中國文化大學教師教學創新暨教材研發獎勵申請期末報告

計畫名稱:

整合系統建置、稽核實務、證照考取之資訊安全稽核教材創新計畫

資訊管理學系

賴谷鑫

中華民國一〇四年七月

目錄

壹、計畫名稱…… 3
貳、實施課程、授課教師姓名…….. 3
參、前言
肆、計畫特色與具體內容…… 3
伍、實施成效以及影響……. 3
陸、結論…….. 6
柒、執行計畫活動照片 …….. 6

壹、計畫名稱

整合系統建置、稽核實務、證照考取之資訊安全稽核教材創新計畫。

貳、實施課程、授課教師姓名

本計畫欲實施的課程名稱為資管系三年級之資訊安全稽核、實施教師為資管系專任助理教授賴谷鑫老師。

參、前言

行政院資通安全會報規定，資安等級 A、B 級政府單位須於 2008 年前建置完成資安管理系統，並取得第三方認證通過。目前資訊安全管理系統的標準為 ISO 27001，該標準規定通過驗證者每年需要複檢以及三年必須重驗一次。因此目前業界對於資訊安全管理系統的建置以及稽核人才需求量極大。

雖然資訊安全管理系統的建置以及稽核十分重要，但是目前坊間卻缺乏相關的書籍或是教材。目前學生想學習相關方面知識只有到外面專業的教育訓練單位學習，但是引發幾個問題。第一個問題也是最主要的問題就是市面上根本無相關良好的教材以及教科書可以提供做為上課教材。第二個問題為學費十分昂貴。下圖一為 BSI 教育訓練機構針對 ISO 27001 所開設課程大綱以及價格。由下圖一可以看到相關的教育訓練價格昂貴。

圖 1:當前 ISO 27001 外部教育訓練介紹

而第三個問題為資訊安全管理的稽核以及建置兩大議題缺乏整合。大部分的教育訓練中心將資訊安全管理系統的稽核以及建置分開授課，這代表著就算授課老師取得目前外部教育訓練單位的教材也需要整合。而最後一個問題為缺乏真實案例的個案探討。目前教材均只針對標準做一簡單的描述，缺乏以個案探討的方式學習資訊安全管理系統的建置以及稽核。

本計畫的目的則是為了改善上述四個問題問題，本計畫將撰寫資訊安全管理與稽核的教材，其重點有(1)整合資訊安全管理系統建置以及稽核的內容；(2)整合業界 ISO 27001 主導稽核員教材協助學生考取證照;(3)利用真實組織的 4 階文件作為個案探討以及教學文件。透過本計畫所提供的教材，學生可以(1)學習到完整資訊安全管理系統建議己及稽核；(2)增進問題解決的能力；(3)了解業界所需，增強自我競爭力；(4)協助學生通過 ISO 27001 主導稽核員教育訓練課程考試。

肆、計畫特色

本計畫特色為整合資訊安全管理系統稽核以及建置。結合外部教育訓練單位教材以及真實組織四階文件(預計將使用 KPMG 教育訓練教材以及南部某大專院校四階文件)。透過真實本計畫所設計的整合式教材，勢必可以增進學生資訊安全稽核的基本知識。本計畫的執行方法如下圖 2 所示。

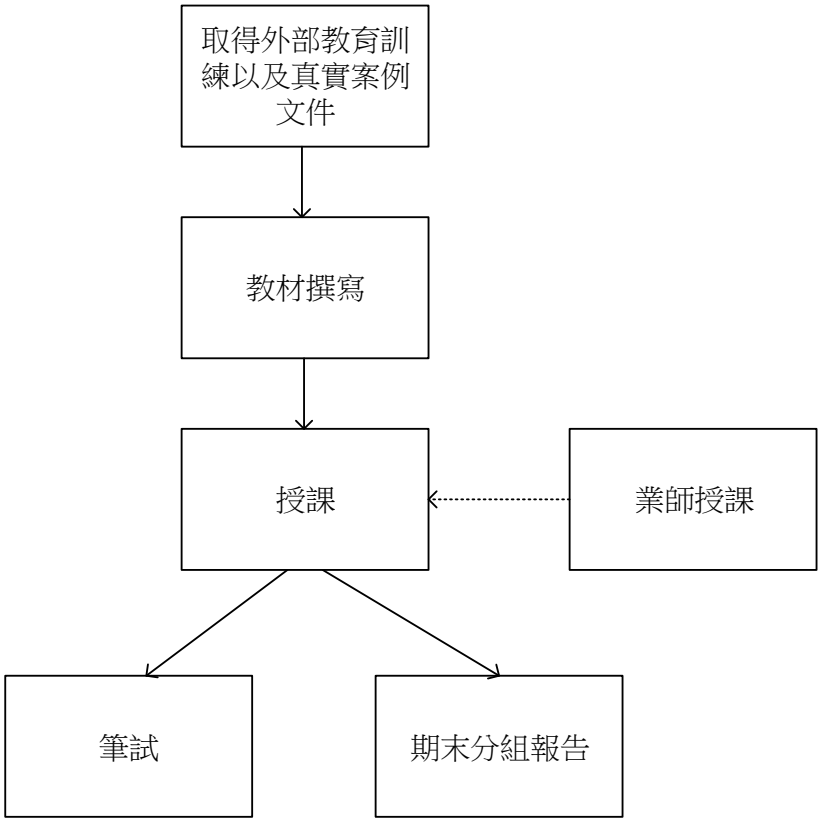


圖 1:專案執流程圖

Step 1: 取得外部教育訓練以及真實案例文件: 本計畫將使用 KPMG 主導稽核員教育訓練教材，該教材主要強調為稽核的規畫以及執行部分。而在強化資訊安全管理系統的建置上，本計畫將使用 CNS 27001、CNS 17799 中文文件做為教材主體，然而 CNS 27001 與 CNS 17799 內容太過精簡，本計畫取得南部某大專院校資訊安

全管理系統之所有文件，藉以製作整合式的教材。

Step 2: **教材撰寫:**上述的文件皆無法製作成獨立教材。本計畫規劃首先以資訊安全管理系統建置為主，該部分教材主要以 CNS 27001、CNS 17799 以及本計畫取得之真實個案為主。而隨後在整合 KPMG 教育訓練教材作為稽核教材主體。在稽核教材部分還會整合真實個案內的文件以及原始表單。透過教材的整合可以使學生學習到完整的資訊安全管理系統的建置與稽核知識。

Step 3: **授課:**本計畫所預計採用的授課方式為課堂授課、分組報告以及業師授課。課堂授課為本計畫所編寫的教材；於分組報告部分，本課程會透過分組方式，分組報告有兩個議題，第一個議題為資訊安全技術以及解決方案的報告，此議題主要為學生選擇幾個資訊安全的技術以及解決方案做報告，該分組報告的主要目的為使學生對業界資訊安全技術有所了解，藉以用相關知識作為之後資訊安全管理系統的建置；分組報告的第二的主題為資訊安全管理系統的建置以及稽核。本課程預計將學生分組分為建置組以及稽核組，透過角色模擬以及分組報告來學習相關知識。而本課程也已經安排業師授課，該業師為資深網路安全人員，業師授課可以使資深網管人員以及學生進行零距離的互動，對於學生解惑扮演十分重要腳色。

Step 4: **計畫與教學評量:**為了評量學生的學習成果，本課程利用筆試以及其中分組報告作為教學評量。其中分組報告需上台報告資訊安全相關技術以及資訊安全管理系統的建置以及稽核報告。分組報告可以了解該組學生對於資訊安全管理系統有無深入了解。但是分組報告無法評量每位組員是否對於資訊安全管理系統課程有深入的了解，因此本課程也會採用筆試的方式針對學生的基本知識作評量。本課程期望達到至少每位學生對於資訊安全管理系統的基礎知識都有所了解而進而了解業界知識。

伍、實施成效以及影響

本計畫目前已經執行完畢，已經完成所有教材編撰以及業師授課，本教材共分 ISO 27001 稽核部分、個人資料保護稽核部分以及業師經驗分享教材部分。下圖 2、3 為 ISO 27001 教材部分截圖。

圖 2、ISO 27001 教材截圖

圖 3、ISO 27001 教材截圖

而本計畫目標是要結合證照考試、因此下圖 4 為 ISO 27001 證照考試教材介紹。

圖 4、ISO 27001 考試介紹

而目前業界主流是結合 ISMS 以及 PIMS，也就是結合資訊安全管理系統以及個人資料保護管理系統。因此本計畫也製作相關教材，並且教導如何結合此兩種系統。下圖 5、6 為 PIMS 教材截圖。

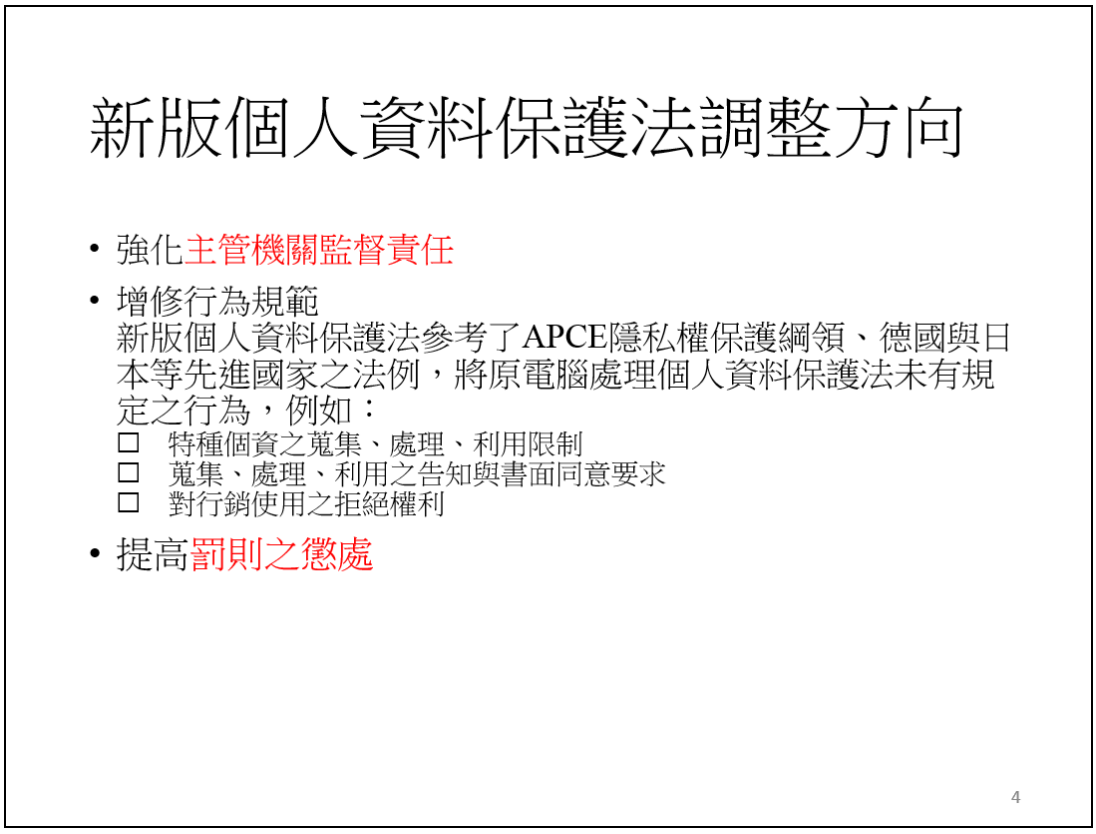


圖 5、PIMS 介紹

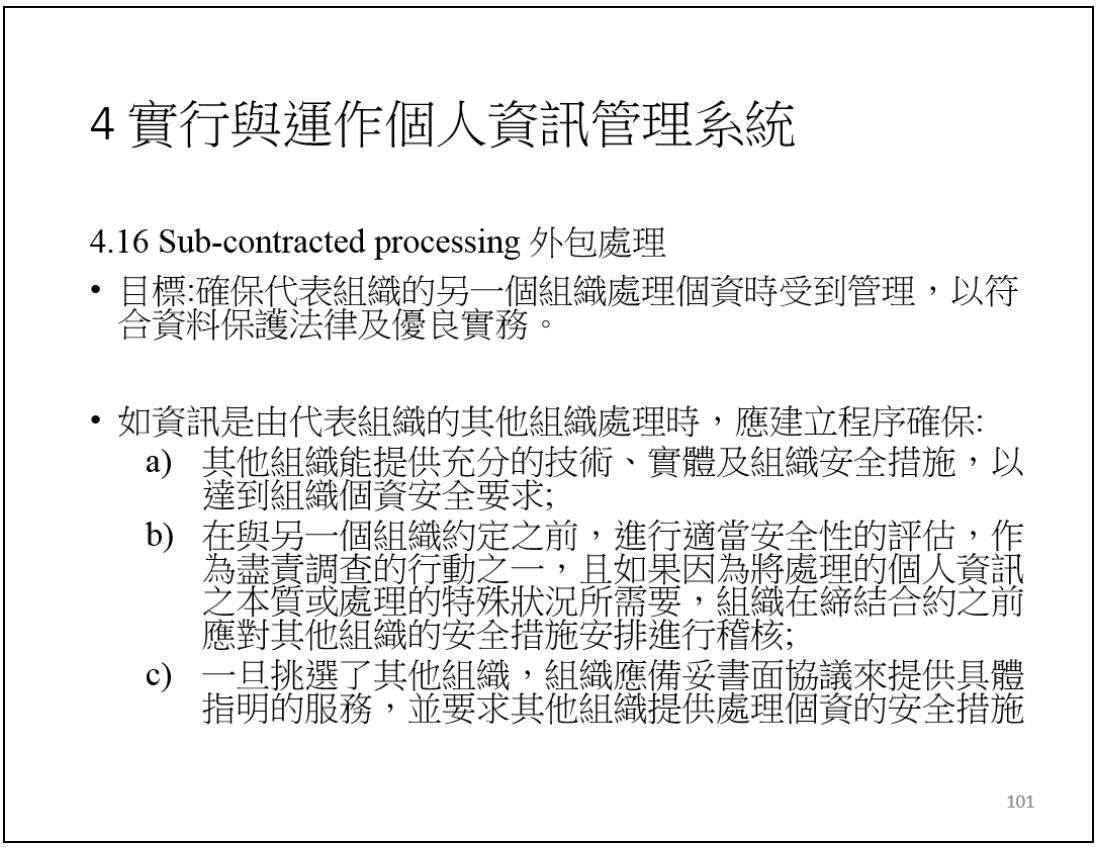


圖 6、PIMS 實作

除了理論教學以及證照輔導外，業界經驗十分重要，本本計畫於 5 月 19、5 月 16 號請業師上課，下圖 7、8 為業師授課講義截圖。

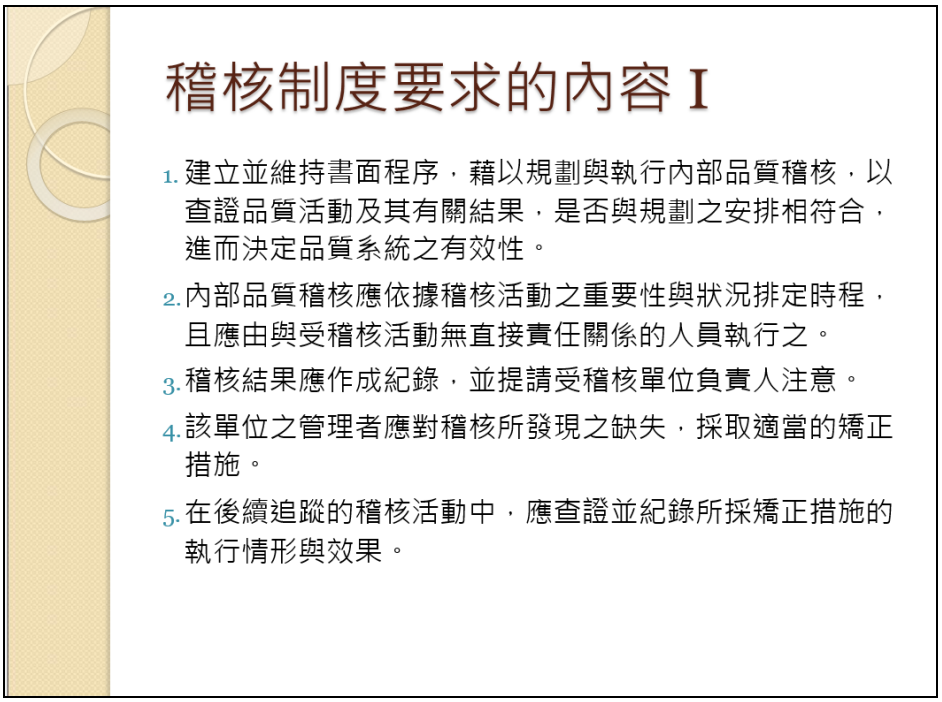


圖 7: 業師教材

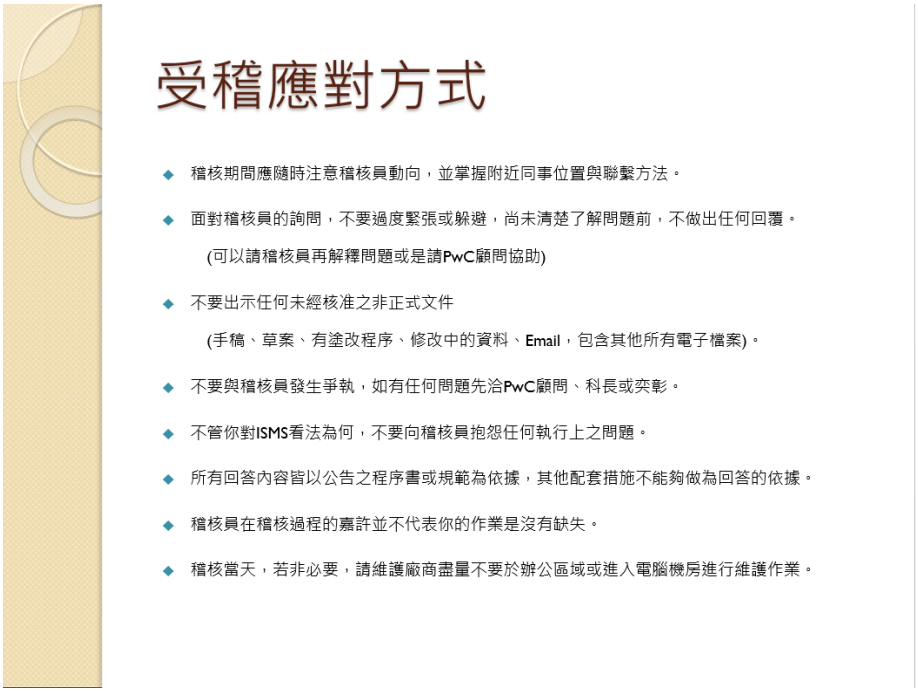
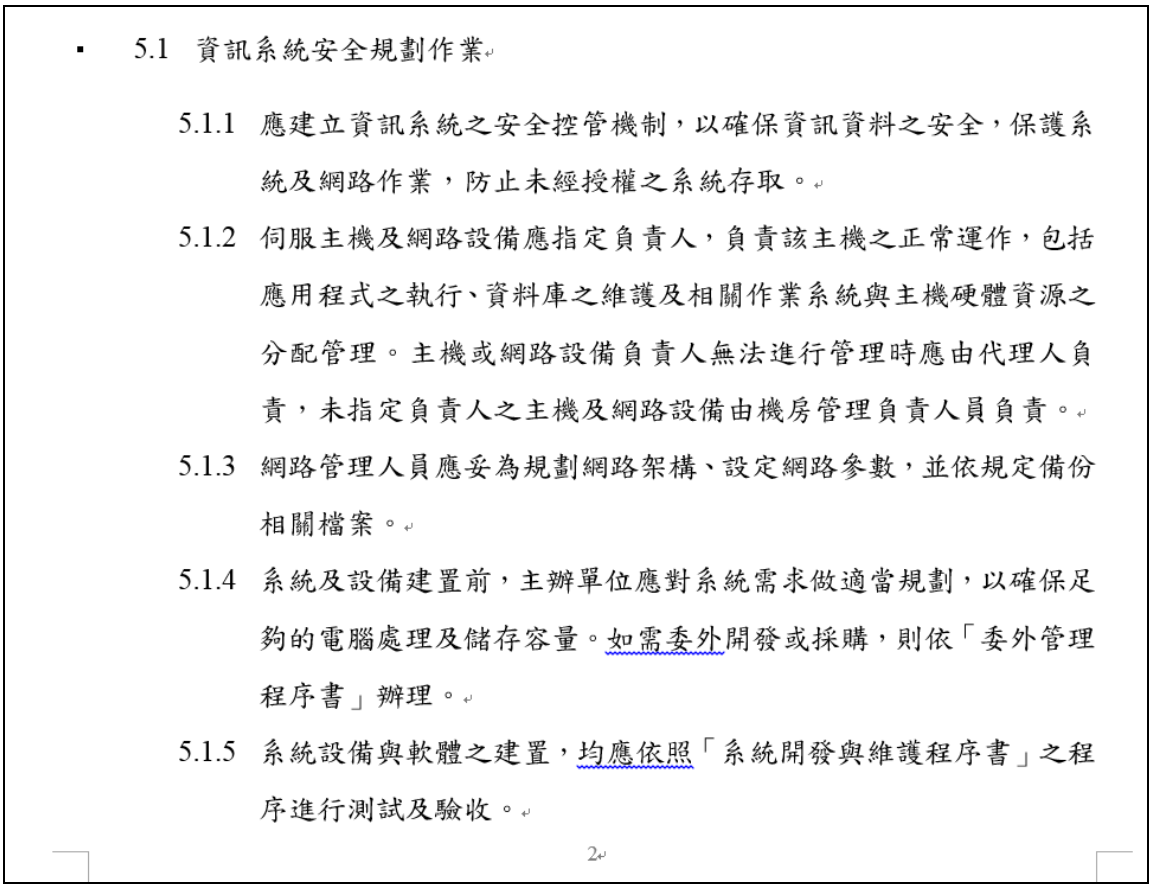


圖 8: 業師經驗分享

而不論是資訊安全稽核或是個人資料保護的稽核，文件都佔據重要腳色，因此取得真實稽核文件作為教材是本計畫的重點，下圖 9 與 10 為本計畫所使用的真實案例文件教材截圖。



- 5.1 資訊系統安全規劃作業

5.1.1 應建立資訊系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。

5.1.2 伺服主機及網路設備應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理。主機或網路設備負責人無法進行管理時應由代理人負責，未指定負責人之主機及網路設備由機房管理負責人員負責。

5.1.3 網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。

5.1.4 系統及設備建置前，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。如需委外開發或採購，則依「委外管理程序書」辦理。

5.1.5 系統設備與軟體之建置，均應依照「系統開發與維護程序書」之程序進行測試及驗收。

2

圖 9: 真實文件分享

5.4.1 應訂定使用授權軟體與遵守著作權規範，違反規範者應依相關程序議處。

5.4.1.1 使用軟體與資訊產品不得超過允許的最高使用人數。

5.4.1.2 使用軟體與資訊產品應遵守相關規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。

5.4.1.3 取得之合法軟體不得從事或轉讓予非授權範圍之使用。

5.4.1.4 從公共網路取得之合法軟體與資訊須遵守原著作權者與電腦處理個人資料保護法之規定。

5.4.1.5 對公共系統的存取不得擅自存取其所相連的網路。

5.4.2 應妥善保管採購軟體產品之授權書、原版光碟、手冊等等證明。

5.4.3 經由網際網路下載之公開授權軟體，應在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

- 5.5 網路安全管理

5.5.1 網路服務之管理

5.5.1.1 避免利用公共網路傳送敏感等級（含）以上資訊，應保護資

圖 10:真實文件分享

本計畫實施至今深受同學歡迎，同學滿意度表現於其中教學評量上，下圖 11 為本課程其中教學評量、而下圖 12 為期末評量。根據評量成績，顯示同學皆滿意此教學教材以及規劃。

查詢範圍 103 查詢 ：學生留言

學年期	1032	授課教師	A10056賴谷鑫
開課資料	UBIMD資管系 JB	科目中文	IT2500資訊安全稽核
選課人數	26	填答人數	2

大項	小項	是(人數)	否(人數)	是(%)	否(%)
1.教師基本職責	1-1準時上下課	2	0	100.00	0.00
	1-2注重出席率	2	0	100.00	0.00
	1-3維持課堂秩序	2	0	100.00	0.00
	1-4提供課外或課後時間輔導	2	0	100.00	0.00
	1-5樂於回答學生問題	2	0	100.00	0.00
	1-6具教學熱忱	2	0	100.00	0.00
2.教學方法	2-1師生互動良好	2	0	100.00	0.00
	2-2表達方式易懂	2	0	100.00	0.00
	2-3能引發學習興趣	2	0	100.00	0.00
	2-4鼓勵學生表達意見	2	0	100.00	0.00
	2-5依據學生程度或反映調整教學方式	2	0	100.00	0.00
	2-6運用課輔平台促進(數位)學習	2	0	100.00	0.00
3.教材內容設計	3-1符合授課計畫	2	0	100.00	0.00
	3-2內容有組織紙具連貫性	2	0	100.00	0.00
	3-3上課提供講義或使用ppt(數位)教材	2	0	100.00	0.00
	3-4教材生動活潑具創意	2	0	100.00	0.00
4.評量考核方式	4-1公平合理	2	0	100.00	0.00
	4-2反映學習成效	2	0	100.00	0.00
	4-3評量標準清楚	2	0	100.00	0.00
	4-4評量方式多元，如採計作業或討論等成績	2	0	100.00	0.00
5.整體產生興趣程度	我對本科目產生興趣	2	0	100.00	0.00
6.整體滿意度	我對本科目感到滿意	2	0	100.00	0.00

圖 11:期中教學評量

本計畫實施至今深受同學歡迎、成果豐碩，於質化的成效部分如下：

1. 目前市面上並無公開的相關教材:透過本計畫的實行可以使得學生上課有更適合的教材。

2. 目前可取得教材缺乏整合問題:就算是夠過管道取得，也缺乏整合性。透過本計畫所撰寫教材的補強，可以增加方法論的完整性，學生可以藉此學習連貫且完整的知識。

3. 目前學生無法與企業接軌問題:學生雖然學習到完整的理論，但是缺乏實際案例做完參考，本計畫所提供的真實文件可以使學生學得真正資訊安全管理系統建置以及稽核的實際案例。

4. 協助證照考取:本計畫所撰寫的教材將有助於有興趣的學生通過 ISO 27001 主導稽核員訓練課程考試。

陸、結論

資訊安全稽核與管理為未來資訊人員重要技能之一，然而除了外面教育機構外，學校教育並無此類相關課程。除此之外，相關教材也極難取得。本計畫結合授課教師本身經驗、實務文件取得、教材編寫以及業師授課充實學生素養以及專業能力。而本計畫可以透過學生課堂報告以及期末報告與考試確保學生學習成效。

柒、執行計畫活動照片

本計畫於 5 月 19、5 月 16 號請業師上課，下圖 12、13 為業師上課情況

圖 12:業師授課

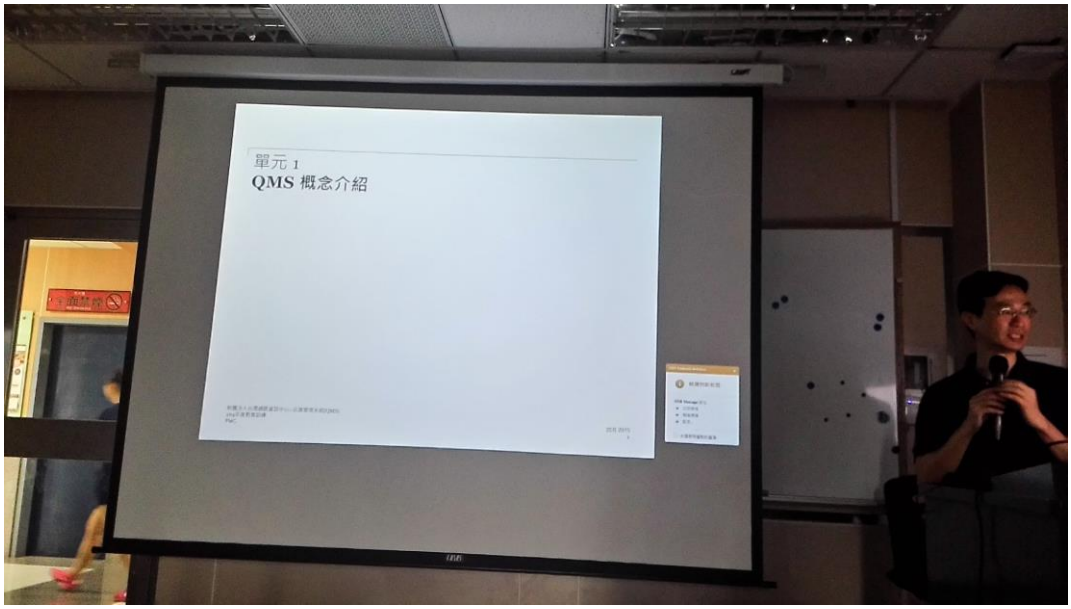


圖 13:業師授課

而圖 14 以及 15 為同學參與紀錄。

圖 14、同學參與紀錄

附件 3

圖 15、同學參與紀錄