《資通安全法令與規範》

一、請說明資通安全情資分享辦法中不得分享的情況及分享安全措施的相關規範。（25分）

試題評析	本題係為近年熱門之資通安全情資分享考題。
考點命中	《高點・高上資通安全管理講義》第1章，張又中編撰，頁1-13。

答：

依據資通安全情資分享辦法第4條，情資有下列情形之一者，不得分享：

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。

二、其他依法規規定應秘密或應限制、禁止公開之情形。

情資含有前項不得分享之內容者，得僅就其他部分分享之。

另依據同辦法第5條：公務機關或特定非公務機關（以下簡稱各機關）進行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。

【參考書目】資通安全情資分享辦法。

二、請說明公務機關資通安全事件通報的作業流程。（25分）

試題評析	資通安全管理法與施行細則之延伸考題。
考點命中	《高點・高上資通安全管理講義》第1章，張又中編撰，頁1-23～24。

答：

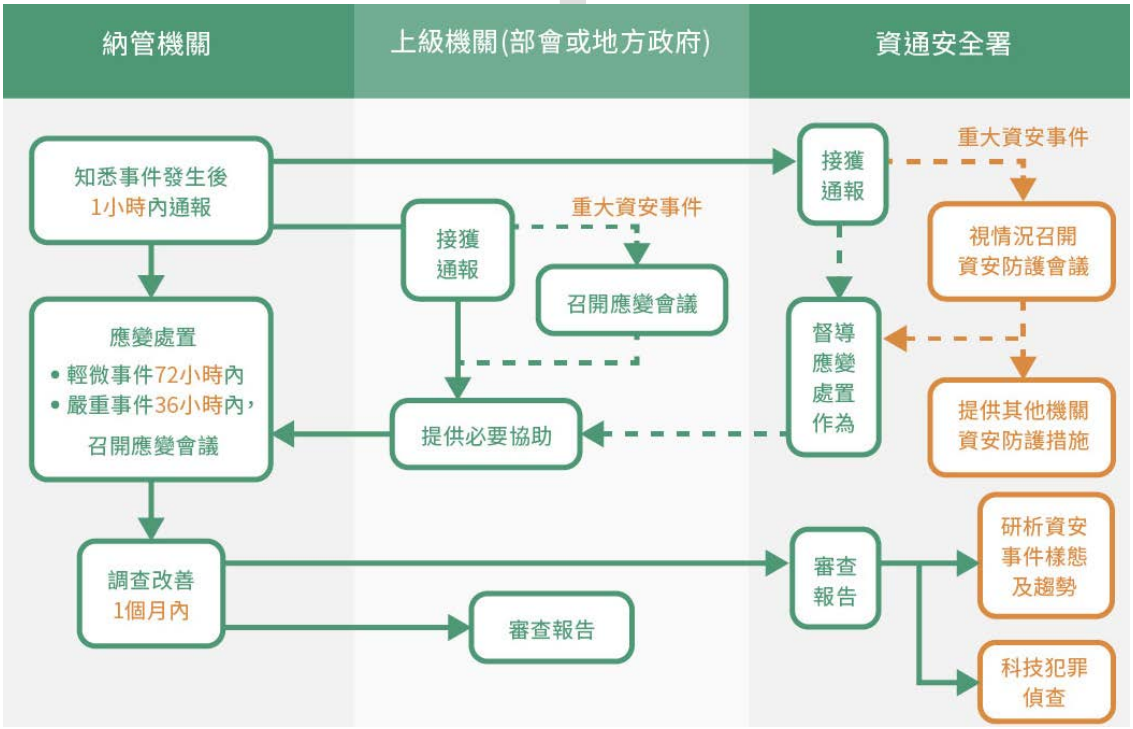
依據資通安全事件通報及應變辦法第4條：公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。

公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

公務機關資通安全事件通報的作業流程如下圖所示：



資料來源：數位發展部資通安全署

【參考書目】資通安全事件通報及應變辦法。

三、請說明業務持續運作管理程序應包含之步驟。（25分）

試題評析	屬資訊安全管理系統（Information Security Management System, ISMS）之範疇。
考點命中	《高點・高上資通安全管理講義》第1章，張又中編撰，頁1-3～7。

答：

業務持續運作管理（Business Continuity Management, BCM）旨在確保組織遭受中斷事件（安全威脅、人為錯誤、技術故障或自然災害等）後，能夠及時且有效地恢復關鍵業務功能，並將業務中斷的影響降到最低。BCM為一持續過程，涵括規劃、實施、測試和持續改進，以確保組織的韌性與永續。

BCM程序的主要步驟如下：

(1) 識別和評估風險：確定可能影響組織業務運作的潛在威脅和弱點。

(2) 業務影響分析（Business Impact Analysis, BIA）：評估不同業務功能的RTO（Recovery Time Objective）與RPO（Recovery Point Objective），以確定業務功能的重要性，需要在中斷後優先復原。

(3) 制定業務持續計畫：依據BIA結果制定具體的業務持續計畫，包括復原策略、人員安排、資源分配與溝通方案等。

(4) 實施和測試：執行業務持續計畫，定期進行演練和測試，以確保計畫有效性。

(5) 持續改進：根據測試結果和實際情況不斷地改進和更新業務持續計畫，以保持其與時俱進，符合組織的實際需求。

【參考書目】ISO 27001: 2022。

四、對於資安事件處理過程中，所蒐集到的資料，皆應妥善進行保存，以便未來需重新檢視證據或查驗之使用。請說明資安事件資料保存的實務作法。（25分）

試題評析	為數位證據（Digital Evidence）、數位鑑識（Digital Forensic）之考題。
考點命中	《高點・高上資通安全管理講義》第1章，張又中編撰，頁1-4。

答：

依據政府機關（構）資安事件數位證據保全標準作業程序第6條，資安事件資料保存的實務作法如下：

(1) 各機關得視其資訊人力資源進行不同程度之揮發性及邏輯性資料擷取。

(2) 相關標的設備處於開機狀態下，數位證據保全人員應考量資安事件類型及現場狀況後，擷取揮發性資料，以避免部分儲存於記憶體中之重要資料因系統關機而消失。

(3) 數位證據保全人員應考量資安事件類型及現場狀況後，擷取邏輯性資料，如：作業系統資訊、網路狀態、執行程序資訊、系統稽核日誌紀錄及使用者上網行為紀錄等。

(4) 針對防火牆設備、入侵偵測或防禦設備、紀錄保存與資安事件分析設備、防毒設備、流量控管或網路監控設備、應用系統及資料庫等設備，若各機關有資訊人力，得在數位證據保全人員檢視下，由應用系統或網路管理人員將稽核日誌檔案匯出至特定目錄內，由數位證據保全人員對其進行邏輯性資料擷取。

(5) 數位證據保全人員於擷取揮發性與邏輯性資料完畢後，應產生相對應之雜湊運算值，並記錄擷取之資訊或以自動化工具所產生之報表為之，如：擷取日期與時間、電腦名稱、所蒐集之揮發性與邏輯性資料項目、雜湊運算值等，經執行人員與資安事件發生單位主管簽章確認。

(6) 記錄人員應以全程錄影或拍照方式記錄揮發性與邏輯性資料擷取之步驟。

(7) 數位證據保全人員應將揮發性與邏輯性資料進行封緘，並視需要運送至上級機關或鑑識單位。

【參考書目】政府機關（構）資安事件數位證據保全標準作業程序。

高點・高上公職

考取學長姊大推的優秀師資

資料結構

王致強(蕭立人)

- 獨創「程式碼記憶法」，大幅縮短記憶　和答題的時間！
- 教學採考題導向，範圍由淺入深，即使是底子不好，也能茅塞頓開！

廖○成(高大資管畢)

應屆考取　113高考資訊處理

資料結構要掌握這門科目對我來說非常不容易，**不過王致強老師教得非常好**，教學中有時候連比國考難的研究所考題都會提點，也讓大家能夠掌握國考所需再更以上的資料結構實力，我覺得非常不錯！

資通安全

金乃傑(魏取向)

- 以「學習地圖」概念展現資訊管理多構面的知識，並引入自創圖示標記知識所在位置及相連概念；輔以口訣背誦關鍵名詞、要點。

蔡○諺(中興應數畢)

跨域考取

113高考資訊處理【狀元】

題庫班專注於實戰演練，通過不斷作題，能更快適應考試題型，並且針對薄弱環節進行強化。**金乃傑老師在今年考試中預測的範圍非常準確**，特別是在加密演算法與資料保護法規的部分，考題幾乎全中。

資訊管理

蕭維文

- 具有產業與學術經驗，從不同角度提供最客觀的科技觀點。
- 時事與理論精準結合科技產業，透過精闢分析讓同學理解資訊界。

李○翌(北市大資科畢)

應屆考取

113高考資訊處理、普考資訊處理

資訊管理這科廣到沒有範圍，如果有寫考古題就會發現講義是由各種考古題的解答堆疊出來的，因此**蕭維文老師的魚骨解答法就顯得非常重要**，只需把改卷教授想要的關鍵字搭配以上的方法就可以把答案湊出來。

更多命中實證

更多上榜經驗分享

考點命中實證

《資料結構》

一、某一公司有下圖所示的8個優先順序分別為高或低的待執行工作，且將依順序自A至H每間隔一天的時間放入對應的高優先執行佇列（Qucue）或低優先執行佇列（Qucue），例如A（低）表示A工作排於第一天放入低優先執行佇列，而C（高）表示C工作排於第三天放入高優先執行佇列。此外，執行每個工作所需完成的時間均於工行名稱下顯示，例如執行A工作需要2天時間完成，而執行B工作需要1天時間完成。最後，各個工作的執行規則為，當高優先執行佇列內有工作待完成時，須優先執行該佇列內的工作（由第一個開始執行），直到高優先執行佇列內沒有任何待完成工作時，才可執行低優先執行佇列內的工作（由第一個開始執行）。

自A至H每間隔一天的時間放入對應的高優先佇列或低優先佇列

H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
1	2	1	1	2	2	1	2

（一）試計算執行此8個工作需要多少天方可完成。（10分）

（二）試計算此8個工作自放入佇列至開始執行的平均等待時間。（15分）

試題評析　佇列相關的基本應用問題，題目本身十分平易。在題意確實掌握的狀況下，正常操作佇列，計算正確時間，取分不難。

考點命中　《資料結構》，高點文化出版，王致強編著，頁4-16～4-17。

答：

（一）總共需要12天可以完成8個工作，如下圖：（灰底為執行中工作，括號為工作剩餘天數）

天數	12	11	10	9	8	7	6	5	4	3	2	1
到達工作					H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
所需天數					1	2	1	1	2	2	1	2
高優先佇列				G(1)	G(2)	G(2)E(1)	F(1)D(1)	D(2)	D(2)C(1)	C(2)		-
低優先佇列	H(1)	H(1)E(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	E(1)B(1)	E(1)B(1)	E(1)B(1)	B(1)	B(1)	B(1)A(1)	A(2)

（二）各項工作等待時間如下表：

工作	H	G	F	E	D	C	B	A
等待時間	4天	1天	1天	6天	1天	0天	8天	0天

《資通網路與安全》

五、防火牆（Firewall）是當今企業常見的安全防護設備，請問：

（一）企業常用防火牆隔離出一個網段，稱為DMZ（Demilitarized Zone），請詳細說明其用意為何。（5分）

（二）WAF（Web Applicatiou Firewall）和傳統的封包過濾式防火牆（Packet filtered Firewall）有何不同？請詳細說明。（10分）

（三）防火牆常根據從外部收到的IOC（Indicator of Compromise）來做規則調整，請問IOC的意義為何？（5分）

試題評析　本題為資訊安全之防火牆種類及安全網路架構之題型。

考點命中　《高點・高上資通安全講義》第二回，金乃傑編撰，頁14～28，第三章防護架構，二、防火牆（Firewall）與相關技術。

答：

（一）DMZ（Demilitarized zone）是介於內外路由器間的區域，用於放置組織對外重要的伺服器。DMZ 照字面直翻是指非軍事區域，而電腦網路中 DMZ 可以解析為一個既不屬於內部網域同時也不屬於外部網域的一個特殊區域，其目的就是了為防止外來人侵者直接存取內部機密資料，針對不同資源而提供不同安全級別的保護區域。一般企業將網路伺服器放在 DMZ 供網際網路使用者查詢使用，這些伺服器無法連接到內部資料，因此如果不幸被外來人侵者侵入，重要的資料仍不至於外洩。

（二）WAF（Web Application Firewall）提供應用層的訊息過濾與轉送處理，主要依據應用層的資訊來決定是否放行封包流量，與傳統的封包過濾式防火牆相較，WAF 可過濾傳送的資料內容與命令，確保應用層協定的安全；亦可過濾封包內容與命令，阻斷針對應用協定的攻擊。

（三）IOC 為電腦鑑識中的工具器物(Artifact)，其可從網路或作業系統中觀察，與電腦入侵高度相關。傳統的 IOC 包含病毒特徵、IP 位址、惡意檔案的 MD5 雜湊值，或是殭屍網路(Botnet)命令與控制伺服器的網址或網域名稱。通過事件回應與電腦鑑識的處理過程識別 IOC 後，其可用於入侵檢測系統(Intrusion Detection System, IDS)與防病毒軟體，對未來的攻擊嘗試進行早期檢測。