《資訊管理與資通安全》

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）

試題評析	此題為較新穎的概念與考題，同學第一次看到可能會較為慌亂，但是它其實只是資安管理議題的延伸而已，搭配上事件處理的應對方式，回答時只有回想上課所提及的資安應用與相對應處理方式即可完整回答此題。

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，其好處可分為以下三點：

1.快速識別企業內外部網路安全現況

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，企業同時可以針對威脅態勢獲得更完整之掌握，讓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，並可讓資安團隊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、技術及程序快速偵測、應對，使防禦從被動變為主動。

其重要性為可以協助組織達到以下目的：

1.幫助企業降低資安風險。

2.協助企業辨識、評估、監控及回應資安威脅，強化資安整體整備度。

3.提升企業之資訊安全及整體利益。

4.綜合跨領域知識、認知、理解及經驗，提升企業決策之有效性。

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）

試題評析	5G為2020年的重點政策實施項目，所以對於5G各位同學在近幾年要有全面性的了解，並需要在應用、技術和資安上有大量的著墨與認知。此題為較新穎的概念與考題，同學第一次看到可能會較為慌亂，但是它其實只是資安管理議題的延伸而已，搭配上事件處理的應對方式，即可游刃有餘的回答。
考點命中	《高點・高上資訊管理與資通安全》第二回，蕭老師編撰，頁47-50。

答：

由於物聯網設備和邊緣運算的快速擴展，最大的挑戰是面對突然的攻擊，其攻擊將呈現指數性的成長。

(一)組織內部管理

1.企業內部的資安需要整體考量從物聯網邊緣到核心企業網路，再到分支機構和多個公有雲才能實現邊緣到邊緣的安全性。所以，需要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，並驗證所有連線訪問網路資源的請求。

2.安全性還必須支持彈性的的混合系統，將經過驗證的傳統策略與新方法相結合。

儘管分段網絡連接是一種相對有效的技術，可以控制網絡安全風險並保護機密且敏感的資源，但舊策

略可能不適用於5G世界。新的細分策略需要同時考慮本地和遠端資源，這些資源混合了企業可以控製或無法控制的市場。IT團隊需要評估在實施5G網絡和公有雲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。

(二)組織防禦攻擊方式

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。

2.對雲端優化的分佈式網路，相關應用程式的支援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.數位化轉型將產成大量數據，其中大部分都會經過加密的處理。當前，加密數據將佔網絡流量的70%以上。只有使用加密程序來保護傳輸的數據時，此百分比才會增加。這將需要物聯網和其他邊緣設備中的高性能安全工具，這些工具可以快速且大規模地檢查這些加密的流量。

4.諸如網路分段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。

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）

試題評析	本題主要是考ISO 27001的相關概念，在答題上只要抓緊其A.15的供應商管理相關知識即可。
考點命中	《高點・高上資訊管理與資通安全》第三回，蕭老師編撰，頁68-72。

答：

根據ISO 27001控制措施，可以實行A.15的供應商關係控制，其包含以下：

(一)A.15.1 供應商關係的資訊安全

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。

(二)A.15.2 供應商服務交付管理

1.A.15.2.1 供應商服務的監控與審查
- 組織應定期監控、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）

試題評析	商業智慧一直是考試非常容易出現的考題，同學需要對其基本架構有通透的理解外，也要知道它的應用領域與相關技術。此題看似新穎，但是其實在考它的相關技術與實際使用方式，但是限縮於雲端運算上，故答題上只要能掌握這個概念即可。
考點命中	《高點・高上資訊管理與資通安全》第一回，蕭老師編撰，頁55-56。

答：

(一)商業智慧指的是將企業運作的系統資料，例如：ERP、SCM、CRM或非結構化的資料像是PDF、Excel等資料，提取出有用的部份進行整理，然後經過資料的擷取、轉換與匯入的程序，將資料合併到資料倉儲或是資料超市中；之後透過OLAP(Online Analytical Processing)技術將資料匯整成多維度結構 (cube)，以提高查詢速度。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。

主要架構圖如下：

(二)在商業智慧上，運用雲端運算可以把資料與應用託管到「軟體即服務」供應商，一方面可以通過雲的資料倉儲實現海量資料的高效率運算，另一方面也可以實現線上使用及支付資料採礦工具和商業智慧相關的分析處理軟體的費用。

透過雲端運算可以在以下方面加強商業智慧：

1.資料搜集

利用雲端運算可以更有效率地搜集組織的內外部資料，透過在資料傳輸的各節點上進行分析、萃取與轉換等動作來達到資料有效率搜集之目的。

2.資料儲存

運用雲端運算所提供的大數據、NoSQL資料庫…等，可以更有效率且以量計價的方式儲存資料。

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.資料展現

透過雲端運算的資料視覺化技術，可以完整且豐富的呈現各資料的維度與相關分析結果。