工業技術研究院
Industrial Technology
Research Institute

信息安全管理體系(ISMS,ISO/IEC 27001:2013)

規劃與建置管理師培訓課程

■ 課程簡介

信息安全管理體系 (ISMS, ISO/IEC 27001:2013) 規劃與建置管理師 培訓課程，是協助組織建立信息安全管理體系最佳方法，可以直接降低顧問與諮詢費用與縮短建立管理系統基礎文件所需要的時間。

課程當中，除了與學員詳細討論、介紹標準的要求之外，本課程直接提供學員管理體系基礎文件範本，在小組討論活動中，講師協助學員進行實作，協助組織快速建立管理體系所需要的政策、程序等文件基礎。

■ 課程目標：

本課程結合課堂簡報、小組討論、經驗交流、角色扮演、情境演練等，透過參與式 (participated learning) 學習，培養學員下列的能力：

- 了解資訊安全管理系統、文件化要求與目的。
- 實作管理文件，包含政策、程序等管理系統基礎文件，包含
  - 選擇與訂定 合適資訊安全管理系統實施範圍與認證範圍
  - 訂定 資訊安全管理政策與目標
  - 了解 資訊安全管理文件化與紀錄要求
  - 建立 資訊安全組織
  - 建立 資訊資產與資訊安全風險管理(風險識別、分析、評估與控制) 機制
  - 建立人員 (員工、外包商、供應商)風險控制機制
  - 建立安全技術 (加密、行動裝置、冗餘)風險控制機制
  - 建立實體與環境風險管理機制
  - 建立網絡與通信風險管理機制
  - 建立資訊系統風險管理機制
  - 建立軟件開發與應用程式風險管理機制
  - 建立技術與規範符合性風險管理機制
  - 建立資安事件與異動管理風險管理機制
  - 建立 組織持續營運計畫過程當中的資訊安全風險管理機制

工業技術研究院
Industrial Technology
Research Institute

■課程效益

- 組織具備根據國際標準 ISO/IEC 27001，執行資訊安全管理系統**規劃(Planning) 與 建置(Implementing)**的能力，符合認證要求。
- 參與課程並通過考試學員，將獲得課程證書，展現執行資訊安全管理系統**規劃**與**建置**的專業知識與技能，**符合管理系統要求經理人應該具備之能力(Competence)**。
- 協助組織**有效地**執行資訊安全管理系統**規劃**與**建置**，有助於確保組織保護敏感資料 (例如，個人資料、公司商業機密等)，符合利害相關方的期望與公司治理要求。
- 了解現行資訊安全管理系統與國際標準的**差異**，持續強化管理系統能力。

■ 適合對象：

管理系統是組織日常營運活動的一部份，**任何參與組織營運活動的內、外部人員**，對於國際標準的了解，皆有助於組織業務相關活動的推動與提升有效性。本課程建議組織中，擔任下列功能的人員參加：

- 資訊技術 (IT) 與信息安全 (IS) 相關經理人
- 風險管理相關經理人
- 公司治理、政策制定經理人
- 諮詢、顧問
- 審核員

■ 參加本課程的學員，必須具備下列知識：

1. 瞭解什麼是管理系統持續改善循環 (PDCA)
2. 資訊安全管理：瞭解下列資訊安全管理原則與概念：
    - 瞭解資訊安全的需要與重要性
    - 組織內，每位員工被賦予資訊安全的責任，與重要性
    - 管理階層承諾、利害相關方與要求
    - 資訊安全如何提高組織的價值與社會責任
    - 如何透過風險評鑑結果，決定適切的風險管控措施，並且達到風險可接受程度
    - 如何將資訊安全整合到組織的資訊、通訊網路、系統等，成為不可或缺的一部份
    - 資訊安全事件的預防、偵測活動
    - 確保組織落實資訊安全管理
    - 持續進行風險評估，並且進行適當的調整

3. 瞭解資訊安全管理系統標準 (ISO/IEC 27001)：了解 ISO/IEC 27001 資訊安全管理系統要求 (包含 ISO/IEC 27002 資訊安全管理指引)，以及 ISO/IEC 27000 資訊安全管理系統常用的名詞與定義。如果需要，建議您參加我們提供的**資訊安全管理系統基礎課程**中獲得相關知識。
4. 備註：課程認證考試內容，除了 ISO/IEC 27001 之外，可能會跟本課程必備知識有關

■課程大綱

第一天：資訊安全管理手冊 - (Management System Manual - PDCA)

- 選擇與訂定 合適資訊安全管理系統實施範圍與認證範圍
- 訂定 資訊安全管理政策與目標
- 了解 資訊安全管理文件化與紀錄要求
- 建立 資訊安全組織

第二天：建立資訊安全風險管理機制 (Information Security Risk Management Process)

- 建立 資訊資產管理機制 (包含，資訊儲存、處理設備之資產清冊、所有人、申請與核准機制、分類、標示與處理等)
- 建立 資訊資訊安全風險管理(包含，風險與機會識別、分析、評估與控制) 機制
- 建立 資訊資產風險評估報告 (Risk Assessment Reprot)
- 建立 資訊資產風險處理計畫 (Risk Treatment Plan)
- 建立 資訊安全風險控制適用性聲明書(SoA, Statement of Applicability)

第三天：建立資訊安全風險控制機制，包含人員、環境、網絡與通訊之資訊安全管理

- 建立人員 (員工、外包商、供應商)風險控制機制
- 建立安全技術 (加密、行動裝置、多重備援/冗餘)風險控制機制
- 建立實體與環境風險管理機制
- 建立網絡與通訊風險管理機制

第四天：資訊系統、應用程式之資訊安全管理

- 建立資訊系統風險管理機制
- 建立軟件開發與應用程式風險管理機制
- 建立技術與規範符合性風險管理機制

第五天：資訊安全事件管理、營運繼續計畫過程中之資訊安全管理

- 建立資安事件與異動管理風險管理機制
- 建立 組織持續營運計畫過程當中的資訊安全風險管理機制
- 課程考試(考試通過標準為 70%，考試時間 1 小時)

工業技術研究院
Industrial Technology Research Institute

■ 舉辦日期：106/06/05(一)~06/09(五) 09:00 -18:00 (共 40hrs)

■ 費　　用：每人 35,000 元(課程包含一次中文筆試測驗，合格者將授予英文證書；未通過中文筆試測驗者，課程結束後 6 個月內，有一次免費補考機會；如果還是沒能通過補考者，則還有一次可自費補考的機會(補考費用$2000 元)。)

■ 講師為 IRCA 認定之講師

■ 注意事項：請參加學員自備筆記型電腦(需要能上網)