如何量化資安風險

達文西個資暨高科技法律事務所　所長
葉奇鑫 (奇哥/Simon)

2021/5

歡迎訂閱【達文西個資週報】

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

ISACA

中華民國電腦稽核協會
Computer Audit Association

- 1995年律師、司法官考試及格
- 美國富蘭克林皮爾斯法學院研究
- 東吳大學法學碩士
- 交通大學電子工程系工學士

現任

- 達文西個資暨高科技法律事務所 所長
- 東吳大學 法律系兼任助理教授
- 電腦稽核協會理事長（ISACA臺灣分會會長）
- 國發會 個資法諮詢委員
- 智慧局著作權 顧問暨調解委員
- 永豐金控 董事
- 台灣網際網路暨電子商務協會 監事
- 高科技法務經理人協會 理事
- 台灣雲端安全聯盟 理事

曾任

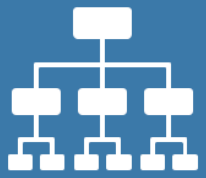
- 露天拍賣 營運長
- eBay交易安全長
- 法務部檢察司、資訊處檢察官
- 板橋地檢署電腦犯罪與智慧財產權專組檢察官
- 「霍夫曼計算法」程式設計人
- 刑法第36章妨害電腦使用罪章草擬人

大綱

1. 人類喜歡量化
2. 風險量化：資安治理手段
3. 資安風險量化之現實困境
4. 資安風險量化之實作挑戰
5. 做好資安風險量化的關鍵
6. 未來：是否還有更佳框架？

人類喜歡量化

量化的優點



1

一目了然

2

客觀

3

協助
有效決策

最擅長量化風險的產業

- **金融業是最擅長量化風險的產業**
  - BSM(Black-Scholes-Merton) 公式

$$C(S,K,t,T,r,\sigma) = S(t)N(d_1) - Ke^{-r(T-t)}N(d_2)$$

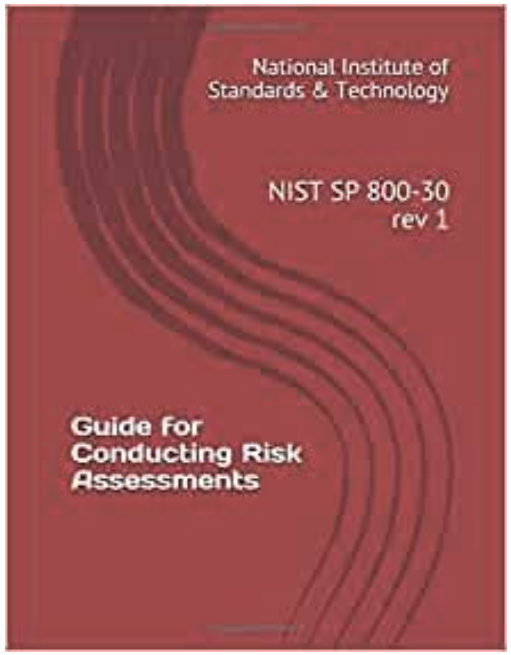
$$d_1 = \frac{\ln\left(\frac{S}{K}\right) + \left(r + \frac{\sigma^2}{2}\right)(T-t)}{\sigma\sqrt{T-t}},\ d_2 = d_1 - \sigma\sqrt{T-t}$$

S(t): 股票在時刻t的價格　　t: 當前時間　　r: 無風險利率
K: 行權價格　　T: 到期時間　　σ: 股票波動率

風險量化
資安治理手段

主流風險量化框架

- COBIT 2019
- ISO 27005
- NIST SP800-30
- OCTAVE
- OWASP



資安風險量化之現實困境

資安風險量化之現實困境

- Uneven contours of risk scoring methods
  風險評估方法不一致
- Inconsistent and/or incompatible risk scales
  風險級距劃分不統一
- Obsession with data 只重資料輕忽分析
- Misconceptions of data as a result of cognitive disparities 資料認知偏差未排除
- Measuring too much, too soon; measuring too little, too late 資料規模與品質不理想

資安風險量化之實作挑戰

資安風險量化之實作挑戰

- Uncertainties inherent to probabilistic approach
  或然率方法本質之不確定性
- Greater coordination required by multifactorial data fusion 多因素資料分析之協調難度
- Limitations of data without empirical input
  經驗不足導致資料分析之限制
- Talents in short supply
  相關人才稀缺

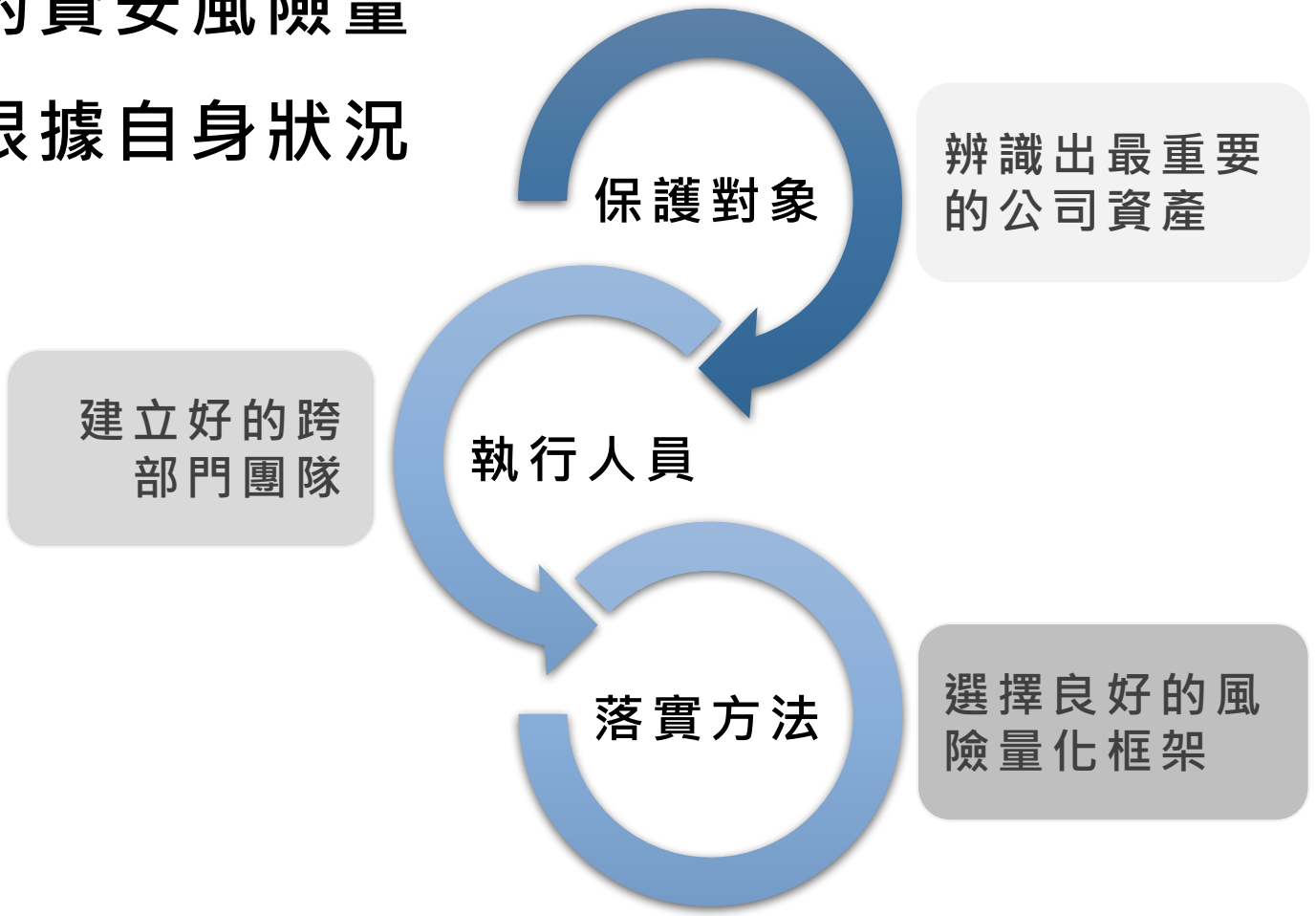
做好資安風險量化的關鍵

客觀分析三項基本要件

- 風險＝威脅＋漏洞＋資產

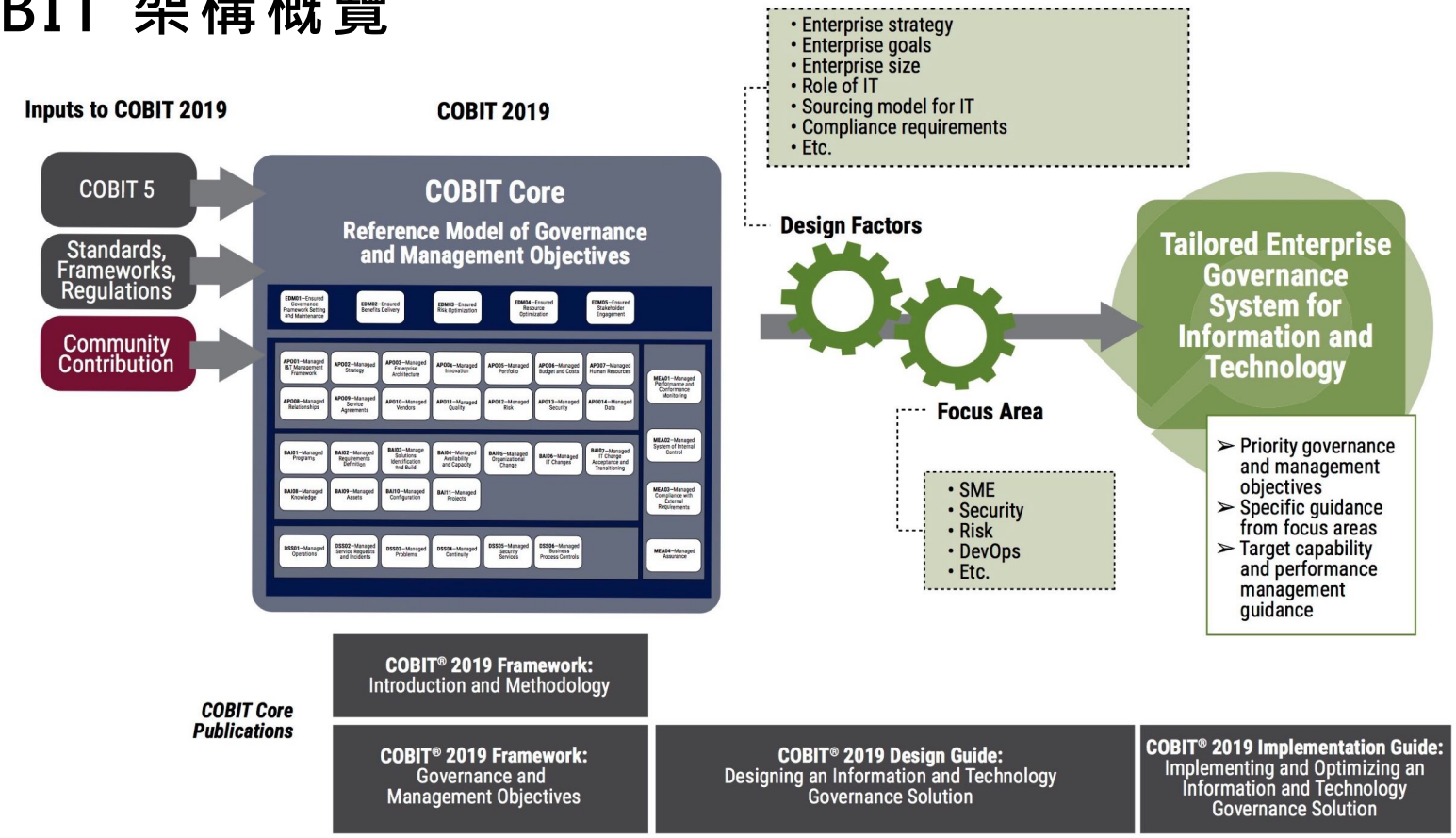
綜合評估三類構成要素

- 每家公司的資安風險量化都需要根據自身狀況量身訂做



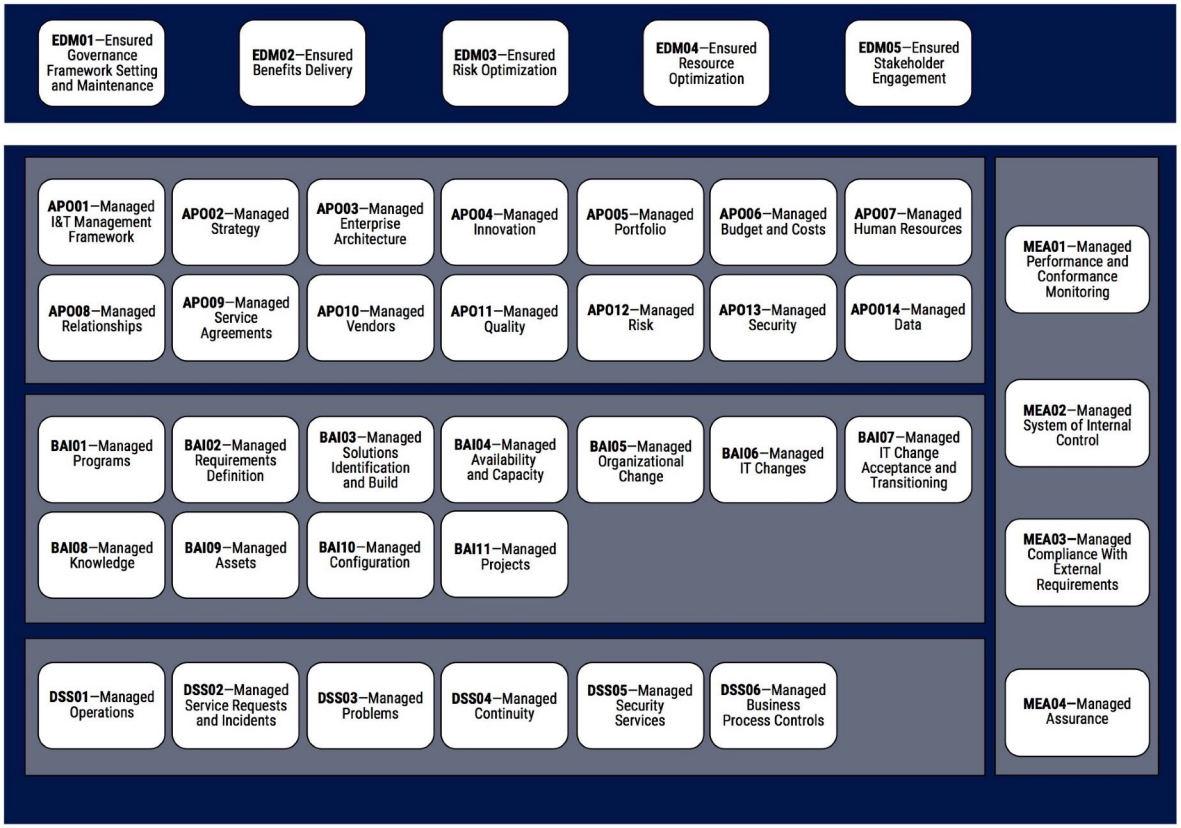
選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 架構概覽



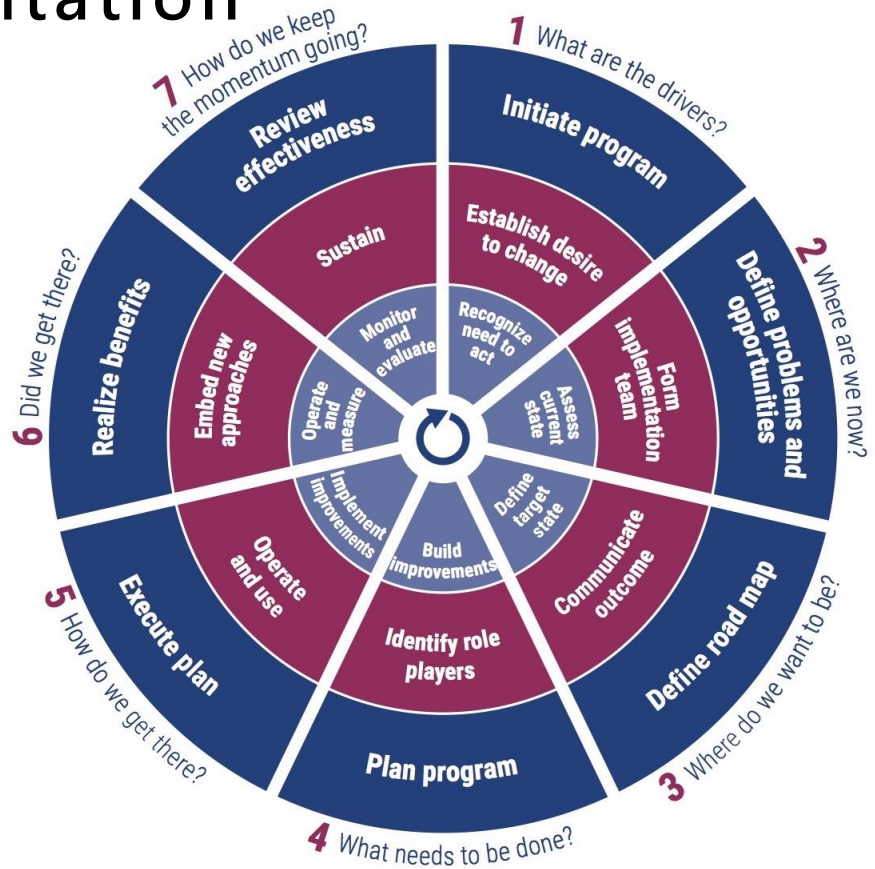
選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 核心要素



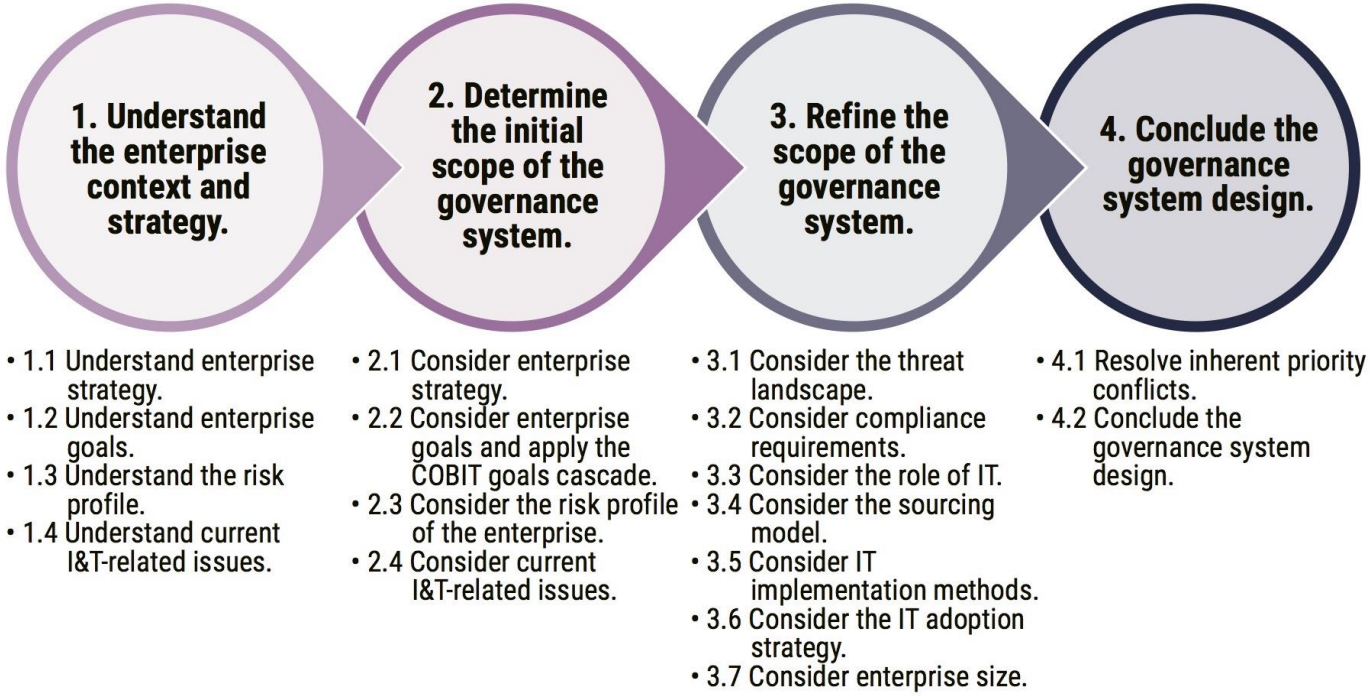
選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT Implementation Road Map



選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 資安治理系統設計流程



選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 風險類別示例

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	5	3	●
Program and projects lifecycle management	4	2	●
IT cost and oversight	5	1	●
IT expertise, skills and behavior	4	4	●
Enterprise/it architecture	4	2	●
IT operational infrastructure incidents	4	2	●
Unauthorized actions	4	3	●
Software adoption/usage problems	3	2	●
Hardware incidents	4	2	●
Software failures	3	2	●
Logical attacks (hacking, malware, etc.)	3	4	●
Third-party/supplier incidents	4	2	●
Noncompliance	2	3	●
Geopolitical issues	2	2	●
Industrial action	2	1	●
Acts of nature	2	1	●
Technology-based innovation	5	3	●
Environmental	3	1	●
Data and information management	4	3	●

●	Very High Risk
●	High Risk
●	Normal Risk
●	Low Risk

選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

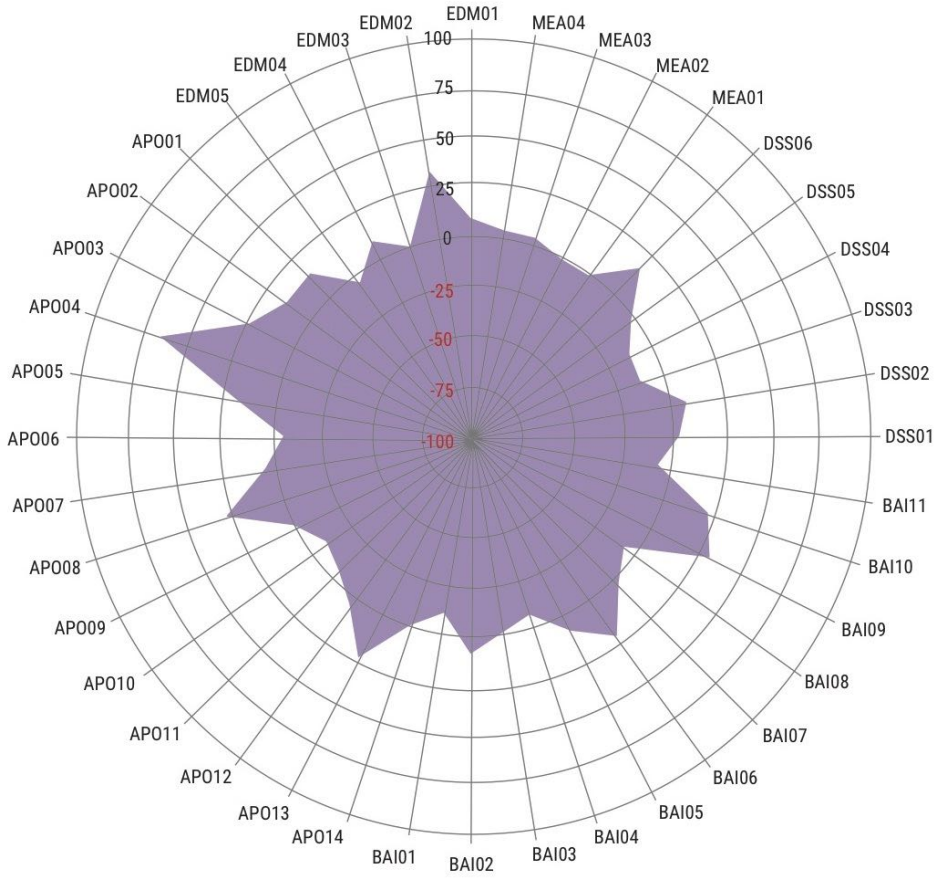
- COBIT 資安風險評分標準示例

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✔	*2*
Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	✔	*2*
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	!	*2*
Service delivery problems by the IT outsourcer(s)	!	*2*
Failures to meet IT-related regulatory or contractual requirements	✔	*2*
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✔	*2*
Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	!	*2*
Duplications or overlaps between various initiatives, or other forms of wasted resources	✔	*2*
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	X	*2*
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	!	*2*
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	!	*2*
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✔	*2*
Excessively high cost of IT	!	*2*
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	X	*2*
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	!	*2*
Regular issues with data quality and integration of data across various sources	X	*2*
High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	✔	*2*
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	✔	*2*
Ignorance of and/or noncompliance with privacy regulations	✔	*2*
Inability to exploit new technologies or innovate using I&T	!	*2*

✔	No Issue
!	Issue
X	Serious Issue

選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 風險評分結果示例



選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 資安風險量化結果示例

DF3	RISKCAT01 IT Investment Decision Making, Portfolio Definition & Maintenance	RISKCAT02 Program & Projects Life Cycle Management	RISKCAT03 IT Cost & Oversight	RISKCAT04 IT Expertise, Skills & Behavior	RISKCAT05 "Enterprise/ IT Architecture "	RISKCAT06 IT Operational Infrastructure Incidents	RISKCAT07 Unauthorized Actions	RISKCAT08 "Software Adoption/ Usage Problems"	RISKCAT09 Hardware Incidents	RISKCAT10 Software Failures
EDM01	3	2	3	0	0	0	2	0	0	0
EDM02	3	2	0	0	2	0	0	0	0	0
ED0M3	2	2	0	0	0	0	0	0	0	1
EDM04	3	0	4	3	2	0	0	0	0	0
EDM05	3	1	3	0	0	0	2	0	0	1
APO01	2	3	2	0	2	2	4	2	0	2
APO02	2	0	0	0	3	0	0	2	1	0
APO03	2	0	0	0	4	0	0	2	0	2
APO04	0	0	0	0	1	0	0	0	0	0
APO05	4	2	2	0	2	0	0	2	2	0
APO06	2	3	4	0	0	0	0	0	0	0
APO07	0	0	0	4	0	2	3	3	0	0
APO08	0	0	0	2	2	0	0	4	0	0
APO09	0	0	2	0	0	0	2	3	0	1
APO10	0	2	3	0	0	0	2	2	3	2
APO11	0	3	0	0	0	0	0	2	0	4
APO12	0	0	0	0	0	0	3	0	0	2
APO13	0	0	0	0	0	0	4	0	0	0
APO14	0	0	0	0	0	0	3	2	0	0
BIA01	0	4	0	0	2	0	0	3	0	0
BAI02	2	2	0	0	2	0	0	3	0	2
BAI03	0	3	0	0	2	0	0	2	0	3
BAI04	0	1	0	0	0	0	0	0	0	0
BAI05	0	2	0	2	0	0	0	4	0	0
BAI06	0	0	0	0	0	3	4	0	0	2
BAI07	0	0	0	0	0	2	3	2	0	4
BAI08	0	0	0	2	0	3	0	3	0	3
BAI09	0	0	0	0	0	1	3	0	0	0
BAI10	0	0	0	0	0	2	4	0	0	2
BAI11	0	4	0	0	0	0	0	0	0	0
DSS01	0	0	0	0	0	4	3	0	4	0
DSS02	0	0	0	0	0	3	2	3	2	2
DSS03	0	0	0	0	0	3	1	4	0	3
DS0S4	0	0	0	0	0	3	3	0	3	0
DSS05	0	0	0	0	0	3	4	0	2	0
DSS06	0	0	0	0	0	3	4	2	0	0
MEA01	1	2	2	0	0	2	2	0	0	2
MEA02	1	2	2	0	0	3	3	0	0	2
MEA03	0	1	0	0	0	1	2	0	0	0
MEA04	1	2	0	0	0	0	3	0	0	2

DF3	RISKCAT11 Logical Attacks (Hacking, Malware, etc.)	RISKCAT12 "Third-Party/ Supplier Incidents"	RISKCAT13 Noncompliance	RISKCAT14 Geopolitical Issues	RISKCAT15 Industrial Action	RISKCAT16 Acts of Nature	RISKCAT17 Technology-Based Innovation	RISKCAT18 Environmental	RISKCAT19 Data & Information Management
EDM01	0	0	3	2	0	0	2	2	2
EDM02	0	0	1	0	0	0	3	1	3
ED0M3	2	0	3	3	0	0	0	2	3
EDM04	0	2	1	0	2	0	0	2	3
EDM05	0	1	3	3	0	0	0	2	2
APO01	3	3	3	0	0	0	3	2	3
APO02	1	2	0	0	0	0	2	2	1
APO03	2	2	0	0	0	0	2	0	3
APO04	0	0	0	0	0	0	4	0	0
APO05	0	0	0	0	0	0	2	0	0
APO06	0	2	0	2	0	0	2	2	0
APO07	2	0	0	2	4	0	2	2	0
APO08	2	2	0	0	0	0	3	0	2
APO09	2	3	0	0	0	0	0	0	0
APO10	2	4	2	2	0	0	0	0	0
APO11	0	0	0	0	0	0	0	0	2
APO12	3	0	0	0	0	2	0	0	0
APO13	4	0	3	0	0	0	0	0	0
APO14	2	0	3	0	2	4	2	0	4
BIA01	0	0	0	0	0	0	0	0	0
BAI02	2	0	0	0	0	0	0	0	0
BAI03	3	0	0	0	0	0	0	0	0
BAI04	0	0	0	0	0	0	0	0	0
BAI05	0	0	0	0	0	0	0	0	0
BAI06	3	0	0	0	0	0	0	0	3
BAI07	2	0	0	0	0	0	0	0	0
BAI08	0	0	0	0	2	0	0	0	2
BAI09	0	0	0	0	0	0	0	0	0
BAI10	3	0	0	0	0	0	0	0	0
BAI11	0	0	0	0	0	0	0	0	0
DSS01	2	0	0	0	0	0	0	2	0
DSS02	4	0	0	0	0	0	0	0	0
DSS03	1	0	0	0	0	0	0	0	0
DS0S4	4	0	2	0	3	4	0	0	2
DSS05	4	0	3	0	3	2	0	0	3
DSS06	2	0	2	0	0	0	0	0	3
MEA01	3	2	2	2	0	2	0	0	2
MEA02	3	2	2	3	0	2	0	0	2
MEA03	3	2	4	2	0	0	0	0	2
MEA04	3	2	2	4	0	2	2	0	2

選擇良好的風險量化框架
ISACA COBIT 2019評估框架初探

- COBIT 資安
  風險量化結果
  用於決策示例

Decision Topic	Scope	Responsible, Accountable, Consulted, Informed (RACI)							
		Executive Committee	I&T Governance Board	Enterprise Risk Committee	Portfolio Manager	Steering (Programs/Projects) Committee	IT Management[15]	Business Process Owners	Employees
Governance	• Integrating with enterprise governance • Establishing principles, structures, objectives	A/R	R	C			C	R	I
Enterprise strategy	• Defining enterprise goals and objectives • Deciding where and how I&T can enable and support enterprise objectives	A/R	R	C			C	R	I
I&T policies	• Providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders • Developing and rolling out I&T policies • Ensuring that policies result in beneficial outcomes in accordance with guiding principles • Enforcing I&T policies	I	A	C			R	C	C
I&T strategy	• Incorporating IT and business management in the translation of business requirements into service offerings and developing strategies to deliver these services in a transparent and effective manner • Engaging with business and senior management in aligning I&T strategic planning with current and future business needs • Understanding current I&T capabilities • Providing a prioritization scheme for business objectives that quantifies business requirements	I	A	C	I		R	C	C

未來：
是否還有更佳框架？

加入ISACA資安風險量化討論

Webinar

Quantifying Cyber Risk

Upcoming: June 10 2021

ISACA
資安風險量化
Webinar

時間：2021/06/10

連結：https://www.isaca.org/education/online-events/lms_w061021。

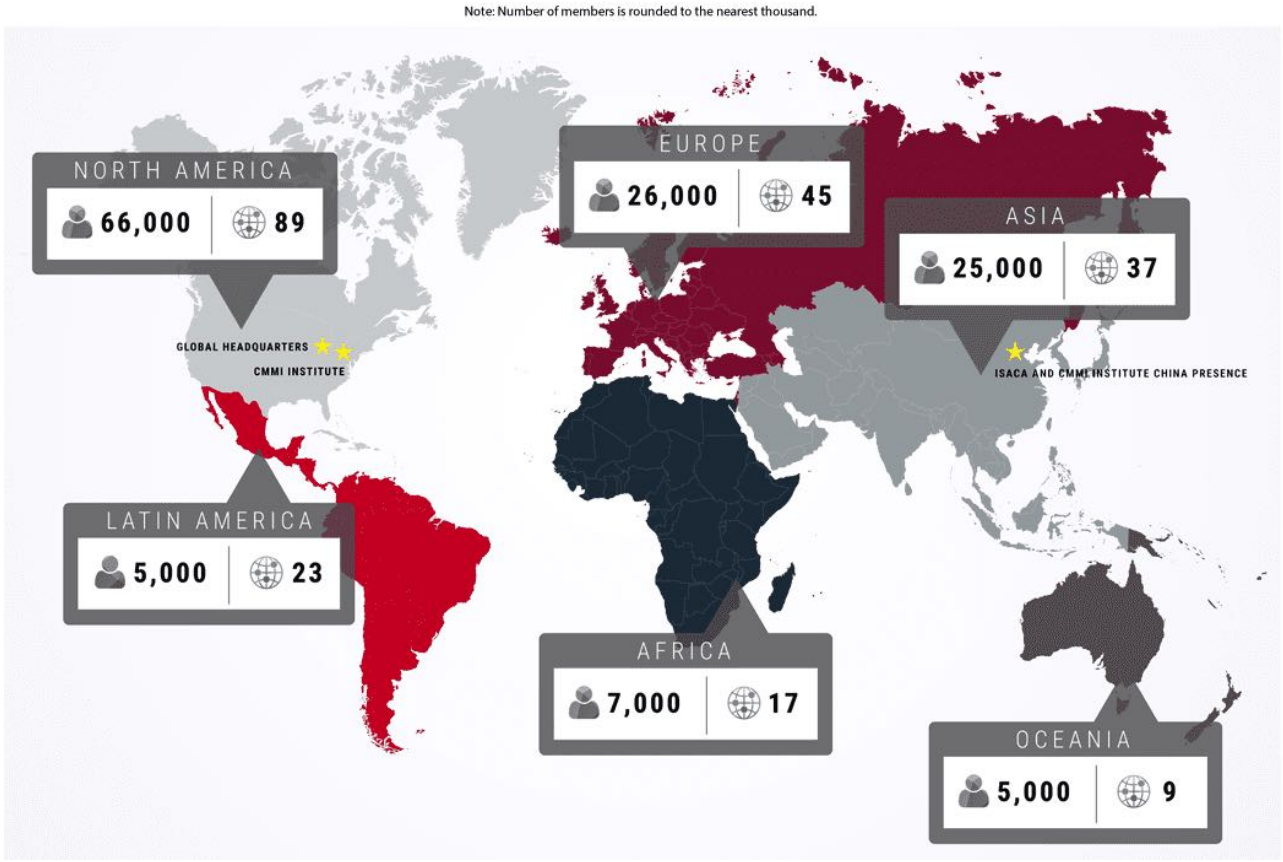
ISACA Taiwan Chapter

認識ISACA

Explore Our Global Impact & Find Your Local Chapter

135,000 MEMBERS

220 CHAPTERS



ISACA
國際電腦稽核協會

是一個幫助個人及企業積極發揮技術潛力的全球性協會。現今的世界以資訊技術為動力，ISACA為專業人士提供知識、認證、訓練和社群服務，以提升他們的事業與組織變革。

ISACA Taiwan Chapter

認識ISACA

網路研討會 | 培訓課程 | 會議論壇 | 虛擬培訓 | 考試準備 | 線上活動

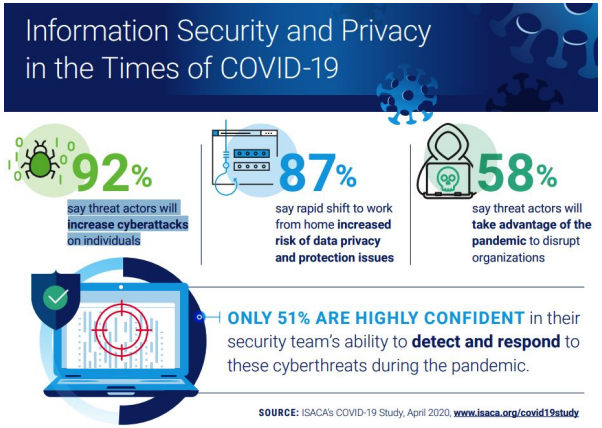
ISACA

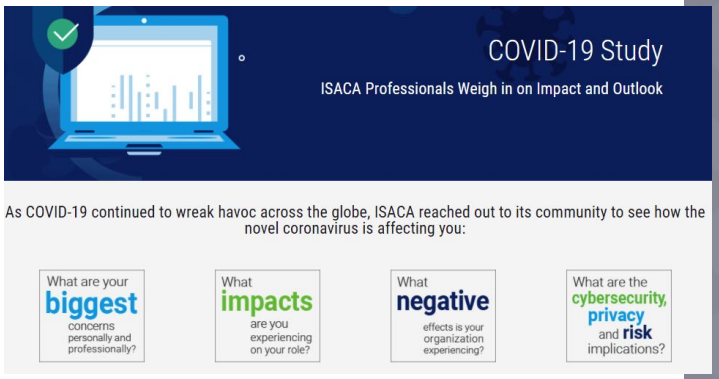
訓練與活動

增加您的知識。

提高您的技能。

隨時隨地向專家學習。





ISACA Taiwan Chapter

認識ISACA

CISA

Validate your experience and know-how in IT audit, security and control. Boost your career and salary potential.

CRISC

Propel your career forward in enterprise IS/IT risk management and control. Boost your career and pay.

CISM

Propel your career to senior management roles. Contribute to your enterprise from a strategic standpoint.

CGEIT

Validate your expertise in strategic enterprise governance. Gain visibility at the executive level.

CSX-P

Attest to your advanced cybersecurity practitioner skills in managing risk and addressing threats.

CDPSE

Designed to assess a privacy professional's ability to implement privacy by design.

Certificate Programs

COBIT

Attests to your advanced cybersecurity practitioner skills in managing risk and addressing threats.

Certificate Programs

Cybersecurity Audit

Gain the critical knowledge you need to excel in cybersecurity audits and the certificate to prove it.

Certificate Programs

CSX CYBERSECURITY NEXUS

Choose from a variety of certificates to attest to your cybersecurity practitioner skills and know-how.

ISACA 專業認證

在您的名字之後的CISA，CRISC，CISM，CGEIT，CSX-P或CDPSE，證明您擁有應對現代企業挑戰的專業知識。

ISACA Taiwan Chapter

成為 ISACA 6C 專業人士

CISA 國際電腦稽核師

CGEIT 國際企業資訊治理師

CRISC 國際資訊風險控制師

CISM 國際資訊安全管理師

CSX-P 國際執業資安專家

CDPSE 國際資料隱私防護師

在人群中脫穎而出

在招募和晉升過程中獲得關注，並通過我們全球認可的認證來驗證您的專業知識。

ISACA Taiwan Chapter

謝謝聆聽

THANKS FOR YOUR ATTENTION

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

達文西個資暨高科技法律事務所
10089 台北市中正區衡陽路51號6樓之9
Tel：02-2367-0902