資訊安全與法律特訓教材-練習與討論解答

第一章 資訊安全管理概念

1. 試解釋資訊安全的三個目標：機密性、完整性及可用性，並各舉一例說明。

   答：參考 1.3 資訊安全目標 (P1-12, 1-13, 1-14)。

2. 參考圖 1-12 資訊安全管理，假想一個日常生活上使用電腦的情境，分別說明使用電腦的目的（營運目標）、為達此目的有哪些資安需求、如何規劃及執行？

   答：

   - 使用電腦的目的（營運目標）：理財規劃。
   - 資安需求：理財規劃資料不可讓無關人知道，也必須要有備份，以免毀損。
   - 規劃：基本防護要有本機防火牆、防毒軟體及加密軟體。要有定期備份機制，至少每週備份至隨身碟。
   - 執行：設定 Windows 防火牆阻擋外部攻擊及入侵；安裝防毒軟體，並設定定期每日中午 12:00 執行硬碟掃毒；使用 Windows 內建的 EFS 功能，設定理財資料的目錄為加密目錄；使用 Windows 的免費備份工具 SyncToy，設定每週備份至隨身碟。

3. 試說明什麼是資訊安全管理系統（ISMS）？

   答：參考 P1-23 及 1.5 資訊安全管理標準與規範。

4. 說明 ISMS 的國際標準 ISO/IEC 27001 與 ISO/IEC 27002 的差異為何？

   答：參考 P1-32。

5. 參考圖 1-6 資料安全的不同面向，舉例說明組織、網路、系統、程式、資料，可能遭遇何種攻擊或有何種弱點？

   答：

   - 組織：常發生資安事故，沒有制定資訊安全政策

- 人員：釣魚郵件攻擊，沒有資安認知
- 網路：駭客攻擊，沒有防護系統
- 系統：惡意程式感染，沒有安裝防毒軟體
- 程式：駭客攻擊，沒有資訊安全的設計
- 資料：資料遭竊，沒有適當的加密保護設計