國立高雄科技大學
National Kaohsiung University of Science and Technology

雲世代資通安全管理與技術人才培育班

110/06/28-08/24 09:30-16:30 週一至週五，共200小時 **第一校區**

*課程審查中，最後結果將依勞動部高屏澎東分署公告為主

訓練對象

1.年滿15歲至29歲本國籍待業青年(每月最高可領8000元學習獎勵金)
非屬日間部在學生(進修部學生，無工作、無投保勞保者可參加)
2.需具備大學畢業學歷

課程大綱

本課程以資通安全管理和技術核心知識和技能為核心，
並搭配證照BOK作為課程設計主軸，進行下述七大課程模組之規劃

1.資通安全概論
2.資訊安全管理系統稽核
3.網路攻擊技術與行為分析
4.資安健診與滲透測試
5.個資保護
6.證照模考與實戰經驗分享
7.訓練發展及職涯策略規劃

掃我報名

報名方式

1.請先掃QRcode至教推中心報名完成個人資料。
2.待審查通過後以Email通知至台灣就業通(掃QRcode)
加入會員，並登錄台灣就業通會員，完成「我喜歡做的事」測驗。
3.產業新尖兵試辦計畫(掃QRcode)報名課程。
4.開課通知將以E-MAIL及電話通知錄取學員。

台灣就業通　新尖兵網站　LINE客服　簡章下載

聯絡我們：
07381452 6#12844-12847

勞動部勞動力發展署

雲世代資通安全管理與技術人才培育班

【產業新尖兵試辦計畫補助課程招生簡章】

【辦訓單位】國立高雄科技大學

【招生對象及資格】

1.本計畫經費補助適用對象 15 歲至 29 歲之本國籍待業青年。

2.學員參訓須以結訓後直接就業為目標，無就業意願或有升學計劃者，請勿報名。

3.歡迎應屆畢業生，有意願轉職或轉換跑道的青年。

【開訓日期】110 年 06 月 28 日至 08 月 24 日

【訓練時數】共 200 小時

【訓練時間】週一至週五 09:30-16:30

【訓練地點】高科大第一校區 E 棟一樓 E116 實驗室

【訓練費用】100,000 元(產業新尖兵計畫補助，符合資格者免費參訓)*每人以補助一班為限

【報名時間】即日起至 110/06/15 日前

【課程簡介】

本課程以資通安全管理和技術核心知識和技能為核心，並搭配證照 BOK 作為課程設計主軸，進行下述七大課程模組之規劃：

1. 模組 1 (學科)：資通安全概論：資訊安全管理概論(密碼學、資通安架構、加解密與金鑰管理)及資訊安全技術概論(網路與通訊安全、作業系統與應用程式安全、資安維運技術、新興科技安全)。(42 小時)
2. 模組 2 (術科)：資訊安全管理系統稽核(ISO 27001 / ISMS)：國際認驗證機構體制簡介、資訊安全管理系統(ISMS)概述、ISO 27001/ISO27002 標準、風險評鑑、ISO 27001 稽核、稽核計畫與執行。(36 小時)
3. 模組 3 (術科)：網路攻擊技術與行為分析：封包檢測工具與通訊協定分析、DDoS 攻擊與防禦實務、弱點掃描、滲透測試、電子郵件社交工程。(36 小時)
4. 模組 4 (術科)：資安健診與滲透測試：SCO 資安監控服務維運機制、中繼站安全防護技術、行動裝置 APP 安全威脅與檢測、數位鑑識與資安事件調查實務。(36 小時)
5. 模組 5 (術科)：個資保護：個資保護相關法規、隱私保護與個資管理、去識別化、TPIPAS 介紹。(21 小時)
6. 模組 6 (術科)：證照模考與實戰經驗分享：結合前述課程並針對考證內涵(iPas 與 ISO 27001 進行輔導)，此外邀請業者針對網路攻擊等環節進行實戰經驗分享(資安情資之蒐集與分享、關鍵基礎設施之資安、新科技與資安新議題)。(21 小時)
7. 模組 7 (術科)：訓練發展及職涯策略規劃：訓練內容的職涯規劃的功能及類型、職涯探索三元素與認識自我、撰寫自傳分析法、模擬面試、性別平等課程。(8 小時)

【課程目標】

為引導 5+2 產業創新計畫產業於發展創新產品或服務之過程，融入資安相關防護及設計，行政院於 107 年通過「資安產業發展行動計畫(107-114 年)」，希望透過六大核心戰略產業與 5 + 2 產業創新計畫等各產業推動平台，協助盤點並導入各核心產業所需之資安解決方案。

在此框架下，本課程期望以代表性的資安管理和技術面的知識技能和訓練為基礎，並參考行政院國家資通安全會報所認可之資通安全專業證照，做為培訓與驗證之基礎，期藉此助培養資安管理和技術人才。在此架構下，本課程規畫涵蓋上述六大課程模組(不含模組七)，並期達成以下四大目標：

1. 確保學員掌握資通安全技術面的核心基礎知識與技能(搭配 iPas 中級資訊安全工程師能力鑑定)。
2. 確保學員掌握資通安管理知識與技能(搭配 ISO 27001 考證)。
3. 透過業師實戰案例分享，理解資安管理實務，以及網路攻擊行為模式及資安健診報告之解讀。
4. 掌握個資去識別化與店家在個資保護與管理實作的具體內涵和發展趨勢(並評估結合 TPIPAS 考證的可能)。

【就業展望】

- 就業展望: 資訊安全管理師、資訊安全工程師、資安外部稽核人員、、網路安全分析師、資訊安全防護師、資安服務與設備的 Presale。
- 課程連結就業之初步規劃: 邀請有志培養資安管理人員之資訊公司、法人機構與資安管顧公司進行授課並提供就業機會。

【篩選策略】

※具備大學畢業學歷

- 透過預先報名方式，理解既有工作經驗和參與本次訓練後之期望目的，做為甄選依據

具備資訊或ISO訓練相關背景者，或是具備數據分析能力者優先；同時，如有表達後續持續投入於資安通管理領域並搭配實務考取證照者優先

【課程模組規劃表與師資簡介】

科別	課程模組	課程主題簡介	時數	師資 (現職)	講師最高學歷
學科	資通安全概論	資訊安全管理概論(密碼學、資通安架構、加解密與金鑰管理)及資訊安全技術概論(網路與通訊安全、作業系統與應用程式安全、資安維運技術、新興科技安全)。	42	1. 國立高雄科技大學專任師資 2. 中國文化大學資安產碩專班專兼任師資 3. 行政院國家資通安全會報技術服務中心推薦師資	1. 博士級專業師資 2. 博士級專業師資 3. 碩博士級專業師資
術科	資訊安全管理系統稽核 (ISO 27001 / ISMS)	國際認驗證機構體制簡介、資訊安全管理系統 (ISMS) 概述、ISO 27001/ ISO27002 標準、風險評鑑、ISO 27001 稽核、稽核計畫與執行。	36	1. 資策會師資 2. NII 師資 3. 中國文化大學資安產碩專班專兼任師資	1. 碩士級專業師資 2. 碩士級專業師資 3. 博士級專業師資
術科	網路攻擊技術與行為分析	封包檢測工具與通訊協定分析、DDoS 攻擊與防禦實務、弱點掃描、滲透測試、電子郵件社交工程。	36	1. 資策會師資 2. 行政院國家資通安全會報技術服務中心推薦師資 3. 中國文化大學資安產碩專班專兼任師資	1. 碩士級專業師資 2. 碩博士級專業師資 3. 博士級專業師資
術科	資安健診與滲透測試	SCO 資安監控服務維運機制、中繼站安全防護技術、行動裝置 APP 安全威脅與檢測、數位鑑識與資安事件調查實務。	36	1. 資策會師資 2. 行政院國家資通安全會報技術服務中心推薦師資 3. 中國文化大學資安產碩專班專兼任師資	1. 碩士級專業師資 2. 碩博士級專業師資 3. 博士級專業師資
術科	個資保護	個資保護相關法規、隱私保護與個資管理、去識別化、TPIPAS 介紹。	21	1. 資策會師資 2. 中國文化大學資安產碩專班專兼任師資	1. 碩博士級專業師資 2. 博士級專業師資

術科	證照模考與實戰經驗分享	針對鎖定之證照 (iPas與 ISO 27001)進行輔導與模考、邀請業者針對網路攻擊等環節進行實戰經驗分享。	21	1. 行政院國家資通安全會報技術服務中心推薦師資 2. 中華軟協師資 3. 資策會推薦師資 4. 台北市政府資訊局推薦師資	1. 碩博士級專業師資 2. 碩士級專業師資 3. 碩士級專業師資 4. 碩士級專業師資
術科	訓練發展及職涯策略規劃	職涯規劃的功能及類型、職涯探索三元素與認識自我、撰寫自傳分析法、模擬面試、性別平等課程。	8	國立高雄科技大學師資	碩博士級專業師資

課程執行	特色說明
整體課程執行特色	為引導 5+2 產業創新計畫產業於發展創新產品或服務之過程中，融入資安相關防護及設計，據此打造我國產品安全品牌及印象，行政院於 107 年通過「資安產業發展行動計畫(107-114 年)」，希望透過六大核心戰略產業與 5＋2 產業創新計畫等各產業推動平台，協助盤點並導入各核心產業所需之資安解決方案。此外，蔡總統於 109 年 5 月就職演說提出六大核心戰略產業，並表示將發展可結合 5G 時代、數位轉型，及國家安全的資安產業，藉此打造可有效保護自己，也能被世界信賴的資安系統及產業鏈。在此結構下，資訊安全毋庸置疑地被定位為推升國產品之安全服務水準，發揮輔導產業創新轉型加乘力道的重要動能。 在此框架下，本課程期望以代表性的資安管理和技術面的知識技能和訓練為基礎，並參考行政院國家資通安全會報所認可之資通安全專業證照，做為培訓與驗證之基礎，期藉此助培養資安管理和技術人才。在此架構下，本課程規畫涵蓋上述六大課程模組，並期達成本課程四大目標。 此外，為期呼應就業導向之目的，本課程執行特色主要涵蓋以下幾項：(1)結合資安通辦認可之國內外證照進行培訓；(2)搭配實作的術科導向訓練；(3)邀請具潛在人才需求之業者參與授課，期提升就業媒合之可能。
針對「學科」課程教學設計	本課程之「學科」教材涵蓋模組一：資通安全概論。「學科」課程的整體教學目標在於訓練學員有關資通安全管理和資通安全技術的基礎內涵，藉此滿足目標一和二的核心基礎知識層面(即確保學員掌握資通安全管理和資通安全技術的核心基礎知識)之環節，至於相關設計內涵，簡述如下。 一、資通安全概論 (一) 課程目標：針對資訊安全管理面(包括基礎密碼學、資通安架構、加解密與金鑰管理等)及資訊安全技術面 (包括網路與通訊安全、作業系統與應用程式安全、資安維運技術、新興科技安全)的基礎環節和知識進行系統化介紹。 (二) 課程時數：42 小時。 (三) 教學方法：由授課教師自編課程內容。 (四) 教學評量：將根據學員出席率、期中期末筆試成績，給予教學評量綜合分數。

針對「術科」課程教學設計	本課程之「術科」教材涵蓋六大模組：資訊安全管理系統稽核(ISO 27001 / ISMS)、網路攻擊技術與行為分析、資安健診與滲透測試、個資保護、證照模考與實戰經驗分享，以及訓練發展及職涯策略規劃。「術科」課程的整體教學目標在於訓練學員理解和實作資通安實務應用，並透過證照取得方式檢核應具備之技能，藉此達成本訓練課程的四大目標(如下，其中目標一和二的部分，在術科重在技能面的養成，和學科強調知識面的環節，屬於互補)。 1. 目標一: 確保學員掌握資通安全技術面的核心技能(搭配 iPas 中級資訊安全工程師能力鑑定)。 2. 目標二: 確保學員掌握資通安管理所需技能(搭配 ISO 27001 考證)。 3. 目標三: 透過業師實戰案例分享，理解資安管理實務，以及網路攻擊行為模式及資安健診報告之解讀。 4. 目標四: 掌握個資去識別化與店家在個資保護與管理實作的具體內涵和發展趨勢(並評估結合 TPIPAS 考證的可能)。 至於相關設計內涵，簡述如下。 一、資訊安全管理系統稽核(ISO 27001 / ISMS) (一) 課程目標：對資訊安全管理系統(ISMS)稽核之整體內容、ISMS 稽核之實務稽核作業流程，以及政府機關 ISMS 稽核作業流程等環節進行系統性地說明。 (二) 課程時數：36 小時。 (三) 教學方法：除針對 ISO/IEC 27001 進行講授外，亦將搭配講師自編課程講義進行教授與實際練習。 (四) 教學評量：將根據學員出席率、上課表現、相關報告、考試成績等給予教學評量綜合分數。 二、網路攻擊技術與行為分析 (一) 課程目標：探討近年網路攻擊技術與其行為分析、瞭解資安事件資料分析開發流程，並說明如何人工智慧資安提供自動防護機制的作法。 (二) 課程時數：36 小時。 (三) 教學方法:除透過講師自編課程講義進行教授外,亦將搭配實際練習。 (四) 教學評量：將根據學員出席率、實作成果與報告等成績給予教學評量綜合分數。 三、資安健診與滲透測試 (一) 課程目標：透過相關知識和實務工具與案例之操作，進行實務練習，期對於後續就業求職，可直接運用，以達到掌握目前資安基本技能原理與技巧之目的。

	(二) 課程時數：36 小時。 (三) 教學方法:除透過講師自編課程講義進行教授外,亦將搭配實際練習。 (四) 教學評量：將根據學員出席率、實作成果與報告等成績給予教學評量綜合分數。 四、個資保護 (一) 課程目標:協助學員了解個人資料保護法規定及要領,並透過 TPIPAS 規範講解及實作練習，學習自主導入與建置全方位個人資料管理制度之方式，進而強化企業或組織內部個人資料管理能量。 (二) 課程時數：21 小時。 (三) 教學方法：預設透過講師自編課程講義及 TPIPAS 提供之教材，進行教授與討論。 (四) 教學評量：將根據學員出席率、上課表現、考試成績等給予教學評量綜合分數。 五、證照模考與實戰經驗分享 (一) 課程目標：結合前述課程並考證內涵進行輔導，同時為期讓授課內容連結目前產業動態與趨勢，邀請業者針對實戰作法與案例進行分享。 (二) 課程時數：21 小時。 (三) 教學方法：除透過相關題庫與教材進行輔導外，另一半時數則是搭配業者演講進行。 (四) 教學評量：根據學員出席率、課程參與、模考結果等給予教學評量綜合分數。 六、訓練發展及職涯策略規劃 (一) 課程目標：職涯規劃的功能及類型、職涯探索三元素與認識自我、撰寫自傳分析法、模擬面試、性別平等課程。 (二) 課程時數：8 小時。 (三) 教學方法：由資訊科技公司主管講解自編課程內容，並請學員分組完成模擬面試報告。 (四) 教學評量：將根據學員出席率、面試成績、口頭報告等給予教學評量綜合分數。

本課程將於 110 年 6 月至 8 月期間辦理，並於規劃學員參與相關職業知能系列課程，共 40 日、計 200 小時。(不含就業媒合；請參閱表一至表九)

(表一)培訓系統課程規劃—第一週(6/28-7/02)

	星期一 (6/28)	星期二 (6/29)	星期三 (6/30)	星期四 (7/01)	星期五 (7/02)
第一節 09:30	資通安全概論 (管理面知識)	資通安全概論 (管理面知識)	資通安全概論 (管理面知識)	資通安全概論 (技術面知識)	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	資通安全概論 (管理面知識)	資通安全概論 (管理面知識)	資通安全概論 (管理面知識)	資通安全概論 (技術面知識)	--
第五節 14:30					
第六節 15:30					
第七節 16:30	iPAS 報名說明	iPAS 報名	iPAS 報名	iPAS 報名	

(表二)培訓系統課程規劃—第二週(7/05-7/09)

	星期一 (7/05)	星期二 (7/06)	星期三 (7/07)	星期四 (7/08)	星期五 (7/09)
第一節 09:30	資通安全概論 (技術面知識)	資通安全概論 (技術面知識)	網路攻擊技術與行為分析	網路攻擊技術與行為分析	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	資通安全概論 (技術面知識)	資通安全概論 (技術面知識)	網路攻擊技術與行為分析	網路攻擊技術與行為分析	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

(表三)培訓系統課程規劃—第三週(7/12-7/16)

	星期一 (7/12)	星期二 (7/13)	星期三 (7/14)	星期四 (7/15)	星期五 (7/16)
第一節 09:30	網路攻擊技術與行為分析	網路攻擊技術與行為分析	網路攻擊技術與行為分析	網路攻擊技術與行為分析	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	網路攻擊技術與行為分析	網路攻擊技術與行為分析	網路攻擊技術與行為分析	網路攻擊技術與行為分析	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

(表四)培訓系統課程規劃—第四週(7/19-7/23)

	星期一 (7/19)	星期二 (7/20)	星期三 (7/21)	星期四 (7/22)	星期五 (7/23)
第一節 09:30	資安健診與滲透測試	資安健診與滲透測試	資安健診與滲透測試	資安健診與滲透測試	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	資安健診與滲透測試	資安健診與滲透測試	資安健診與滲透測試	資安健診與滲透測試	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

(表五)培訓系統課程規劃—第五週(7/26-7/30)

	星期一 (7/26)	星期二 (7/27)	星期三 (7/28)	星期四 (7/29)	星期五 (7/30)
第一節 09:30	資安健診與滲透測試	資安健診與滲透測試	資訊安全管理系統稽核	資訊安全管理系統稽核	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	資安健診與滲透測試	資安健診與滲透測試	資訊安全管理系統稽核	資訊安全管理系統稽核	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

(表六)培訓系統課程規劃—第六週(8/02-8/06)

	星期一 (8/01)	星期二 (8/02)	星期三 (8/03)	星期四 (8/04)	星期五
第一節 09:30	資安健診與滲透測試	資安健診與滲透測試	資訊安全管理系統稽核	資訊安全管理系統稽核	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	資安健診與滲透測試	資安健診與滲透測試	資訊安全管理系統稽核	資訊安全管理系統稽核	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

(表七)培訓系統課程規劃—第七週(8/09-8/13)

	星期一 (8/09)	星期二 (8/10)	星期三 (8/11)	星期四 (8/12)	星期五
第一節 09:30	資訊安全管理系統稽核	資訊安全管理系統稽核	資訊安全管理系統稽核	資訊安全管理系統稽核	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	資訊安全管理系統稽核	資訊安全管理系統稽核	資訊安全管理系統稽核	資訊安全管理系統稽核	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

註: 8/14(六) iPAS 證照考試(未列入上課時數)

(表八)培訓系統課程規劃—第八週(8/16-8/20)

	星期一 (8/16)	星期二 (8/17)	星期三 (8/18)	星期四 (8/19)	星期五 (8/20)
第一節 09:30	個資保護	個資保護	個資保護	個資保護	證照模考與實戰經驗分享
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	個資保護	個資保護	個資保護	訓練發展及職涯策略規劃(2 小時)	證照模考與實戰經驗分享
第五節 14:30					
第六節 15:30					
第七節 16:30					

(表九)培訓系統課程規劃—第九週(8/23-8/25)

	星期一 (8/23)	星期二 (8/24)	星期三 (8/25)	星期四 (8/26)	星期五 (8/27)
第一節 09:30	訓練發展及職涯策略規劃	就業媒合活動	--	--	--
第二節 10:30					
第三節 11:30					
午休(12:30~13:30)					
第四節 13:30	訓練發展及職涯策略規劃	就業媒合活動	--	--	--
第五節 14:30					
第六節 15:30					
第七節 16:30					

備註: 「就業媒合活動」為本計畫協助學員進行就業媒合所規畫執行的活動，非屬於實體課程的項目(故未計入課程時數)。