從零開始的資安治理學習之路

CISSP/CISA/CISM/CRISC/CGEIT

Hello!

I Am Kuro Huang

Cyber Security Consultant
Enterprise Security Architect
IT Security Auditor
CISSP, CISA, CISM, CRISC, CGEIT, CEH, ECSA, CPSA, CSA, CTIA, NSPA, CCNP Enterprise & Security, ISO 27001 LA, ISO 17025

contact@kuronetwork.me
https://kuronetwork.me
FB: Kuro的資安學習手記
Kuro Huang | LinkedIn

@高雄蚵寮漁村小搖滾

十萬個為什麼

大家都治理都講的不一樣?
如何開發與實施Security Program?
廠商和顧問的意見就是對的嗎？
什麼觀點是國際認可的?
技術人遇上管理單位好吃虧？
提案常常被拒絕？
考到CISSP/CISM是不是直接就變大師

透過證照學好最基礎的定義

風險(Risk)的定義？

風險管理（Risk Management）的定義？

Policy （政策）是什麼意思？

職涯沒有發現的盲點

“透過工作經驗與 On The Job Training 學資安的過程中，很容易帶給我們似是而非或是錯誤的觀念，而透過國際證照學習可以有效率並有依據的學到國際上認可的正確思維”

Source :
https://medium.com/blacksecurity/benefits-of-certifications-ec8880639df8

從證照學習風險、業務目標與管理思維

一般常見的傳統網路架構檢視：

- 只看資安設備缺什麼、只看網段區隔、設備規則等技術面做起手式

增加一些管理思維與風險考量的網路架構檢視：

- Policy（高階管理層意圖）、固有風險、差距分析、業務目標、環境威脅、風險評鑑、利害關係人想法、風險容忍度、風險胃納、資源投入優先級

缺 DLP？直接買來 DLP 就解決了嗎？

- 請先資料盤點、分類、保護
- 請先考量業務目標與環境威脅、風險評鑑
- 乙方廠商/顧問不會比你更了解組織內業務與風險，買方要可以自己評斷
- 買賣方能力要是對等的，這樣才可以發現問題

How to think like a Manager!

- 組織戰略目標、業務目標
- 組織核心業務、高階管理意圖
- 組織重要資訊資產
- 成本效益與預算 / 優先級與資源分配

UCCU Hacker
7月21日下午9:23 ·

等等!! 讓我講完!!
==========
#也不管別人受得了受不了
#然後就被Mute了
Credit: Unkonwn

https://www.facebook.com/UCCU.Hacker/photos/a.746549245484834/2314827138657029/

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/five-cybersecurity-memes-and-what-they-say-about-cybersecurity-today

HI Kuro ，講這麼多
所以有標準、有系統化的學習方法嗎？

ISACA證照

學習資安治理與風險管理

如何確保學習到正確的資安管理與資安治理觀念？
想對非技術領域有知識增長？
提升與高階管理層之間的溝通效率？

ISACA

ISACA 國際電腦稽核協會為一個為資訊管理、控制、安全和稽核專業設定規範的全球性組織。它的資訊系統稽核和資訊系統控制標準為全球執業者所遵循。它的研究工作針對那些挑戰其重要原則的疑難專業事項。

Source :
https://www.isaca.org.tw/
https://www.isaca.org/

熱門證照

CISA 國際電腦稽核師

全面的了解各個領域基本知識，了解稽核手法與基本技術概念，透過證照了解如何評估風險，使用基於風險的稽核，同時去了解 GRC 的重要性，協助組織保護和控制資訊系統

統計至2022年4月止，台灣持有CISA證照之ISACA會員人數為273人

https://www.caa.org.tw/cisa-license.php?id=CISA

CISM 國際資安經理人

建立國際通用且正確的治理觀念，能夠清楚了解管理與治理的重點、方向，學習「資訊安全治理、管理、規劃（Program）、事故管理」，訓練高階管理思維，從Top-Down 方式評估企業資訊安全風險。

統計至2022年4月止，台灣持有CISM證照之ISACA會員人數為126人

https://www.caa.org.tw/cisa-license.php?id=CISM

提升風險管理深度與換位思考

CRISC 國際資訊風險控制師

風控（CRO）專家、熱愛「風險管理」的資安顧問，資安從業者，那可以考慮取得 CRISC。CRISC 所聊的風險管理，也延伸了 CISM 、CISA 知識，學習正確的 IT 風險評估、風險分析、探討 KCI （Key Control Indicators）與 KRI （Key Risk Indicators）設計，強化風險監控與回應細節。

統計至2022年4月止，台灣持有CRISC證照之ISACA會員人數為38人

https://www.caa.org.tw/cisa-license.php?id=CRISC

CGEIT 國際企業資訊治理師

了解企業治理、 IT 治理、資源與績效管理，是 IT 與維運需要的必要能力，讓 IT 對齊業務目標創造價值等議題。在有資安技術的單位中，對於資安設備維運也會用上其觀念，資安人也要能夠與 IT 同心協力，了解 IT 的目標與所面臨的困境。

統計至2022年4月止，台灣持有CGEIT證照之ISACA會員人數為28人

https://www.caa.org.tw/cisa-license.php?id=CGEIT

完整細節參考：ISACA證照學習組合包與教材總整理

CISA vs. ISO 27001 LA

- ✓ CISA 更注重要求考生理解組織業務與戰略目標， 書上會指導許多實務作法，不僅考慮單一框架，更強化各領域知識上所必要的深度。
- ✓ 成為(考取) CISA 的要求更具難度，考試內容包含風險管理知識、治理管理觀念與應具備的技術知識， 需要更深入地瞭解資訊系統的原理，並如何識別可能危害資訊系統的風險。
- ✓ 為世界公認的資訊領域稽核認證，並需要維持CPE。

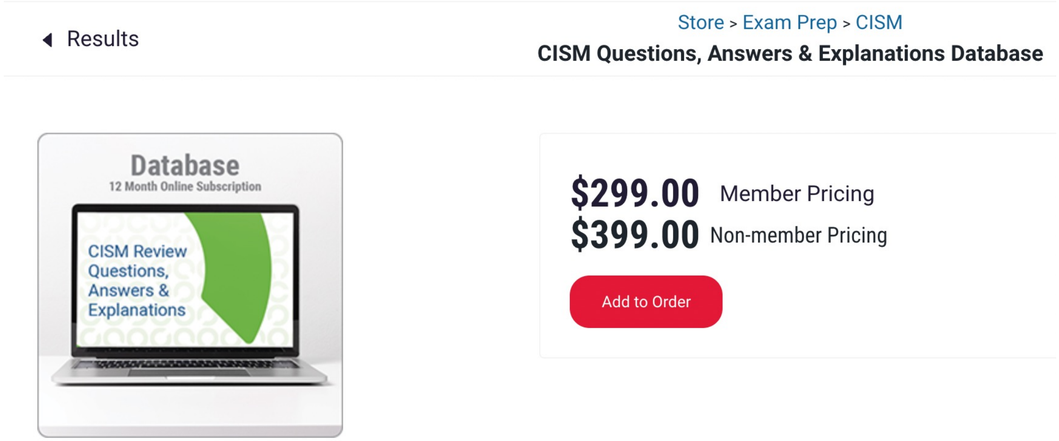
Kuro 對於CISSP 證照的觀點

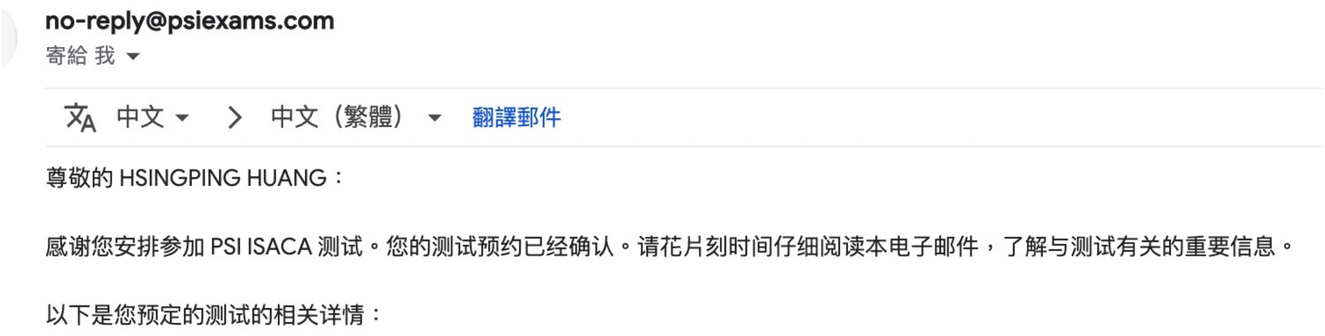
- ✓ CISSP 是管理考試，不是技術考試！思維轉換很重要
- ✓ 透過 CISSP 系統化學習不同領域基礎知識，為了提升自己在資安這行**基本溝通能力，資安要成功，要有良好的溝通！**
- ✓ CISSP / CISM等認證只是資安的起點，我認為是一張想入門資安管理所必要知道的基本知識，CISSP學廣但不深，但卻是這行所必備的核心基本知識！！（CISSP 後面還有進階認證！）
- ✓ 考完 CISSP / CISM 不會直接上大師，而是建立基本知識與良好的觀念，要持續研究想發展的領域，所以並不是所謂考上就成為頂級資安專家，專家要透過長時間的經驗累積與練習，考完證照只是奠定往後學習的基本能力，再發展所擅長的部分！
- ✓ CISSP 是資安管理基本功，打底的基礎，往後可延伸學習「資安資訊治理」、「深入風險管理」
- ✓ **資安管理師、資安顧問的基本證照**，顧問有正確的基本觀念才有辦法帶給客戶好的建議！

IT Security Architect, Engineer, and Management Certifications | CISSP Concentrations | (ISC)² (isc2.org)

如何順利的都一次考到管理證照？

- 真心想學習知識的心，工作經驗不能保證是學到國際上認可且正確的觀點
- 先刷卡報名考試，這是考上的第一步。
- ISACA 的證照請購買官方線上學習系統學習（Questions answers and explanations database）
- 確保你對齊官方觀點（特別是你有多張不同組織的證照），轉換管理思維
- 工作經驗可能會讓你考不過考試，因為大部分工作上並沒有對齊官方觀點，也很可能並非使用對的方式去執行資安
- 不管多少內容，每天持續不間斷的練習





那...考證照有用嗎?

“

“你會不知道自己不知道什麼。因此，用證照來梳理我至少最低需要知道什麼，或者某個角色需要具備什麼能力，也是我自己為什麼會去考的原因” – Alan Tsai

“從證照學習的過程中比考到證照更重要”

Source :
https://medium.com/blacksecurity/benefits-of-certifications-ec8880639df8
https://blog.alantsai.net/posts/2020/02/microsoft-certification-01-should-i-get-certified-index-page-of-series-post
https://blog.miniasp.com/post/2016/03/22/Does-Certification-Exam-Useful

透過證照這個手段推自己一把

- 有根據的學習正確觀念與思維
- 找到自己還欠缺什麼能力
- 建立明確的學習目標推動自己向前走
- 幫助判斷同事或廠商/顧問提的建議是否觀念正確
- 有憑有據，溝通時能提出觀點的參考來源

Source :
https://medium.com/blacksecurity/goodauditor-134c07fdf0d0

好啦，所以...我適合？

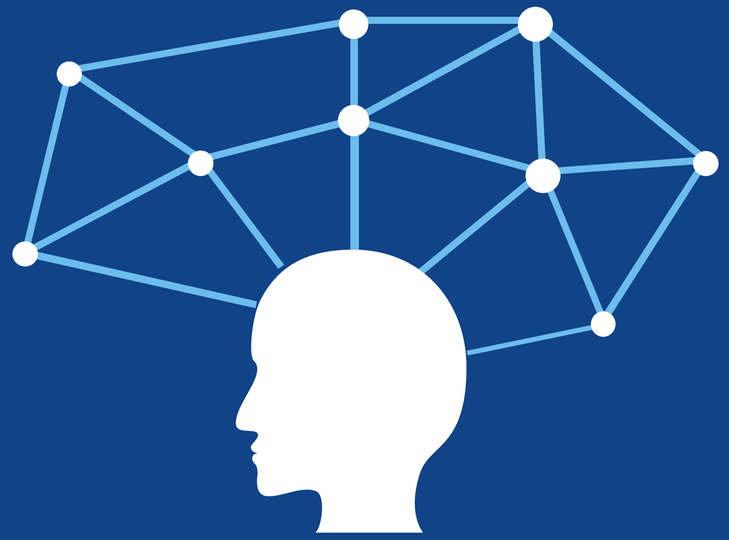
白話文聊聊

- ✓ 我愛稽核想要成為評估王：CISA （必要）+ CRISC （可選）
- ✓ 工作夠用就好，強化治理、管理面與業務面的溝通能力：CISM
- ✓ 目標是風險管理（~~神奇寶貝~~）大師：CRISC + CISM/CISA（二選一）
- ✓ 很肝資安顧問：CISA + CISM
- ✓ 技術人與 IT 維運人：CISM +CGEIT
- ✓ 資源利用與效益實現：CGEIT
- ✓ 管理通用基本功：CISSP

角色職責

- ➢電腦/資安稽核（IT Auditor）：CISA
- ➢資安管理/維運（CISO） ：CISM
- ➢風控單位（CRO） ：CRISC
- ➢資訊管理（CIO） ：CGEIT

學習歷程



learning journal （ISACA）

April

01

CISM
專注於學習的資安治理與規劃的觀念。

CISA
各領域觀念打底，了解稽核方法，學習評估各領域可能面臨的風險。

02

August

September

03

CRISC
深入了解風險管、風險控制、風險監控與風險回應的議題。

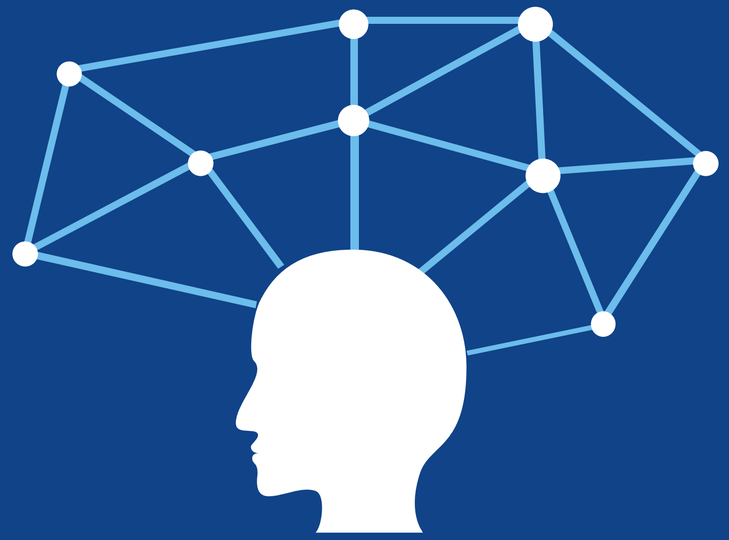
CGEIT
了解 IT 目標，提升資源管理、價值交付與資源優化

04

October

入門學習資安治理與管理： ISACA 證照學習組合包與教材總整理 (CISA/CISM/CRISC/CGEIT)
https://medium.com/blacksecurity/cybersecurity-isaca-governance-4d81fd50ec91

技術人思維轉型



當技術人學會治理與管理

技術能力

具有一定能量的技術底子可以幫助執行風險評鑑、評估控制措施與提升資安管理的深度，與 IT 等技術單位溝通也會更順暢，一起討論弱點與修復方式，結合基於風險的思考與技術力，最大化人才的資安能力。

管理能力

學習對齊戰略、風險管理、風險評鑑、評估控制措施等方式，並找出失效的根因，如流程中的控制不當、應實施持續風險監控等。透過成本效益分析與評估資源優先順序，提升與稽核、客戶、高階管理層的溝通順暢度。

雙管齊下

當同時具有技術與正確的管理、治理思維後，在對於風險的識別、各單位(客戶)溝通、提出解決方案與供應商管理上將大大加分，知己知彼了解彼此。

成本效益

能夠根據目前的業務環境風險去評估優先順序，從成本效益的觀點思考，提升自身說服力與主管/客戶之間的溝通效率。

規劃能力

搭配自身技術經驗，將更有能力判斷中長期資安規劃的合理性，用對的方式提出務實且有成本效益的解決方案。

高階管理層意向

了解管理與治理的思考邏輯，提案時後判斷高階管理層或客戶的意向，減少被否決的機會。

Thanks!

Any questions? Welcome!

You can find me at :

- contact@kuronetwork.me
- https://kuronetwork.me
- FB: Kuro的資安學習手記
- Kuro Huang | LinkedIn

如果真心想要學習
我一定會幫你！