101年公務人員高等考試三級考試試題　　代號：36280　　全一頁

類　　科：資訊處理
科　　目：資訊管理與資通安全
考試時間：2小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、試比較封包過濾防火牆（Packet Filter Firewall）、網路型入侵偵測系統（Network-based Intrusion Detection System, IDS）與網路型入侵防禦系統（Network-based Intrusion Prevention System, IPS）在資安防護上之功能區別。（15分）

二、跨網站腳本攻擊（Cross Site Script, XSS）與資料隱碼（SQL Injection）是目前政府機關網頁應用程式最常受到的兩大威脅。試說明 SQL Injection 與 XSS 弱點發生原因，並舉例說明測試方法以及其防範方式。（20分）

三、㈠請說明 BS 25999 標準中，營運持續管理（Business Continuity Management, BCM）實施的四個階段內容，包括：「了解組織」、「決定營運持續管理策略」、「發展與執行營運持續管理作為」及「演練、維護與審查」。（20分）
㈡其中在「了解組織」中，最重要的就是以營運衝擊分析（Business Impact Analysis, BIA）與風險評鑑（Risk Assessments, RA）二大方法進行。試說明此二者實施目的之不同。（5分）

四、在資訊委外作業中，「委外服務水準的管控」被視為委外服務成敗的一個重要因素。
㈠何謂服務水準協定（Service-Level Agreements, SLA）與操作水準協定（Operational Level Agreements, OLA）？（10分）
㈡雲端環境的委外比傳統委外更需注重那三個因素？（10分）

五、智慧資本是企業與政府組織的寶貴資產，為了創造與保存這項資產，可以透過組織管理與資訊科技的輔助而達成。
㈠請說明組織在知識創造過程所扮演的角色與作為，並請舉例說明。（10分）
㈡資料挖掘（Data Mining）具備那些功能？並各舉一應用例。（10分）