

2023 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



--CISA 專區--

◆黃景偉 (2023 年 1~6 月 CISA EXAM PASSERS NO.1、
2023 年 7~12 月 CRISC EXAM PASSERS NO.2)

ISACA 的相關認證考試，具有相當水準，且國際知名度高，很推薦想要從事資安領域的人可以準備相關認證。

本身從事 IT/資安領域十餘年，不論在資安維運、制度推行與稽核皆有相關經歷，然而在取得 ISACA 考試認證之前，總覺得不是很能夠精確的掌握一些資安的核心精神，在某次尋找資安解決方案當中，無意間從網路上看到了 ISACA 一系列的認證，從電腦稽核(CISA)、資安治理與管理(CISM)、風險管理(CRISC)、個資保護(CDPSE)皆有完整知識體系與認證，因此下定決心要好好精進自己，並開始準備一系列的自我進修與證照考取。起初從最一開始的 CISA 開始進行，在考試準備方面，購買了原廠的教材與 QAE，這是準備考試過程中很重要的素材，特別是原廠的 QAE 一定要買來做，每一題的練習題中都有很清楚的解釋，這對考試幫助很大，學習的階段也輔以 Udemy 上的課程來幫助準備考試，準備 CISA 的過程中也參加了電腦稽核協會的考題講解線上課程，透過不斷的淬鍊，讓自己能夠更加清楚的掌握其核心精神與觀念。

資安的領域相當廣泛，在通過 CISA 的認證之後，覺得似乎還是有所不足，想要在資安領域擁有更紮實的知識，因此決定繼續往下扎根 CISM、CRISC、CDPSE 等資安各面向領域，透過這個學習與考證照的過程，真的讓自己成長了很多，讓過往很多不清楚的觀念更加的清晰，這對實務上推動資訊安全真的有很大的幫助。

在考題方面，個人覺得難易度算是中等偏高，如果沒有紮實準備，基本上不可能通過，算是相當具有鑑別度與水準的考試，也正因如此，才具備其價值，不過與此同時，考試準備過程也會相當辛苦，依照科目與個人專業背景不同，準備期間可能會需要兩個月至半年不等，是一項滿具挑戰的任務。

最後，真的鼓勵想要在資安領域深耕的人，可以準備這一系列的證照考試，透過準備證照的學習過程，可以很好的拓展自己的視野，對齊國際觀點，並學習到正確觀念，讓自己朝向專家領域邁進。

2023 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



--CISA 專區--

◆李信成 (2023 年 1~6 月 CISA EXAM PASSERS NO.2)

個人在非營利組織擔任內部稽核，資訊安全是日益重要的議題，此前僅有粗淺的 IT 基礎架構及資安稽核概念，為了自我提升專業能力以善盡職責，在多方蒐集參考先進們分享的資訊後，決定報考 CISA 認證考試。

回顧備考歷程，以下幾項對我幫助最大，在此與大家分享：

1.擬定適合自己的學習計畫

年齡來到 50 以後，記憶力和專注力是不得不列入優先考量的弱項，長期抗戰式的備考，看似時間較充裕，實則容易學後忘前，故規劃以半年的時間，每天用 1 小時準備。對於複雜、相關或容易混淆的觀念，我會自己整理圖表或對照表，一方面幫助知識理解、內化，一方面也便於考前快速複習。

2.選用可信、有效的教材和工具

協會的認證研習課程、考前模擬題講解、ISACA 官方教材和線上練習題庫，幫助我正確、有效的理解、掌握考試重點及自己應試時容易發生的錯誤態樣，例如：題幹沒看清楚、專有名詞搞混、精神不濟致誤判或選錯…等；而官方線上題庫可以隨時運用零碎時間練習，並衡量自己準備程度，是極力推薦的備考利器。

3.最最重要的是先報名繳費

以終為始，合理有彈性的備考計畫仍需要開始付諸執行，繳了錢有了明確的時間，可強化備考過程每天的時間規劃與專注的投入。

通過考試是過程，持續學習才是目的，祝大家不只順利拿下證照，也在專業路上越走越穩，收穫更多信心並增加專業價值！

◆曾國恭 (2023 年 7~12 月 CISA EXAM PASSERS NO.1)

起初會備考 CISA 與 CISM 是為了轉職稽核員而準備的，由於是 2 年前考的，準備過程我也忘的差不多了。以下我只說明兩張證照對我工作上的幫助。CISA 認證為 ISO 27001 稽核員提供了專業的稽核方法論和技術，提升稽核過程的效率和有效性。其知識體系強調結構化的稽核流程，從稽核規劃到證據收集和評估，使稽核員能夠系統地評估組織的資訊安全控制，能夠更精準地識別控制中的不足與改進機會，並根據業務風險提供針對性建議。

而 CISM 著重於資訊安全治理、風險管理、方案開發與事件管理，例如：在 ISO 27001 本文關於領導力的可以評估其有效性，確保組織資安與業務策略一致，亦可檢視組織風險評估與處理流程，判斷其與業務目標的契合度及資安管理系統(ISMS)的整體成熟度及實施效果，以及組織資安事件應對計畫的有效性與實用性。

以上是這兩張證照對我在稽核工作上的幫助，謝謝！

2023 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



--CISA 專區--

◆王志華 (2023 年 7~12 月 CISA EXAM PASSERS NO.2)

備考經驗：

自己沒有上課，是經由 Udemy 查找相關的課程，加上官方的書籍來準備，之後再上網找相關的考古題參考，並且比對每一個章節相關著重的重點研讀。

考試心得：

因為是遠端考試，一定要先閱讀好官方相關的規定，如果您是中文愛好者，請一定要知道部份單字，因為監考官會請你拿著筆電檢查考試空間(乾淨的桌面和沒有其它 3C 用品的房間)是否符合要求，在答題時一定要記得人為本，才能執行相關資安業務，祝各位考試順利。

◆莊沛晨 (2023 年 7~12 月 CISA EXAM PASSERS NO.3)

考試不只考知識，更重視資訊安全管理的決策與判斷能力。題目多為情境題，需從管理者角度思考風險、治理、事件處理等策略。建議應熟讀 ISACA 官方教材與考題解析，並站在管理者的高度、以風險導向的思維去推斷最合適的答案，實務經驗與邏輯推理能力是通過考試的關鍵。

--CISM 專區--

◆蔡赫豪 (2023 年 1~6 月 CISM EXAM PASSERS NO.2)

CISM 考試著重實務經驗與管理思維，四大領域需理解資訊安全治理、風險管理、計畫建立及事件應變。準備期間建議使用官方題庫反覆練習，理解題意與實務經驗結合有助於快速掌握情境題，考試時間充足但題目較長，需穩定心態作答。

◆薛勇州 (2023 年 7~12 月 CISM EXAM PASSERS NO.1)

卡先刷下去，就踏出第一步，參加訓練課程，利用零碎時間，練習考古題，水到渠成，通過拿證。

2023 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



--CISM 專區--

◆張廣燦 (2023 年 7~12 月 CISM EXAM PASSERS NO.2)

CISM 考證歷程：資安管理思維的轉變

在通過 CISSP 後，便決定報考 CISM。為快速建立觀念並善用之前累積的學習經驗，先是閱讀 Mike Chapple 的《CISM Study Guide》，再搭配 ISACA 官方線上題庫進行深入練習。具備 CISSP 基礎確實有很大的幫助，但 CISM 的核心更看重理解與權衡。它不只看技術細節，也不會盲目追求資安的絕對防護，而是要求我們以達成組織目標和考量成本效益為核心來進行決策。

準備過程中，一些觀念特別令人印象深刻，例如：「一味禁止不如有效管理」的實務思維；「緊急變更後文件可後補」的彈性；還有在某些情境下，「合規性也需權衡高昂成本」的務實考量。這趟學習旅程，讓資安治理與管理的理解更為全面且貼近實務。

◆辜麟傑 (2023 年 7~12 月 CISM EXAM PASSERS NO.3)

很高興能在 2023 年的 CISM 考試中取得前三名。準備的過程讓我深刻體會到，CISM 考試最重視的是管理層級的思維與決策能力，準備時要培養站在管理者角度思考問題的習慣。考試著重於思路與心態，而不是技術細節，建議考生將重點放在理解流程與策略上。CISM 課程內容實用，對未來想從事資安管理的人來說，是建立全方位知識的好機會。準備時，建議每天撥出固定的時間專心準備，持之以恆才能有效吸收知識。上完課後，建議先評估自己對內容的掌握度，再預估所需準備時間，並直接預約考試，這一點對邊工作邊準備考試的朋友尤其重要，因為在忙碌的生活中，提前規劃與設定明確目標，能更有效利用有限的時間，也能避免拖延，讓準備過程更有動力。另外也推薦大家直接選擇英文版考試，以避免因兩岸用語差異和簡中翻譯落差產生的困擾。幾個小技巧分享給大家，首先，課本教材不需死記硬背，而是要理解背後的邏輯和原理，這樣才能靈活應對不同情境的題目。課本中的題目建議反覆練習，做完後若覺得不夠，可以購買官方練習題，或上網、去圖書館找更多資源練習。遇到問題時，隨時向老師、學長姐請教或上網搜尋資料，善用網路資源，如：YouTube 上的 CISM 學習影片就很多，可以幫助釐清觀念。但提醒考生，網路上的練習資源有些解答可能是錯誤的，建議考生要有自己的判斷能力，不要只背正確答案，而是要理解每個選項背後的原因。最後，雖然成功考取證照很開心，但千萬不可因此自滿，因為威脅、科技與思維都在不斷的演進。取得證照只能證明你具備了這些知識和思維，但不斷的學習與進步，才是真正專業的資安人員應該具備的心態，希望這些心得與建議，能对大家有所幫助！共勉之。



--CRISC 專區--

◆沈政佑 (2023 年 7~12 月 CRISC EXAM PASSERS NO.1)

很幸運能夠在自修的情況下，順利地通過測驗並取得證照。個人覺得 ISACA 的試題中，常會出現許多看似相近，但選項或問法不同的問題，準備時不必過度死記課本細節，因為同一題目會以類似的形式出現在考試中，且因扮演的角色不同，答案也可能完全不同。建議有意應試者多花時間理解練習題背後的管理意涵，以及各選項的深層含義。我將準備過程分為三階段，供有意應試者參考：

1.報名階段

先確定考試日期並購買考試卷，避免拖延。建議選擇準備期不超過六個月的考試時間，並確定後不輕易更改。

2.準備階段

建議使用 ISACA 官方教材，名詞與答案較準確。平日每天投入約 1 小時，假日 1.5 小時，循環學習 2 至 3 輪。先快速瀏覽手冊，再做題確認理解，記錄並深入釐清錯題，採用 PDCA 持續改進，且避免外務干擾影響學習效果。

3.考試階段

考前加強複習錯誤率較高的領域，理解題目背後的管理意涵並以題目中的角色帶入思考。正式考試時，可以中間出去喝水，若覺得思緒有點抽離，可先出去透個氣再繼續作答。最後，祝有意應試者能順利取得認證。