

# (ISC)<sup>2</sup>系列資安認證與考試資訊介紹



(ISC)<sup>2</sup>國際資訊系統安全核準聯盟，是一家為全球資訊安全人員，提供教育訓練及認證服務的非營利國際組織，亦是當今最被各大企業與政府單位所信賴的公正組織之一。在台灣，(ISC)<sup>2</sup>獨家授權恆逸教育訓練中心為(ISC)<sup>2</sup>於台灣的教育聯盟機構，提供台灣資安人員與全球同步的(ISC)<sup>2</sup>資安認證教育訓練。(ISC)<sup>2</sup>資安認證課程均以國語教授並輔以英語教材，恆逸授課講師群已通過(ISC)<sup>2</sup>嚴格的師資培訓訓練與認證，是國內資安人員考取最具公信力的(ISC)<sup>2</sup>資安系列認證的最佳選擇。



## SSCP<sup>®</sup>資訊安全專業人員認證 System Security Certified Practitioner

SSCP<sup>®</sup>認證是針對在企業組織中負責網路及系統管理的相關人員，有資訊安全技術能力且具實務經驗者而設，此證照以公正客觀的標準，界定企業組織中實際負責運作及落實資安政策相關從業人員的實務工作範圍、角色與職務。取得SSCP<sup>®</sup>認證，代表應具備SSCP<sup>®</sup>CBK七大領域的相關知識，包括瞭解各個常規工作範圍在推行、監督、運作上所運用的基本原則、組成部分及應用技術。



## CISSP<sup>®</sup>資訊安全系統專家認證 Certified Information Systems Security Professional

CISSP<sup>®</sup>認證被譽為資訊安全界的至高標準！並且是第一張經由ANSI美國國家標準學會認可符合ISO/IEC 17024國際標準要求的資訊安全證照；CISSP<sup>®</sup>認證是針對在企業組織中的專業資安人員、資安顧問，或是資訊部門管理階層而設。雇主可以更有信心相信其所聘用的CISSP資訊安全人員，擁有所需要的技術水準與經驗，並能有效的處理及執行企業之資訊安全系統與政策。



## CSSLP<sup>®</sup>資訊安全軟體開發專家認證 Certified Secure Software Lifecycle Professional

(ISC)<sup>2</sup>推出與軟體安全開發有關的準則及認證，藉此期望降低軟體開發在安全上的問題。在(ISC)<sup>2</sup>所提出的準則中，其將軟體安全開發所需具備的知識，劃分為八大知識體系(CBK<sup>®</sup>)，藉由取得CSSLP<sup>®</sup>認證，將可視為軟體開發人員對於安全軟體開發八大知識領域專業程度的展現。



## CCSP<sup>®</sup>雲端資安專家認證 Certified Cloud Security Professional

CCSP<sup>®</sup>認證是二大安全組織 - (ISC)<sup>2</sup>及CSA(雲端安全聯盟)兩大國際原廠聯手打造的頂級雲端資安認證。透過此認證，主要用於表彰其持有者對於資訊及雲端安全的專業與能力，藉此以協助組織維持重要雲端基礎設施的正常運作、免於危害。

|              | SSCP                                                                                                                                                                                                     | CISSP                                                                                                                                    | CSSLP                                                                                                                                  | CCSP                                                                                                                                                                 |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 主要差異         | 偏重資安工作的日常維運能力                                                                                                                                                                                            | 偏重資訊安全的管理能力                                                                                                                              | 偏重資安軟體開發管理知識                                                                                                                           | 偏重雲端安全管理能力                                                                                                                                                           |
| 報考資格         | 擁有一年以上專業經驗；並於七個SSCP CBK範圍中擁有最少一個領域的相關工作經驗                                                                                                                                                                | <ul style="list-style-type: none"> <li>八個CISSP CBK範圍中具有二個或多個領域五年以上工作經驗</li> <li>具備大學學位或持有(ISC)<sup>2</sup>認可之證書者，可抵免最多一年之工作經驗</li> </ul> | <ul style="list-style-type: none"> <li>八個CSSLP CBK範圍中具備至少一個領域滿四年工作經驗</li> <li>具備大學學位或持有(ISC)<sup>2</sup>認可之證書者，可抵免最多一年之工作經驗</li> </ul> | <ul style="list-style-type: none"> <li>五年IT工作經驗，其中3年為資安工作經驗及CCSP CBK範圍中1年工作經驗</li> <li>取得CSA CCSI認證者可抵免CCSP CBK範圍中一年工作經驗</li> <li>取得CISSP認證者可抵免CCSP所有年資要求</li> </ul> |
| 工作經驗不足之報考者   | 可報考Associates of (ISC) <sup>2</sup> for SSCP(準會員)，兩年內累積足夠專業經驗，得到審核及推薦後可正式成為SSCP                                                                                                                          | 可報考Associates of (ISC) <sup>2</sup> for CISSP(準會員)，六年內累積足夠專業經驗，得到審核及推薦後可正式成為CISSP                                                        | 可報考Associates of (ISC) <sup>2</sup> for CSSLP(準會員)，五年內累積足夠專業經驗，得到審核及推薦後可正式成為CSSLP                                                      | 可報考Associates of (ISC) <sup>2</sup> for CCSP(準會員)，六年內累積足夠專業經驗，得到審核及推薦後可正式成為CCSP                                                                                      |
| 知識領域科目       | 7個                                                                                                                                                                                                       | 8個                                                                                                                                       | 8個                                                                                                                                     | 6個                                                                                                                                                                   |
| 考試費用         | 249美元                                                                                                                                                                                                    | 699美元                                                                                                                                    | 599美元                                                                                                                                  | 599美元                                                                                                                                                                |
| 考試題目         | 通過3小時，共125題選擇題的英文測驗                                                                                                                                                                                      | 報考英文版考試：<br>通過3小時，100-150題電腦互動式測驗(CAT)；<br>或報考簡體中文或其他語系考試：<br>通過6小時，250題線性測驗                                                             | 通過3小時，共125題單選題的英文測驗                                                                                                                    | 通過3小時，共125題單選題的英文測驗                                                                                                                                                  |
| 證書申請資格與流程    | 1. 通過考試。<br>2. 完成線上申請 <a href="https://apps.isc2.org/">https://apps.isc2.org/</a> 程序。須由 (ISC) <sup>2</sup> 或其會員背書。持 (ISC) <sup>2</sup> 有效證書者，皆為其會員。<br>3. (ISC) <sup>2</sup> 將對應試者，抽樣執行稽核審核查其應試者之相關工作經驗。 |                                                                                                                                          |                                                                                                                                        |                                                                                                                                                                      |
| 會員年費         | 不論持有證照數量每年皆為 125 美元                                                                                                                                                                                      |                                                                                                                                          |                                                                                                                                        |                                                                                                                                                                      |
| CPE (持續教育積分) | <ul style="list-style-type: none"> <li>SSCP可在三年內取得60分CPE，否則須重新參加考試。</li> <li>每年至少需取得20分CPE，累積三年共60分CPE。</li> </ul>                                                                                       | <ul style="list-style-type: none"> <li>CISSP可在三年內取得120分CPE，否則須重新參加考試。</li> <li>每年至少需取得40分CPE，累積三年共120分CPE。</li> </ul>                    | <ul style="list-style-type: none"> <li>CSSLP可在三年內取得90分CPE，否則須重新參加考試。</li> <li>每年至少需取得30分CPE，累積三年共90分CPE。</li> </ul>                    | <ul style="list-style-type: none"> <li>CCSP可在三年內取得90分CPE，否則須重新參加考試。</li> <li>每年至少需取得30分CPE，累積三年共90分CPE。</li> </ul>                                                   |

請依據(ISC)<sup>2</sup>相關規定報名考試，考試報名可經由VUE考試中心報名預約考試時間。

考試報名網址：<http://www.pearsonvue.com/isc2/>

CPE手冊網址：<https://www.isc2.org/cpe-handbook>

SSCP

## SSCP資安專業人員認證課程

Systems Security Certified Practitioner Course

時數：40小時 | 費用：40,000元 | 點數：11點 | 教材：(ISC)<sup>2</sup>原廠教材

## 適合對象

1. 對資訊安全工作有興趣者
2. 欲取得SSCP<sup>®</sup>認證資格者
3. 欲充實本身資安技術能力的IT人員

## 預備知識

網路安全基礎概念

## 課程內容

- 第一章—介紹安全及符合風險管理之資產管理
1. 認識安全觀念
  2. 參與資產管理
  3. 認識風險管理流程
  4. 認識風險管理流程-風險處置
- 第二章—認識管理風險之選項並使用存取控制保護資產
1. 記錄、建置與維護功能性之安全控制措施
  2. 建置存取控制-存取控制模型
  3. 參與身份識別管理生命週期
  4. 建置與維護鑑別方式-身份識別與存取管理
- 第三章—密碼學
1. 認識密碼學基礎觀念
  2. 認識密碼學基礎觀念-加密方式
  3. 認識公開金鑰基礎設施系統
  4. 認識密碼學基礎觀念-金鑰管理
  5. 認識與支援安全協定
- 第四章—保護軟體、使用安全協定並保護遠端用戶
1. 保護軟體
  2. 識別與分析惡意程式碼與活動
  3. 建置與操作端點裝置安全
  4. 操作與設定雲端安全
- 第五章—網路與網管
1. 認識網路與網管
  2. 認識網路關鍵元件-通訊埠與協定
  3. 認識網路攻擊與對策
  4. 管理網路安全
- 第六章—無線網路、通信、雲端組態、監控系統及端點安全
1. 操作與設定雲端安全及虛擬化
  2. 操作與設定無線技術
  3. 管理網路存取控制-POTS與PBX
- 第七章—安全測試與事故處置
1. 操作與維護監控系統
  2. 執行安全評估活動
  3. 支援事故生命週期
  4. 認識與支援持續營運計畫及災難復原計畫活動
  5. 認識及支援鑑識調查
- 第八章—實體安全、異動管理與人員訓練
1. 參與異動管理
  2. 參與實體安全作業
  3. 參與安全認知訓練

## 備註事項

1. 白天班之上課時間為09:00~18:00
2. 課程結束後，出席率達80%以上者將獲頒發(ISC)<sup>2</sup>官方培訓證書
3. 報名本課程者，原報名班級開課日起一年內，可享有同一版本課程免費一次辦理重聽之機會
4. 通過考試後，欲申請SSCP<sup>®</sup>認證必須符合(ISC)<sup>2</sup>相關規定
5. 課程優惠方案：
  - 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT\$36,000元
  - 學生優惠價：參加校園IT職涯學習護照方案，享有5折優惠價NT\$20,000元

## 後續推薦課程

CISSP：CISSP資安系統專家認證課程



獨家課程



CSSLP認證



PDU學分



此課程為「行政院國家資通安全會報」認可之資通安全專業證照

CSSLP

# CSSLP資安軟體開發專家認證課程

Certified Secure Software Lifecycle Professional Course

時數：40小時

費用：50,000元

點數：12.5點

教材：(ISC)<sup>2</sup>原廠教材

CSSLP



適合對象

1. 參與系統或軟體開發之相關人員  
2. 軟體專案經理、系統架構師、系統分析師

3. 程式設計師、軟體測試人員  
4. 稽核人員

預備知識

軟體開發生命週期

課程內容

本課程涵蓋CSSLP®CBK®SDLC八大領域。課程內容不涉及特定開發技術，而是著重在如何進行安全程式開發的流程與方法。

第一章—軟體安全概論

Module 1: 軟體安全核心概論

Module 2: 軟體安全設計原則

第二章—安全軟體生命週期與風險管理

Module 1: 定義安全策略與路線圖

Module 2: 安全組態與強化

Module 3: 於軟體開發方法中管理安全性

Module 4: 定義與編撰安全性文件

Module 5: 制定安全指標

Module 6: 汰除軟體

Module 7: 報告安全狀態

Module 8: 整合風險管理

Module 9: 作業風險分析

Module 10: 提升軟體開發中的安全文化

Module 11: 持續改善

第三章—軟體安全需求

Module 1: 定義軟體安全需求

Module 2: 識別須分析遵循需求

Module 3: 識別須分析資料分級需求

Module 4: 識別須分析隱私需求

第四章—軟體安全架構與設計

Module 1: 建立威脅模型

Module 2: 定義安全架構

Module 3: 設計安全介面

Module 4: 安全設計考量

Module 5: 檢討安全架構與設計

第五章—軟體安全開發

Module 1: 安全開發最佳實務

Module 2: 常見應用程式風險

Module 3: 建構安全措施

Module 4: 安全的使用第三方元件或函式庫

Module 5: 安全的整合元件

Module 6: 於建置過程應用安全

第六章—軟體安全測試

Module 1: 制定測試案例 - 功能性與非功能性

Module 2: 制定安全測試策略與計畫

Module 3: 分析測試結果的安全影響

Module 4: 安全錯誤的分級與追蹤

Module 5: 保護測試資料

Module 6: 確認與檢查測試

Module 7: 確認與檢查文件

第七章—部署、操作與維護安全軟體

Module 1: 整合與部署安全軟體

Module 2: 儲存與管理安全資料

Module 3: 安全軟體安裝

Module 4: 取得安全性維護授權

Module 5: 部署後之安全性測試

Module 6: 持續監控安全性

Module 7: 支援安全事故應變

Module 8: 修補與弱點管理

Module 9: 執行階段保護

Module 10: 持續營運

第八章—軟體安全供應鏈

Module 1: 安全供應鏈風險管理

Module 2: 分析第三方軟體安全

Module 3: 確保採購過程之供應商安全性要求

備註事項

1. 白天班之上課時間為09:00~18:00

2. 課程結束後，出席率達80%以上者，將獲頒發(ISC)<sup>2</sup>官方培訓證書

3. 報名本課程者，原報名班級開課日起一年內，可享有同一版本課程免費一次辦理重聽之機會

4. 通過考試後，欲申請CSSLP®認證必須符合(ISC)<sup>2</sup>相關規定

5. 精誠資訊恆逸教育訓練中心為PMI®認可之授權訓練教育中心，代號：3150。本課程符合PMI®國際專案管理學會PDU專業學分，需自行上網登錄

6. 課程優惠方案：

早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT\$45,000元

後續推薦課程

CISSP：CISSP資安系統專家認證課程

獨家課程 CISSP認證 PDU學分 此課程為「行政院國家資通安全會報」認可之資通安全專業證照

CISSP

## CISSP資安系統專家認證課程

Certified Information Systems Security Professional Course

時數：40小時 | 費用：56,000元 | 點數：14點 | 教材：(ISC)<sup>2</sup>原廠教材

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 適合對象   | 安全開發人員、網路系統工程師、資安分析人員、資安系統工程師、資訊部門主管、資訊長、資安顧問、欲取得CISSP <sup>®</sup> 認證資格者、欲從事資訊安全管理/顧問工作者                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |
| 預備知識   | 資訊安全通識體系八大領域任意兩個領域以上之相關基礎知識                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| 課程內容   | <div> <p><b>Domain 1—安全暨風險管理</b></p> <ol style="list-style-type: none"> <li>1. 認識與應用機密性、完整性及可用性</li> <li>2. 評估與應用安全治理原則</li> <li>3. 判斷遵循性要求</li> <li>4. 認識全球背景下的資訊安全法令、法規議題</li> <li>5. 認識、遵守與推廣職業道德</li> <li>6. 制定與執行資訊安全之政策、標準、程序及指引</li> <li>7. 識別、分析與區分持續營運要求</li> <li>8. 建立與強制人員安全政策與程序</li> <li>9. 認識與應用風險管理</li> <li>10. 認識與應用威脅模型</li> <li>11. 供應鏈風險管理</li> <li>12. 建立與維護資訊安全認知、教育與訓練</li> </ol> <p><b>Domain 2—資產安全</b></p> <ol style="list-style-type: none"> <li>1. 資訊與資產識別與分級</li> <li>2. 確認與管理資訊與資產擁有權</li> <li>3. 隱私防護</li> <li>4. 確保適當保存</li> <li>5. 決定資料管控措施</li> <li>6. 建立作業要求</li> </ol> <p><b>Domain 3—安全架構與工程</b></p> <ol style="list-style-type: none"> <li>1. 採安全設計原則建置與管理工程生命週期</li> <li>2. 認識安全模型</li> <li>3. 基於系統安全要求選擇控制措施</li> <li>4. 認識資訊系統安全能力</li> <li>5. 評估與減少安全性架構、設計與解決方案之弱點</li> <li>6. 評估與減少網站系統安全弱點</li> <li>7. 評估與減少行動系統安全弱點</li> <li>8. 評估與減少嵌入式裝置與連網系統安全弱點</li> <li>9. 應用密碼學</li> <li>10. 空間設計時應用安全原則</li> <li>11. 設計與建置設施安全</li> </ol> <p><b>Domain 4—通訊及網路安全</b></p> <ol style="list-style-type: none"> <li>1. 採安全原則設計網路架構</li> <li>2. 保護網路元件</li> <li>3. 基於設計建立安全通道</li> </ol> </div> <div> <p><b>Domain 5—識別暨存取控制</b></p> <ol style="list-style-type: none"> <li>1. 資產的實體及邏輯存取控制</li> <li>2. 管理人員與裝置的識別與鑑別</li> <li>3. 整合第三方識別服務</li> <li>4. 建置與管理授權機制</li> <li>5. 管理識別與存取供應生命週期</li> </ol> <p><b>Domain 6—安全性評估與測試</b></p> <ol style="list-style-type: none"> <li>1. 設計與驗證評估、測試與稽核策略</li> <li>2. 測試安全控制</li> <li>3. 收集安全流程資料</li> <li>4. 分析測試結果與產出報告</li> <li>5. 執行或協助安全稽核</li> </ol> <p><b>Domain 7—安全性作業</b></p> <ol style="list-style-type: none"> <li>1. 認識與支援調查過程</li> <li>2. 認識不同調查類型之要求</li> <li>3. 紀錄與監控</li> <li>4. 安全地供應資源</li> <li>5. 認識與應用安全性作業</li> <li>6. 使用資源防護技術</li> <li>7. 事故回應</li> <li>8. 偵測與預防性措施之操作與維護</li> <li>9. 建置與支援修補及弱點管理</li> <li>10. 參與及認識異動管理流程</li> <li>11. 建置復原策略</li> <li>12. 建置災難復原流程</li> <li>13. 測試災難復原計畫</li> <li>14. 參與營運持續計畫執行</li> <li>15. 建置與管理實體安全</li> <li>16. 解決人員安全與安全顧慮</li> </ol> <p><b>Domain 8—軟體開發安全性</b></p> <ol style="list-style-type: none"> <li>1. 認識與應用軟體開發生命週期安全性</li> <li>2. 落實開發環境安全控制措施</li> <li>3. 評估軟體安全果效</li> <li>4. 評估外購軟體安全</li> <li>5. 制定與應用安全開發指引與標準</li> </ol> </div> |  |
| 備註事項   | <ol style="list-style-type: none"> <li>1. 白天班之上課時間為09:00~18:00</li> <li>2. 課程結束後，出席率達80%以上者，將獲頒發(ISC)<sup>2</sup>官方培訓證書</li> <li>3. 報名本課程者，原報名班級開課日起一年內，可享有同一版本課程免費一次辦理重聽之機會</li> <li>4. 通過考試後，欲申請CISSP<sup>®</sup>認證必須符合(ISC)<sup>2</sup>相關規定</li> <li>5. 獨家贈送原廠CISSP 125題練習題，提供考前學習評估實力</li> <li>6. 精誠資訊恆逸教育訓練中心為PMI<sup>®</sup>認可之授權訓練教育中心，代號：3150。本課程符合PMI<sup>®</sup>國際專案管理學會PDU專業學分，需自行上網登錄</li> <li>7. 課程優惠方案：<br/>早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT\$50,400元</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |
| 後續推薦課程 | CEH：EC-Council CEH駭客技術專家認證課程                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |



CISSP-offtime

# CISSP資安系統專家認證課程-假日進修班

Certified Information Systems Security Professional Course

時數：40小時 | 費用：32,000元 | 點數：14點 | 教材：(ISC)<sup>2</sup>原廠教材



**適合對象** 安全開發人員、網路系統工程師、資安分析人員、資安系統工程師、資訊部門主管、資訊長、資安顧問、欲取得CISSP®認證資格者、欲從事資訊安全管理/顧問工作者

**預備知識** 資訊安全通識體系八大領域任意兩個領域以上之相關基礎知識

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 課程內容 | <p><b>Domain 1—安全暨風險管理</b></p> <ol style="list-style-type: none"> <li>1. 認識與應用機密性、完整性及可用性</li> <li>2. 評估與應用安全治理原則</li> <li>3. 判斷遵循性要求</li> <li>4. 認識全球背景下的資訊安全法令、法規議題</li> <li>5. 認識、遵守與推廣職業道德</li> <li>6. 制定與執行資訊安全之政策、標準、程序及指引</li> <li>7. 識別、分析與區分持續營運要求</li> <li>8. 建立與強制人員安全政策與程序</li> <li>9. 認識與應用風險管理</li> <li>10. 認識與應用威脅模型</li> <li>11. 供應鏈風險管理</li> <li>12. 建立與維護資訊安全認知、教育與訓練</li> </ol> <p><b>Domain 2—資產安全</b></p> <ol style="list-style-type: none"> <li>1. 資訊與資產識別與分級</li> <li>2. 確認與管理資訊與資產擁有權</li> <li>3. 隱私防護</li> <li>4. 確保適當保存</li> <li>5. 決定資料管控措施</li> <li>6. 建立作業要求</li> </ol> <p><b>Domain 3—安全架構與工程</b></p> <ol style="list-style-type: none"> <li>1. 採安全設計原則建置與管理工程生命週期</li> <li>2. 認識安全模型</li> <li>3. 基於系統安全要求選擇控制措施</li> <li>4. 認識資訊系統安全能力</li> <li>5. 評估與減少安全性架構、設計與解決方案之弱點</li> <li>6. 評估與減少網站系統安全弱點</li> <li>7. 評估與減少行動系統安全弱點</li> <li>8. 評估與減少嵌入式裝置與連網系統安全弱點</li> <li>9. 應用密碼學</li> <li>10. 空間設計時應用安全原則</li> <li>11. 設計與建置設施安全</li> </ol> <p><b>Domain 4—通訊及網路安全</b></p> <ol style="list-style-type: none"> <li>1. 採安全原則設計網路架構</li> <li>2. 保護網路元件</li> <li>3. 基於設計建立安全通道</li> </ol> | <p><b>Domain 5—識別暨存取控制</b></p> <ol style="list-style-type: none"> <li>1. 資產的實體及邏輯存取控制</li> <li>2. 管理人員與裝置的識別與鑑別</li> <li>3. 整合第三方識別服務</li> <li>4. 建置與管理授權機制</li> <li>5. 管理識別與存取供應生命週期</li> </ol> <p><b>Domain 6—安全性評估與測試</b></p> <ol style="list-style-type: none"> <li>1. 設計與驗證評估、測試與稽核策略</li> <li>2. 測試安全控制機制</li> <li>3. 收集安全流程資料</li> <li>4. 分析測試結果與產出報告</li> <li>5. 執行或協助安全稽核</li> </ol> <p><b>Domain 7—安全性作業</b></p> <ol style="list-style-type: none"> <li>1. 認識與支援調查過程</li> <li>2. 認識不同調查類型之要求</li> <li>3. 紀錄與監控</li> <li>4. 安全地供應資源</li> <li>5. 認識與應用安全性作業</li> <li>6. 使用資源防護技術</li> <li>7. 事故回應</li> <li>8. 偵測與預防性措施之操作與維護</li> <li>9. 建置與支援修補及弱點管理</li> <li>10. 參與及認識異動管理流程</li> <li>11. 建置復原策略</li> <li>12. 建置災難復原流程</li> <li>13. 測試災難復原計畫</li> <li>14. 參與營運持續計畫執行</li> <li>15. 建置與管理實體安全</li> <li>16. 解決人員安全與安全顧慮</li> </ol> <p><b>Domain 8—軟體開發安全性</b></p> <ol style="list-style-type: none"> <li>1. 認識與應用軟體開發生命週期安全性</li> <li>2. 落實開發環境安全控制措施</li> <li>3. 評估軟體安全果效</li> <li>4. 評估外購軟體安全</li> <li>5. 制定與應用安全開發指引與標準</li> </ol> |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 備註事項 | <ol style="list-style-type: none"> <li>1. 假日進修班贈送2天認證總複習(價值NT\$20,000元)</li> <li>2. CISSP舊生可以NT\$1,000元參加CISSP認證總複習課程</li> <li>3. 報名本優惠課程限開二聯式發票</li> <li>4. 白天班之上課時間為09:00~18:00</li> <li>5. 課程結束後，出席率達80%以上者，將獲頒發(ISC)<sup>2</sup>官方培訓證書</li> <li>6. 報名本課程者，原報名班級開課日起一年內，可享有同一版本課程免費一次辦理重聽之機會</li> <li>7. 通過考試後，欲申請CISSP®認證必須符合(ISC)<sup>2</sup>相關規定</li> <li>8. 獨家贈送原廠CISSP 125題練習題，提供考前學習評估實力</li> <li>9. 精誠資訊恆逸教育訓練中心為PMI®認可之授權訓練教育中心，代號：3150。本課程符合PMI®國際專案管理學會PDU專業學分，需自行上網登錄</li> </ol> |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**後續推薦課程** CEH：EC-Council CEH駭客技術專家認證課程

CCSP

## CCSP雲端資安專家認證課程

Certified Cloud Security Professional Course

時數：40小時 | 費用：50,000元 | 點數：12.5點 | 教材：(ISC)<sup>2</sup>原廠教材

## 適合對象

1. 對雲端安全有興趣者
2. 欲取得CCSP<sup>®</sup>認證者
3. 欲從事雲端暨資訊安全管理、顧問工作者
4. 資訊系統安全管理人員、系統工程師、系統/安全架構師、資安顧問、資安工程師、IT部門主管

## 預備知識

資訊、資安暨雲端安全基礎知識

## 課程內容

- 第一章—雲端之觀念、架構與設計
1. 認識雲端運算之觀念
  2. 說明雲端參考架構
  3. 認識雲端運算相關之安全觀念
  4. 認識安全雲端運算之設計原則
  5. 評估雲端服務供應商
- 第二章—雲端治理—法律、風險與遵循
1. 清楚地了解雲端環境中的法律要求與獨特風險
  2. 支援數位鑑識
  3. 認識隱私議題
  4. 認識稽核流程、方法及適應雲端環境
  5. 認識雲端對企業風險管理的影響
  6. 認識委外與雲端合約設計
- 第三章—雲端資料安全
1. 雲端資料安全觀念
  2. 設計與建置雲端資料儲存架構
  3. 設計與應用資料安全技術與策略
  4. 密碼學
  5. 認識與建置資料探索與分級技術
  6. 設計與建置資訊版權管理
  7. 規劃與建置資料保存、刪除與封存政策
  8. 設計與建置資料事件稽核、追蹤及責任
- 第四章—雲端平台及基礎設施安全
1. Module 1: 理解雲端基礎設施元件
  2. Module 2: 安全的雲端資料中心設計
  3. Module 3: 雲端基礎設施風險分析
  4. Module 4: 設計與規劃雲端實體與邏輯基礎設施之安全控制措施
  5. Module 5: 設計適合的身份與存取管理解決方案
  6. Module 6: 規劃災難復原及持續營運
- 第五章—雲端應用程式安全
1. 討論應用程式安全之訓練與認知
  2. 說明安全軟體開發生命週期流程
  3. 應用安全軟體開發生命週期流程
  4. 應用雲端軟體保證與驗證
  5. 使用驗證過之安全軟體
  6. 解釋明確之雲端應用程式架構
- 第六章—雲端安全作業
1. 操作與管理雲端環境之實體與邏輯基礎設施
  2. 建置可操作之控制措施與標準
  3. 相關單位之溝通管理
  4. 安全作業管理

## 備註事項

1. 白天班之上課時間為09:00~18:00
2. 課程結束後，出席率達80%以上者，將獲頒發(ISC)<sup>2</sup>官方培訓證書
3. 報名本課程者，原報名班級開課日起一年內，可享有同一版本課程免費一次辦理重聽之機會
4. 精誠資訊恆逸教育訓練中心為PMI<sup>®</sup>認可之授權訓練教育中心，代號：3150。本課程符合PMI<sup>®</sup>國際專案管理學會PDU專業學分，需自行上網登錄
5. 課程優惠方案：  
早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT\$45,000元

## 後續推薦課程

CEH：EC-Council CEH駭客技術專家認證課程