2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

--CISA 專區--

◆呂建和

大家好，跟各位先進分享我的準備考試心得。首先建議大家擬定讀書計畫，雖然準備考試過程中也可以學習到許多 IT 的知識，但最終目的還是考取證照，所以我的方式以短期內快速閱讀計畫爲主，因爲我已有相當的 IT 經驗，所以當初是安排三個月的讀書計畫(可視你對 IT 領域的熟悉度增加至六個月)，我的計畫內容大約安排是至少兩次的完整閱讀教材以及每週讀書進度，追蹤自己的讀書進度，而爲了讓自己能有明確著目標進行的決心，我會依讀書計畫的期程直接報名考試。另外，閱讀教材的部份，我是直接使用官方的教材，分享兩次的閱讀教材方式如下：

第一次：

■要完整看完所有內容。

■以理解內容爲主，並建立大網並留下印象。

■記得畫重點。

■立刻做考古題，主要觀察出題的重點，檢視自己認爲的重點相不相符。

■不會的答案不要猜題，每做完一次試題要立刻對答案。

第二次：

■重點式、加強需記憶的地方。

■作筆記或貼小紙條。

■完成第二次後，再一次總複習。

■第二次考古題模擬測驗計分。

■檢討考題後，再去修正筆記。

各位先進大部份應該都是在職狀態，在考前一天建議可安排休假暫時放下工作事務作重點式復習、閱讀小筆記及模擬測驗，最後記得早睡早起。考試當天提早一小時到達考場，熟悉環境放鬆心情即可，以上是我的分享，希望對大家有幫助，謝謝。

◆易進源

CISA 很難考，所以要花很久的時間準備，其過程必定辛苦，故要有決心與計畫，每個人的計畫都不同，但要有排除萬難的準備，而且要徹底落實計畫。準備過程中，要著重理解，千萬不要死背，才能應付千變萬化的題目。最後一點，考試時間很長，務必要堅持住，控制好時間，不要讓自己的注意力渙散。

◆黃履州

準備時，加強理解與重複練習，堅持不懈。

2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

◆舒惠荃

1.參加電腦稽核協會之 CISA 考試準備課程及解題班。
2.研讀 ISACA 出版之 CISA Review Manual 重點及資訊安全相關書籍。
3.購買 ISACA 出版之 CISA 最新題庫，勤做練習並研讀解題說明。
4.安排每日複習進度，儘快預約報名，於三個月內參加考試。

◆鐘仁駿

因本身從事電腦稽核工作，有較多機會可以了解書本上的實務內容，也較能從中區別出技術和資安管理面的區別。舉個例子來說，傳統 IT 人傾向崇拜高大上的技術達人，專案無非是採購當下最新的技術和設備，設備都要虛擬化，權限控管都要登入側錄搭配 DLP(資料外洩防護)。但後來在竹科園區有機會當上資安稽核，代表公司去海外和客戶介紹公司資安環境以爭取訂單，從此觀點即發現，資安的管控如能和組織業務相結合，才能真正在組織內部推動。公司也才願意大力投資資安相關解決方案，資安標準(ISO 27001)等才能真正落實。故本考試建議從管理角度來思考較能得分，如：機房火災時優先考慮人員安全，而不是設備毀損等議題。模擬題方面也建議專注在官方提供的模擬題即可，做題貴在融會貫通而不在多。我也有參加電腦稽核協會舉辦的 CISA 班，透過學員間的交流更加奠定應考的決心，畢竟有好多稽核高手群聚一堂呢！考試時還是多檢查一下，題目相當多務必再次確認答題重點，畢竟蠻多題目四個選項實務上都是對的喔，但仍需從中選擇最合適答案，這就要有相當耐心審題了。最後祝各位都能順利通過考試。

◆劉昌輝

CISA 考試的準備，首先要先取得相關的教材(包括講義與題庫)，因爲範圍比較大，如果一開始就針對講義從頭讀到尾，可能會無法知道重點在哪裡，建議先將題庫問題做一遍，然後針對錯的題目去講義中尋找答案，並且理解他，然後針對第一次錯的題目去做第二次，針對第二次錯的題目去做第三次，以此類推，大約做個五、六次後，錯的題目就會越來越少，最後，即具備有一定的基礎能夠上考場。

◆劉家宏

本人考試準備的期間大約三個月，主要準備方向是從題庫著手，安排考試計畫的重點爲：

1.至少所有題庫要看過四輪以上。
2.每日念書時間不求多，但要持之以恆。
3.第一輪時，一個章節最多四天內要做完，並記錄不瞭解的名詞解釋，閱讀教材或查詢網路上相關資料。 (下頁接續)

4.第二輪之後，一個章節三天內做完，並在每天做完之後針對答錯的題目再看一次，確認是否能融會貫通。
5.針對答錯兩次以上的題目，深入瞭解問題所在，不硬背答案。
6.第四輪以後，答題正確率需達到 80%以上。 (下頁接續)
考試當天盡量排除其他外務，提早至考場準備，考試時將比較沒把握的題目先進行標記，全部題目做完一輪後再針對標記的題目做出判斷，並注意考試剩餘時間，穩定的作答。
希望以上心得能對於欲考取 CISA 的考生們有些許的幫助。

--CISM 專區—

◆莊鴻國

正如電腦稽核協會介紹，國際資訊安全經理人(CISM)的特色著重於資訊安全管理工作上應有的經驗、思維與態度，這非常重要，因爲技術人員與管理人員的想法差異會在考試中顯現。

爲掌握考試技巧，當時有報名電腦稽核協會所辦的「CISM_國際資訊安全經理人認證研習班」，非常感謝講師提醒，「資訊安全治理」及「資訊風險管理」是考試範疇中較難的部分，原因是「CISM Review Manual」教材的內容會遠比我們實務上所認知的還要多且廣，做法也可能與您個人目前職務分工有所差異，這可能會影響到考試作答，所以在研讀這兩個工作實務時，請讓自己再成爲一個海綿，把教材的內容吸收起來，取分就不會有太大問題，在工作也有很大的助益。另外「資訊安全計劃開發與管理」與「資訊安全事故管理」這兩個工作實務對已具備資訊專業者，得分就相對容易。

在讀書計畫方面，因了解「資訊安全治理」及「資訊風險管理」兩個工作實務應留心，個人安排這兩個章節先研讀教材後再作考題，以印證並適時調整思維，在「資訊安全計劃開發與管理」與「資訊安全事故管理」部分，則是從考題練習完再回頭看教材，練習考題時，除了對的答案外，其他答案也都要理解透徹，考題的答案也是觀念的陳述，以個人當次考試經驗，考古題沒有出現，所以觀念不清楚，硬背題目答案，恐無助於實際考試。

最後再分享見人見智的看法供參，我們都是從英文或簡中二種語文擇一，以個人考 CISA 英文版兩次(當時僅有英文試題)，CISM 簡中版考一次，若對英文沒信心者或許選簡中版來考會較適宜，雖然專有名詞在簡中及繁中的翻譯不同，但比起英文版考題，還是可以減少猜題意時間，就有機會增加通過機率。

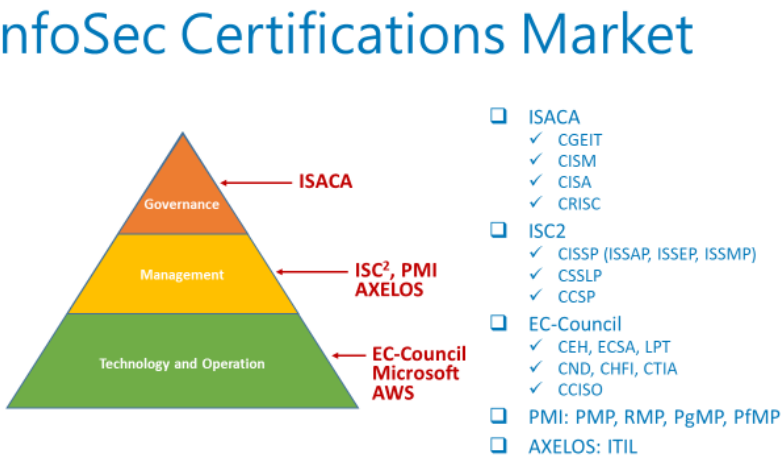
祝 考試順利！

2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

◆吳文智 (同年再考上 CRISC、CISA、CGEIT)

去年(2018)通過 CISSP 考試後，覺得 CISSP 在資訊安全治理及風險管理的領域談得不夠深入，因此決定繼續參加 CISM 的考試。隨後因金融業的朋友－董世文(小董)先生建議投入資安教育訓練領域，爲了強化成爲資安講師的資格，所以延續了原本的考照計畫，繼續考取 CRISC、CISA 及 CGEIT 等證照。

這次的考試計畫同樣採取明確的目標管理及充分的預算準備，再加上有紀律的執行，因此相當順利；四張證照總計投入時間爲 49 天，合計 175 小時，平均每天研讀約 3.5 小時。



我個人把 ISACA 的證照定位在治理層次(事實上 ISACA 也刻意區分治理與管理的差異)，考試所談的議題及 ISACA 建構的知識體系相當符合我的期待與需求。CISM 完全是由治理的角度出發，亦即由經營階層(董事會及高階主管)的角度來定位及指導資安的角色與發展。例如：治理的目的在於交付價值，必須由使命與願景來展開目標與策略，並搭配策略執行框架(如 PMI 的 OPM)來實現策略；因此必須進行計畫與專案(program/project)管理、投入資源及衡量績效等。治理的同時必須考量風險及符合性(compliance)，也就是企業賺錢必須深謀遠慮，且兼顧君子愛財、取之有道之明訓。它的挑戰在於必須把看似空洞的理論，對應至企業經營的實務與個人的工作經驗；由於個人在資訊領域已有二十多年的工作經驗，加上公司成立十年來也充分運用了 EMBA 所學，再加上剛考過 CISSP，資安相關的知識都還在記憶中，因此 CISM 考試相當輕鬆，前後投入了 40 小時。

CRISC 是我的第二個考試科目，它算是其它 ISACA 考試的通識科目。準備 CISSP 及 CISM 時，事實上已研讀了資安的風險概念，再加上之前已取得 PMI 的 RMP 風險管理師證照；因此準備 CRISC 時的挑戰，反而是如何整合各家風險理論的說法，如：ISO、NIST、ISACA 及 PMI 等。我個人把資安視爲風險管理的分支，因此非常建議把多一點時間分配在風險管理上，尤其是企業風險管理、資訊風險及專案風險等的整合。

(下頁接續)

2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

CISA 是內容最多的一個科目，必須同時兼顧治理、管理及技術的議題，挑戰性不低。由於 CISA 大多數內容在準備 CISSP、CISM 及 CRISC 的過程都唸過了，所需加強的部份只有稽核領域的議題；因此 CISA 考試也順利過關，前後投入了 50 小時。

CGEIT 基本上是 IT 主管的考試，而不是資安；但它的 IT 策略執行跟 PMI 的 OPM 策略執行框架很吻合，再加上資安也與 IT 營運有高度的相關性，因此決定繼續考 CGEIT，以作爲我個人 2018 年度的學習與成長計畫的收尾。取得 CGEIT 後，其實可以考慮 PMI 的 PgMP 或 PfMP 證照，以充實更完整的策略執行議題，並與策略規劃接軌。

ISACA 的這四張證照，基本上都架構在很紮實的知識體系上，也許初次接觸會覺得過於理論；但搭配自身的工作經驗來解讀這些觀念或理論，事實上會有很大的收穫。例如：讓自己的工作經驗得到理論支撐；或者遇到沒有處理過的議題，則可以有一個理論或參考架構可以依循；與同事或客戶溝通時，能夠有共同或更精準的語言，除了能增加自身的專業感，也能讓客戶更有信心。

準備 ISACA 的考試，建議務必購買官方教材及訂閱官方線上題庫。ISACA 的考試雖然可以自行研讀及報考，但參加協會或其它訓練機構所舉辦的教育訓練課程，則可以釐清考試方向與觀念、節省時間，以及諮詢或協助報考、申請資歷驗證與取得證照等問題。

最後，明確的目標與讀書計畫、時間管理、公司與家人的溝通與支持、十足的預算準備、對自己的學習承諾與紀律、有效的讀書方法與教材，以及擁有一起考試的伙伴及導師(mentor)，都是通過考試的重要因素。

我的考試經驗也同時分享在個人部落格(https://WentzWu.com)。

若大家有任何問題，歡迎隨時與我連絡。

敬祝各位先進前輩 身體健康、考試順利！

◆李民偉

1.也許是理論與實務總有些許的差距，建議考生應考之前還是要把官方教科書至少讀過一遍，以便校正自己的觀念，過度依賴實務經驗作答相當有可能會吃虧。

2.應試時要把「資安只是手段，不是目的」的根本觀念深植在腦海中，面對所有決策(考題)，要以業務遂行與組織營運目標作爲最高的考量，而不是爲安全而安全，亦即各行各業的實務運作中，資安長需足以扮演跟各業務單位以及決策階層間的橋樑。

2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

◆陳耀勳 (同年再考上 CGEIT、CRISC)

2017 年起 ISACA 的認證考試改爲線上測驗，考試的時程安排變的很有彈性，應考中心也逐年增加，對於時間有限的上班族，提升了規劃考試的便利性，同時站在客戶的立場提供更佳體驗！

因爲稽核工作的需要，2017 年先考 CISA，從一路摸索中找到一些考試經驗，所以 2018 年 CISM、CGEIT 及 CRISC 能優化成績到前 3 名。經驗分享如下列 3 項：

1.下定決心&念書：考試及 Review Manual 的費用都很高，要認真念，官方複習手冊讀 3 次：第 1 次看大綱、結構、標題及圖表，第 2 次章節詳讀，第 3 次訂正時專項精讀。

2.模擬試題&檢討：官方模擬考題做 3 次，認真訂正搞懂，每個選項對與錯的原因徹底理解，那怕第 1 次錯誤率很高，只要做到每次迭代，每次要比前次進步的正確趨勢。

3.心理建設&應考：完成前兩項行程，基本上已經具有考上的資質，考前一天睡好，當天適量用餐，安心進行 4 小時大考。

確實落實執行，每 4 個月可以通過 1 個考試，加上原有的 IT 工作經歷，就能順利申請及取得認證。

今天跨出第一步，穩定而堅定，目標達成就愈來愈近了！

◆李冠樟

非常榮幸也非常幸運能以高分考取 CISM。CISM 是一張很適合從事資安工作 3 年以上且有實際碰過資安管理面、策略面的人可以去嘗試考取的證照。我本身從事資安顧問業超過 6 年，我是先考取 CISA 後才考 CISM 的，這兩張 ISACA 的證照都對我提供客戶專業服務非常有幫助。和 CISA 比較起來，CISM 考的 4 個領域比較偏管理面，考題本身也比較著重測試考生對於資安治理及風險管理的瞭解程度。因此我建議在準備 CISM 考試的時候，不需要花太多時間去硬背太細節的東西，反倒可以多花點心力去理解資安經理人所注重的管理議題。實際考試作答時，是要測試考生選出最佳解答，所以若依照過去的工作經歷與經驗去思考，乍看可能會感覺每個答案都有道理，但這時只要靜下心來，以資安經理人的角度與立場去思考，你就會發現有一個答案正在發光，那就是正確答案！！

祝福大家都能順利考取 ISACA 的各類證照！

2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

--CRISC 專區—

◆孫文良 (同年再考上 CGEIT)

在準備 ISACA 的考試在每個科目的選擇會與準備的方向不同，選擇考 CRISC 與 CGEIT，一定要讓自己從不同的角度看事情，CRISC 與 CGEIT 都是具有難度的考試，要避免想要用嘗試的方式來過關，必需要有充份準備應戰的心態，在前一年通過 CISA 與 CISM 考試到現在 CRISC 與 CGEIT，就有如導入一個 ISO 管理系統一樣，需要不斷的精進改善維持，在每一次的考試，我也一直不斷的驗證讀書方法的有效性，如果您不是天才型的選手，就要掌握好的讀書方法。

分享我的讀書方法與考試技巧如下：

一、讀書方法

首先，制定讀書計畫，依計畫按部就班達成，執行重點如下：

1.分析自己擁有的時間(考試時間=投入時間)，要在愈短的時間考試，就要在愈短時間投入愈多的讀書時間。

2.依據官方 Review Manual 的章節頁數，對應可使用的時間，例如：距離考試的時間是 4 個月，每週一～五要上班，而週六、日時間較多，就可以安排週一～五的時間讀新的頁數(求持續閱讀但不求多)，而在週六、日的時間，除大幅增加新的頁數外，做一次當週整體的複習，務必整理屬於自己的筆記(這是考前最後要看的精華)，確認相關知識都有理解，Review Manual 應安排在 3 個月內讀完。

3.排定計畫完成之後，就刷卡報名考試，正式訂下考試日期，給自己一個必須要達成的期限(壓力)。

4.開始進行閱讀，在每一章節讀完後，另安排週六或週日時間利用官方練習題進行該章節的測驗(約 50 題)，驗證理解的程度，這裡只需知道測驗成績，但不要看解答的內容(因爲看了以後題目就沒辦法再用了)。

5.最後一個月，每週一～五，每日進行 30～50 題的隨機測驗，分數要維持在 80%之上，週六、日的部份，每日進行 1 次 150 題的連續時間測驗，並在測驗後檢討錯誤的題目(看解答)，徹底理解錯誤之處。

二、考試技巧

1.最重要的就是在考試前日保持充足的睡眠，沒有好的精神就沒有好的思路。

2.記得要去考試。

3.150 題的測驗認真做完也需一定的時間，捕捉關鍵字，不確定的一定要 Mark 起來，待 150 題都答完後，逐一 Review，確認無問題，善用考試的每一分鐘來增加自己的分數。

4.提醒考試時，調整自己的思考的身份，例如：考 CRISC 時，你就是高位的風險管理者，要用高位者的角度來思考，思考的面向與結果一定會是不一樣的。

以上希望提供給未來的應試生一些方向，也預祝都能順利過關。

2018 年新科 CISA / CISM / CRISC / CGEIT 前三名心得分享

◆蘇德音

準備考試一定要反覆詳讀「複習考題」，並熟悉出題模式，以利於正式考試時迅速釐清考題重點及找出正確答案。

--CGEIT 專區—

◆張育豪 (同年再考上 CISM、CRISC)

1.依個人時間安排讀書計畫。

2.仔細閱讀 Review Manual。

3.做 Review Questions 的練習題。

4.檢討題目，了解答對與答錯的原因。

5.針對比較薄弱的部份再加強閱讀 Review Manual。

6.考試答題時先看清楚題目，想一想，再回答。

7.留意考試時間。