考科編號：20

臺灣港務股份有限公司 108 年度新進從業人員甄試

專業科目試題

筆試科目：系統專案管理與資訊管理與資通安全

甄選類科：17 師級_資訊

題號	題　　目
1	簡述系統建置專案從起始至系統上線營運的主要階段以及各階段的工作內容。
	配分：25 分
2	建立資訊安全管理系統(Information Security Management System，ISMS)旨在保障企業或組織之資訊資產的機密性(Confidentiality)、完整性(Integrity)以及可用性(Availability)，請回答以下問題： (一) 請分別說明該三項資訊安全特性為何？ (二) 國內外最廣泛使用的資訊安全管理系統標準就是知名的 ISO/IEC 27001 和 ISO/IEC 27002，請釐清這兩個標準個別的目的為何？ (三) 導入上述標準時須製作許多文件，其中一份文件是適用性聲明書(Statement of Applicability，SOA)，請說明該份文件之用途。
	配分：第 1 小題 15 分，第 2 小題 10 分，第 3 小題 5 分，共 30 分。
3	請回答以下問題： （一）解釋公開金鑰基礎建設（Public Key Infrastructure，PKI） （二）說明哪些情況下須廢止用戶的憑證？
	配分：每小題各 10 分，共 20 分。

題號	題　　目
4	對稱密碼系統(symmetric cypher)中，密碼區塊鏈結(Cipher-block chaining，CBC)是相當常用的工作模式(mode of operation)之一，密碼區塊鏈結工作模式的加密過程為 $C_i = E_K(P_i \oplus C_{i-1})$ 及 $C_0 = IV$，解密過程則為 $P_i = D_K(C_i) \oplus C_{i-1}$ 及 $C_0 = IV$，請回答以下問題： （一）請將加密過程以流程圖繪製出來。 （二）請將解密過程以流程圖繪製出來。 （三）請問此類密碼系統在加密時可否針對多個明文區塊平行處理？ （四）假設多個密文區塊同時抵達接收裝置，請問此類密碼系統在解密時可否針對多個密文區塊平行處理？ （五）假設在傳輸過程中，密文區塊有一個位元(bit)發生錯誤，請問所造成的影響為何？ 【第(三)題及第(四)題請說明原因方可計分】
	配分：每小題各 5 分，共 25 分。