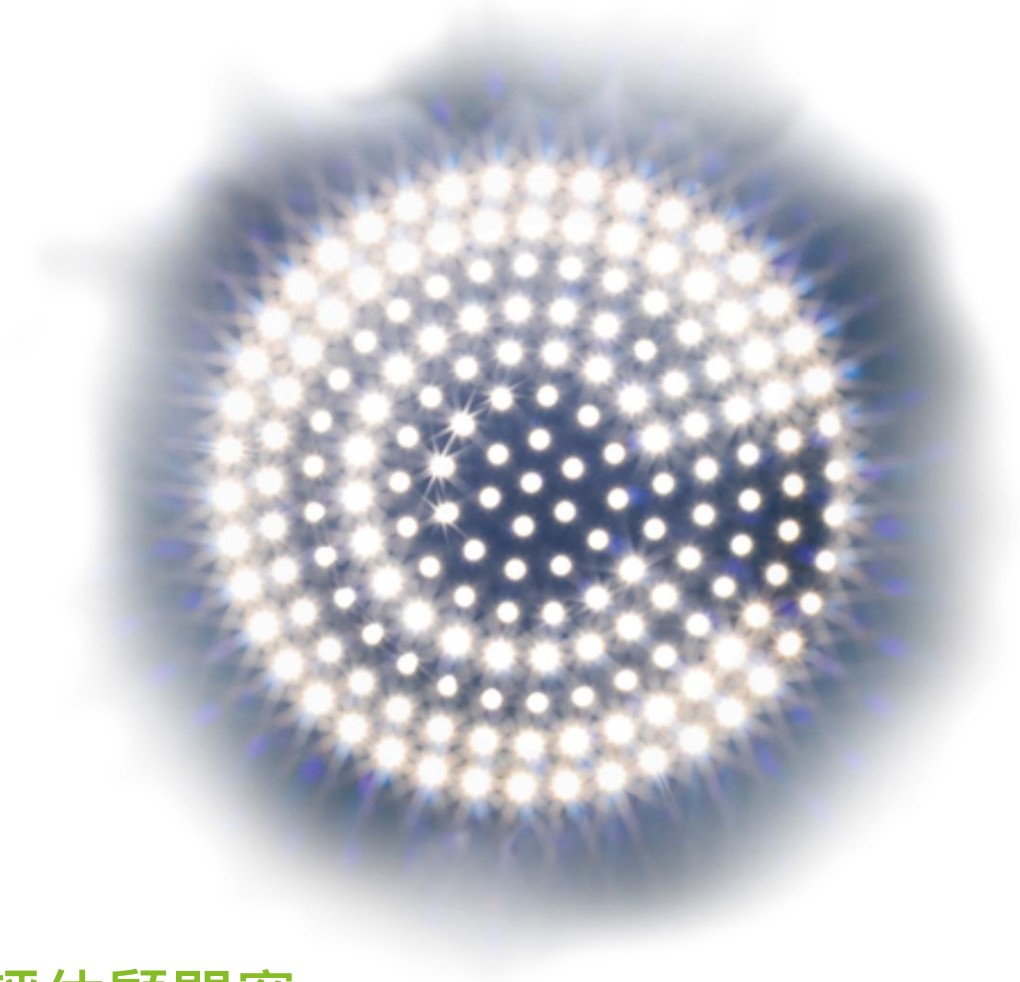
Deloitte.
勤業眾信



臺灣證券交易所
證券商資安治理成熟度評估顧問案
說明會議

勤業眾信 風險諮詢服務 2025.5.19

Agenda

- 專案目標與範圍
- 成熟度訪談進行方式
- 專案團隊
- 意見交流

專案目標與範圍

臺灣金管會金融資安行動方案 - 資安治理成熟度分析評估作業

強化資安監理

型塑金融機構重視資安的組織文化、完備資安規範、強化資安監理職能、加強金融資安查核。

1. 型塑金融機構重視資安的組織文化
2. 完備資安規範
3. 強化資安監理職能
4. 加強金融資安查核

深化資安治理

加強資安管理、強化資安監控、加強資安人才培育。

5. **加強資安管理**
6. 強化資安監控
7. 加強資安人才培育

精實金融韌性

增進營運持續管理量能、加強資安演練、建構資料保全避風港。

8. 增進營運持續管理量能
9. 加強資安演練
10. 建構資料保全避風港

發揮資安聯防

資安情資分享與合作、建立金融資安事件監控與應變體系。

11. 資安情資分享與合作
12. 建立金融資安事件應變體系
13. 建立金融資安事件監控體系

5.2推動金融資安治理成熟度評估

由FISAC研議訂定金融機構資安治理成熟度評估方法

鼓勵金融機構辦理資安治理成熟度評估

專案目的與範圍

專案目標

1. 依據證券商113年所執行資安治理成熟度評估之結果，再次追蹤本年度填寫情形，分析證券商資安治理成熟度的趨勢，以追蹤證券商本年度資訊安全成熟度與過往執行情形的比較。
2. 並考量CAT與NIST問項差異，設計本年度證券商訪談問卷，提供19家證券商填寫，藉此讓各證券商能夠評估更廣的議題範疇，並熟悉國際上主流的資安成熟度評估框架。
3. 根據證券商填寫結果與顧問團隊問卷訪談的紀錄，列出證券商整體可改善的方向，並以此作為本年度評估報告的依據。評估報告不僅可讓主管機關了解當前證券商的資安治理情形，更可提供各證券商持續精進的方向。

評估工具

1. 美國聯邦金融機構監督委員會（Federal Financial Institutions Examination Council, FFIEC）發展之「網路安全評估工具」（Cybersecurity Assessment Tool, CAT)。
2. 參考AI 治理、作業委外、雲端應用的議題，並考量CAT與NIST問項差異，設計本年度證券商訪談問卷

評估範圍

20家本國證券業者，較前一年度新增**新光證券、致和證券**

專案時程

114年10月31日完成所有工作內容。

成熟度評估進行方式

成熟度評估進行方式 – 問卷發放、填寫、回收

問卷填寫 → 訪談時間與進行方式 → 報告產出

	5月初發放	訪談前一週提供	訪談結束一週內
	問卷發放	**問卷回收**	**後續微調**
勤業執行項目	• 提供證券商成熟度檢核項目問卷，共25題。 • 提供證券商494題全部等級題目	• 回收各家證券商問卷 • 於訪談中了解各證券商達成與無法達成的原因，確認實際情形與填寫結果一致	• 若於訪談中或訪談結束後得到證券商更新的資訊，協助調整訪談結果
券商配合事項	• 請各位於**訪談前一週提供** • 問卷更新：特別針對**基礎、發展中、中等這三個等級更新**，若有導入資安工具，請檢視進階、創新等級題目是否需要更新。 • 第一次填寫CAT：新光證券、致和證券另須進行2次的問卷填寫輔導	• 參與訪談，訪談時間請見後方簡報 • 尚未回覆可訪談時間者，請於**5/23前確認時間**。	• 各證券商若在訪談結束後**有資訊需要調整，請於一週內提供**給勤業眾信顧問團隊

成熟度評估進行方式– 問卷填寫範例

問卷填寫 → 訪談時間與進行方式 → 報告產出

描述如何達成

提出無法達成的原因及日後規劃

控制因子 (Assessment Factor)	控制措施 (Component)	題項	該題已達成文字範例	該題無法達成文字範例
資訊治理	監督	由董事會(董事委員會)指派的管理階層負責執行與管理資訊安全及營運持續計畫。	本公司經由董事會指派之資安單位專責資訊安全之管理，並每年擬定營運持續計畫。	本公司尚無相關專責單位，因目前人力不足，未來規劃配置相關人力。
		管理階層至少每年提供一份關於資訊安全與營運持續計畫的整體現狀書面報告予董事會(董事委員會)。	本公司每年至少執行一次營運持續計畫，並將其結果與資安整體營運情形於管理審查會中呈報董事會，使管理階層皆能定期檢視資安活動。	本公司尚無舉行相關定期會議，日後擬定相關場合以確保管理階層了解整體資安活動。
		管理階層將關鍵基礎設施(如電信、能源)對組織造成的風險納入考量。	本公司執行之營運持續演練，皆有將基礎設施失能的情形考量進計畫中。	目前營運持續演練只著眼在備份與備援正常執行，之後將規劃將基礎設施納入演練計畫中。

成熟度評估進行方式 – 訪談方式

問卷填寫 → **訪談時間與進行方式** → 報告產出

參與證券商

- 元大證券
- 群益證券
- 凱基證券
- 永豐金證券
- 富邦證券
- 康和證券
- 國票證券
- 兆豐證券
- 國泰證券
- 元富證券
- 合庫證券
- 亞東證券
- 第一金證券
- 統一證券
- 中信證券
- 台新證券
- 玉山證券
- 華南證券
- 新光證券
- 致和證券

訪談方式

- CAT訪談時間為一個上/下午，約需**2~3小時**
- 25題問卷訪談時間皆為半個上/下午，約**1.5小時**
- 實體進行，待5/23確認全部證券商時間後，統一發送會議邀請

訪談內容

- CAT：針對完整版(抽樣)與基礎題目的回覆做討論，確認填寫結果與實際情形一致
- 25題問卷：針對題目的回覆做討論，確認填寫結果與實際情形一致

證券商提供各項文件時程

證券商	證券商名單	交付項目	時程
20家證券商	• 元大證券 • 群益證券 • 凱基證券 • 永豐金證券 • 富邦證券 • 康和證券 • 國票證券 • 兆豐證券 • 國泰證券 • 元富證券 • 合庫證券 • 亞東證券 • 第一金證券 • 統一證券 • 中信證券 • 台新證券 • 玉山證券 • 華南證券 • 新光證券 • 致和證券	• 附件一_114年度證券業金融資安治理成熟度評估_固有風險	• 8月31日以前提供 • 首次填寫的新光證券、致和證券請於**第一次訪談前一週提供**
		• 附件二___114年網路安全成熟度自評問卷	• 8月31日以前提供 • 首次填寫的新光證券、致和證券請於**第一次訪談前一週提供**
		• 附件三_(25題)成熟度檢核項目問卷	• 訪談前一週提供

成熟度評估進行方式 – 訪談時間

問卷填寫 → 訪談時間與進行方式 → 報告產出

星期一	星期二	星期三	星期四	星期五
			5/1	9/2
5/5 發放問卷	5/6	5/7	5/8	5/9
5/12	5/13 啟動會議	5/14	5/15	5/16
5/19 評估說明會議	5/20	5/21	5/22	5/23 回覆訪談時間deadline
5/26	5/27	5/28	5/29	5/30

成熟度評估進行方式 – 訪談時間

問卷填寫 → 訪談時間與進行方式 → 報告產出

星期一	星期二	星期三	星期四	星期五
6/16	6/17	6/18	6/19	6/20
6/23	6/24 上午：元富證券	6/25	6/26	6/27
6/30	7/1 下午：統一證券	7/2	7/3	7/4
7/7	7/8	7/9	7/10	7/11
7/14	7/15	7/16	7/17	7/18
7/21	7/22 下午：國泰證券	7/23	7/24	7/25
7/28	7/29	7/30	7/31	8/1
8/4	8/5	8/6	8/7	8/8

成熟度評估進行方式 – 報告產出

問卷填寫 → 訪談時間與進行方式 → **報告產出**

彙整及分析評估成果並產製報告

彙整20家證券商成熟度評估結果

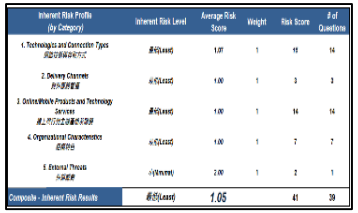
- 依據訪談結果，協助彙整並分析證券商25題檢核項目問卷之結果。
- 協助新光證券與致和證券商進行CAT評估，並協助計算相關分數。

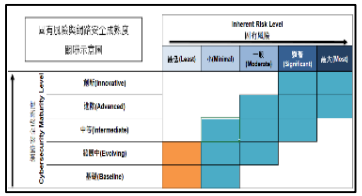
分析證券商不符合之原因

- 逐條分析基礎題目證券商無法達成之原因

產製證券商成熟度評估報告

- 依據前述分析結果，產製證券商成熟度評估報告。
- 提出現行證券商自律法規修訂建議與依據。





專案組織

聯繫資訊

專案期間主要專案成員主責項目及聯繫資訊

角色	姓名	分機	負責項目
專案經理	Cherry Yu 游千瑩	7578	專案管理、進度掌控與溝通
專案團隊負責人	Evan Lee 李奕澄	2296	專案管理(窗口)、進度掌控與溝通、訪談施作與報告產出
專案團隊成員	Hailey Hsu 許芳瑜	6768	訪談施作與報告產出

勤業眾信連絡電話 02-2725-9988

意見交流

Deloitte.

勤業眾信