Deloitte.
勤業眾信

TAIWAN STOCK EXCHANGE 臺灣證券交易所

證券期貨商資訊安全防護標準研究報告說明

大綱

- 證券期貨業者分級說明
- 證券期貨業者分級資通安全防護標準草案
- 意見交流

證券期貨業者分級說明

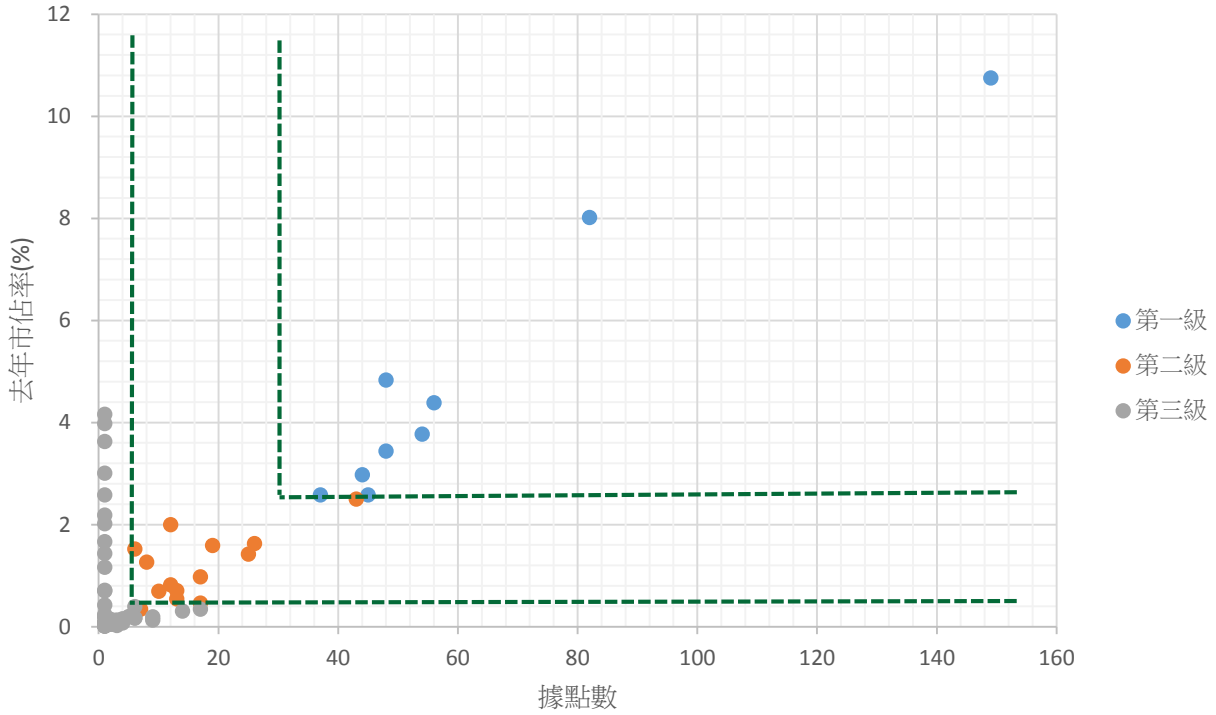
證券商分級

方案	第一級	第二級	第三級
資本額(指撥營運資金)	達100億以上	40億至100億	40億以下
金控子公司(或) 上市/櫃	是	是	否
符合券商數	9	16	49

第一級：資本額(指撥營運資金)達100億元以上之業者；
第二級：資本額(指撥營運資金)介於40億元以上到未達100億元之業者；
第三級：資本額(指撥營運資金)未達40億元之業者；

資本額(指撥營運資金)未達40億元，但為上市櫃或為金融控股公司之子公司證券商者。

證券商分級補充說明



等級	綜合證券商	去年市佔率	據點數
第一級	是	>2.5%	>30
第二級	是	2.5~0.5%	>7
第三級	否	<0.5%	<7

- 現訂分級方式大致符合以上級距

證券商分級列表

第一級	第二級		第三級			
群益證券	華南永昌證券	*福邦證券	彰銀證券	富隆證券	福勝證券	港商麥格理證券
凱基證券	國票證券	*新光證券	土銀證券	花旗環球證券	北城證券	高盛亞洲證券
富邦證券	亞東證券		台灣企銀證券	法銀巴黎證券	新百王證券	瑞士信貸證券
元大證券	康和證券		聯邦銀行證券	永全證券	萬通證券	港商德意志證券
永豐金證券	台新證券		大和國泰證券	陽信證券	日進證券	香港商野村證券
日盛證券	第一金證券		致和證券	高橋證券	光隆證券	港商法國興業證券
統一證券	中國信託證券		美林證券	光和證券	全泰證券	瑞銀證券
元富證券	國泰證券		台中銀證券	台灣匯立證券	信富證券	
兆豐證券	合庫證券		摩根大通證券	永興證券	豐農證券	
	玉山證券		台灣摩根士丹利證券	日茂證券	石橋證券	
	*宏遠證券		德信證券	寶盛證券	萬泰證券	
	*大慶證券		犇亞證券	金港證券	中農證券	
	*臺銀證券		香港上海匯豐證券	安泰證券	大鼎證券	
	*大展證券		大昌證券	盈溢證券	鑫豐證券	

*低於40億但有上櫃

*低於40億但有金控背景

證券期貨業者分級資通安全防護標準草案

主要規範項目

- 資訊系統分類分級
- ISMS推動作業
- 資安專責人力
- 風險評估
- CA認證與憑證管理
- 稽核方式
- 業務持續運作演練(含事件通報)
- 弱點掃描
- 防護縱深
- 監控管理
- 資安健診
- 社交工程演練
- 資安教育訓練及專業證照
- 滲透測試
- 原始碼檢測
- 情資分享

分級資安防護標準(1/8)

等級	(一)資訊系統分類分級	(二)ISMS推動作業
參考資料	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 □OCIE □FINRA ■IIROC ■IOSCO	■資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 ■保險業辦理電子商務應注意事項 □OCIE □FINRA ■IIROC □IOSCO
第一級	完成資訊系統分級並且每年檢視一次資訊分級妥適性	1. 成立資訊安全推動小組 2. 關鍵系統完成ISMS 導入 3. 關鍵系統通過第三方驗證
第二級	完成資訊系統分級並且每年檢視一次資訊分級妥適性	1. 成立資訊安全推動小組 2. 關鍵系統完成ISMS 導入
第三級	完成資訊系統分級並且每年檢視一次資訊分級妥適性	成立資訊安全推動小組

分級資安防護標準(2/8)

等級	(三)資安專責人力	(四)風險評估
參考資料	■資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 □OCIE ■FINRA ■IIROC □IOSCO	□資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC ■IOSCO
第一級	指定資安主管及資安專責人力2人	每年至少2次
第二級	指定資安主管及資安專責人力1人	每年至少1次
第三級	資安專責人力1人	每年至少1次

分級資安防護標準(3/8)

等級	(五)CA認證與憑證管理	(六)稽核方式
參考資料	□資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 □OCIE □FINRA □IIROC □IOSCO	■資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA □IIROC ■IOSCO
第一級	1. 網際網路下單業者應訂定憑證交付程序，避免非本人取得憑證 2. 網際網路下單業者應全面使用認證機制	1. 依據「建立證券/期貨商資通全檢查機制」之查核週期辦理 2. 網際網路下單業者應設有電腦稽核人員
第二級	1. 網際網路下單業者應訂定憑證交付程序，避免非本人取得憑證 2. 網際網路下單業者應全面使用認證機制	1. 依據「建立證券/期貨商資通全檢查機制」之查核週期辦理 2. 網際網路下單業者應設有電腦稽核人員
第三級	1. 網際網路下單業者，應訂定憑證交付程序，避免非本人取得憑證 2. 網際網路下單業者應全面使用認證機制	1. 依據「建立證券/期貨商資通全檢查機制」之查核週期辦理 2. 網際網路下單業者應設有電腦稽核人員

分級資安防護標準(4/8)

等級	(七)業務持續運作演練(含事件通報)	(八)資安教育訓練及專業證照
參考資料	■資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE □FINRA ■IIROC □IOSCO	■資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC ■IOSCO
第一級	1. 訂定故障復原程序及營運持續計畫 2. 每年至少演練1次	1. 每年資安人員(資訊人員)至少 2 人次須接受12小時以上資安專業課程訓練 2. 每年全體員工與主管至少須接受 3 小時資安宣導課程並通過課程評量 3. 每年維持至少2張國際資安專業證照之有效性
第二級	1. 訂定故障復原程序及營運持續計畫 2. 每年至少演練1次	1. 每年資安人員(資訊人員)至少 1 人次須接受12小時以上資安專業課程訓練 2. 每年全體員工與主管至少須接受 3 小時資安宣導課程並通過課程評量 3. 每年維持至少1張國際資安專業證照之有效性
第三級	1. 訂定故障復原程序及營運持續計畫 2. 每年至少演練1次	1. 每年資安人員(資訊人員)至少 1 人次須接受12小時以上資安專業課程訓練 2. 每年全體員工與主管至少須接受 3 小時資安宣導課程並通過課程評量

分級資安防護標準(5/8)

等級	(九)防護縱深	(十)監控管理
參考資料	■資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE □FINRA ■IIROC □IOSCO	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC □IOSCO
第一級	1. 建立防毒、防火牆、郵件過濾裝置 2. 建立入侵偵測系統(IDS)或入侵防禦系統(IPS) 3. 建立Web 應用程式防火牆 4. 建立進階式威脅(APT)攻擊防禦 5. 網際網路下單業者，應導入流量清洗或流量分流機制	建立關鍵系統之SOC監控
第二級	1. 建立防毒、防火牆、郵件過濾裝置 2. 建立入侵偵測系統(IDS)或入侵防禦系統(IPS) 3. 建立Web 應用程式防火牆 4. 網際網路下單業者，應導入流量清洗或流量分流機制	建立關鍵系統資訊安全監控機制，識別關鍵系統之異常紀錄並發出警示通知
第三級	1. 建立防毒、防火牆、郵件過濾裝置(如公司自建郵件伺服器) 2. 網際網路下單業者，應導入流量清洗或流量分流機制	建立關鍵系統資訊安全監控機制，識別關鍵系統之異常紀錄並發出警示通知

分級資安防護標準(6/8)

等級	(十一)弱點掃描	(十二)滲透測試
參考資料	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 ■建立證券商資通安全檢查機制 ■建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 □OCIE ■FINRA ■IIROC □IOSCO	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 □OCIE ■FINRA ■IIROC □IOSCO
第一級	每年至少辦理 2 次關鍵系統弱點檢測，並完成高風險漏洞修補	每年至少辦理 1 次對外服務關鍵系統滲透測試，並完成高風險漏洞修補
第二級	每年至少辦理 2 次關鍵系統弱點檢測，並完成高風險漏洞修補	每2年至少辦理 1 次對外服務關鍵系統滲透測試，並完成高風險漏洞修補
第三級	每年至少辦理 2 次關鍵系統弱點檢測，並完成高風險漏洞修補	每2年至少辦理 1 次對外服務關鍵系統滲透測試，並完成高風險漏洞修補

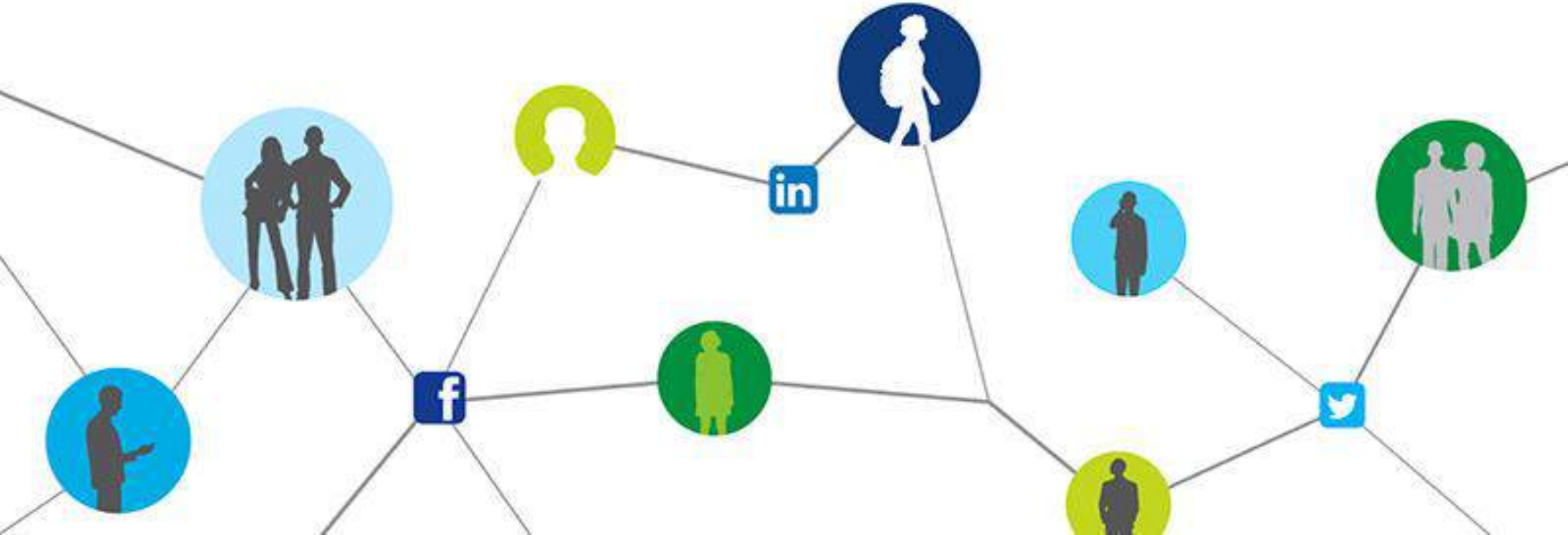
分級資安防護標準(7/8)

等級	(十三)原始碼檢測	(十四)資安健診
參考資料	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC □IOSCO	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC □IOSCO
第一級	當關鍵系統異動時應進行原始碼檢測，並每年至少辦理一次原碼檢測	每年至少辦理 1 次資安健診，其內容應包含 ●網路架構檢視 ●網路惡意活動檢視 ●使用者端電腦檢視 ●伺服器主機檢視 ●目錄伺服器及防火牆安全設定檢視
第二級	當關鍵系統異動時得進行原始碼檢測，並每年至少辦理一次原碼檢測	每2年至少辦理 1 次資安健診(內容比照第一級辦理)
第三級	當關鍵系統異動時得進行原始碼檢測，並每年至少辦理一次原碼檢測	NA

分級資安防護標準(8/8)

等級	(十五)社交工程演練	(十六)資安健診
參考資料	■資通安全責任等級分級作業規定 ■金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 ■壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC □IOSCO	□資通安全責任等級分級作業規定 □金融機構辦理電腦系統資訊安全評估辦法 □建立證券商資通安全檢查機制 □建立期貨商資通安全檢查機制 □壽險業辦理資訊安全防護自律規範 □保險業辦理電子商務應注意事項 ■OCIE ■FINRA ■IIROC ■IOSCO
第一級	每年至少辦理1次社交工程演練	加入至少1個情資分享組織
第二級	每年至少辦理1次社交工程演練	加入至少1個情資分享組織
第三級	每年至少辦理1次社交工程演練	加入至少1個情資分享組織

Q&A



Deloitte.

勤業眾信

期貨商分級

方案	第一級	第二級	第三級
資本額(指撥營運資金)	達100億	100億至40億	40億以下
上市/櫃	是	是	否
符合券商數	0	2	13

第一級	第二級	第三級
	元大期貨	大昌期貨
	群益期貨	統一期貨
		澳帝華期貨自營
		永豐期貨
		凱基期貨
		康和期貨
		日盛期貨
		元富期貨
		兆豐期貨
		國泰期貨
		華南期貨
		國票期貨
		富邦期貨

- 第一級：資本額(指撥營運資金)達100億元以上之業者；
- 第二級：資本額(指撥營運資金)介於40億元以上到未達100億元之業者；
- 第三級：資本額(指撥營運資金)未達40億元之業者；

- 資本額(指撥營運資金)未達40億元，但為上市櫃期貨商者，列為第二級，兼營業者則依本業之分級為準。