財團法人國家實驗研究院
國家地震工程研究中心

『資訊安全管理制度維護案』

教育訓練

資安法令宣導及ISO27001標準介紹課程(二)

98年06月09日(二)

講師：邱瑩青

財團法人中華民國國家資訊基本建設產業發展協進會

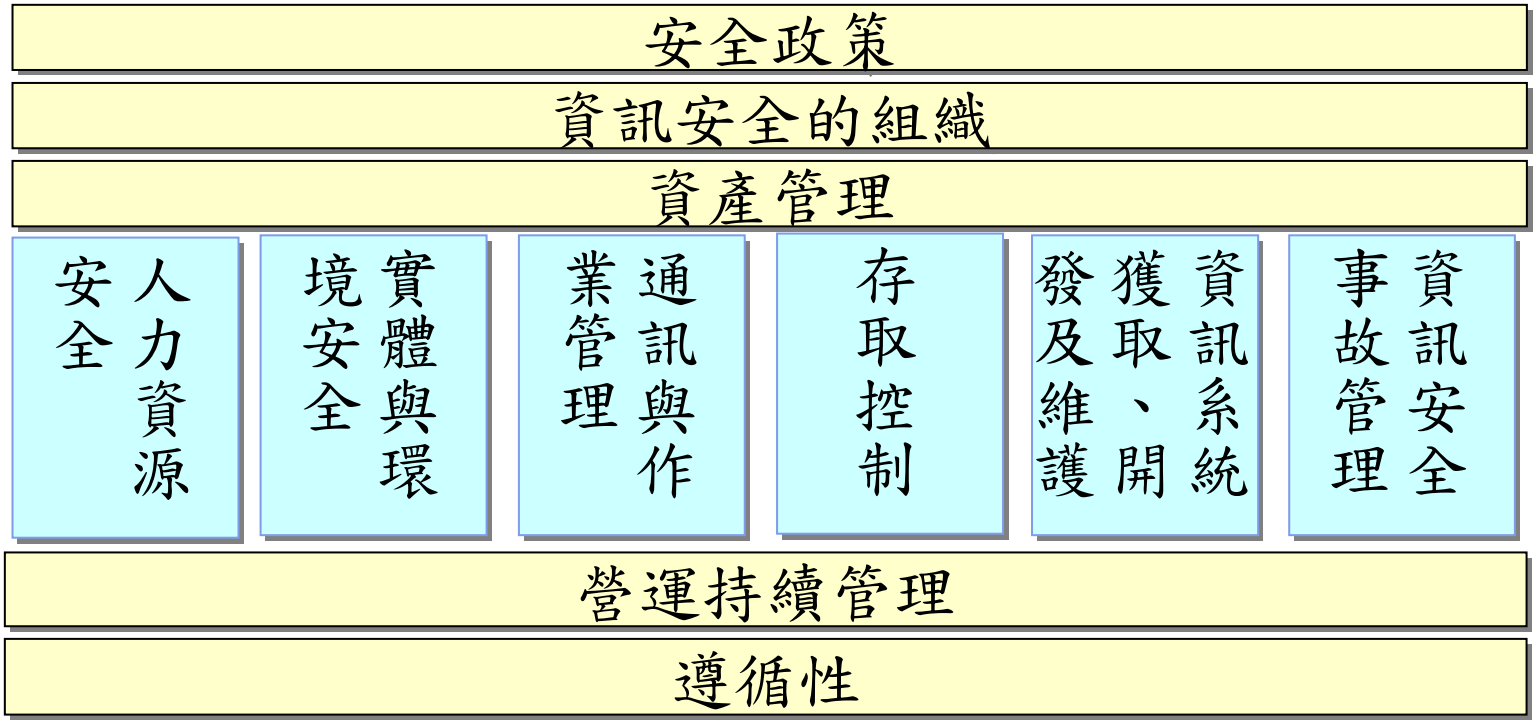
目錄

ISO/CNS 27001:2005

附錄 A 控制目標和控制措施

財團法人中華民國國家資訊基本建設產業發展協進會

11 個領域、 39 個控制目標、 133 個控制措施



安全政策

財團法人中華民國國家資訊基本建設產業發展協進會

A.5.1 安全政策

- 目標

  依照營運要求及相關法律與法規，提供管理階層對資訊安全之指示與支持。

- 控制要點
  - A.5.1.1資訊安全政策文件
  - A.5.1.2資訊安全政策之審查

資訊安全的組織

財團法人中華民國國家資訊基本建設產業發展協進會

A.6.1 內部組織

- 目標

  於組織內管理資訊安全。

- 控制要點
  - A.6.1.1 管理階層對資訊安全的承諾
  - A.6.1.2 資訊安全協調工作
  - A.6.1.3 資訊安全責任的配置
  - A.6.1.4 資訊處理設施的授權過程

A.6.1 內部組織

- 控制要點(續)
  - A.6.1.5 機密性協議
  - A.6.1.6 與主管機關的接觸
  - A.6.1.7 與特殊利害相關團體的聯繫
  - A.6.1.8 資訊安全的獨立審查

A.6.2 外部團體

- 目標

  維持外部團體所存取、處理、管理或與其通信之組織資訊與資訊處理設施的安全。

- 控制要點
  - A.6.2.1 與外部團體相關的風險之識別
  - A.6.2.2 處理客戶事務的安全說明
  - A.6.2.3 第三方協議中之安全說明

資產管理

財團法人中華民國國家資訊基本建設產業發展協進會

A.7.1 資產責任

- 目標

  達成及維持組織資產的適切保護。

- 控制要點
  - A.7.1.1 資產清冊
  - A.7.1.2 資產的擁有權
  - A.7.1.3 資產之可被接受的使用

A.7.2 資訊分類

- 目標

  確保資訊受到適切等級的保護。

- 控制要點
  - A.7.2.1 分類指導綱要
  - A.7.2.2 資訊標示與處置

人力資源安全

財團法人中華民國國家資訊基本建設產業發展協進會

A.8.1 聘僱之前

- 目標

  確保員工、承包者及第三方使用者了解其責任，並勝任其所被認定的角色，以降低竊盜、詐欺或設施誤用的風險。

- 控制要點
  - A.8.1.1 角色與責任
  - A.8.1.2 篩選
  - A.8.1.3 聘僱條款與條件

A.8.2 聘僱期間

- 目標

  確保所有員工、承包者及第三方使用者認知資訊安全的威脅與關切事項、其基本責任與強制責任，並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險。

- 控制要點
  - A.8.2.1 管理階層責任
  - A.8.2.2 資訊安全認知、教育及訓練
  - A.8.2.3 懲處過程

A.8.3 聘僱的終止或變更

- 目標

  確保員工、承包者及第三方使用者以有條理的方式脫離組織或變更 。

- 控制要點
  - A.8.3.1 終止責任
  - A.8.3.2 資產的歸還
  - A.8.3.3 存取權限的移除

實體與環境安全

財團法人中華民國國家資訊基本建設產業發展協進會

A.9.1 安全區域

- 目標

  防止組織場所與資訊遭未經授權的實體存取、損害及干擾。

- 控制要點
  - A.9.1.1 實體安全周界
  - A.9.1.2 實體進入控制措施
  - A.9.1.3 保全辦公室、房間及設施
  - A.9.1.4 對外部與環境威脅的保護
  - A.9.1.5 在安全區域內工作
  - A.9.1.6 公共進出、收發及控制措施裝卸區

A.9.2 設備安全

- 目標

  防止資產的遺失、損害、竊盜或破解，並防止組織活動的中斷。

- 控制要點
  - A.9.2.1 設備安置與保護
  - A.9.2.2 支援的公用設施
  - A.9.2.3 佈纜的安全
  - A.9.2.4 設備維護

A.9.2 設備安全

- 控制要點(續)
  - A.9.2.5 場所外設備的安全
  - A.9.2.6 設備的安全汰除或再使用
  - A.9.2.7 財產的攜出

通訊與作業管理

財團法人中華民國國家資訊基本建設產業發展協進會

A.10.1 作業之程序與責任

- 目標

  確保正確與安全地操作資訊處理設施。

- 控制要點
  - A.10.1.1 文件化作業程序
  - A.10.1.2 變更管理
  - A.10.1.3 職務的區隔
  - A.10.1.4 開發、測試及運作設施的分隔

A.10.2 第三方服務交付管理

- 目標

  實作與維持適切等級之資訊安全及服務交付，並能與第三方服務交付協議一致。

- 控制要點
  - A.10.2.1 服務交付
  - A.10.2.2 第三方服務的監視與審查
  - A.10.2.3 第三方服務變更的管理

A.10.3 系統規劃與驗收

- 目標

  使系統失效的風險最小化。

- 控制要點
  - A.10.3.1 容量管理
  - A.10.3.2 系統驗收

A.10.4 防範惡意碼與行動碼

- 目標

  保護軟體與資訊的完整性。

- 控制要點
  - A.10.4.1 對抗惡意碼的控制措施
  - A.10.4.2 對抗行動碼的控制措施

A.10.5 備份

- 目標

  維持資訊及資訊處理設施的完整性與可用性。

- 控制要點
  - A.10.5.1 資訊備份

A.10.6 網路安全管理

- 目標

  確保對網路內資訊與支援性基礎建設的保護。

- 控制要點
  - A.10.6.1 網路控制措施
  - A.10.6.2 網路服務的安全

A.10.7 媒體的處置

- 目標

  防止資產被未經授權的揭露、修改、移除或破壞，以及營運活動的中斷。

- 控制要點
  - A.10.7.1 可移除式媒體的管理
  - A.10.7.2 媒體的汰除
  - A.10.7.3 資訊處置程序
  - A.10.7.4 系統文件的安全

A.10.8 資訊交換

- 目標

  維護組織內及與任何外部個體所交換資訊與軟體的安全。

- 控制要點
  - A.10.8.1 資訊交換政策與程序
  - A.10.8.2 交換協議
  - A.10.8.3 輸送中的實體媒體
  - A.10.8.4 電子傳訊
  - A.10.8.5 營運資訊系統

A.10.9 電子商務服務

- 目標

  確保電子商務服務的安全性及其安全的使用。

- 控制要點
  - A.10.9.1 電子商務
  - A.10.9.2 線上交易
  - A.10.9.3 公眾可用的資訊

A.10.10 監視

- 目標

  偵測未經授權的資訊處理活動。

- 控制要點
  - A.10.10.1 稽核存錄
  - A.10.10.2 監控系統的使用
  - A.10.10.3 日誌資訊的保護
  - A.10.10.4 管理者與操作者日誌
  - A.10.10.5 失誤存錄
  - A.10.10.6 鐘訊同步

存取控制

財團法人中華民國國家資訊基本建設產業發展協進會

A.11.1 存取控制的營運要求

- 目標

  控制資訊的存取。

- 控制要點
  - A.11.1.1 存取控制政策

A.11.2 使用者存取管理

- 目標

  確保經授權使用者對資訊系統的存取與防止未經授權的存取。

- 控制要點
  - A.11.2.1 使用者註冊
  - A.11.2.2 特權管理
  - A.11.2.3 使用者通行碼管理
  - A.11.2.4 使用者存取權限的控制措施審查

A.11.3 使用者責任

- 目標

  防止未經授權的使用者存取資訊與資訊處理設施，以及使其遭受破壞或竊盜。

- 控制要點
  - A.11.3.1 通行碼的使用
  - A.11.3.2 無人看管的使用者設備
  - A.11.3.3 桌面淨空與螢幕淨空政策

A.11.4 網路存取控制

- 目標

  防止網路服務遭未經授權的存取。

- 控制要點
  - A.11.4.1 網路服務的使用政策
  - A.11.4.2 外部連線的使用者鑑別
  - A.11.4.3 網路設備識別
  - A.11.4.4 遠端診斷與組態埠保護

A.11.4 網路存取控制

- 控制要點(續)
  - A.11.4.5 網路區隔
  - A.11.4.6 網路連接控制
  - A.11.4.7 網路選路控制

A.11.5 作業系統存取控制

- 目標

  防止作業系統遭未經授權的存取。

- 控制要點
  - A.11.5.1 保全登入程序
  - A.11.5.2 使用者識別與鑑別
  - A.11.5.3 通行碼管理系統
  - A.11.5.4 系統公用程式的使用

A.11.5 作業系統存取控制

- 控制要點(續)
  - A.11.5.5 會談期逾時
  - A.11.5.6 連線時間的限制

A.11.6應用系統與資訊存取控制

- 目標

  防止應用系統中的資訊遭未經授權的存取 。

- 控制要點
  - A.11.6.1 資訊存取限制
  - A.11.6.2 敏感系統的隔離

A.11.7行動計算與遠距工作

- 目標

  確保使用行動計算與遠距工作設施時之資訊安全。

- 控制要點
  - A.11.7.1 行動計算與通信
  - A.11.7.2 遠距工作

資訊系統
取得、開發與維護

財團法人中華民國國家資訊基本建設產業發展協進會

A.12.1 資訊系統的安全要求

- 目標

  確保安全是整體資訊系統的一部分。

- 控制要點
  - A.12.1.1 安全要求分析與規格

A.12.2 應用系統的正確處理

- 目標

  防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。

- 控制要點
  - A.12.2.1 輸入資料的驗證
  - A.12.2.2 內部處理的控制措施
  - A.12.2.3 訊息完整性
  - A.12.2.4 輸出資料確認

A.12.3 密碼控制措施

- 目標

  藉由密碼方式以保護資訊的機密性、鑑別性或完整性。

- 控制要點
  - A.12.3.1 使用密碼控制措施的政策
  - A.12.3.2 金鑰管理

A.12.4 系統檔案的安全

- 目標

  確保系統檔案的安全。

- 控制要點
  - A.12.4.1 作業軟體的控制
  - A.12.4.2 系統測試資料的保護
  - A.12.4.3 程式源碼的存取控制

A.12.5 開發與支援過程的安全

- 目標

  維持應用系統軟體與資訊的安全。

- 控制要點
  - A.12.5.1 變更控制程序
  - A.12.5.2 作業系統變更後的應用系統技術審查
  - A.12.5.3 套裝軟體變更的限制
  - A.12.5.4 資訊洩漏
  - A.12.5.5 委外的軟體開發

A.12.6 技術脆弱性管理

- 目標

  降低因利用已公佈的技術脆弱性所導致的風險。

- 控制要點
  - A.12.6.1 技術脆弱性控制

資訊安全事故管理

財團法人中華民國國家資訊基本建設產業發展協進會

A.13.1 通報資訊安全事件與弱點

- 目標

  確保與資訊系統相關的資訊安全事件與弱點，被以能夠採取及時矯正措施的方式傳達。

- 控制要點
  - A.13.1.1 通報資訊安全事故
  - A.13.1.2 通報安全弱點

A.13.2 資訊安全事故與改進的管理

- 目標

  確保採用一致與有效的作法於資訊安全事故的管理。

- 控制要點
  - A.13.2.1 責任與程序
  - A.13.2.2 從資訊安全事故中學習
  - A.13.2.3 證據的收集

營運持續管理

財團法人中華民國國家資訊基本建設產業發展協進會

A.14.1 營運持續管理的資訊安全層面

- 目標

  為對抗營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時再續(resumption) 。

- 控制要點
  - A.14.1.1 資訊安全納入營運持續管理過程
  - A.14.1.2 營運持續與風險評鑑
  - A.14.1.3 發展與實作包括資訊安全的持續計畫
  - A.14.1.4 營運持續規劃框架
  - A.14.1.5 營運持續計畫的測試、維護及重新評鑑

遵循性

財團法人中華民國國家資訊基本建設產業發展協進會

A.15.1 遵循適法性要求

- 目標

  避免違反任何法律、法令、法規或契約義務，以及任何安全要求。

- 控制要點
  - A.15.1.1 識別適用之法條
  - A.15.1.2 智慧財產權
  - A.15.1.3 組織紀錄的保護
  - A.15.1.4 個人資訊的資料保護與隱私
  - A.15.1.5 防止資訊處理設施的誤用
  - A.15.1.6 密碼控制措施的規定

A.15.2 安全政策與標準的遵循性以及技術遵循性

- 目標

  避免違反任何法律、法令、法規或契約義務，以及任何安全要求。

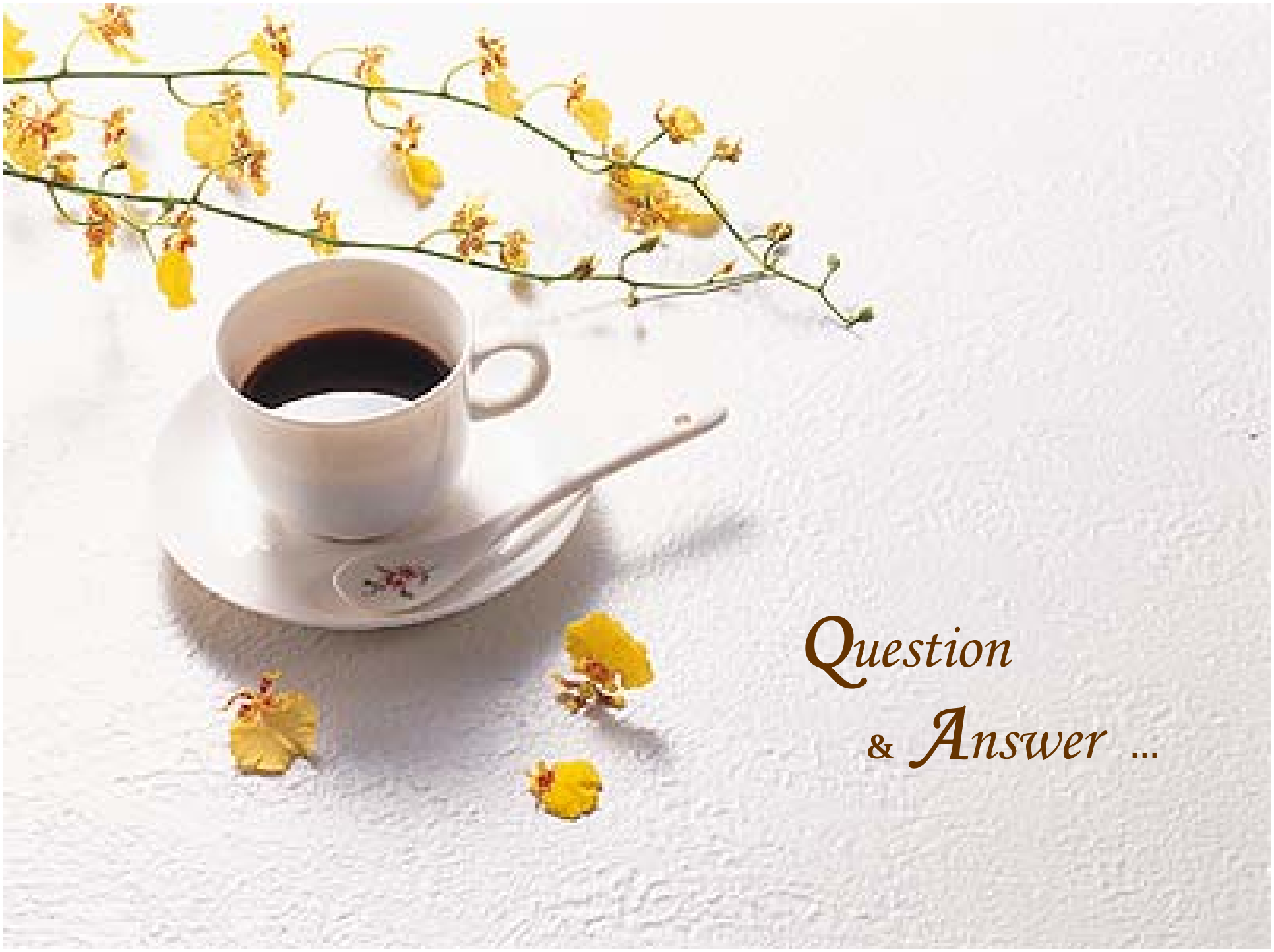
- 控制要點
  - A.15.2.1 安全政策與標準的控制措施遵循性
  - A.15.2.2 技術遵循性查核

A.15.3 資訊系統稽核考量

- 目標

  使資訊系統稽核過程的有效性最大化，並使其產生或受到之干擾降至最低。

- 控制要點
  - A.15.3.1 資訊系統稽核控制
  - A.15.3.2 資訊系統稽核工具控制措施的保護


Question
& Answer ...