2021 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

--CISA 專區--

◆黃星評 (1～6 月 CISA EXAM PASSERS NO.2、7～12 月 CISM EXAM PASSERS NO.2、7～12 月 CRISC EXAM PASSERS NO.3、7～12 月 CGEIT EXAM PASSERS NO.1)

過往曾任資安管理顧問和資安技術顧問，對技術和管理皆抱有濃厚興趣。擔任資安顧問始終保持著責任感，不斷檢視自己所提供的建議是否準確且符合最佳實務，也常常問自己我給出去的建議是否正確?是否符合最佳實務?在工作上前輩、同事、老闆講的觀念難道就是對的嗎?為什麼是對的呢?自己閱讀思考並與不同專家討論，這些知識才是自己的東西。

自我學習被我視為最佳的方式之一。廣泛閱讀國際認可的教材遠比取得證照更重要，證照是讓自己知識成長的手段之一。閱讀教材的過程不僅能矯正我們的觀念，確保我們引導公司與客戶走向正確的方向。資安人員的每句話都具有重要性。我認為，從事資安管理的從業者必須深入理解這些教材中的基本概念，更重要的是將這些概念逐步應用於工作中。

ISACA 的教材觀念實際上大同小異，區別僅在於每個證照的特定知識點，而且每一張證照都有重複與關聯的主題，當把五張證照學習完成後，會發現所有的觀念都可以完整串起來了！因此，通過 CISA、CISM 後，接著考 CRISC、CGEIT 和 CDPSE，通常只需準備約兩三周即可順利通過，並同時能夠為其它國際資安管理證照內容打下良好的基礎。歡迎搜尋「資安工作者的學習之路」閱讀我分享許多管理與技術證照的準備心得。

在準備證照期間，切記要站在每個證照所代表的角色上思考，放下部分工作經驗和成見。這是因為實際工作經驗可能並不總是最正確的方式，即便證照的教材在理論上很理想，也未必能完全套用在工作上，但如果不知道最正確的做法，很難逐步引導自己的公司和客戶走向更高的資安水準。

對稽核師來說 Domain 1 是核心觀念，另外 Domain 3、Domain 4 與 Domain 5 中技術原理比重也很高，代表著這些知識非常重要。在管理和稽核實務上，了解技術原理是必要的，以避免稽核誤判或受騙。因此，稽核人員必須同時具備風險管理、稽核技巧和技術原理的基本能力，要有足夠多的專業能力才可以執行相關的工作任務。

最後想跟考生分享：管理觀念通，考試很輕鬆。

◆林晉宇 (1～6 月 CISA EXAM PASSERS NO.3)

我自己在準備此考試時，因為習慣線上筆記，使用該方式每天發文，針對每個章節用自己的話寫出心得，加上搜尋到的圖片、自己繪製的流程圖及心智圖。一開始寫的時候也許覺得內容零碎，持續寫約兩周左右開始可以串聯其他章節，開始重新排序之前寫的文章，直到可以串起來後就可以練習題目了。期間常常以自己受稽核時被問的內容及流程去換位思考稽核員想要什麼資訊，去對應書上的手法，更有效的理解內容。

--CISA 專區--

◆劉旭翔 (7～12 月 CISA EXAM PASSERS NO.2)

準備考試時，已有三年電腦審計工作經驗，實務經的累積，絕對是準備 CISA 的最大優勢。此外，另有購買 ISACA 官方出版之《CISA 考試複習手冊》以及《CISA 複習考題及解答手冊》，平時多以刷複習考題磨練題感，複習手冊則是針對自己不熟或涉略較少的章節，進行重點加強。刷題重點：即使能夠選出正確答案，也應該好好思考其他選項不是正確答案的原因，以及可能使這些選項成為最佳解答的情境，在 CISA 考試中，很容易因為題目的一個關鍵名詞變換，而使最佳解答不同。若能在前述做法下，達到 80%以上的對題率，想必將能順利通過考試！

◆楊安傑 (7～12 月 CISA EXAM PASSERS NO.3)

考試著重電腦稽核知識及技巧，我覺得還蠻看中相關工作經驗的，我在有相關工作經驗的情況下，備考時間約三個月，準備方式就是不斷的寫題目並進行檢討，尤其要跟自己的工作經驗相結合，確實理解題目的意涵，不要死背！祝大家順利。

--CISM 專區--

◆陳昭名 (1～6 月 CISM EXAM PASSERS NO.2、7～12 月 CISA EXAM PASSERS NO.1)

在銀行業的資訊與資安單位服務多年，取得 CISSP 證照後，期許自己持續精進在資安管理與電腦稽核領域的認知，因此參加 CISA/CISM 考試，經由自學閱讀 ISACA 教材的知識點，結合工作中的對應經驗，持續知識內化與觀念釐清，順利的在半年內取得 CISM 及 CISA 證照。很感謝 ISACA 用心編寫的學習教材，讓後學的我在學習上能有所依循。我的讀書計畫如下：

(1)以 ISACA 官網上的 Exam Content Outline 當學習地圖，確認自己研讀方向正確。
(2)研讀 ISACA 出版的 Review Manual 重點。
(3)練習 ISACA 出版的題庫本，勤做練習並研讀解題說明，務必理解到 85%以上。
(4)整理自己的混淆點筆記。
(5)重復以上 1～4 步驟。
(6)善用工具資源，將不理解的知識內容持續在網路上找到資料釐清。
(7)社群學習：加入一些資安學習社群(FB 或 line 群)，透過與朋友、先進分享討論，增加廣度與深度。

(接下頁)

考試技巧分享：

(1)刪去法：定義真的要多熟悉，考試不難，兩個選項"覺得難決定"就考驗定義理解的基本功了。

(2)歸納法：用換位思考，我是企業中的資安經理(CISM)或電腦稽核(CISA)，遇到這個情境要如何「要以大局為重」，找到對公司、對業務，在資訊安全的前題下最適合的方式。

(3)心理建設：鼓勵自己不慌張，穩穩的一題一題作答，心定下來就成功一半。

以上簡單分享，祝福先進學習之旅順利，未來一同在資安路上相互學習扶持。

◆林銘鴻 (1～6 月 CISM EXAM PASSERS NO.3)

藉由 20 多年的資訊背景以及近年來從事資訊安全技術訓練的工作，深知 Certified Information Security Manager(CISM)國際資訊安全經理人證照內容注重組織資安治理，其中包含風險評估、資安計畫、資安事件應對及處理等等，換句話說，CISM 主要著重在資安治理而非資安技術層面。先以(ISC)²的 CISSP 認證知識為起手式，待完成 CISSP 考試之後，利用了 1 個月的時間瀏覽 CISM review manual，並結合自身的經驗，進行知識微調。再加上自身從事客戶需求的 ISO 27001 ISMS 管理系統的輔導，統合了技術、管理及顧問服務等知識領域，個人也使用 CISM Exam Prep APP，也善加利用了 ISACA 有不錯的論壇，得以順利的一次性的通過考試，ISACA 官網裡面有許多資訊可供準備考試的人討論及參考 https://engage.isaca.org/。

◆林經晟 (7～12 月 CISM EXAM PASSERS NO.1)

考試是一個需要充分準備和計劃的過程。以下是我個人的備考經驗，希望對你有所幫助：

1.制定合理學習計劃

請制定一個合理的學習計劃。請先確定考試日期，再分配準備時間，以確保在考試前能夠覆蓋所有主題。建議每天持續學習，以分散學習進度，避免在短時間內閱讀大量內容，影響吸收程度。可以考慮使用時間管理工具，增加學習效率，例如：番茄鐘工作法。

2.選擇學習資源

請依據個人學習風格和時間規劃，選擇最適合你的學習資源，例如：實體課程、線上影片、課本、筆記、模擬題庫等。建議同時搭配多種學習資源，協助你更全面地理解教材內容。

(接下頁)

3.整理學習筆記

請將學習內容或測驗詳解做成筆記，以利回頭複習。另外，建議使用自己的語言解釋專有名詞或觀念，不僅有助於理解，還可以幫助你加深印象。考前不妨根據學習筆記進行重點式複習。

4.平衡理論和實務

考試強調理論觀念或最佳實務，然而實務工作上難免有些權宜變通，不一而足。為了能順利通過測驗，在學習過程中，請接納 ISACA 的觀點，暫將實務工作經驗放在第二位，無需爭辯對錯，請依當下情境判斷。

準備考試是一個漫長的過程，找到最適合你的方法和節奏將是關鍵，祝你成功！

◆黃星評 (7～12 月 CISM EXAM PASSERS NO.2、1～6 月 CISA EXAM PASSERS NO.2、7～12 月 CRISC EXAM PASSERS NO.3、7～12 月 CGEIT EXAM PASSERS NO.1)

身為資安管理人員或資安顧問，我們需要了解教材中如何展現資安的價值並與組織業務保持一致，CISM 要特別注意資安計劃設計的基本觀念，實務上運作良好的資安治理仍需學習基本技術原理。個人評估 CISM 是五張證照中最容易上手的。

◆林育陞 (7～12 月 CISM EXAM PASSERS NO.3、7～12 月 CRISC EXAM PASSERS NO.1)

每個人對於追求證照的動機有所不同，但我個人希望大家能夠遠離投機取巧的方法，以真正的學習為基礎來獲得證照。如果證照只成為了機械性死記硬背的象徵，而非知識與能力的實質體現，那麼我們所珍惜的這些證照將失去了其價值。

證照存在的核心意義在於向大眾保證持證者具備一定的專業能力。因此，在追求證照的過程中，我們應該不僅僅是盡力記住教材中的知識點，更需要理解背後的原則，並能夠將這些知識應用於實際工作中。僅僅擁有理論知識，卻不懂得如何將其轉化為實際能力，那麼獲得證照也只是徒有虛名。

回到正題，我想分享一些關於考試技巧的建議。模擬題是一個極為寶貴的自我檢測工具，而官方教材中的答案解釋也能夠補充課本未涵蓋的知識或邏輯。如果在考試前能夠深入理解課程教材和模擬題所傳遞的內容，我相信每個人都有能力在考試中獲得出色的成績。最終，我祝福大家都能取得優異的成績，實現自己的目標，走向成功的道路。

透過學習這個領域的知識，我們能夠掌握如何以正確的步驟為公司建立資安管理制度。在台灣，許多資安管理專業人士僅關注政策規範標準，而忽略了在這之前更為關鍵的專案和策略。這些學習不僅能讓我們具備更完整的資安視野，同時也能夠瞭解如何為企業制定可行的資安計劃。

(接下頁)

此外，我們還能夠學習如何適當地規劃資安組織架構，並深刻認識公司管理思維以及支持業務的關鍵性。通過這種學習，我們能夠站在企業的角度來思考資訊安全，而不僅僅是追求絕對安全。這樣的思維轉變能夠幫助我們更好地理解如何在保障資訊安全的同時，實現業務目標的平衡。

在準備 CISM 考試時，我們應該站在資訊安全主管或高階主管的立場去思考。這不僅能夠幫助我們更全面地理解資訊安全的挑戰和策略，還能夠培養我們的戰略性思維。這種角度能夠幫助我們更好地應對考試中的情境題目，並更深入地理解資訊安全在企業環境中的實際應用。

--CRISC 專區--

◆林育陞 (7～12 月 CRISC EXAM PASSERS NO.1、7～12 月 CISM EXAM PASSERS NO.3)

我一直認為從管理的角度來討論資訊安全，事實上是在探討風險管理。可以說，對於企業而言，將資訊安全(Cyber Security)視為資訊風險管理(IT Risk Management)更為貼切。在學習這個領域的知識時，我們必須深刻理解風險的本質，並牢記組織的風險胃納和風險容忍度在風險管理領域中扮演著極其重要的角色。

◆高健欽 (7～12 月 CRISC EXAM PASSERS NO.2)

CRISC 的考試內容除了風險方面的知識需要投入較多時間研讀與理解外，因本身在 2020 年初取得 CISSP 證照故在管理與技術領域知識的準備上較游刃有餘。準備 CRISC 的時間大約 1 個月，準備方式首先快速看過 Review Manual 一遍(大約 20 小時)，其餘時間全放在 Review QAs & Explanations(大約 80 小時)，QA 完整做了兩輪後再針對錯題反覆練習並加強理解直到沒有錯題為止。

◆黃星評 (7～12 月 CRISC EXAM PASSERS NO.3、1～6 月 CISA EXAM PASSERS NO.2、7～12 月 CISM EXAM PASSERS NO.2、7～12 月 CGEIT EXAM PASSERS NO.1)

實際上，大多數證照很少深入探討「風險」本身的意義，多半只是套用公版流程，任意使用「風險」一詞。但對「風險」的定義和相關細節，許多人並不清楚。CRISC 能夠使風險管理從業者更深入了解「風險」的精神，加強風險管理的維運，設定適當的關鍵風險指標(KRI)，在這個考試中需要很清楚的了解不同名詞定義與運用情境，非常適合想要學習進階風險控制的從業者。

--CGEIT 專區--

◆黃星評 (7～12 月 CGEIT EXAM PASSERS NO.1、1～6 月 CISA EXAM PASSERS NO.2 7～12 月 CISM EXAM PASSERS NO.2、7～12 月 CRISC EXAM PASSERS NO.3、)

較為沒有 IT 背景的資安從業者，可能比較無法了解 IT 治理的主要目標和精神，個人以資安從業者角度來看，CGEIT 的知識除了能夠協助提升資訊部門的安全性，同時能從 IT 的角度思考，以不同的觀點解決問題，減少與 IT 之間的衝突。這對想要增進與 IT 溝通能力的資安從業者來說是非常適合的。在考試中需要從資安轉換成資訊人員的觀點，站在資訊治理的角度去準備，建議可額外閱讀 COBIT 的教材會更好瞭解 CGEIT 教材的觀念。