《資訊管理與資通安全》

一、請根據資通安全事件通報及應變辦法回答下列問題：

(一)請說明資通安全事件通報內容應包括之項目。（15分）

(二)請說明公務機關資通安全事件之通報及應變的流程。（15分）

試題評析	此題完全依照「資通安全事件通報及應變辦法」來答題即可，算是中規中矩的題目。若同學在當下無法背誦出來，可以依照《高點・高上資訊管理與資通安全》第三回，蕭老師編撰，頁91-95，資訊安全事件之描述與老師上課講解，嘗試用類似的方法描述主管機關的流程，這是針對完全沒看過之題目的解題心法。

答：

(一)依據民國110年所修訂的「資通安全事件通報及應變辦法」第三條，資通安全事件之通報內容，應包括下列項目：

1.發生機關。
2.發生或知悉時間。
3.狀況之描述。
4.等級之評估。
5.因應事件所採取之措施。
6.外部支援需求評估。
7.其他相關事項。

(二)依據「資通安全事件通報及應變辦法」中所列的流程：

1.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。
2.主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：
(1)通報為第一級或第二級資通安全事件者，於接獲後八小時內。
(2)通報為第三級或第四級資通安全事件者，於接獲後二小時內。
3.總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。
4.前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審核結果通知主管機關，並提供審核依據之相關資訊。
5.公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：
(1)第一級或第二級資通安全事件，於知悉該事件後七十二小時內。
(2)第三級或第四級資通安全事件，於知悉該事件後三十六小時內。
6.公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。
7.前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。
8.上級、監督機關或主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。

二、請回答下列資訊安全相關問題：

（一）請說明雜湊函數與常見的演算法。（10分）

（二）請說明雜湊函數的碰撞與不建議使用之原因。（10分）

試題評析	雜湊函數是常用於加密或是用來識別檔案或文件有無被竄改的機制，但要記住雜湊函數不等於加密，其為兩種不同的概念。此題只需依照老師課堂補充，即可明確的解答何為雜湊、碰撞跟使用時機，針對常見的演算法，只需要說明幾項即可，老師這邊將大多數常見的做法都列出。
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78-80，加密技術課堂補充。

答：

(一)雜湊（英語：Hashing）是電腦科學中一種對資料的處理方法，通過某種特定的函式（雜湊函式）/演算法將要檢索的項與用來檢索的索引（稱為雜湊，或者雜湊值）關聯起來，生成一種便於搜尋的資料結構（稱為雜湊表），且所計算出來的雜湊值必須符合「由雜湊值是無法反推出原來的訊息」和「雜湊值必須隨明文改變而改變」。它也常用作一種資訊安全的實作方法，由一串資料中經過雜湊演算法（Hashing algorithms）計算出來的資料指紋（data fingerprint），經常用來識別檔案與資料是否有被竄改，以保證檔案與資料確實是由原創者所提供。常見的演算法有（參考：https://iter01.com/43610.html）：

1.直接定址法：取關鍵詞或關鍵詞的某個線性函式值為雜湊地址。即H(key)=key或H(key) = x • key + y，其中x和y為常數。

2.數字分析法：分析一組資料，比方一組員工的出生年月日，這時我們發現出生年月日的前幾位數字大體同樣，因此出現衝突的機率就會非常大，可是我們發現年月日的後幾位表示月份和詳細日期的數字區別非常大，假設用後面的數字來構成雜湊地址，則衝突的機率會明顯減少。因此數字分析法就是找出數字的規律，儘可能利用這些資料來構造衝突機率較低的雜湊地址。

3.平方取中法：取關鍵詞平方後的中間幾位作為雜湊地址。

4.摺疊法：將關鍵詞切割成位數同樣的幾部分，最後一部分位數能夠不同，然後取這幾部分的疊加和（去除進位）作為雜湊地址。

5.隨機數法：選擇一隨機函式，取關鍵詞的隨機值作為雜湊地址，通常使用於關鍵詞長度不同的場合。

6.除留餘數法：取關鍵詞被某個不大於雜湊表表長m的數p除後所得的餘數為雜湊地址。即 H(key) = key MOD p, p<=m。不僅能夠對關鍵詞直接取MOD，也可在摺疊、平方取中等運算之後取MOD。對p的選擇非常重要，若p選的不好，容易產生碰撞。

(二)所有雜湊函式都有如下一個基本特性：如果兩個雜湊值是不相同的（根據同一函式），那麼這兩個雜湊值的原始輸入也是不相同的。這個特性是雜湊函式具有確定性的結果，具有這種性質的雜湊函式稱為單向雜湊函式。但另一方面，雜湊函式的輸入和輸出不是唯一對應關係的，如果兩個雜湊值相同，兩個輸入值很可能是相同的，但也可能不同，這種情況稱為「雜湊碰撞（collision）」，這通常是兩個不同長度的輸入值，刻意計算出相同的輸出值。輸入一些資料計算出雜湊值，然後部分改變輸入值，一個具有強混淆特性的雜湊函式會產生一個完全不同的雜湊值。故當碰撞機率過大時，則不建議使用。

三、請回答下列有關微型服務的問題：

（一）請說明微型服務的特性。（6分）

（二）請說明微型服務的優勢。（24分）

試題評析	此題即為SOA的應用，同學在答題上可以針對老師所講述的SOA概念回答，這邊再列出Amazon所定義的微服務之定義與優勢給同學參考，讓答題可以更為豐富。
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34-35

答：

(一)根據Amazon的定義（https://aws.amazon.com/tw/microservices/），微型服務是一種架構式和組織式的軟體開發方法，其中軟體由小型獨立服務組成，並透過定義良好的API進行通訊。這些服務由小型的獨立團隊所擁有。微型服務架構可讓應用程式更輕鬆擴展並加快開發速度，不僅促進創新，更縮短新功能的上市時間。

在微型服務架構中，應用程式會建立為獨立元件，並會以服務的形式執行個別應用程式程序。這些服務使用輕量型API，透過定義良好的界面進行通訊。服務係針對商業功能所建立，且每項服務皆可執行單一功能。因為每項服務皆獨立運作，因此可以個別更新、部署和擴展，以滿足應用程式特定功能的需求。其具有以下兩個重要的特性：

1.自發：微型服務架構中的每項元件服務都可以自由開發、部署、運作和擴展，並不會影響其他服務的功能。這些服務不需要與其他服務分享任何程式碼或實作。獨立元件之間會經由定義良好的API進行所有通訊。

2.專門：每項服務專為一組功能設計，並著重於解決特定問題。如果開發人員不斷提供更多程式碼，導致服務變得更加複雜，可以將服務分解成較小型的服務。

(二)根據Amazon（https://aws.amazon.com/tw/microservices/），其優勢為：

1.敏捷性

微型服務促進組織組成小型獨立團隊，並具備其處理之服務的擁有權。團隊可在小型簡易的環境中行動，並能夠更獨立且快速地工作。這有助於縮短開發週期時間。彙總的組織輸送量能為您帶來莫大好處。

2.可彈性擴充

微型服務可讓每項服務獨立擴展，以滿足其支援的應用程式功能的需求。這可讓團隊依架構需求調整合適的大小、準確地衡量功能的成本，以及在服務出現需求激增時維持可用性。

3.輕鬆部署

微型服務可持續整合和持續交付，方便您嘗試新點子，並在發生問題時進行復原。失敗的成本較低，可讓您進行實驗，以便更新程式碼，並縮短新功能的上市時間。

4.技術的自由

微型服務架構不適用於「一體適用」的方法。團隊可自行選擇可解決其特定問題的最佳工具。因此，建立微型服務的團隊可為每項工作選擇最佳工具。

5.可重複使用的程式碼

將軟體劃分為定義良好的小型單元，可讓團隊將功能用於多種用途。專為特定功能撰寫的服務可充當其他功能的建構模塊。這可讓應用程式自行引導操作，以便開發人員建立新功能，而無需從頭開始撰寫程式碼。

6.恢復能力

服務的獨立性可提升應用程式的受挫能力。在巨型架構中，如果單一元件故障，可能會造成整個應用程式故障。在微型服務中，應用程式可將功能降級，以處理整個服務故障問題，避免造成整個應用程式當機。

四、請回答下列資訊系統風險評鑑相關問題：

(一)請說明風險識別及其步驟。（8分）

(二)請說明風險估計及其步驟。（8分）

(三)請說明風險評估。（4分）

試題評析	較為中規中矩的題目，只需要依照細則來回答即可。此題可以根據ISO27001來答之外，也可以依據「行政院國家資通安全會報技術服務中心」所公布之風險提供方法來答題，此題老師列出後者來讓同學參考。
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84-90。

答：

(一)「風險識別」是針對資訊系統鑑別出每個資訊資產、該資訊資產脆弱性被威脅利用的難易度、相關威脅發生的可能性、威脅與脆弱性結合發生事故時對組織衝擊的嚴重性及其資訊資產現有控制措施等；完成前述之識別後，為便於找出各個威脅與脆弱性組合之風險的優先順序，對威脅發生之可能性、脆弱性被利用的難易度及衝擊之嚴重性各給予一個數值，再計算各個威脅與脆弱性組合之風險值。

1.資產識別（Identification of Assets）：機關可藉由此資訊系統所提供的業務流程活動，識別該資訊系統之資訊資產。

2.威脅與脆弱性識別（Identification of Threats and Vulnerabilities）：針對各項現有控制措施識別（Identification of Existing Controls），資訊資產分別鑑別其在使用或處理過程中，各項可能的威脅，運用該資訊資產脆弱性對「機密性（C）」、「完整性（I）」及「可用性（A）」造成之衝擊。

3.現有控制措施識別（Identification of Existing Controls）：了解現有控制措施之施行成效與已規劃的控制措施，再參考「安全控制措施參考指引」，確切描述安控措施，以避免重複的資源浪費。

4.後果識別（Identification of Consequences）：識別資訊資產發生事故之後，對組織造成的後果。

(二)資訊資產相關的風險識別完成後，需要估算每一個資訊資產的相對風險大小，故需藉由量化資訊資產的價值、後果對機關衝擊的嚴重性，及事故發生的可能性，以估算風險值。

1.鑑別資訊資產價值（Identification of Assets Value）：以資訊資產在事故發生時，破壞「機密性」、「完整性」及「可用性」造成的後果，對組織衝擊的嚴重性，鑑別資訊資產的價值，並將識別的後果（普、中、高）分別給予一個值，將每一資產的「機密性」、「完整性」及「可用性」代表值相加，即可得到資訊資產的價值。資訊資產價值的計算方式，如下列公式所示：

資訊資產價值＝機密性鑑價＋完整性鑑價＋可用性鑑價

2.評鑑事故可能性（Assessment of Incident Likelihood）：事故可能性是由分析威脅發生的可能性與脆弱性被運用的難易度組合而成，給予威脅發生的可能性與脆弱性被運用的難易度（普、中、高）各一個值，分別代表「威脅等級」與「脆弱性等級」。在評鑑事故可能性時，請在現有控制措施識別完成之後，考量在現有控制措施實施之下，仍會發生事故的可能性來作評鑑。

3.估計風險等級（Level of Risk Estimation）：估計風險等級乃是將量化的資訊資產價值、後果對組織衝擊的嚴重性，及事故發生的可能性結合，計算每一個資訊資產的價值與風險值。資訊資產風險值計算方式，如下列公式所示：

資訊資產風險值＝資訊資產價值×威脅發生可能性×脆弱性利用難易度

(三)

1.訂定風險等級：將所有資訊資產相關風險值，在其最大值與最小值區間等分為「普、中、高」3個等級。初次風險評鑑，可先依據理論值計算公式，風險值將落在3至81分之間，區分為3個等級。

2.決定「可接受風險等級」：依據「建立全景階段」所訂「風險接受準則」，再檢視資訊資產風險清單，訂定組織可以承受的風險等級，以決定風險處理的範疇。此階段政府機關亦可再依其所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，修正風險的接受準則。

3.根據「風險接受準則（普、中、高）」，針對「未能接受」之風險，判斷風險處理的「資產」對象。即依「高風險」、「中風險」、「普風險」之資產，建議從「安全控制措施參考指引」中，對照選擇「適合」該資產類型之相對風險的「高防護等級」、「中防護等級」、「普防護等級」的控制措施。

4.根據「風險評估準則」，針對「未能接受」之風險，判斷風險處理的優先順序。