臺灣銀行 109 年新進人員甄試試題

進用職等／甄試類別【代碼】：8 職等／海外資安儲備人員【Q6107】、
8 職等／資訊安全人員(一)【Q6108】

科目二：綜合科目，含：(1)資安事件分析；(2)資訊安全管理理制度；(3)網路安全管理；(4)資通安全設備管理(含 Firewall、IPS、WAF、AD 與 Exchange Server、SIEM)等實務

＊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，該節不予計分。
②本試卷為一張單面，非選擇題共 4 大題，請參考各題配分，共 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，並請**依標題指示之題號於各題指定作答區內作答**。
④請勿**於答案卷上書寫應考人姓名、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：

根據美國國家標準與技術局（National Institute of Standards and Technology, NIST）所出版的《Computer Security Incident Handling Guide》（資訊安全事故處理指南）文件及國家資通安全通報應變網站通報單之內容，請回答下列問題：

（一）資安事件應變程序的生命週期應包含哪四個階段？【12 分】

（二）在國家資通安全通報應變網站通報單中，將資安事件分成哪五大類事件？【10 分】

（三）續小題（二），在國家資通安全通報應變網站通報單中，評估事件影響等級分類是以哪三大類進行分級？【6 分】此外，在該表內依事件的嚴重等級，由輕至重分為幾個等級？【2 分】

第二題：

資訊安全應用與稽核的通用標準為 ISO 27001，企業組織在它的業務與所面臨的風險中，以 PDCA 模型為基礎推動 ISMS，請回答下列問題：

（一）請問 PDCA 分別為哪四個英文單字之縮寫？【8 分】

（二）以 PDCA 來區分，請說明「實作及操作 ISMS」、「維護及改進 ISMS」、「監控及審查 ISMS」與「建立 ISMS」分別屬於 PDCA 模型中的哪一部份？【8 分】

（三）依稽核角色來區分，稽核的類型分為幾種類型，其中組織內部的稽核屬於哪一類型？【4 分】

第三題：

請回答下列問題：

（一）身為公司資安人員，面對駭客的威脅，應對措施可以分成很多層面，請說明弱點掃描與滲透測試的差異。【10 分】

（二）請說明：

(a)何謂 OWASP TOP 10？【2 分】

(b)何謂注入攻擊 (Injection)？【4 分】

(c)何謂跨站攻擊(Cross-Site Scripting, XSS)？【4 分】

第四題：

請回答下列問題：

（一）在企業或機關團體中，網域服務系統在資訊服務中是非常重要的服務，在 Microsoft 產品中 Active Directory 為網域服務，簡稱 AD。請說明 AD 的主要功能及架設 AD 服務的優點為何？【14 分】

（二）網站應用程式防火牆(Web Application Firewall, WAF)分為軟體式和硬體式運作模式，請簡述 WAF 的功能及其軟體式與硬體式運作模式。【10 分】

（三）請說明何謂 SIEM(Security Information Event Management)？【6 分】