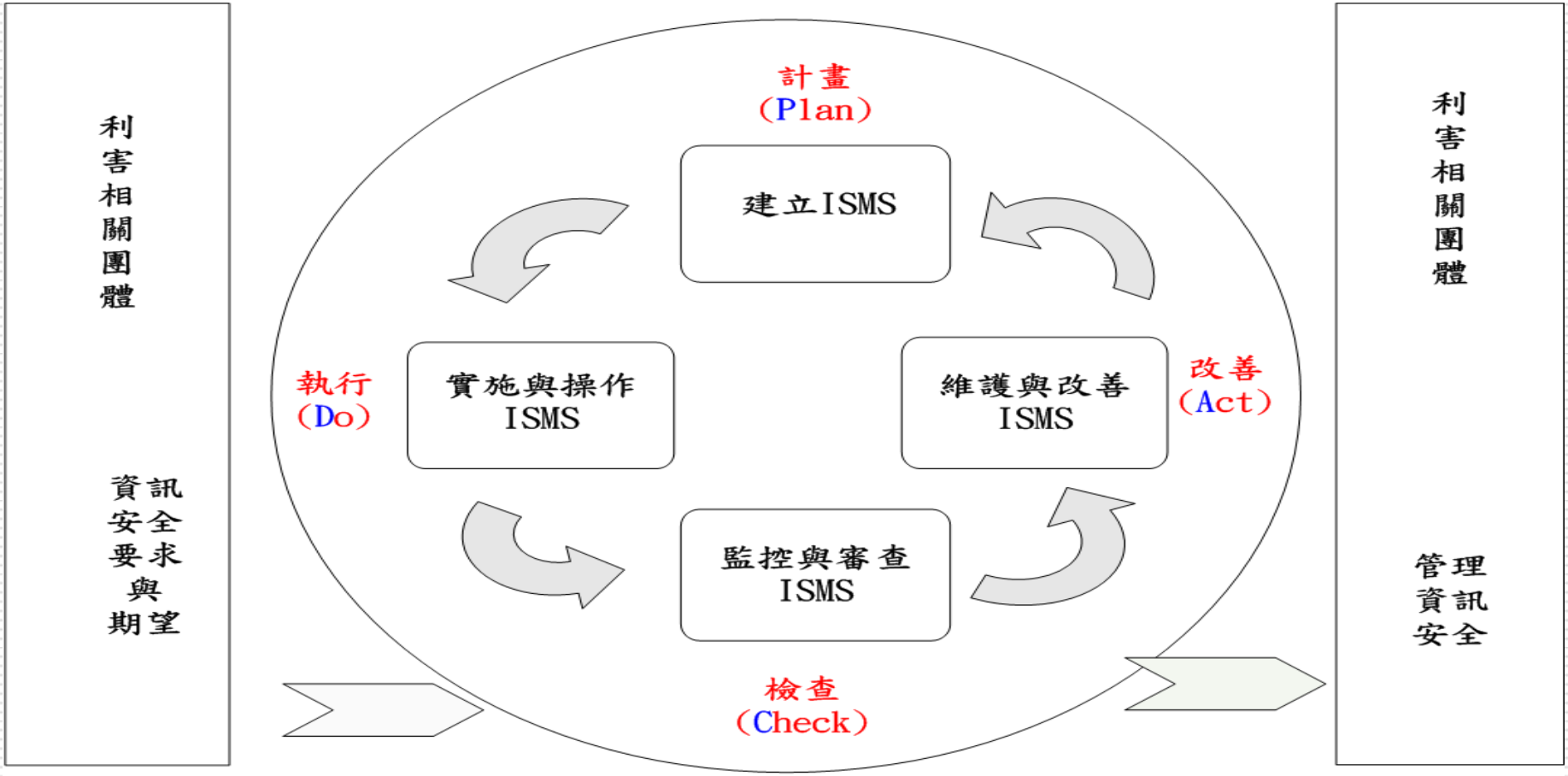
ISO 27002 ISMS實務準則

- 運用風險評鑑與風險治理觀念，提供企業或政府機關建置資訊安全管理系統(ISMS)的參考依據，包含：安全政策、組織資訊安全、資產管理、人力資源安全、實體與環境安全、通信與作業管理、存取控制、資訊系統取得開發與維護、資訊安全事故管理、營運持續管理及遵循性共計11個領域、39個控制目標及133項控制措施 。
- 適用性聲明(Statement of Applicability ，SOA)

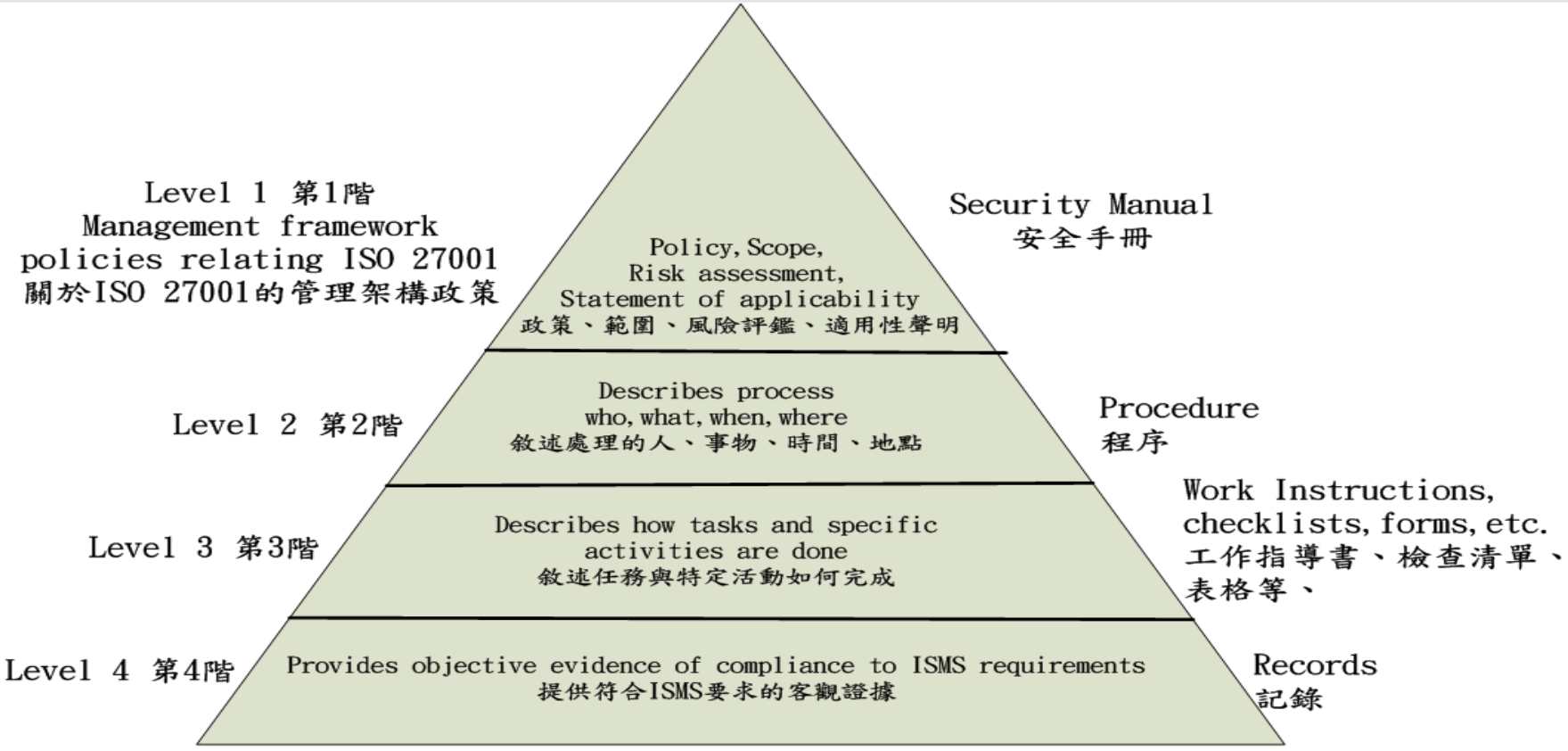
ISO 27001相關管理規範



ISO 27001 PDCA模式



ISO 27001文件規範



資料來源:BSI ISO/IEC 27001上課資料

資訊安全管理系統領域

- 安全政策
- 組織資訊安全
- 資產管理
- 人力資源安全
- 實體與環境安全
- 通信與作業管理
- 存取控制
- 資訊系統取得開發與維護
- 資訊安全事故管理
- 營運持續管理
- 遵循性

資訊安全系統控制措施

領域	控制目標
安全政策	資訊安全政策
組織資訊安全	內部組織、外部組織
資產管理	資產責任、資產分類
人力資源安全	聘僱之前、聘僱期間、聘僱終止或變更
實體與環境安全	安全區域、設備安全

資訊安全系統控制措施

領域	控制目標
通信與作業管理	作業程序與責任、第三方服務遞送管理作業、系統規劃與驗收、防範惡意碼與行動碼、備份、網路安全管理、處理媒體、資訊交換、電子商務服務、監控
存取控制	存取控制的營運要求 、使用者存取管理 、使用者責任 、網路存取控制 、作業系統存取控制 、應用與資訊存取控制 、行動式電腦作業與遠距工作

資訊安全系統控制措施

領域	控制目標
資訊系統取得開發與維護	資訊系統的安全要求、應用系統的正確處理、密碼控制措施 、系統檔案的安全、開發及支援過程的安全、技術脆弱性管理
資訊安全事故管理	通報資訊安全事件與弱點、管理資訊安全事故與改善
營運持續管理	營運持續管理的資訊安全層面
遵循性	遵循法規要、遵循安全政策與標準、資訊系統稽核的考量

檔案資訊諮詢服務中心

- 99.05.14遷入電子檔案長期保存實驗室
- 檔案資訊諮詢服務中心

  電話：(02) 2775-1580 按 2

  傳真：(02) 2775-1507

  MSN帳號：NAACallCenter@hotmail.com

  Skype帳號：NAACallCenter
- 電子公文檔案管理系統客服中心

  電話：(02) 2775-1580 按 3

  傳真：(02) 2775-1507