ISACA 證照的取證之路

楊宸賓

CISSP, CISA, CISM, CRISC, CDPSE, CEH, JCCP

前金融機構資安主管

現為第三方資安稽核員

證照考取歷程：

2022 年 2 月 CISM，2022 年 8 月 CISA，2023 年 1 月 CRISC，2023 年 3 月 CDPSE。

先從 4 個問題來討論，那也是摸索時問自己的 4 個問題。

考證照的目的是什麼？

資通安全證照清單有！
別人有我也要有！
被別人推坑！
拓展人脈！
提升競爭力！
提升專業知識！

在資訊與資安領域工作多年，重新檢視自己的專業能力是否可以因應當前的環境。資安事故每天檯面上與檯面下一直在發生，攻擊手法不斷翻新，光靠過去的技術經驗已經無法在應付現在對內、對外的狀況。從公司下到上的管理，上到下的傳達，橫向的溝通，如何用「人話」讓公司同仁都能理解。資訊資安不是全新的領域，但在公司內部往往就是讓高層及業務部門公認是「花錢」，問為什麼要投資，技術人都是用技術腦再回應高層。

從證照考試檢視自己觀念是最佳的入門，官方教材已經幫忙把一個領域的重點整理出來，證照所需的流程與知識體系。ISACA 證照約每 3~4 年會因應環境現況更新知識，線上資源則會不定期的更新，持續深耕這領域或年度目標規劃都是值得參考、學習的資源。

了解證照的本質嗎？

各位先進考證照前一定都會去爬證照資訊與通過心得分享，但ISACA 這幾張證照 CISA、CISM、CRISC、CGEIT、CDPSE 這幾張證照的著重的核心價值與知識體系是什麼？備考前必須要先去了解。

官方對於證照的基本條件可上協會官方網站查詢或者參考Certification Exam Candidate Guides。ISACA證照是專業證照不是入門級證照，能通過考試是一回事，取得證照又是另一件事，每一張證照都需有相關經驗的年資要求並須要有人背書。

CISA（國際資訊系統稽核師認證）

本質是「稽核」，必須站在第三方的客觀角度去看符合性（Compliance）的持續有效性。

符合性：1.國際驗證標準。2.法令、法規。3.組織內部程序。4.高階承諾。5.關注方（利害關係人）的合約要求與期許。6.產業規範。

CISM（國際資訊安全經理人認證）

本質是「資訊安全治理」，治理為組織高層的管理作為，從公司營運的預算、成本、風險考量下規劃並實作符合組織資訊安全措施。

CRISC（國際資訊系統風險控制師認證）

本質是「在諸多限制下達到組織的風險胃納」，在不同領域不同產業活用相關的風險評鑑方法論，且使用的方法論前後可以比較。

風險管理：風險評鑑、風險處置

風險評鑑：風險識別、風險分析、風險評估

風險處置：接受、轉移、緩解、規避

CDPSE（資料隱私解決方案工程師認證）

本質是「合理的使用資料」，在符合性要求下的資料生命週期做到時時都安全，及其所使用的架構處處都安全。

個人通過這 4 張證照以難易度比較CRISC > CISA > CDPSE > CISM，建議準備順序 CRISC->CISM->CDPSE->CISA。（CGEIT 準備中故無列入比較）

思維改變了嗎？

換了位子就要換腦袋，了解這幾張證照的本質，在備考或考試過程中思維有跟著改變嗎？答案還是一如往常技術解！ISACA 認證考試方向跟日常作業情境很雷同。

個人在備考 CISA 時，遇到有問題的題目請教恩師（孫嘉明教授），他回我：你現在是稽核不是資安工程師。頓時柯南的靈光乍現，我知道了，思維沒轉選擇就會錯。

以風險（CRISC）為基礎，有效處置組織風險達到風險胃納（可接受程度）。站在組織高層的角度（CISM）且在成本效益（Business Case）實現符合組織的資訊安全方案，並在符合性（CDPSE）的要求下達到時時都安全，處處都安全的合理使用資料。稽核（CISA）必須客觀

且找尋符合性證據，提出有價值的風險。

證照取得了，有在用嗎？

公司的存在就是為了賺錢，如何將這些死硬的技術語言轉換成高階主管想看到的錢。1 個管理問題可能有 10 種解決方式，哪個方法才是最符合公司組織想要的方法？

用魔法打敗魔法，例如用稽核思維回覆被退了 5678 次的稽核缺失報告，成功救援部門。用資安治理的思維高度抓到高階主管想要的部門目標報告。用 I（Input）P（Process）O（Output）的流程概念進行問題追蹤。用時間序（事前、事中、事後）各階段的系統檢核點。用 NIST CSF 的架構彙整出公司資安縱深防禦還需加強的部分，作為後續年度計畫執行目標。

通過考試取得證照只是敲門磚，會不會用是一回事，能不能活用才是專業。或許有先進會說工作上就很難用上，一種狀況是還沒學會怎麼跟非同溫層的人講人話，另一種狀況是機會是自己創造。

最後想學知識、活用知識並且通過考試，官方 Questions, Answers & Explanations（簡稱 QA）做好做滿，了解 4 個選項在說什麼，解釋說明要理解，回頭翻 Renew manual（簡稱 RM）看好看滿，並跟專業人士討論。管理類證照須要有流程思維，不要只用單一章節拆開來看，這樣無法有效的內化知識點。**祝各位先進考試順利。**