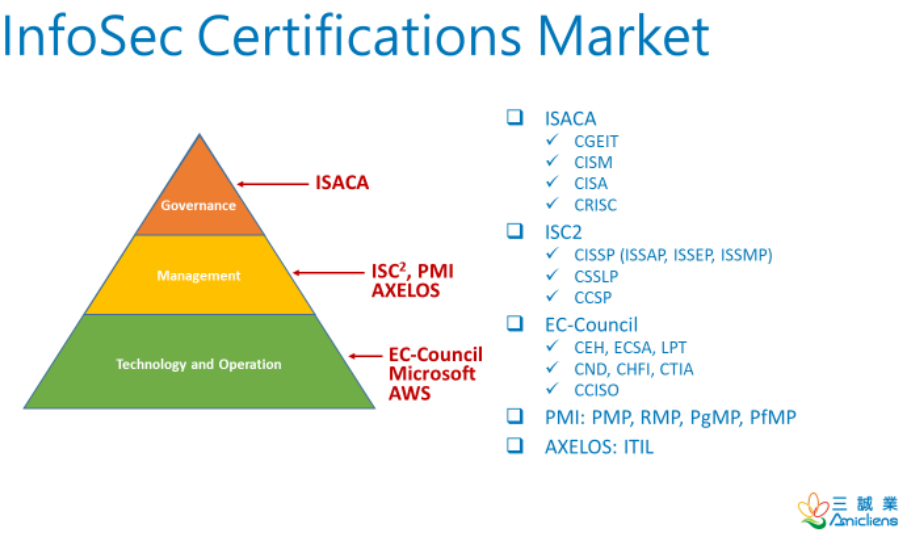
我的 ISACA 考試經驗分享－吳文智

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，為了強化成為資安講師的資格，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為 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。我個人把資安視為風險管理的分支，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。

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，以作為我個人 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！

三誠業服務科技
總經理　吳文智

EMBA/CBAP/PMP/ACP/PBA/RMP
CGEIT/CISM/CRISC/CISA
CISSP-ISSMP, ISSEP, ISSAP/CCSP/CSSLP
CEH/ECSA/AWS-CSAA/MCSD/MCSE/MCDBA
SCRUM: PSM Level I/PSPO Level I/PSD Level I
ISO 27001 LA/ISO 27552 LA Courses Completed