

中國輸出入銀行 108 年資訊人員甄試試題

甄試類組【代碼】：資訊人員(一)【O7901】、資訊人員(二)【O7902】

科目三：資訊安全管理

*入場通知書編號：_____

注意：①作答前先檢查答案卷，測驗入場通知書編號、座位標籤、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卷作答者，不予計分。
②本試卷一張單面，非選擇題共 4 大題，每題各 25 分，總計 100 分。
③非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採橫式作答，請參照答案卷所載注意事項，於各題指定作答區內作答，並標明題號及小題號。
④請勿於答案卷上書寫姓名、入場通知書編號或與答案無關之任何文字或符號。
⑤本項測驗僅得使用簡易型電子計算器（不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝（錄）影音、資料傳輸、通訊或類似功能），且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑥答案卷務必繳回，未繳回者該節以零分計算。

第一題：

一般我們在講資訊安全管理制度時，常會聽到戴明的 PDCA 循環，這通常表示資訊安全管理制度運作的四個主要階段。請分別就 PDCA 這四個階段，舉出一個屬於該階段的程序。
【25 分】

第二題：

按照我國目前所訂定之資通安全責任等級分級辦法，在附表十「資通系統防護基準」當中有列出，如果系統防護需求為「中」或「普」的系統，在系統發展生命週期的測試階段，需要執行「弱點掃描」安全檢測，而系統防護需求為「高」的系統，則需要更進一步進行「滲透測試」。請問：

（一）滲透測試與弱點掃描的差異為何？【15 分】

（二）如果某單位已經執行了滲透測試，可否用滲透測試的報告來取代弱點掃描報告？為什麼？【10 分】

第三題：

目前銀行為了提高金融服務效率、智慧體驗與降低人事成本，引進 AI 技術（人工智慧技術），提供帳戶人臉辨識、語音聲紋辨識等系統應用，請闡述與舉例以上兩種 AI 人工智慧金融應用可能產生什麼樣的資安攻擊風險？【25 分】

第四題：

近年國際駭客入侵金融機構事件頻傳，如果您是金控的資安長，請問您會推行哪些具體作業規範來強化內部的資安防護，請提出至少五項？【提示：帳號管理、系統與網路維護、交易行為、社交工程、事件應變等】【25 分】