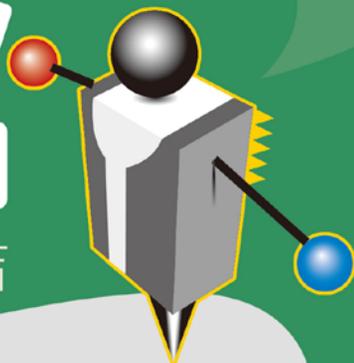


法政瘋高點



LINE@生活圈

共榮共享 · 好試連結



司特/調特考前提示★LINE好友版考猜★

★刑事訴訟法：劉律(劉睿揚)

★犯罪學：陳逸飛(施馭昊)



8/7(一)
限時下載

@get5586

8/12~14考場限定

報名指定法律好課，加贈高點圖書禮券1,000元

司特/調特★線上解題講座★

行政法：8/24(四)

民法：8/25(五)

刑法：8/29(二)

刑訴：8/30(三)



嶺律 (陳熙哲)



龍律 (陳義龍)



劉律 (劉睿揚)

FB粉絲團

首播



高點線上
影音學習



【台北】台北市開封街一段2號8樓

02-2331-8268

【台南】台南市中西區中山路166-6號5樓

06-223-5868

【台中】台中市東區大智路36號2樓

04-2229-8699

【高雄】高雄市新興區中山一路308號8樓

07-235-8996

各分班立案核准



《系統分析與設計》

一、您是一家軟體公司的專案經理，公司剛剛承接了市政府的一個資訊系統開發專案。該市府的資訊處承辦要求這次的系統開發必須落實以下的【安全軟體設計原則】，請說明這些原則所代表的意義為何？（每小題 5 分，共 25 分）

- (一) Economy of Mechanism：機制經濟原則
- (二) Leveraging Existing Components：元件槓桿原則
- (三) Defense in Depth：縱深防禦原則
- (四) Fail Secure：失敗安全原則
- (五) Least Privilege：最小權限原則

命題意旨	安全軟體設計原則。
答題關鍵	可參考系統專案管理、網路總複習課程與上課補充。
考點命中	1.《高點系統專案管理講義》，張又中編撰，第8章，頁8-45~46 2.《高點網路總複習講義》，張又中編撰，第1章，頁1-12~13。

【擬答】

- (一)設計越簡單越好(As Simple as Possible)，因為越複雜的系統越容易產生安全漏洞，且不易找出安全問題的根源。
- (二)使用現有、經過安全測試或認證的元件，以避免新元件可能造成的未知風險。
- (三)亦稱分層防禦(Layered Defense)，在軟體單一環節或進入路徑採用多重的安控措施。
- (四)系統故障時不會造成傷害，或是將傷害最小化。
- (五)應為使用者及系統配置必須、最小的權限以完成其工作；雖限制了系統操作的範圍，但可將系統故障、損壞或濫用對安全的影響降至最低，且可簡化模組的安全性分析。

二、貴公司正在準備針對某個政府標案進行投標，該標案要求專案的進行必須採用所謂的安全軟體發展生命週期（SSDLC）來進行開發。

- (一)請問為什麼客戶會要求採用 SSDLC 而非傳統的 SDLC 進行該系統的開發？（10 分）
- (二)請說明 SSDLC 在需求分析、系統設計...等各個 SDLC 階段，如何將安全性納入這些軟體的開發中？（15 分）

命題意旨	SSDLC
答題關鍵	SSDLC各階段，可參考課程內容。
考點命中	1.《高點系統專案管理講義》，張又中編撰，第2章，頁2-4~6。 2.《高點系統專案管理講義》，張又中編撰，第8章，頁8-41~44。

【擬答】

- (一)賴溪松提出，在考量系統功能性的同時導入安全性的思維，於系統開發之初進行各項必要的安全防護措施，雖然拉長了設計的時程，卻降低了系統後續維護的成本，以及遭受到攻擊行為的損失。
- (二)SSDLC 各階段如下：
 - 1.需求分析
配合相關人員的期望進行各項資安措施的分析與規劃，於符合成本考量下達成安全需求。
 - 2.系統設計
需考量系統任務目標、功能關聯、邊界範圍、各階層使用者的角色等各項內容，建立相關的控管程序及防護措施，作為程式實作階段的基礎。
 - 3.系統開發
為資安防護實作最為重要的一環，需針對各項可能的入侵手法考量其中的漏洞及威脅，建立層層的防護機制。

4.系統測試

考量目前系統內各項控管程序與防護措施，是否能夠有效的防禦目前已知的攻擊手法，並依據測試的結果進行必要的調整。

5.系統部署

考量系統部署後，各項安全控管機制與防護措施的運作狀況，確保其正常無誤。

6.系統維護

著重於資安防護措施的持續維護以及變更管理，考量廠商的技術能力，並掌控系統原始程式碼。

三、您正在幫國內知名的傳統連鎖餐飲企業-阿豪鹹粥建置線上點餐系統，過去阿豪的菜單都是各種鹹粥跟單點品項分別計價。但是在專案進行中，老闆想要改變原有的訂餐方式。他想讓每位客人先點基本鹹粥一份，才能加點不同組合價格的魚肚、魚腸等單品。雖然你覺得這樣的定價方式跟原來專案所規劃的作法不符，邏輯也不夠嚴謹，但是客戶的要求也不該忽視。因此，你準備針對此次變更要求執行變更管理程序。

(一)請解釋為何你不能直接聽命於出錢老闆的意思，讓此一變動必須經過正式變更程序？(10分)

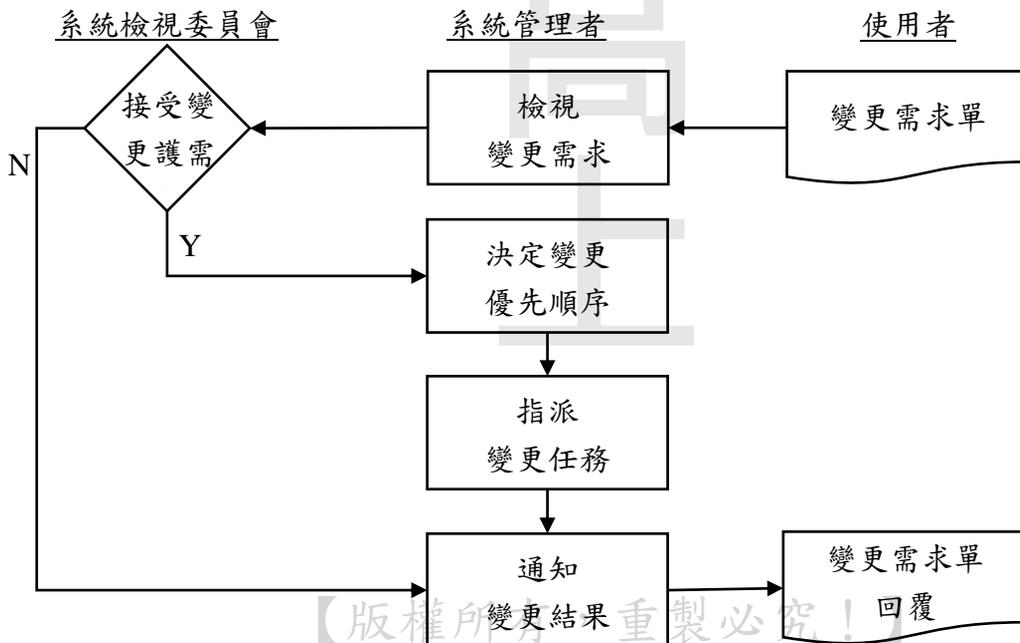
(二)請問你會建議這個需求變更程序該如何進行？(15分)

命題意旨	需求變更。
答題關鍵	需求變更程序，請參考課程內容。
考點命中	1.《高點系統專案管理講義》，張又中編撰，第4章，頁4-37~38。 2.《高點系統專案管理講義》，張又中編撰，第10章，頁10-28~32。

【擬答】

(一)以軟體發展過程而言，變更(Change)幾乎無可避免，如果任意變更將對整體專案的交期與品質造成影響。因此，如何有效控制變更，經過正式變更程序核定，來降低變更對軟體專案造成的衝擊。

(二)需求變更程序如下圖所示：



四、貴機關正在規劃全新的遠端連線安全存取的規範，請問關於遠端存取的資通安全管理措施，應該採取那些措施？並請說明這些措施。(25分)

命題意旨	遠端連線安全存取規範。
答題關鍵	遠端連線存取的資通安全管理措施，可由如遠端登入、雲端整合儲存的角度切入。
考點命中	1.《高點系統專案管理講義》，張又中編撰，第8章，頁8-41~45。 2.《高點網路總複習講義》，張又中編撰，第1章，頁1-12~13。

【擬答】

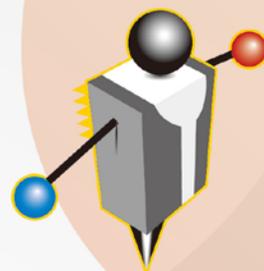
- 1.遠端連線的可用性：如遠端連線是否採用高可用性(High Availability)的架構設計。
- 2.遠端連線加密機制：是否導入如 SSL、IPsec 等連線加密機制。
- 3.遠端連線權限控管：使用者、角色的權限設定。
- 4.遠端連線的多因子認證：如二因子認證(Two-Factors Authenticaion)、三因子認證等。
- 5.遠端連線資料的機密層級管控：主體與受體的機密設定。
- 6.遠端連線備援線路及備援機制：如備援迴路及其切換機制的建立。
- 7.遠端連線登入、行為的 Log 紀錄：需記錄遠端連線帳號的登入與存取行為。
- 8.遠端連線的復原性、BCP 所需時間：相關復原時間是否符合資訊安全規範。
- 9.遠端連線所及資料的多重機制備份：如完整備份、差異備份、增量備份等。
- 10.遠端連線的即時更新，避免漏洞造成的威脅：包含連線程式、應用軟體，以及資料存取的安全性更新。

高上

【版權所有，重製必究！】

司法特考·調查局特考

高點考季友賞



8/31前，憑司特、調特准考證享全年最優惠

8/12~14報名113面授/VOD課程>加贈高點圖書禮券1,000元

★司法特考四等

類別	面授/VOD專業全修	雲端全修年度班
法警/執達員/執行員	特價 22,000 元	特價 35,000 元
法院書記官	特價 28,000 元	特價 38,000 元
監所管理員	特價 23,000 元	特價 32,000 元

★司法特考三等

- 面授/VOD：特價 **32,000**元起
- 雲端：特價 **44,000**元起

★調查局特考三等

- 面授/VOD：特價 **38,000**元起
- 雲端：特價 **46,000**元起

★差異科目/弱科加強 (限面/VOD)

- 監所管理員全修+警察法規概要：特價 **36,000**元
- 四等書記官+公務員法概要：特價 **40,000**元
- 法警+公務員法概要：特價 **35,000**元
- 四等小資：特價 **16,000**元起

★實力進階

類別	面授/VOD	雲端
申論寫作班	單科特價 3,000 元起	單科 7 折起
矯正三合一題庫班	特價 4,000 元	單科 7 折起
犯罪學題庫班	特價 1,700 元	單科 8 折起
四等狂作題班	限面授 全修 15,000 元、單科 5,000 元	

※諮詢&報名詳洽【法政瘋高點】LINE 生活圈(ID: @get5586)
 ※報名全修考生若當年度考取相同等級類科，二週內可回班辦理退費

