

ISC2系列資安認證與考試資訊介紹



ISC2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，ISC2獨家授權恆逸教育訓練中心為ISC2於台灣的教育聯盟機構，提供台灣資安人員與全球同步的ISC2資安認證教育訓練。ISC2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ISC2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ISC2資安系列認證的最佳選擇。



SSCP®資訊安全專業人員認證 System Security Certified Practitioner

SSCP®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®認證，代表應具備SSCP®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®資訊安全系統專家認證 Certified Information Systems Security Professional

CISSP®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®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®資訊安全軟體開發專家認證 Certified Secure Software Lifecycle Professional

ISC2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ISC2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®)，藉由取得CSSLP®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®雲端資安專家認證 Certified Cloud Security Professional

CCSP®認證是二大安全組織 - ISC2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於資訊及雲端安全的專業與能力，藉以此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	- 八個CISSP CBK範圍中具有二個或多個領域五年以上工作經驗 - 具備大學學位或持有ISC2認可之證書者，可抵免最多一年之工作經驗	- 八個CSSLP CBK範圍中具備至少一個領域滿四年工作經驗 - 具備大學學位或持有ISC2認可之證書者，可抵免最多一年之工作經驗	- 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 - 取得CSA CCSP認證者可抵免CCSP CBK範圍中一年工作經驗 - 取得CISSP認證者可抵免CCSP所有年資要求
工作經驗不足之報考者	可報考Associates of ISC2 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 ISC2 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 ISC2 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 ISC2 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	749美元	599美元	599美元
考試題目	從2025年10月1日起，SSCP將採電腦自適應測驗(CAT)的考試方式。考生將回答100-125題選擇題，考試時間為2小時。	從2025年10月1日起，CISSP將採電腦自適應測驗(CAT)的考試方式。考生將回答100-150題選擇題，考試時間為3小時。	考生將回答125題的選擇題測驗，考試時間3小時。	從2025年10月1日起，CCSP將採電腦自適應測驗(CAT)的考試方式。考生將回答100-150題選擇題，考試時間為3小時。
證書申請資格與流程	1. 通過考試。 2. 完成線上申請 https://apps.isc2.org/ 程序。須由ISC2或其會員背書。持ISC2有效證書者，皆為其會員。 3. ISC2將對應試者，抽樣執行稽核審核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135美元			
CPE (持續教育積分)	- SSCP可在三年內取得60分CPE，否則須重新參加考試。 - 每年至少需取得20分CPE，累積三年共60分CPE。	- CISSP可在三年內取得120分CPE，否則須重新參加考試。 - 每年至少需取得40分CPE，累積三年共120分CPE。	- CSSLP可在三年內取得90分CPE，否則須重新參加考試。 - 每年至少需取得30分CPE，累積三年共90分CPE。	- CCSP可在三年內取得90分CPE，否則須重新參加考試。 - 每年至少需取得30分CPE，累積三年共90分CPE。

註1：2024下半年CISSP簡體中文考試僅於2024年9/1-9/30、12/1-12/31開放報名考試。

註2：CCSP考試於2024年8月1日起調整為3小時125題。

註3：相關資訊ISC2視情況動態調整，考試資訊以官方最新公布為準。

請依據ISC2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>

欲了解更多CAT考試訊息，請參考：<https://www.isc2.org/certifications/computerized-adaptive-testing>

ISC2全系列費用將在2026年1月起調漲，詳細情形以官網公告為準



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：ISC2原廠電子教材



課程目標	對於有志從事資訊安全工作者，該如何為跨入資安領域並做好準備，是首先必須要面對的課題；對於在資安領域中默默耕耘的資安技術者而言，該如何證明自身的專業技術能力，更是一大課題；再者身為企業內的員工該如何與資訊技術同僚合力實施企業的資安政策，又是另一項考驗！SSCP®資安專業人員認證(Systems Security Certified Practitioner)是一張針對企業組織中負責網路及系統管理的相關人員，擁有資安技術能力且具實務經驗者所設立的證照。取得SSCP®認證，可確認受測者在資安技術領域中具有一定的專業實務能力。 有志於跨入資安領域、希望提升資安知識的資訊人員，取得相關證照是最快速的途徑之一；然而如何在取得證照之前為自己的專業技術能力做好準備，是值得深思的重要問題。現今大多資安相關證照無不與特定的產品相關連，欲取得該證照，受測者必須熟悉其產品進而參加認證考試取得證照。但除了證明受測者對特定產品有一定的熟悉程度外，其實對自身專業能力的展現，並無絕對助益。 精誠恆逸特別與SSCP®發照單位ISC2合作，引進ISC2官方SSCP CBK®研習班課程。課程中將針對企業資安實務所需SSCP®認證所測驗的七大領域進行介紹。對於有志於從事資安工作，以及希望提升資安知識的資訊科技工作者而言，本課程可以做為一窺資安領域的最佳途徑。本課程由ISC2認證講師帶領，以七大領域為主軸，介紹資安相關技術與觀念，為您從事資安相關工作做好準備。
適合對象	1. 對資訊安全工作有興趣者 2. 欲取得SSCP®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	1. 第一章 Introducing Security and Aligning Asset Management to Risk Management 介紹安全及符合風險管理之資產管理 2. 第二章 Understanding Risk Management Options and the Use of Access Controls to Protect Assets 認識管理風險之選項並使用存取控制保護資產 3. 第三章 Cryptography 密碼學 4. 第四章 Securing Software, Data and Endpoints 保護軟體、資料與端點 5. 第五章 Network and Communications Security 網路與通訊安全 6. 第六章 Cloud and Wireless Security 雲端與無線安全 7. 第七章 Incident Detection and Response 事故偵測與應變 8. 第八章 Maturing Risk Management 強化風險管理
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ISC2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，可享受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®認證必須符合ISC2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，享有早鳥恆逸銀卡優惠價 - 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 6. ISC2全系列將於2026年1月調漲，詳細資訊以官網公告為準
後續推薦課程	CISSP：CISSP資安系統專家認證課程



此課程為「數位發展部資通安全署」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：ISC2原廠電子教材

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。

Domain 1—安全軟體概念

- L1.1 定義軟體開發的核心安全目標
- L1.2 描述資訊安全三要素並解釋資訊機密性、完整性和可用性的主要機制
- L1.3 描述資訊安全與資料隱私之間的關係
- L1.4 辨識影響軟體安全的監管考量
- L1.5 解釋安全方法如何透過存取控制減輕弱點
- L1.6 描述軟體安全中多層保護的目的和功能
- L1.7 描述安全文化和實踐如何影響資料隱私和安全

Domain 2—安全軟體生命週期管理

- L2.1 探討軟體開發的預測性和適應性方法中的安全性
- L2.2 描述將軟體安全實踐納入軟體開發生命週期過程中
- L2.3 辨識DevOps和DevSecOps
- L2.4 認識安全性組態標準和基準
- L2.5 描述以安全為重點的組態管理過程
- L2.6 確定軟體弱點和漏洞的安全標準
- L2.7 解釋OWASP的軟體保證成熟模型和建立安全性成熟模型
- L2.8 在DevSecOps管道中定義軟體安全里程碑和檢查點
- L2.9 解釋系統安全計畫
- L2.10 辨識與安全相關的文件
- L2.11 辨識軟體開發中的指標
- L2.12 詳細說明軟體停用政策和流程
- L2.13 解釋DevSecOps中的安全性報告機制
- L2.14 描述風險評估和風險管理
- L2.15 審查安全運作流程的實施
- L2.16 辨識容器生命週期中的安全考慮

Domain 3—安全軟體需求

- L3.1 描述需求管理以及軟體安全需求的來源
- L3.2 辨識功能性和非功能性需求
- L3.3 解釋SCRUM/SCRUM相似方法中以安全為重的故事的影响
- L3.4 描述軟體安全需求的來源
- L3.5 分析安全政策及其支援元素作為內部安全需求的來源
- L3.6 解釋遵循要求，並辨識法律、法規和行業標準作為外部安全需求的來源
- L3.7 討論安全標準和架構
- L3.8 描述資料治理和所有權
- L3.9 描述資料分類以及安全標籤和標記
- L3.10 辨識結構化和非結構化的資料類型
- L3.11 描述資料生命週期
- L3.12 辨識旨在減輕隱私風險的隱私法律和法規
- L3.13 討論資料匿名化並列舉各種匿名化方法
- L3.14 在隱私情境中解釋使用者同意、資料保留和資料處理
- L3.15 辨識跨境資料轉移的影響以及個人資料轉移的限制
- L3.16 描述使用者和軟體資料存取規定
- L3.17 描述誤用和濫用案例以及它們與已知攻擊模式的相關性
- L3.18 描述安全需求追蹤矩陣
- L3.19 辨識第三方供應商的安生性需求

Domain 4—安全軟體架構和設計

- L4.1 描述架構和相關的安全設計模式
- L4.2 辨識介面設計的安全性標準
- L4.3 比較並區分各種身分驗證和授權機制
- L4.4 描述憑證管理
- L4.5 辨識網路安全中使用的原則和工具
- L4.6 描述維護資料庫安全性的方法
- L4.7 辨識威脅建模的過程、工具和方法
- L4.8 指出可攻擊面評估和管理的過程
- L4.9 討論威脅情報和網絡威脅資訊的來源
- L4.10 描述架構風險評估的過程
- L4.11 辨識非功能性安全性特性和限制
- L4.12 辨識安全操作架構的考量

Domain 5—安全軟體建置

- L5.1 辨識安全編碼標準的特點
- L5.2 描述在受控應用程式中建置安全性的不同方法
- L5.3 辨識軟體中的常見缺陷以及相應的緩解策略
- L5.4 解釋常見的安全開發實踐
- L5.5 辨識在傳輸中和儲存中的資料保護方法
- L5.6 辨識列在最常見弱點清單和資料庫中的軟體弱點
- L5.7 描述軟體保證工具的功能和方法
- L5.8 描述按類型和功能對控制的分類
- L5.9 辨識防止常見網路應用程式弱點的控制措施
- L5.10 描述制定包括軟體風險考量的安全策略的過程
- L5.11 辨識使用第三方和開源組件和庫時相關的風險
- L5.12 描述各種整合類別及其對軟體安全性的相關性
- L5.13 描述建構自動化過程
- L5.14 解釋軟體保證中使用的技術

Domain 6—安全軟體測試

- L6.1 辨識常見的安全測試技術
 - L6.2 描述測試環境
 - L6.3 辨識組織的軟體安全標準和指南
 - L6.4 解釋群眾外包安全性和獎金計劃的好處
 - L6.5 辨識安全測試的指南
 - L6.6 辨識各種安全性測試案例
 - L6.7 認識建立誤用和濫用案例的重要性
 - L6.8 描述文件驗證和驗證
 - L6.9 解釋OWASP的應用程式安全驗證標準的結構和目標
 - L6.10 描述未記錄的功能和原始碼
 - L6.11 解釋測試結果的安全性影響
 - L6.12 區分測試結果的類型
 - L6.13 描述追蹤安全性缺陷的過程
 - L6.14 解釋風險評分系統和常見弱點評分系統
 - L6.15 解釋測試數據的生成以及使用生產數據的後果
 - L6.16 描述驗證和驗證測試的過程
- Domain 7—安全軟體部署、運營、維護**
- L7.1 在ISO 31000系列的背景下描述操作風險分析
 - L7.2 描述安全配置管理(SecCM)
 - L7.3 辨識安全持續整合和持續交付管道的元素
 - L7.4 解釋應用程式安全工具鏈
 - L7.5 辨識識別應用程式弱點的步驟
 - L7.6 比較和區分常見的存儲和管理安全資料的方法
 - L7.7 描述安全的安裝過程和方法
 - L7.8 解釋安全的軟體啟動機制
 - L7.9 辨識運營授權(ATO)過程中的步驟和方法
 - L7.10 解釋如何執行資訊安全持續監控
 - L7.11 描述涉及事件應對計劃的階段
 - L7.12 將修補管理過程與整體軟體安全實踐相關聯
 - L7.13 描述用於弱點管理的方法和工具
 - L7.14 描述控制如何在執行階段以控制措施保護應用程式
 - L7.15 比較和區分業務持續性和災害復原計劃如何支援作業的連續性
 - L7.16 解釋並區分服務水準協議 (SLA)、服務水準目標 (SLO) 和服務水準指標 (SLI)，以實現供應商的持續性

Domain 8—安全軟體供應鏈

- L8.1 描述軟體供應鏈
- L8.2 審查軟體供應鏈風險管理的過程
- L8.3 解釋與第三方軟體相關的安全風險
- L8.4 將風險與點對點應用程式和文件共享相關聯
- L8.5 解釋程式碼儲存庫和環境安全
- L8.6 表達具有密碼學雜湊和數位簽章的元件
- L8.7 辨識軟體取得中的安全需求和原則
- L8.8 詳細說明軟體取得的關鍵考慮因素
- L8.9 解釋軟體取得的合約要求

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ISC2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ISC2相關規定
5. 精誠資訊恆逸教育訓練中心為PMI®認可之授權教育訓練中心，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，享有早鳥恆逸銀卡優惠價
7. ISC2全系列將於2026年1月調漲，詳細資訊以官網公告為準

後續推薦課程

CISSP：CISSP資安系統專家認證課程



此課程為「數位發展部資通安全署」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：ISC2原廠電子教材



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	Domain 1—安全與風險管理 1.1 理解、遵守並促進專業倫理 1.2 理解並應用安全概念 1.3 評估、應用並維持安全治理原則 1.4 全面理解與資訊安全相關的法律、法規和合規問題 1.5 理解調查類型的要求 1.6 制定、文件化並實施安全政策、標準、程序和指南 1.7 識別、分析、評估、優先排序並實施營運連續性 (BC) 要求 1.8 貢獻並執行人員安全政策和程序 1.9 理解並應用風險管理概念 1.10 理解並應用威脅建模概念和方法 1.11 應用供應鏈風險管理 (SCRM) 概念 1.12 建立和維護安全意識、教育和培訓計畫 Domain 2—資產安全 2.1 確定並分類資訊和資產 2.2 建立資訊和資產處理需求 2.3 安全提供資源 2.4 管理資料生命週期 2.5 確保適當的資產保留 2.6 確定資料安全控制和合規需求 Domain 3—安全架構與工程 3.1 研究、實施和管理使用安全設計原則的工程流程 3.2 理解安全模型的基本概念 3.3 根據系統安全要求選擇控制 3.4 了解資訊系統的安全功能 3.5 評估和減輕安全架構、設計和解決方案元素的漏洞 3.6 選擇和確定加密解決方案 3.7 了解加密攻擊的方法 3.8 將安全原則應用於場地和設施設計 3.9 設計場地和設施安全控制 3.10 管理資訊系統的生命週期 Domain 4—通訊與網路安全 4.1 在網路架構中應用安全設計原則 4.2 保護網路元件安全 4.3 根據設計實施安全通訊通道 Domain 5—識別與存取管理 5.1 控制對資產的實體和邏輯存取 5.2 設計身份識別和驗證策略 5.3 使用第三方服務實現聯邦式身份 5.4 實施和管理授權機制 5.5 管理身份和存取提供生命週期 5.6 實施身份驗證系統 Domain 6—安全評估測試 6.1 設計並驗證評估、測試和稽核策略 6.2 進行安全控制測試 6.3 收集安全流程資料 6.4 分析測試輸出並產生報告 6.5 進行或促進安全稽核 Domain 7—安全作業 7.1 理解並遵守調查程序 7.2 執行日誌記錄和監控活動 7.3 進行組態管理 7.4 應用基礎安全作業概念 7.5 應用資源保護 7.6 進行事故管理 7.7 操作和維護偵測和預防措施 7.8 實施和支援修補和漏洞管理 7.9 了解並參與變更管理流程 7.10 實施復原策略 7.11 實施災害復原流程 7.12 測試災害復原計畫 7.13 參與營運持續性規劃和演練 7.14 實施和管理實體安全 7.15 解決人員安全 and 安全擔憂 Domain 8—軟體開發安全 8.1 了解並在軟體開發生命週期中整合安全性 8.2 識別並應用軟體開發生態系統中的安全控制 8.3 評估軟體安全性的有效性 8.4 評估所獲得軟體的安全影響 8.5 定義並應用安全程式撰寫準則和標準	
備註事項	1. 白天班之上課時間為09:00~18:00 2. 贈送2天認證總複習(價值NT\$20,000) 3. 可以優惠價NT\$26,900報名CISSP考前衝刺課程(含一張USD 749考試卷) 4. 課程結束後，出席率達80%以上者，將獲頒發ISC2官方培訓證書 5. 報名本課程者，原報名班級開課日起一年內，可享受有同一版本課程免費一次辦理重聽之機會 6. 考試費用USD 749元，通過考試後，欲申請CISSP®認證必須符合ISC2相關規定 7. 獨家贈送原廠CISSP 125題練習題，提供考前學習評估實力 8. 精誠資訊恆逸教育訓練中心為PMI®認可之授權教育訓練中心，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 9. 課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥恆逸銀卡優惠價 10. ISC2全系列將於2026年1月調漲，詳細資訊以官網公告為準	
後續推薦課程	CCISO：EC-Council CCISO資安長課程	



獨家課程



CISSP認證



PDU學分



此課程為「數位發展部資通安全署」認可之資通安全專業證照

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：ISC2原廠電子教材



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

Domain 1—安全與風險管理

- 1.1 理解、遵守並促進專業倫理
- 1.2 理解並應用安全概念
- 1.3 評估、應用並維持安全治理原則
- 1.4 全面理解與資訊安全相關的法律、法規和合規問題
- 1.5 理解調查類型的要求
- 1.6 制定、文件化並實施安全政策、標準、程序和指南
- 1.7 識別、分析、評估、優先排序並實施營運連續性(BC)要求
- 1.8 貢獻並執行人員安全政策和程序
- 1.9 理解並應用風險管理概念
- 1.10 理解並應用威脅建模概念和方法
- 1.11 應用供應鏈風險管理(SCRM)概念
- 1.12 建立和維護安全意識、教育和培訓計畫

Domain 2—資產安全

- 2.1 確定並分類資訊和資產
- 2.2 建立資訊和資產處理需求
- 2.3 安全提供資源
- 2.4 管理資料生命週期
- 2.5 確保適當的資產保留
- 2.6 確定資料安全控制和合規需求

Domain 3—安全架構與工程

- 3.1 研究、實施和管理使用安全設計原則的工程流程
- 3.2 理解安全模型的基本概念
- 3.3 根據系統安全要求選擇控制
- 3.4 了解資訊系統的安全功能
- 3.5 評估和減輕安全架構、設計和解決方案元素的漏洞
- 3.6 選擇和確定加密解決方案
- 3.7 了解加密攻擊的方法
- 3.8 將安全原則應用於場地和設施設計
- 3.9 設計場地和設施安全控制
- 3.10 管理資訊系統的生命週期

Domain 4—通訊與網路安全

- 4.1 在網路架構中應用安全設計原則
- 4.2 保護網路元件安全
- 4.3 根據設計實施安全通訊通道

Domain 5—識別與存取管理

- 5.1 控制對資產的實體和邏輯存取
- 5.2 設計身份識別和驗證策略
- 5.3 使用第三方服務實現聯邦式身份
- 5.4 實施和管理授權機制
- 5.5 管理身份和存取提供生命週期
- 5.6 實施身份驗證系統

Domain 6—安全評估測試

- 6.1 設計並驗證評估、測試和稽核策略
- 6.2 進行安全控制測試
- 6.3 收集安全流程資料
- 6.4 分析測試輸出並產生報告
- 6.5 進行或促進安全稽核

Domain 7—安全作業

- 7.1 理解並遵守調查程序
- 7.2 執行日誌記錄和監控活動
- 7.3 進行組態管理
- 7.4 應用基礎安全作業概念
- 7.5 應用資源保護
- 7.6 進行事故管理
- 7.7 操作和維護偵測和預防措施
- 7.8 實施和支援修補和漏洞管理
- 7.9 了解並參與變更管理流程
- 7.10 實施復原策略
- 7.11 實施災害復原流程
- 7.12 測試災害復原計畫
- 7.13 參與營運持續性規劃和演練
- 7.14 實施和管理實體安全
- 7.15 解決人員安全和安全擔憂

Domain 8—軟體開發安全

- 8.1 了解並在軟體開發生命週期中整合安全性
- 8.2 識別並應用軟體開發生態系統中的安全控制
- 8.3 評估軟體安全性的有效性
- 8.4 評估所獲得軟體的安全影響
- 8.5 定義並應用安全程式撰寫準則和標準

備註事項

1. 贈送2天認證總複習(價值NT\$20,000)
2. 可以優惠價NT\$26,900報名CISSP考前衝刺課程(含一張USD 749考試卷)
3. 報名本優惠假日班課程限定開立個人(二聯式)發票，不予開立公司統編(三聯式)發票
4. 白天班之上課時間為09:00~18:00
5. 課程結束後，出席率達80%以上者，將獲頒發ISC2官方培訓證書
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
7. 考試費用USD 749，通過考試後，欲申請CISSP®認證必須符合ISC2相關規定
8. 獨家贈送原廠CISSP 125題練習題，提供考前學習評估實力
9. 精誠資訊恆逸教育訓練中心為PMI®認可之授權教育訓練中心，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
10. ISC2全系列將於2026年1月調漲，詳細資訊以官網公告為準

後續推薦課程 CCISO：EC-Council CCISO資安長課程

CPexam

CISSP考前衝刺課程

CISSP Pre-exam Course

時數：7小時 | 費用：26,900元 | 點數：不適用 | 教材：學員課前自備，紙本或數位版本皆可



ISC2 CISSP Certified Information Systems Security Professional Official Practice Tests, 3rd Edition

課程目標

1. 檢測學員對於CISSP核心知識的掌握程度
2. 強化對CISSP各領域的整合性理解及應用能力
3. 訓練考試節奏與時間管理
4. 提供針對關鍵題目的深入解析，鞏固或導正觀念及訓練解題思考策略
5. 提升學員的臨場應變能力與應試信心

適合對象

1. 已完成 CISSP 8 大領域學習並即將參加考試的學員
2. 需要進一步提升解題策略的學員

預備知識

1. 完成CISSP 8大領域的系統化複習
2. 了解CISSP的考試型式

課程內容

1. 模擬考試：125題CISSP模擬考，上課前請學員自備電子書或紙本(ISC2 CISSP Certified Information Systems Security Professional Official Practice Tests 3rd ed.)，上課時請學員使用自己的電子書或紙本聽課，不另外印出紙本
2. 模擬考時間：考試時間3小時，上午9:00~12:00，講師宣布模擬考題組編號(125綜合題庫)，學員看自己的電子書或紙本題目，作答於答案紙
3. 題目解析：下午1:00~5:00，4小時重點模擬考題講解，複習模擬考題出現的重點知識點，解析常見錯誤及正確思維方式

備註事項

1. 本課程含一張USD 749的CISSP考試卷
2. 本課程限報名恆逸CISSP課程者參加

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：ISC2原廠電子教材



適合對象

1. 對雲端安全有興趣者
2. 欲取得CCSP®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

- Domain 1 —雲端概念、架構與設計**
- 1.1 理解雲端運算概念
 - 1.2 描述雲端參考架構
 - 1.3 了解與雲端運算相關的安全性概念
 - 1.4 理解安全雲端運算的設計原則
 - 1.5 評估雲端服務提供商
- Domain 2 —雲端資料安全**
- 2.1 描述雲端資料概念
 - 2.2 設計並實施雲端資料儲存架構
 - 2.3 設計並應用資料安全技術和策略
 - 2.4 實施資料發現
 - 2.5 計畫並實施資料分類
 - 2.6 設計並實施資訊權利管理 (IRM)
 - 2.7 計畫並實施資料保留、刪除和封存政策
 - 2.8 設計並實施資料的可稽核性、可追蹤性和負責任性
- Domain 3 —雲端平台與基礎設施安全**
- 3.1 了解雲端基礎設施和平台元件
 - 3.2 設計一個安全的資料中心
 - 3.3 分析與雲端基礎設施和平台相關的風險
 - 3.4 計畫並實施安全控制
 - 3.5 企業持續性與災害復原的規劃與實施
- Domain 4 —雲端應用程式安全**
- 4.1 倡導應用程式安全的培訓和意識
 - 4.2 描述安全軟體開發生命週期
 - 4.3 運用安全軟體開發生命週期
 - 4.4 運用雲端軟體保證和驗證
 - 4.5 使用已驗證的安全軟體
 - 4.6 了解雲端應用程式架構的特點
 - 4.7 設計適當的身份和存取管理解決方案
- Domain 5 —雲端安全作業**
- 5.1 建置並實施雲端環境的實體和邏輯基礎設施
 - 5.2 運作和維護雲端環境的實體和邏輯基礎設施
 - 5.3 實施作業控制措施和標準
 - 5.4 支援數位鑑識
 - 5.5 管理與相關方的溝通
 - 5.6 管理安全作業
- Domain 6 —法律、風險和遵循性**
- 6.1 闡述雲端環境中的法律要求和特殊風險
 - 6.2 了解隱私議題
 - 6.3 了解稽核過程、方法論和所需的調整
 - 6.4 了解雲端對企業風險管理的影響
 - 6.5 了解外包和雲端合約設計

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ISC2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®認可之授權教育訓練中心，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
5. 課程優惠方案：
早鳥優惠價：開課前2周完成報名繳費，享有早鳥恆逸銀卡優惠價
6. ISC2全系列將於2026年1月調漲，詳細資訊以官網公告為準

後續推薦課程

CEH：EC-Council CEH駭客技術專家認證課程