# 《資訊管理與資通安全》

一、請先說明何謂軟體開發生命週期（Software Development Life Cycle, SDLC）？然後詳細說明以下四種軟體開發方法的內涵、特點及其各適用的情境：瀑布式（Waterfall）、螺旋式（Spiral）、敏捷式（Agile）、DevOps。（25 分）

| | |
|---|---|
| **試題評析** | 此題為中規中矩的標準型考題，在答題上除了要仔細閱讀題目所需要的答案與面向外，最後的比較一定要用表格或條列的方式呈現，才可以獲得較好的分數。 |
| **考點命中** | 《高點・高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁 6-16。 |

**答**：

(一)系統發展生命週期用於描述一個資訊系統從規劃、建立、測試到最終完成部署的全過程。由一系列明確定義的不同工作階段組成，有助於系統工程師和系統開發人員利用對系統的設計、構建、測試和交付進行計劃。從軟體的產生直到報廢的生命週期，週期內有問題定義、可行性分析、總體描述、系統設計、編碼、測試、驗收、運行、維護升級到廢棄等階段，這種按時程分配的思想方法是軟體工程中的一種思想原則，即按部就班、逐步推進，每個階段都要有定義、工作、審查、形成文件以供交流或備查，以提高軟體的質量。

(二)以下針對常見的方法做詳細的描述與比較

| 模式 | 內涵 | 特點 | 適用情境 |
|---|---|---|---|
| 瀑布式（Waterfall） | 在該模型中，首先確定需求，然後擬定規格說明，同樣通過驗證後，進入計劃階段，瀑布模型中至關重要的一點是只有當一個階段的文件已經編寫好並獲得軟體質量保證小組的認可才可以進入下一個階段。瀑布模型通過強制性的要求提供對應文件來確保每個階段都能很好的完成任務。缺點為實際上難以辦到，因為整個的模型幾乎都是以文件驅動的，這對於非專業的用戶來說是難以開始並依此實際操作。 | 1.易於理解和管理。<br>2.重視設計與規劃之文件。<br>3.開發上較不靈活。<br>4.一旦完成階段，幾乎沒有修改的餘地，因此只有進入維護階段才能解決問題。 | 1.需求明確定義的專案。<br>2.解決問題的知識較為簡單或是確定。<br>3.已經有明確的先前經驗或知識的專案。 |
| 螺旋式（Spiral） | 螺旋模型是原型方法和瀑布方法的結合。螺旋模型被認為是最靈活的 SDLC 方法之一。它從迭代模型及其重複中獲得啟發。該專案以“螺旋式”的方式反覆經歷四個階段，直到完成為止，從而可以進行多輪改進，此四個階段為： | 1.強調各開發週期之規劃與風險評估。<br>2.可能會讓專案形成永無止境的螺旋式發展的風險。<br>3.具有風險分析的概念。 | 1.主要用於大型專案，它允許構建高度定製的產品，並且使用者反饋可以在專案的早期就被納入。 |

| | | | |
|---|---|---|---|
| | (1)規劃<br>(2)風險分析<br>(3)工程<br>(4)評價 | | |
| 敏捷式（Agile） | 致力於通過早期交付軟體來適應靈活的需求並滿足使用者和客戶的需求。敏捷專案中的需求和解決方案可能會在開發過程中發展。<br>通過敏捷開發，該產品被分為多個小的建構產品，並以迭代方式交付。將所有任務劃分為較小的時間範圍，以便為每個版本準備工作功能。最終產品版本包含所有必需的功能。敏捷仍然是技術行業中使用最廣泛的 SDLC。 | 1.「人和互動」重於「過程和工具」。<br>2.「可以工作的軟體」重於「求全而完備的文件」<br>3.「客戶協作」重於「合約談判」。<br>4.「隨時應對變化」重於「循規蹈矩」。 | 1.敏捷方法適用於較小的開發團隊。<br>2.使用者需求於開發過程中不斷變化。<br>3.開發團隊與使用者需有良好溝通和互動的機制。 |
| DevOps | 通過自動化基礎架構和工作流程並持續追蹤應用程式效能來執行的。DevOps 方法使可以增加部署頻率，編寫程式碼並縮短部署新程式碼所需的時間，是一種重視「軟體開發人員(Dev)」和「IT 運維技術 人員(Ops)」之間溝通合作的文化與慣例。 | 1.鼓勵開發人員、維運人員和 QA 人員共同努力，以進行持續的開發，測試和部署活動。<br>2.加速創新並交付更高質量和更可靠的軟體產品和功能。 | 需要頻繁交付新版本軟體的團隊。 |

**二、何謂勒索軟體（Ransomware）？通常資料備份是防範勒索軟體攻擊的重要手段，但是許多企業或是組織的備份資料仍可能遭受勒索病毒的攻擊，請先解釋其理由何在？然後詳細說明有那些作法可以降低備份資料遭受勒索攻擊的風險？（25 分）**

| | |
|---|---|
| **試題評析** | 勒索軟體是當紅的時事題類型，答題上以資訊安全防護的角度切入即可，並要搭配勒索軟體的特性，才可以完全答到出題老師想要的答案。 |
| **考點命中** | 1.《109 高點・高上資訊管理與資通安全地方特考重點題神》，蕭老師編撰，題一。<br>2.《高點・高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁 85-89。 |



**答：**

(一)勒索軟體，又稱勒索病毒，是一種特殊的惡意軟體，其與其他病毒最大的不同在於手法以及中毒方式。其中一種勒索軟體僅是單純地將受害者的電腦鎖起來，而另一種則系統性地加密受害者硬碟上的檔案。所有的勒索軟體都會要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的解密金鑰以便解密檔案。勒索軟體通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案，通常會通過假冒成普通的電子郵件等社會工程學方法欺騙受害者點擊連結下載，但也有可能與許多其他蠕蟲病毒一樣利用軟體的漏洞在聯網的電腦間傳播。

(二) 安全軟體不一定能偵測出勒索軟體的實體數據——尤其是加密用的軟體——直到開始加密或是完成加密了才被發現。對於未知的病毒來說更是如此。若攻擊尚在早期階段，加密檔案尚未成功，此時強制移除病毒實體數據就能避免對資料的進一步加密，例如拔除電源等物理性做法也是可以搶救回部分資料。資安專家建議了一些預防措施來應對勒索軟體，例如使用資安軟體或設定以避免已知的勒索軟體執行；保留不與電腦連接的資料備份，尤其某些病毒會將仍與電腦連接的備份檔案一併加密。

雖然勒索軟體的威脅無法被完全革除，使用 IT 業界所稱的多層次預防策略（defense-in-layers security strategy）卻稱得上是不錯的預防手段。多層次預防策略提倡同時部署多種獨立、領域互相重疊的安全措施以建立穩固的安全措施。各安全層被設計和其他安全層互補，使得威脅不易穿透重重防護。例如一個安全策略可能包含下列五層：[1]

- 全面性的、完備的安全政策
- 網路和郵件的內容過濾代理伺服器
- 限制級別存取
- 以密碼上鎖特定功能
- 不間斷的員工警覺性訓練

**三、因應 Covid-19 肺炎疫情，許多企業或是組織採取在家上班，這對組織的資安防護帶來很大的挑戰。請列舉在家上班的資安防護應有那些作為並詳細說明其作法。（25 分）**

| | |
|---|---|
| **試題評析** | 此題也是屬於時事題，今年因為疫情的關係，許多考試都會圍繞在疫情上，同學在準備時應該依照老師的做法，在相關的題型上都要嘗試與疫情做連結，嘗試找出共通性，遇到疫情時事題才可以迎刃而解。此題在回答上與一般資安防護沒有太大的差異，回答上要以家中與公司的資料通訊差異下手，如此才可以完整到出題老師想問的面向。 |
| **考點命中** | 《109 高點・高上資訊管理與資通安全地方特考重點題神》，蕭老師編撰，題十七。 |

**答：**

1.加強連線加密措施：針對客戶端與伺服器連線時，及客戶端與客戶端間，應該實施加密保護措施，並且使用高強度加密協定與演算法，避免中間連線遭人竊聽與破解。

2.帳號強化密碼強度：帳號安全部分，應有密碼強度之要求，避免使用弱密碼遭到駭客暴力破解登入。

3.機敏資料加密保護：由於視訊會議軟體客戶端可能儲存許多機敏資料(包含密碼、聊天紀錄或聯絡名單等)，應對相關資料進行加密保護，倘若資料外洩時，無法直接對加密資料進行讀取。

4.不忘漏洞通報：最後，視訊會議軟體廠商應有漏洞通報管道或獎勵，以鼓勵白帽駭客協助提早發掘軟體漏洞，避免日後成為 Zero-day 漏洞，而遭受更為嚴重的入侵攻擊，甚者導致商譽受損。

5.安全性修補與防毒軟體病毒碼更新：確認所有應用程序和作業系統已安裝至最新版本安全性修補程式等級，防止駭客利用未修補的弱點進行攻擊，資訊系統防毒和防惡意軟體需要更新至最新版本病毒碼，已防範病毒或惡意軟體攻擊。

**四、資訊系統是否滿足使用者需求，往往決定於軟體專案的管理是否得當。請詳細說明軟體專案管理的五個階段（phase）及四個專案需滿足的目標為何？（25 分）**

| | |
|---|---|
| **試題評析** | 此題為基礎的資訊管理題型，答題上相信同學一定游刃有餘，針對各階段除了課本所提到的說法外，同學可以依照自己的想法加上一些補充，如此可以獲得更高的分數。 |
| **考點命中** | 《高點・高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁 1-5。 |

**答：**

(一)專案管理的五個階段：

1.起始階段：主要活動包含製作專案授權書、確認利害關係人、建立專案管理團隊、召開專案啟動會議等。啟始階段的主要目的在確保專案計畫及執行前，所有必要的準備工作被確實地完成，並取得全體

專案管理成員的共識和承諾。啟始的工作主要由專案經理來負責完成，並由專案管理團隊成員來協辦。專案贊助者及專案委員會則負責指導及審核的工作。

2.計劃階段：主要活動在製作細部的專案計畫書，包含範疇、工作、品質、資源、時程、預算、風險、溝通等相關的子計畫。計畫階段主要的目的在確保專案執行前，所有產出及管理的工作被仔細的規劃。計畫工作主要由專案經理及專案管理團隊成員來負責完成，並由各工作小組組長來協辦。專案贊助者及專案委員會則負責指導及審核的工作。

3.執行階段：主要活動包含管理分派驗收及管理產出交付。執行階段的工作主要在確保專案經理確實分派、檢討及驗收所有的專案工作。同時所有工作小組確實接受、督導及交付工作。

4.控管階段：主要活動包含控管現況、解決問題及管理溝通與文件等。控管階段的主要目的在確保專案的所有進度狀況及問題被有效地追蹤記錄、分析評估、及檢討處理。控管的工作由專案經理及專案團隊成員來負責。專案贊助者及專案委員會則負責指導及審核的工作。

5.結案階段：主要活動包含完成最終產出驗收、進行合約及行政結束、進行結案報告及會議、 進行專案後檢討等。結案階段的主要目的在確保專案的最終產出被確實驗收，同時結案相關的工作被有效完成。結案的工作由專案經理及專案團隊成員來負責。專案贊助者及專案委員會則負責指導及審核的工作。

(二)專案需滿足的目標：

1.專案範疇：達成專案目標所需完成的交付物。其所採取之系列步驟與流程，不包含產品功能，但包含工具、設備、 和流程，也可包含組裝線、制定預算、人員訓練、供應鏈、和人員分配。

2.專案時程：規劃專案時程的目的是在建立和管理時程，確保專案中的所有活動都能順利進行。其中包含：規劃時程管理、定義活動、排序活動、估算活動工期、建立專案時程和管制專案時程。

3.專案成本：為確保專案能在獲準的預算內完成，對成本進行規劃、估算、編列預算、融資、籌資、管理，以及管制的過程。其中包含規劃成本管理、估計成本、制定預算等。

4.專案品質：專案品質管理包括執行組織所決定之品質政策、目標和責任，使專案能滿足其所設定需求的一切活動。專案品質管理是透過政策、程序與品質規劃、品質保證及品質管制等過程，以執行品質管理系統，並視需要於專案期間採取持續性之流程改善活動，以使專案品質能達到要求的標準。專案品質管理之流程包括：品質規劃 (Quality Planning)、執行品質保證 (Perform Quality Assurance) 、執行品質管制 (Perform Quality Control)。