CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

CYBER TALENT

資安小白看過來~資安職涯起手式，資安證照與故事

TEAM CYBERSECURITY

黃景偉(Edward), CISSP, CC, CISM, CISA, CRISC, CDPSE,
iPAS資安中級, ISO27001/27701, AWS CCP/SAA

NCU資訊管理學系

AI與資安研究生

海南黃花梨

桃花心木

Ref: https://www.chinatimes.com/realtimenews/20181105003828-260514?chdtv, https://www.taiwanwood.org.tw/product/product2/

選擇　比努力重要!!!

男怕入錯行，女怕嫁錯郎

Agenda

- **職涯起手式**

  半路出家當和尚，也能敲鐘響四方
- **資安大叢林**

  前路茫茫無目標，迷霧中行步難挑
- **逆風也飛翔**

  專業證照來加持，年資多少都不遲
- **選擇大航道**

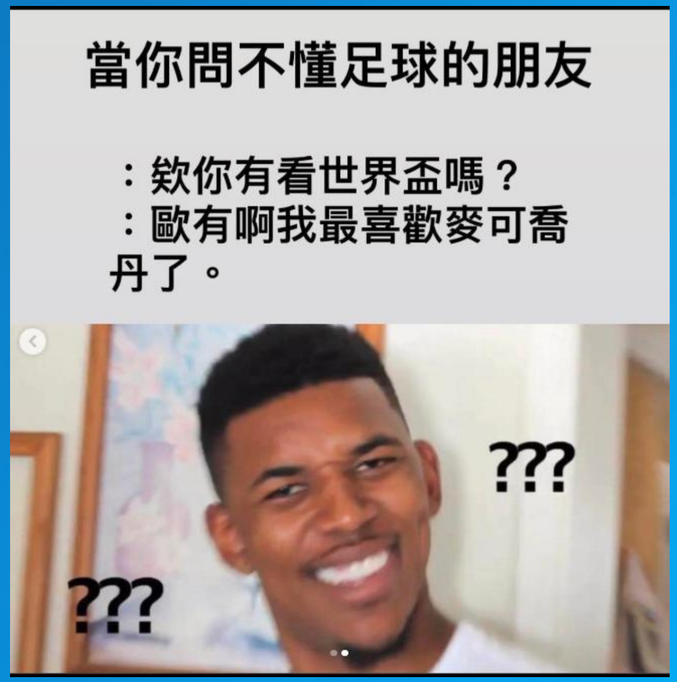
  風浪起伏多挑戰，明確目標破險關

CYBERSEC 2025
臺灣資安大會

聽了這麼多場演講，是否也曾經有以下經驗?

好像聽懂了，但卻又感覺虛虛的

聽懂了講者所表達
不過不知道該怎麼實踐



Agenda

- **職涯起手式**

  半路出家當和尚，也能敲鐘響四方
- **資安大叢林**

  前路茫茫無目標，迷霧中行步難挑
- **逆風也飛翔**

  專業證照來加持，年資多少都不遲
- **選擇大航道**

  風浪起伏多挑戰，明確目標破險關

Goal

- **職涯起手式**

  Information Technology➔Infra、AP、Cloud、Security、AI…..

- **資安大叢林**

  展望全局、細分職能

- **逆風也飛翔**

  展現專業、發光發熱

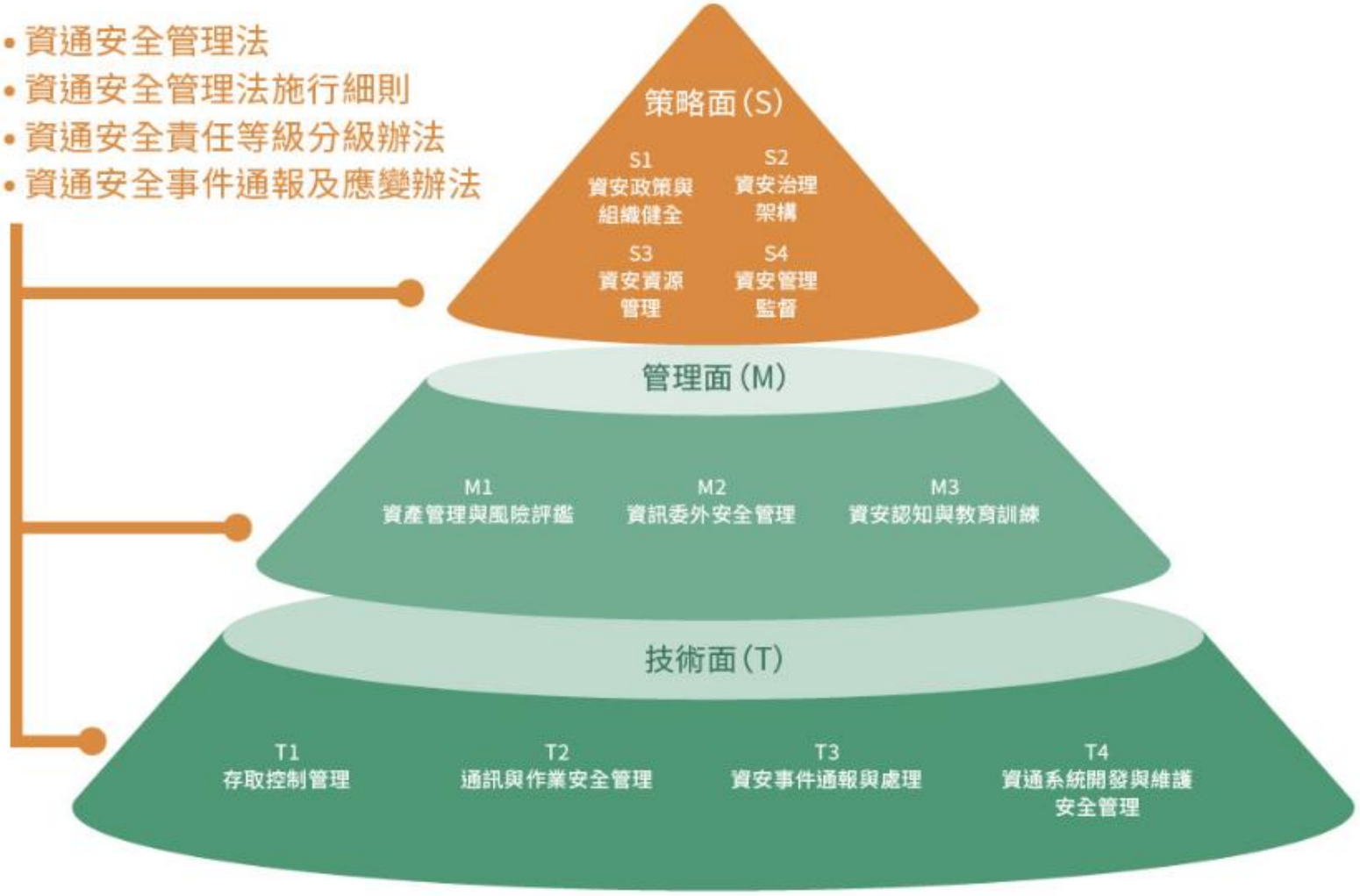
- **選擇大航道**

  資安迷宮，邁向成功

職涯起手式：資訊科技當前三大趨勢

資安大叢林：展望全局架構職能

- 資通安全管理法
- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法



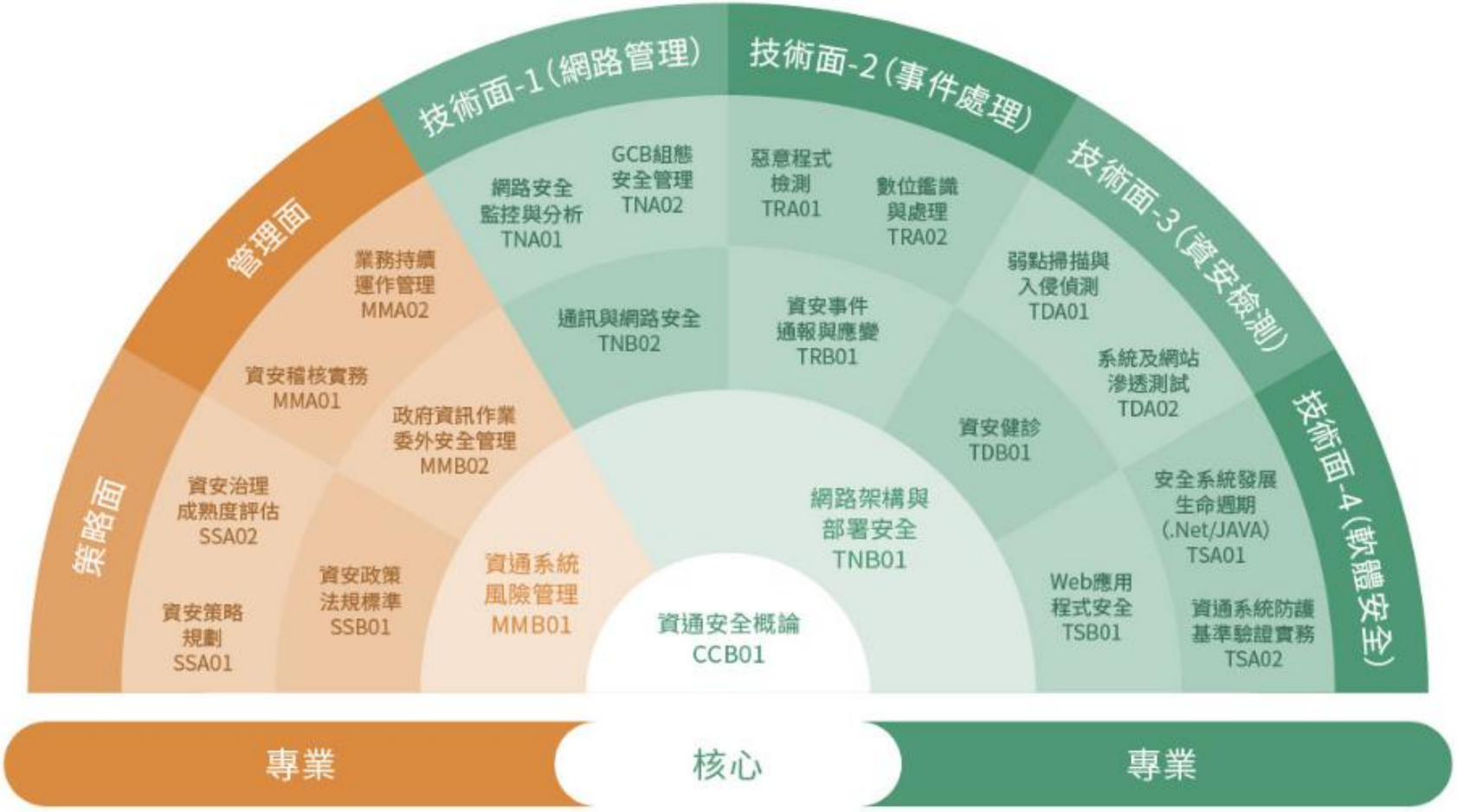
Ref: https://moda.gov.tw/ACS/operations/training/654

資安大叢林：從核心職能走向專業

面向	策略面應備能力	管理面應備能力	技術面應備能力
核心職能	• 具備資通安全基本認知及資通安全法規認知		
專業職能	• 具資安策略規劃與推動能力 • 具資安管理業務審查能力 • 具資安資源協調規劃能力 • 具績效與成果監督能力	• 具資安管理機制規劃與維運能力 • 具資安資源配置與管理能力 • 具資安風險與控制評估能力 • 具業務持續運作管理能力 • 具資安稽核與管理能力	• 具網路管理能力 • 具事件處理能力 • 具資安檢測能力 • 具軟體安全管理能力 • 具系統安全管理能力 • 具情資分析與分享能力

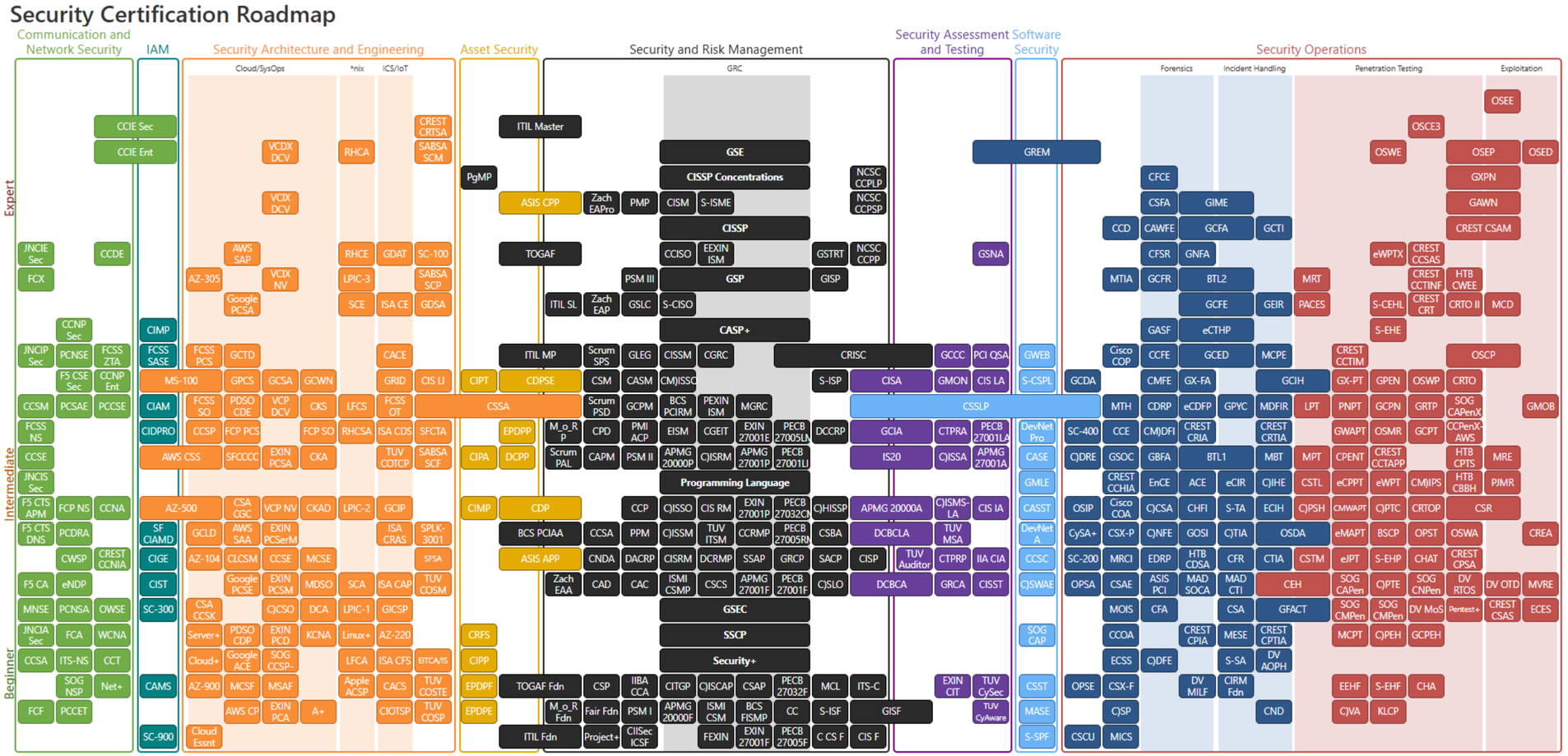
Ref: https://moda.gov.tw/ACS/operations/training/654

資安大叢林：技術職能再細化



Ref: https://moda.gov.tw/ACS/operations/training/654

逆風也飛翔：資安證照路線圖



Ref: https://pauljerimy.com/security-certification-roadmap/

逆風也飛翔：國家認同清單

資通安全專業證照清單

日期：114年1月24日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
1.	已簽署國際認證論壇(International Accreditation Forum, IAF)多邊相互承認協議(ISO/IEC 27006範圍)之認證機構(含TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構[1]	1. ISO/IEC 27001:2013 Information Security Management System (ISMS) Auditor/Lead Auditor (請於114年10月31日前完成轉版) 2. ISO/IEC 27001:2022 Information Security Management System (ISMS) Auditor/Lead Auditor 3. ISO 22301 Business Continuity Management System (BCMS) Auditor/Lead Auditor 4. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor Lead Auditor 相關證照應具有效性，除提出證照外，尚須提供當年度至少有2次實際參與該證照內容有關之稽核經驗證明。	
2.	International Information System Security Certification Consortium (ISC2)[2]	1. Certified Information Systems Security Professional (CISSP) 2. Information Systems Security Management Professional (CISSP-ISSMP) 3. Governance, Risk and Compliance Certification (CGRC)	1. Systems Security Certified Practitioner (SSCP) 2. Certified Cloud Security Professional (CCSP) 3. Certified Authorization Professional (CAP) (認可至114年11月7日止) 4. Certified Secure Software Lifecycle Professional (CSSLP) 5. HealthCare Information Security and Privacy Practitioner (HCISPP) (認可至115年12月1日止) 6. Information Systems Security Architecture Professional (CISSP-ISSAP) 7. Information Systems Security Engineering Professional (CISSP-ISSEP)

資通安全專業證照清單

日期：114年1月24日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
3.	The Computing Technology Industry Association (CompTIA)[3]		1. CompTIA Security+ 2. CompTIA Cybersecurity Analyst (CompTIA CySA+) 3. CompTIA Advanced Security Practitioner (CompTIA CASP+) 4. CompTIA PenTest+
4.	CREST[4]		1. Penetration Testing (1) The CREST Practitioner Security Analyst (CPSA) (2) The CREST Certified Wireless Specialist (CCWS) (認可至114年11月7日止) (3) The CREST Certified Simulated Attack Specialist (CCSAS) (4) The CREST Certified Simulated Attack Manager (CCSAM) 2. Threat Intelligence (1) The CREST Registered Threat Intelligence Analyst (CRTIA) (2) The CREST Certified Threat Intelligence Manager (CCTIM) 3. Incident Response (1) The CREST Practitioner Intrusion Analyst (CPIA) (2) The CREST Registered Intrusion Analyst (CRIA) (3) The Certified Network Intrusion Analyst (CCNIA) (認可至114年11月7日止) (4) The CREST Certified Host Intrusion Analyst (CCHIA) (認可至114年11月7日止) (5) The CREST Certified Malware Reverse Engineer (CCMRE) (認可至114年11月7日止) (6) The CREST Certified

管理：22

技術：89

總數：111

Ref: https://www-api.moda.gov.tw/File/Get/acs/zh-tw/epCm7MlcYGOKmPH

逆風也飛翔：洞察市場需求、進行有效投資

條件要求

工作經歷　10年以上

學歷要求　大學、碩士

科系要求　資訊工程相關、應用數學相關

語文條件　英文 -- 聽 /中等、說 /中等、讀 /中等、寫 /中等

贊助 提升英文能力

擅長工具　Firewall、WAP、IPS

贊助 提升專業能力

工作技能　不拘

其他條件　1.10年以上金融業資訊安全管理相關工作經驗
2.具資安管理工作經驗，有相關證照(CEH、CISSP等)尤佳
3.熟悉各項資安技術與資安法規要求
4.具規劃、管理能力及主動積極、抗壓性
5.通過「銀行內部控制與內部稽核測驗」尤佳

條件要求

工作經歷　不拘

學歷要求　大學、碩士

科系要求　不拘

語文條件　不拘

擅長工具　Cisco、Ethernet、Firewall、LAN、Routers、TCP/IP、VLAN、WAN

贊助 提升專業能力

工作技能　不拘

具備證照　CCNA、CCNP、CCIE、Master ASE

模擬試題免費檢測

其他條件　未填寫

條件要求

工作經歷　2年以上

學歷要求　大學、碩士

科系要求　資訊管理相關、資訊工程相關

語文條件　不拘

擅長工具　不拘

工作技能　不拘

具備證照　ISO 27001資訊安全管理系統主導稽核員

模擬試題免費檢測

其他條件　1. 具備良好專案規劃管理、溝通表達及情緒管理能力。
2. 曾協助組織維運資訊安全管理、個資保護管理制度，並通過 ISO27001 或個資保護管理制度驗證者。
3. 曾擔任資安或個資相關稽核員，並有稽核報告撰寫能力者。
4. 須已通過 ISO27001:2013 或 BS10012:2017 / ISO27701 主導稽核員課程訓練並取得證書，具備國際資安相關證照者，例如：CISA、CISM、CGEIT、CISSP等尤佳。
5. 須具備資訊安全工作服務經驗 2 年以上。
6. 曾擔任顧問輔導方，協助組織通過 ISO27001 個資保護管理制度驗證者佳。
7. 曾協助組織規劃資安教育訓練課程者佳。

條件要求

工作經歷　2年以上

學歷要求　大學、碩士

科系要求　資訊管理相關、資訊工程相關

語文條件　不拘

擅長工具　不拘

工作技能　不拘

具備證照　ISO 27001資訊安全管理系統主導稽核員

模擬試題免費檢測

其他條件　1. 具備良好專案規劃管理、溝通表達及情緒管理能力。
2. 曾協助組織維運資訊安全管理、個資保護管理制度，並通過 ISO27001 或個資保護管理制度驗證者。
3. 曾擔任資安或個資相關稽核員，並有稽核報告撰寫能力者。
4. 須已通過 ISO27001:2013 或 BS10012:2017 / ISO27701 主導稽核員課程訓練並取得證書，具備國際資安相關證照者，例如：CISA、CISM、CGEIT、CISSP等尤佳。
5. 須具備資訊安全工作服務經驗 2 年以上。
6. 曾擔任顧問輔導方，協助組織通過 ISO27001 個資保護管理制度驗證者佳。
7. 曾協助組織規劃資安教育訓練課程者佳。

條件要求

工作經歷　不拘

學歷要求　大學、碩士

科系要求　數學及電算機科學學科類、資訊管理相關、工程學科類

語文條件　英文 -- 聽 /中等、說 /中等、讀 /中等、寫 /中等

贊助 提升英文能力

擅長工具　不拘

工作技能　不拘

具備證照　CEH、ECIH 資安危機處理員認證、CHFI、Security+

模擬試題免費檢測

其他條件　工作技能：System administration, log analysis, automation
其他條件：
1.Project management experience preferred
2.Fluent Chinese and intermediate English (TOEIC score 600 or above)
3.Open to all nationalities with legal residency in Taiwan
4.Excellent communication and leadership skills; strong problem-solving ability; self-motivated with clear logical thinking; resilient under pressure; eager to take on challenges and committed to continuous learning
5.Proficient in automation scripting languages: Python, JavaScript, PowerShell, or BASH

條件要求

工作經歷　2年以上

學歷要求　大學以上

科系要求　不拘

語文條件　不拘

擅長工具　不拘

工作技能　不拘

其他條件　*在資安領域，特別是SOC操作和SOAR技術方面有著豐富的經驗。
*對安全事件的偵測、分析和應變過程有深入的理解。
*具備script和自動化工具的使用經驗。
*熟悉常見的資安框架和標準。
*能獨立解決問題和注重細節。
*強大的溝通和協作能力。
*有相關認證（例如OSCP、CISSP、CEH、GCIH、GCFA等）將會是加分項目。

Ref: 104網站

選擇大航道：資安管理三部曲-1

初階證照（入門適合，較少/無需實務經驗）	
CC(Certified in Cybersecurity)	資安通識初級概念，適合剛接觸資安領域的人員
ITIL Foundation	資訊服務管理的基礎證照，適合初學者
ECIH (EC-Council Certified Incident Handler)	資安事件應變的入門證照，適合剛接觸資安領域的人員
EDRP (EC-Council Disaster Recovery Professional)	災難復原與業務持續計畫的基礎證照，適合初學者
iPAS初級資安工程師	資訊安全初級人員認證，適合有志於從事資安工作的初學者

選擇大航道：資安管理三部曲-2

中階證照（需一定經驗，職場需求高）	
ISO/IEC 27001、27701、22301 Lead Auditor	資訊安全管理系統、隱私資訊管理系統、業務持續營運管理系統的主導稽核員認證適合有稽核經驗的人員
CGEIT （Certified in the Governance of Enterprise IT）	企業IT治理的認證，適合中階管理人員
CDPSE （Certified Data Privacy Solutions Engineer）	資料隱私解決方案工程師認證，適合有隱私保護經驗的人員
TOGAF （The Open Group Architecture Framework）	企業架構框架的認證，適合有一定經驗的資安人員
GLEG （GIAC Law of Data Security & Investigations）	資料安全與調查法律的認證，適合有相關法律知識的人員

選擇大航道：資安管理三部曲-3

高階證照（難度高，需豐富實務經驗）	
CISSP （Certified Information Systems Security Professional）	資安領域的高階認證，適合有豐富經驗的資安專業人員
CISM （Certified Information Security Manager)	資訊安全管理的高階認證，適合資安管理人員
CISA （Certified Information Systems Auditor）	資訊系統稽核的國際認證，適合有一定經驗的資安人員
CRISC （Certified in Risk and Information Systems Control）	資訊風險與控制的高階認證，適合風險管理人員
CGRC(Certified Governance, Risk and Compliance Certification)	治理、風險與合規管理實務認證，適合經驗豐富的資安專業人員

選擇大航道：資安技術三部曲-1

初階證照（入門適合，較少/無需實務經驗）	
CompTIA Security+	入門最熱門，涵蓋基本資安觀念、網路防護、身份驗證
eJPT	滲透測試入門，純實作導向，非常適合紅隊初學者
Cisco CyberOps Associate (CBROPS)	資安適合走向藍隊（SOC）方向，含 log 分析、事件識別
Microsoft SC-900 / AZ-900 AWS CCP / SAA / SAP	雲端平台入門與安全基礎知識
SSCP（Systems Security Certified Practitioner）	比 Security+ 再進階一點，需 1 年工作經驗（可先當 Associate）
CEH（Certified Ethical Hacker）	紅隊基礎知識與工具操作，認知類強、實作較弱

選擇大航道：資安技術三部曲-2

中階證照（具備部分經驗者適合）	
CySA+（Cybersecurity Analyst）	偏向藍隊與資安監控、威脅偵測
GCIA（Intrusion Analyst） GCIH（Incident Handler）	入侵分析、封包解析、IDS 操作能力、實務事件處理與應變、攻擊分析
PenTest+	滲透測試入門證照，偏技術應用
CND（Certified Network Defender）	藍隊網路層級防禦與配置強化
iPAS中級資安工程師	管理實務與防護技術實務相融合，適合有豐富經驗的資安人員

選擇大航道：資安技術三部曲-3

高階證照（需豐富實務經驗，難度高）	
OSCP（Offensive Security Certified Professional）	滲透測試界最具權威的實作型證照，高實戰難度
GPEN（Penetration Tester） GCFA（Forensic Analyst） GREM（Reverse Engineering Malware）	滲透測試中高階，含工具與報告撰寫 進階鑑識分析，需熟悉 disk/memory 分析 惡意碼分析專家等級
CCSP（Certified Cloud Security Professional） CSSLP（Secure Software Lifecycle Professional）	雲端資安高階認證，與雲平台治理、法規相關 開發與 DevSecOps 專業認證，涵蓋 SDLC
OSEP / OSWE / OSED	滲透進階（如針對 AD、開發漏洞分析）
Licensed Penetration Tester Master（LPT (Master)）	已具備 CEH、CPENT、或 OSCP 等滲透經驗的資安專家

考取證照 真的有用嗎?

- 故事一

  一位夥伴(非資訊/資安背景)自從進行考照準備/學習後，某次跟廠商的討論，

  無意發現產品規格寫著SHA-256加密，廠商表示回去再確認....

- 故事二

  某高科技製造業，導入ISO過程，請來顧問協助導入，業務持續營運RTO/RPO填報，

  IT部門全然不知.....

- 故事三

  某甲方承辦於某次跟源碼安全廠商進行個案討論交流，廠商露出不可置信的神情，

  問著承辦，為什麼你懂這麼多.....

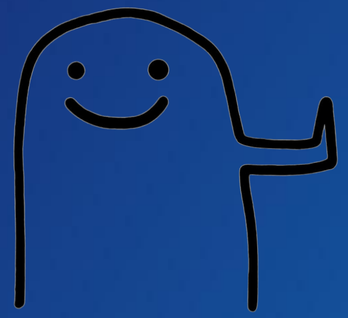
哈佛校長的開學致辭：

教育的目標，就是確保學生能分辨「有人在胡說八道」

to ensure that graduates can recognize when “someone is talking rot.” You learn this through challenging and being challenged, through being confronted by disagreement and difference and amidst it all finding your way.

Ref: https://www.inside.com.tw/article/10573-harvard-freshman-convocation-address-to-class-2021

别说了 沒钱



No Money

No Security

TCAYLBENRT

ISC2 CHAPTER | TAIPEI

【關於我們】

ISC2 Taipei Chapter 是 ISC2 在台灣的分會組織，致力於推廣資安專業知識、交流與社群互助。成員包括經 ISC2 認證的資安專家，及各領域資安專業人士。

【成立宗旨】

提升台灣資安專業社群的能見度與凝聚力。

【使命與活動】

- 推廣資安認證與專業發展
- 舉辦技術講座、各種資安研討活動
- 促進會員交流與跨界合作
- 參與國際資安社群互動

https://www.isc2chapter.tw


contact@isc2chapter.tw

加入 ISC2 Taipei Chapter 讓您的資安之旅，有專家同行！

CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

THANKS FOR YOUR ATTENTION