108 年特種考試地方政府公務人員考試試題

等　　別：三等考試
類　　科：資訊處理
科　　目：資訊管理與資通安全
考試時間：2 小時

一、鑑於國內外資安情資來源逐漸多元，且數量日益增加，國家資安資訊分享與分析中心於107年正式運作。試說明分享資安情資的好處與重要性。（25分）

【解題關鍵】
《考題難易》：★★
《破題關鍵》：根據資通安全管理法之子法-資通安全情資分享辦法，參考 107 高考類似題作答。

【擬答】：

透過情資格式標準化與系統自動化之分享機制，提升情資分享之即時性、正確性及完整性，建立縱向與橫向跨領域之資安威脅與訊息交流，達到情資迅速整合、即時分享及有效應用之目的，提升國家資訊安全整體應變與防護能力。

㈠分享資安情資的好處

1. 快速識別企業內外部網路安全現況：
通過威脅情資有效運用，企業能針對外部威脅環境完整進行掌握，從而依據威脅環境之變化，可有效設計及部署相關安全措施及檢測重點；同時企業如針對威脅態勢能獲得更完整之掌握時，高階管理階段更能做出有效及明確之安全決策。

2. 有效縮短事中應變時間
通過威脅情資分享與分析，原本看似互不相關的資訊能相互進行關聯，並可讓資安事件應變團隊（CSIRT）更有效確認事件發生的來龍去脈，加速確認資安事件發生手法及範圍。

3. 有效提高防守強度及靈活度：
企業可依據外部現況攻擊策略、技術及程序（Tactics, Techniques, and Procedures, TTPs）快速偵測、應對，使防禦從被動變為主動。

㈡分享資安情資的重要性

1. 攻擊複雜度越來越高：單一企業面對複雜之攻擊，其能力、專業知識有時而窮。透過集體的力量，可更有效掌握攻擊活動，有效因應。
2. 違約成本提高：各種法規對於資料外洩或資安管理缺失造成之損害，其賠償金額與法律責任日趨高漲。
3. 情資雜訊充斥：各種威脅情資數量龐雜多樣，須藉助專業分析、過濾後，再將正確、有用的情資分享予會員機構。
4. 監管機構對情資分享之重視：如美國設立的 FS-ISAC、英國的 CiSP、及我國的 F-ISAC 等。

二、第五代行動通訊（5G）即將進入商用階段，其具備高頻寬、高密度、及低延遲等優良特性，可乘載智慧物聯網多元應用服務，將帶動高品質視聽娛樂、智慧醫療、智慧工廠、自駕車、無人機、智慧城市等創新應用。因應5G與智慧物聯網的加入，說明組織內部網路如何管理與防禦攻擊。（25分）

【解題關鍵】
《考題難易》：★★★★
《破題關鍵》：考量 5G 與 AIOT 特性，參考 107 高考類似題作答。

【擬答】：

㈠組織內部網路管理：

1. 自動化網路應用程式管理不僅要高性能，還要高度自適應環境，確保持續更新以達成一致的保護。它還需要企業組織從 DevOps 模型過渡到 DevSecOps 模型，確保將安全性直接整合到開發管理與策略中。
2. 對雲端優化的分佈式網路，相關應用程式的支持將要求在不同網路生態之間達成安全性無縫行動，並且不會丟失工作流程或捨棄安全功能。
3. 數位化轉型將產生大量數據，其中大部分將被加密。加密數據目前將佔網路流量的 70%以上。只有使用加密程序來保護傳輸的數據時，該百分比才會成長。這將需要物聯網和其他邊緣設備中的高性能安全工具，這些設備可以在速度和規模上檢查這些加密流量。
4. 諸如網路切片之類的新策略將使企業能夠更有效地消耗大規模數據環境中的行動資源。這還需要分段和邊緣微分段來保護關鍵資源，同時將它們與開放且安全性較低的環境隔離開來。

㈡組織內部網路防禦：

1. 實現邊緣到邊緣的安全性
   需要從物聯網邊緣到核心企業網路，再到分支機構和多個公共雲端確定企業生態系統相關的所有內容，進行評估其關鍵性並確認相關狀態。然後驗證所有連線訪問網路資源的請求。
2. 支持彈性的，邊緣到邊緣的混合系統
   將經過驗證的傳統策略與新方法相結合，雖然網路分段連線是一種經過驗證的技術，可以控制網路安全風險並保護敏感資源，但舊策略可能不適用於 5G 世界。新的細分策略需要同時顧及本地和遠端資源，這些資源混合了企業可控制或不控制的細分市場。IT 團隊需要評估如何在實施 5G 網路和公共雲端服務時同時管理多個管理系統的複雜性。
3. 共享威脅情報、關聯事件數據和自動事件回應將深入整合到安全技術
   這將需要開發和採用綜合安全架構，機器學習、人工智慧和自動化是加速幫助決策的關鍵，從而縮小檢測和緩解相關差距。
4. 不同安全工具之間的相互操作性還需要建立在新的開放式 5G 安全標準上。
   跨供應商採用的 API 以及可集中管理的機制，是查看安全事件與擬定安全策略不可或缺的管理工具。

三、部分企業與組織的網路或是資訊管理系統是外包廠商負責，例如會計資訊管理系統由A廠商開發，網站應用程式由B廠商開發維護等。說明組織如何做好控管，確保資訊隱私安全與預防攻擊事件。（25分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》：本題以 ISO27001 A.15 供應商關係中的控制措施即可作答，參考 108 地特四等類似題。

【擬答】：

根據 ISO27001，為控管供應商資安風險，可以實行 A.15 供應商關係控制措施，包括下列：

㈠ A.15.1 供應商關係的資訊安全
其目標在確保供應商可存取之組織資產的保護。

1. A.15.1.1 供應商關係的資訊安全政策
   應與供應商協議資訊安全要求，以減少供應商對組織資產存取的風險並加以文件化
2. A.15.1.2 供應商協議內的安全處理
   應建立所有相關的資訊安全要求，並與每項可存取、處理、儲存、傳達組織資訊或提供 IT 基礎設施組件的供應商達成協議。
3. A.15.1.3 ICT 供應鏈
   與供應商的協議，應包含因應有關資訊與通訊技術服務及產品供應鏈之資訊安全風險的要求。

㈡ A.15.2 供應商服務交付管理

其目標在維持議定等級之資訊安全及服務交付，並能與供應商協議一致。

1. A.15.2.1 供應商服務的監控與審查

應定期監控、審查及稽核供應商提供之服務。

2. A.15.2.2 供應商服務變更的管理

供應商所提供服務的變更，包含維持與改進現有的資訊安全政策、程序及控制措施均應加以管理，並考量所涉及之營運系統與過程的重要性及風險重新評鑑。

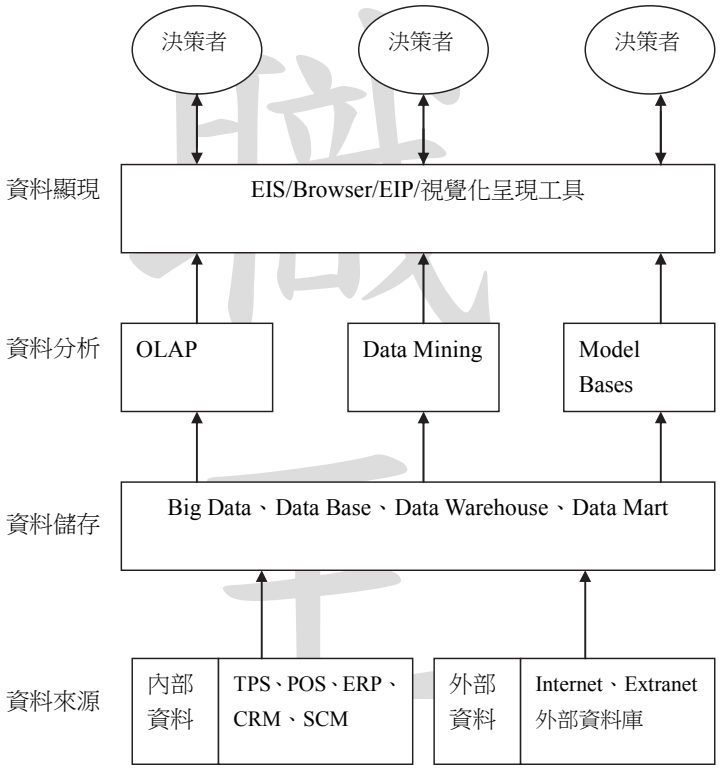
四、組織與企業廣泛應用商業智慧（business intelligence），分析巨量資料，協助組織做決策。面臨巨量資料分析，說明如何運用雲端科技解決巨量資料分析，提供即時商業智慧。（25分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》：運用 BI 整合架構作答，參考 101 地方特考四等類似題。

【擬答】：

㈠根據林東清對 BI 的定義：企業利用快速、即時、整合的資訊科技，來蒐集、分析、企業外部環境的競爭資訊與內部經營的重要關鍵指標，來提供即時、多維度的資訊，以支援決策者的判斷，提升企業競爭能力的一種流程與資訊系統。用於組織、分析並提供接觸資料的管道，以幫助管理者或其他企業使用者根據情報做出決策。

㈡可以如下之 BI 的 IT 整合性架構來解決：



1. 資料來源

透過各種雲端工具蒐集各種內部資料與外部資料，並進行萃取、轉換等資料處理動作，整合與轉換出可能需要的資料。

2. 資料儲存

運用雲端平台提供的大數據、資料庫、資料倉儲、資料超市工具儲存資料與資訊。

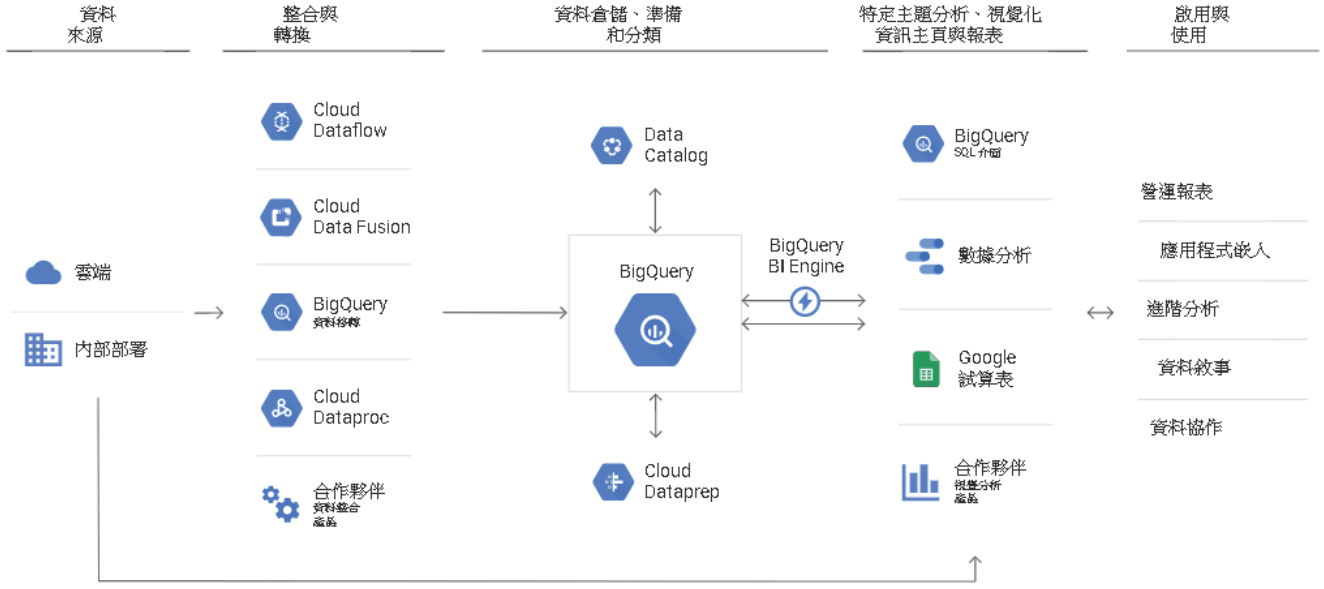
3. 資料分析

運用雲端平台的大數據資料分析工具，包括 OLAP、資料發掘、模式庫等，運用雲端的高速處理能力快速分析。

4. 資料顯現

運用 EIS/Browser/EIP/視覺化呈現工具按照決策者需求呈現資訊。

㈢如下即為 Google cloud BI 架構


資料來源
整合與轉換
資料倉儲、準備和分類
特定主題分析、視覺化資訊主頁與報表
啟用與使用
雲端
內部部署
Cloud Dataflow
Cloud Data Fusion
BigQuery
Cloud Dataproc
合作夥伴
Data Catalog
BigQuery
BigQuery BI Engine
Cloud Dataprep
BigQuery
數據分析
Google 試算表
合作夥伴
營運報表
應用程式嵌入
進階分析
資料敘事
資料協作