

## 2024 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



### --CISA 專區--

#### ◆陳冠宇 (2024 年 1~6 月 CISA EXAM PASSERS NO.2)

先建立五大領域的觀念，再透過大量練習題熟悉 ISACA 的出題邏輯，並整理錯題反覆複習。我認為 CISA 最大的挑戰不是英文，而是思維的轉換。身為工程師，我們習慣直接解決技術問題；但 CISA 更重視風險評估、內部控制、治理流程及管理決策，因此答題時必須從「最佳控制措施」而非「最快技術解法」的角度思考。

取得 CISA 後，我最大的收穫是能以資訊治理與風險管理的觀點檢視工作，不論是防火牆、WAF、或資安專案，都能兼顧技術、法遵與業務需求。建議準備 CISA 的同仁，重視觀念理解、多做題並分析錯誤原因，而非死背答案，才能真正掌握 ISACA 的思維並順利通過考試。

#### ◆張嘉宏 (2024 年 1~6 月 CISA EXAM PASSERS NO.3)

榮獲 2024 年度 CISA 考試第三名，心中充滿了對上帝的感恩與讚美，這份榮耀完全是神的恩典與帶領。

坦白說，我過去並非傳統定義上的考場學霸，甚至不認為自己擅長應付這類高難度的國際證照考試。然而這一次的成果，不僅打破了我對自己的既定框架，更讓我深刻體會到：正確的策略與不懈的堅持，能引領我們突破原有的極限。

在這 5 個月的備考歷程中，時間分配與讀書策略是成功的關鍵。因為平時必須兼顧白天的工作，我採取定時定量的策略，堅持每天晚上抽出 3 小時全力投入讀書。

我的核心備考技巧是「以題為綱」。正因為自知需要更有效率的學習方式，我沒有盲目從頭硬啃厚重的官方教材，而是先以官方練習題（QAE）替自己進行弱點掃描。找出自己的思維盲點與不熟悉的知識點，再帶著這些問題，回頭翻閱官方教材做深度的理解與加強。這樣做不僅能精準抓到 ISACA 的出題邏輯與審計師思維，更能大幅提升夜讀的效率。

感謝主在每個挑燈夜讀的晚上賜予我恆心、體力與智慧。這張證照是專業深耕的新起點，也希望我的這段心路歷程，能帶給正在備考的夥伴們一些信心與實質的幫助！

# 2024 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



## --CISA 專區--

### ◆曾詩韻 (2024 年 7~12 月 CISA EXAM PASSERS NO.1、 2024 年 7~12 月 CISM EXAM PASSERS NO.3)

首先要擬定符合自己實際情況的學習計劃，定好自己可以實現的學習目標。建議每天都安排時間去學習，哪怕是做幾道題也好，給自己身心建立好學習的習慣。

在學習方面，要掌握課程領域架構，建立完整觀念。遇到不太懂的知識點我會搭配 google 搜尋跟 chatgpt 去理解，並查看相關的實務案例。我有訂閱 ISACA 官方版試題去練習，練習時重點在理解題目意圖，理解解析而非死背答案。答題時要把自己的思維融入管理層級與實務經驗之中，培養資安策略抉擇的思維。同時整理錯題、熟悉高頻考點，並透過模擬考練習時間分配，提升應試能力與答題正確率。

考試當天保持冷靜，遇到不確定的問題不要慌，按照自己平時答題的思維一步步去解析即可。祝大家考試順利！

### ◆洪玉珊 (2024 年 7~12 月 CISA EXAM PASSERS NO.3)

#### 一、建立完整知識架構

準備初期，我以 ISACA 官方教材為主，先掌握各領域的核心概念、角色責任與控制目標，再將教材內容與實務經驗相互對照，理解不同控制措施背後所要處理的風險。

#### 二、重視題目背後的判斷邏輯

練習題目的重點，不只是答對多少題，而是理解每個選項成立或不成立的原因。對於答錯或不確定的題目，一定要重新確認觀念，並針對常見的錯誤內容整理筆記，避免只記住答案。

#### 三、掌握 ISACA 的作答思維

CISA 題目常要求選出「最佳」、「最優先」或「首先」應採取的行動。即使多個選項在實務上都有一定道理，仍應依題目情境、作答角色及風險優先順序，從獨立性、證據充分性與風險導向等原則判斷最適當的答案。

#### 四、維持穩定準備節奏

對在職考生而言，穩定而可持續的讀書計畫，比短期大量衝刺更重要，必要時須要抓大放小。建議固定安排教材閱讀、題目練習與錯題複習，每天份量不用多，但貴在堅持，考試時仔細辨識關鍵字並妥善分配時間。只要持續修正自己的理解與判斷方式，備考過程本身也能成為深化專業能力的重要歷程。

## 2024 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



### --CISM 專區--

#### ◆張玉秀 (2024 年 1~6 月 CISM EXAM PASSERS NO.1)

第一次準備 CISM 時，我認為自己已通過 CISSP，因此沿用既有的資安知識架構，並將官方 QAE 題庫完整練習一遍，原以為足以應付考試，沒想到仍與及格失之交臂。這次經驗讓我體會到，CISM 著重的是資訊安全管理、治理與風險決策思維，而非技術知識本身。

第二次備考時，我重新調整讀書策略，以官方教材為核心，搭配 QAE 錯題逐題檢討，釐清每個選項背後的管理觀念，建立正確的答題邏輯。考試時建議先仔細閱讀題意，站在資訊安全經理人的角色思考，避免以技術人員的角度作答，遇到猶豫的題目先標記再回頭確認。相信只要掌握正確的準備方向，持續累積實力，每一次的努力都會成為通過考試的重要養分。祝福所有正在準備 CISM 的考生都能順利通過考試！

#### ◆史哲政 (2024 年 7~12 月 CISM EXAM PASSERS NO.1)

準備 CISA 與 CISM，不只是考試的準備，更是重新認識資訊治理本質的歷程。研讀 Official Review Manual 與官方題庫後我才體會，ISACA 培養的並非知識堆疊，而是 Professional Judgment（專業判斷），『在資訊有限、風險交錯、立場各異的情境下』，依治理原則做出最符合組織長遠利益的決策。

讀書計畫我分三階段：先逐章讀完 Review Manual，畫出各領域的治理關聯；再完整做一輪官方題庫，將錯題分為觀念不清、情境誤判、關鍵字忽略三類；考前只重做錯題並回讀章節，直到能說明每個選項為何不被選中。

考題用字不艱深，難在四個選項多半都可行，差別只在特定情境下的優先順序。作答把握四點：先看題幹限定字（FIRST／BEST／MOST／PRIMARY），往往直接決定答案；辨識自己是稽核人員、資安管理者或管理階層，切勿以工程師視角作答；優先考慮治理與流程面選項，技術控制多為手段而非最佳解；猶豫題先標記、快速通過，最後再回頭處理。

兩張證照的思維主軸不同。CISA 考稽核員的判斷順序，先分析、蒐證，再提建議，別一看到異常就急著上報或修系統；charter 是治理文件不是操作手冊，加速專案要看關鍵路徑而非最長工項。CISM 考管理者的權責視角，先看風險該由誰決定，資訊分類的最終責任在 senior management，風險爭議應升級由高階管理層裁決，風險管理要整合進業務流程而非丟給 IT 獨扛。一句話收攏：CISA 先查清楚再建議，CISM 先看風險誰該決定；兩者遇到 BEST／FIRST 題，都是先想角色、再想順序、最後才想技術。

證照不是學習的終點，而是專業責任的起點。真正值得被認可的，不是擁有多少張證照，而是在每一次關鍵決策中，都能以治理為本、以風險為鑑、以價值為終，成為值得組織信賴的專業人士。



### --CRISC 專區--

#### ◆潘嘉良 (2024 年 1~6 月 CRISC EXAM PASSERS NO.1)

很榮幸有機會與大家分享 CRISC (Certified in Risk and Information Systems Control) 考試的準備心得。對我而言，CRISC 不只是一張專業證照，更是一套協助企業建立資訊風險管理與治理思維的重要架構，準備考試的過程，不僅幫助我順利取得證照，更讓我重新整理並深化了資訊風險管理的觀念，也對日後的工作實務帶來許多啟發。

我的備考時間約三個月。第一個月以官方 CRISC Review Manual 為主，建立四大領域的核心觀念與架構；第二個月搭配官方 CRISC Review Questions, Answers & Explanations (QAE) 反覆練習，熟悉 ISACA 的命題邏輯，並仔細閱讀每一題解析，理解正確與錯誤選項背後的管理思維；第三個月則整理錯題、強化容易混淆的觀念，並透過模擬測驗培養答題節奏與時間掌控能力。

回顧整個備考過程，我最大的體會是：「不要把 QAE 當成測驗，而要把它當成教材」。每答完一題，我都會再思考為什麼這個答案是最佳選項、其他選項又為何不適合，並仔細閱讀每一題解析，試著理解 ISACA 的命題邏輯與管理思維。久而久之，不僅答題的準確度逐漸提升，也讓我對風險治理的觀念有了更深入的理解。

我認為 CRISC 最大的挑戰並非知識記憶，而是思維模式的轉換。考試著重的是如何從企業治理、商業目標與風險管理的角度做出最適當的決策，而不是追求技術上最完美的解決方案。因此，建議考生除了熟讀官方教材與多做練習外，更要理解每一題背後的管理理念，建立符合管理者視角的判斷方式。

最後，祝福所有正在準備 CRISC 的夥伴都能保持穩定的學習節奏，相信只要按部就班、持續累積，成功一定會到來，也期待大家都能將風險管理思維落實於工作實務，持續提升自己的專業價值。

## 2024 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享



### --CGEIT 專區--

#### ◆王聿強 (2024 年 1~6 月 CGEIT EXAM PASSERS NO.1)

準備 CGEIT 時，我認為最重要的是先調整心態，不要把它當成背誦考試，而是培養治理思維。考試重點在於理解企業治理、策略、風險、資源與效益之間的關聯，而不是記住每個名詞定義。建議先建立整體架構，再逐步理解各知識領域的內容，並思考如何與自身工作經驗連結。遇到難理解的觀念，可以試著代入企業決策情境，思考自己會如何判斷與取捨。保持穩定的學習節奏，不急著刷題，而是透過題目驗證觀念是否真正理解，通常會比死記硬背更有效，也更容易通過考試。

#### ◆何宗翰 (2024 年 7~12 月 CGEIT EXAM PASSERS NO.1)

通過 CISA 跟 CISM 後準備考 CGEIT 的時候，發現官方教材的課本跟題庫薄了很多，加上自己以前在金融業工作時對資訊安全作業執行查核過，也待過資訊安全單位實際執行過資訊安全相關作業，這些經歷對準備考試非常有幫助，也可以驗證自己工作上沒有可以改進的部分。

寫題庫跟考試時還是要依 ISACA 的精神作答，像是有公司高層支持的選項出現的話，基本上選他就對了；另外我只有買紙本題庫，雖然考題有出現在題庫的不到二成，但題庫對於選出最符合題目要求的答案非常有用，建議多練習幾遍會對考是很有幫助。