證券商資安作業應辦暨注意事項說明

臺灣證券交易所

TAIWAN
STOCK EXCHANGE

大綱

- 證券商資安查核與輔導
- 資安查核重點
- 常見缺失說明
- 重要事項宣導

TAIWAN
STOCK EXCHANGE

證券商資安查核與輔導

資安事件要怎麼防範

發生的可能性

- 公司沒有價值=不會發生?

影響的程度小

- 損害控管

資料來源：iThome

證券商資安查核與輔導

年度資安例查

- 協助檢視整體資安防護及法規落實情形

選案查核

- 投資人檢舉、主管機關指示

專案查核

- 特定議題對市場之影響或檢視整體辦理情形

加強輔導查核

- 特定態樣強化輔導

證券商資安查核與輔導

近兩年發生缺失本公司相關處置及違約金統計

處置內容	**注意改善** **併課違約金5萬元至43萬元不等**
處置依據 **(營業細則)**	第135條第2項 第138條第2項

證券商資安查核與輔導

如重複發生相同缺失，本公司將依規辦理如下

重複發生	一	二	三	四
處置內容	1.警告 2.併課新臺幣100萬元以下違約金	1.警告 2.併課新臺幣200萬元以下違約金	暫停3個月以下之買賣	暫停買賣
處置依據(營業細則)	1.第136條 2.第138條第2項	1.第136條 2.第138條第3項(半年內再次發生)	第139條	第142條第1項第5款

TAIWAN
STOCK EXCHANGE

資安查核重點

資安查核重點

風險在哪裡？

外部威脅

- 駭客、天災...→防範未然

內部弱點

- 員工、門禁...→防微杜漸

TAIWAN
STOCK EXCHANGE

資安查核重點

資安查核重點

建立證券商資通安全檢查機制

資通安全檢查機制

- 辨識資安風險
- 訂定資安政策
- 配置組織資源
- 清查資訊資產
- 強化人員管理
- 監控環境設備
- 管理通訊作業
- 落實存取控制
- 控管開發維運
- 提升營運韌性
- 實作規範相符
- 納管新興科技

TAIWAN
STOCK EXCHANGE

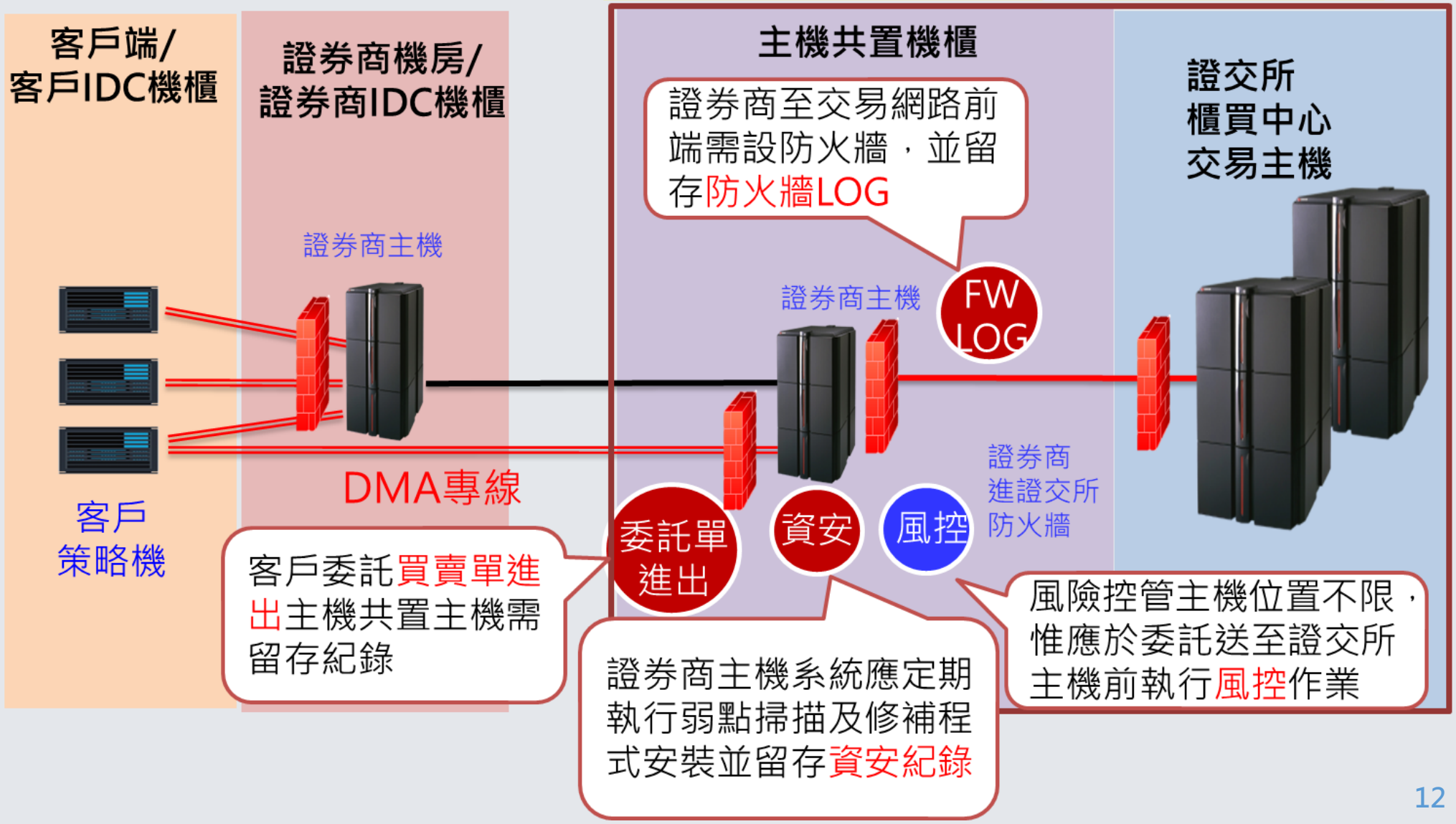
資安查核重點

年度金融檢查重點	• 年度重點(本國銀行、壽險業)、系統參數檢查
機敏資料保護情形	• 端點防護
強化登入及憑證下載驗證	• 網路交易系統驗證完整性
駭客攻擊之防護	• 異常活動檢視、資料備份落實情形

資安查核重點

證券商就上述項目，應訂有內稽內控制度並留存稽核軌跡

主機共置服務



資安查核重點

資安防護彙總

- 資安組織與人力配置
- 網路與系統防護
- 程式變更管理
- 持續營運量能
- 機敏資料防護

TAIWAN
STOCK EXCHANGE

常見缺失說明

常見缺失說明

	查核項目	查核缺失
1	營運持續	未依主管機關「證券期貨市場資通安全事件通報應變作業注意事項」規定，向主管機關辦理資通安全事件通報。
2	存取控制	未定期審查並檢討久未使用之使用者權限。
3	網路安全管理	未定期或適時修補網路運作環境之安全漏洞。
4	網路安全管理	網路下單未採多因子驗證方式。
5	存取控制	資通安全存取控制之密碼管理作業，尚未能全面使用優質密碼設定，或未能定期3個月以內更新相關使用者之密碼。

常見缺失說明

- 未落實資安通報可能造成資安聯防缺口(防範未然、防微杜漸、傷害管控)

資料來源：金融資安資訊分享與分析中心

常見缺失說明

- 未定期審查並檢討久未使用之使用者權限
- 資通安全存取控制之密碼管理作業，尚未能全面使用優質密碼設定，或未能定期3個月以內更新相關使用者之密碼。

資料來源：財團法人台灣網路資訊中心

常見缺失說明

- 網路下單未採多因子驗證方式。
- 重複使用知識因，子進行驗證。

資料來源：資安人

常見缺失說明

- 未依規定期評估網路系統安全。
- 未依評估結果進行弱點修復。

資料來源：iThome

TAIWAN
STOCK EXCHANGE

重要事項宣導

TAIWAN STOCK EXCHANGE

重要事項宣導

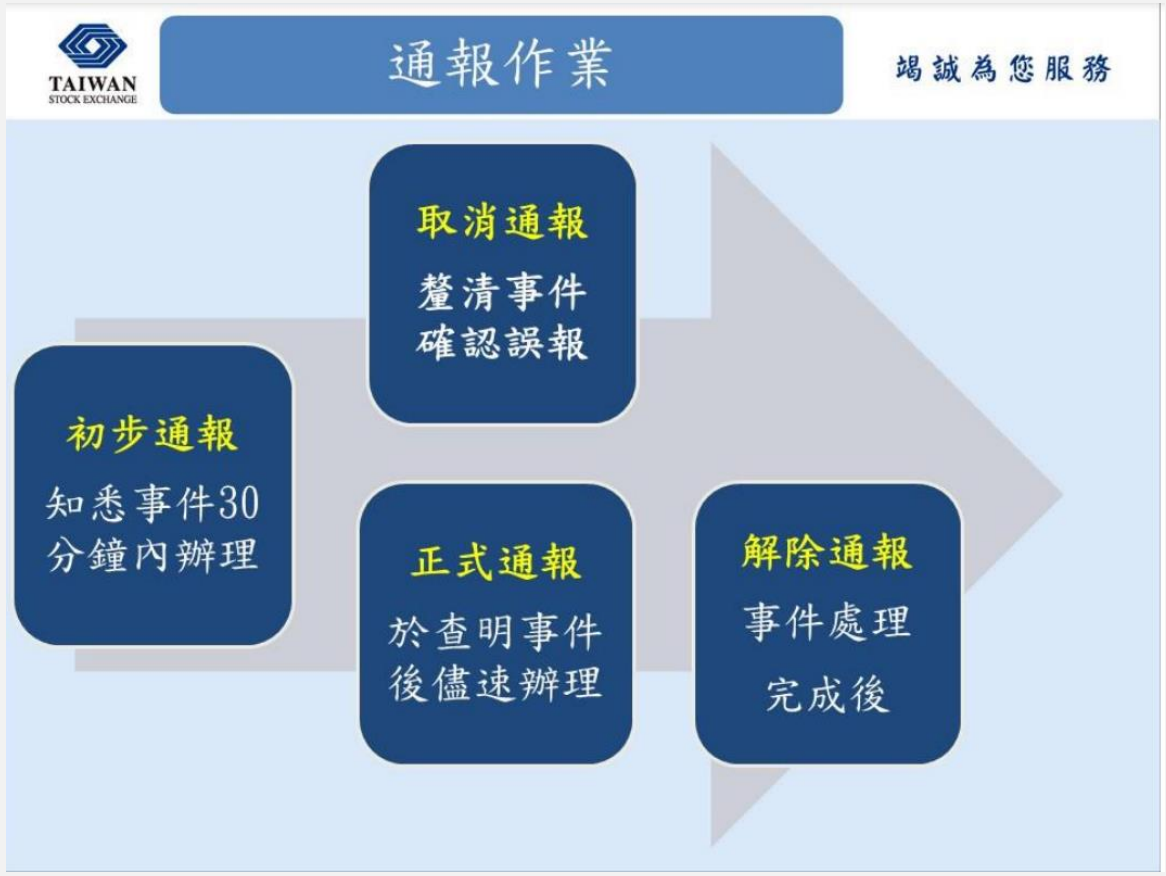
112、113年應完成項目

證券商分級 / 應辦事項	第一級(A級)證券商 實收資本額200億(含)以上	第二級(B級)證券商 實收資本額100億(含)~未達200億	第三級(C級)證券商 實收資本額40億(含)~未達100億	第四級(D級)證券商 實收資本額未達40億
國際標準通過驗證	V	V	V	-
資通安全專業證照	V	V	V	V
資通安全健診	V 每年辦理一次	V 每二年辦理一次	V 每二年辦理一次	-
資通安全威脅偵測(SIEM)管理機制	V	V	V	-
入侵偵測(IPS)及防禦機制	V	V	V	V
應用程式防火牆(WAF)	V	V	V	V
進階持續性威脅攻擊(APT)防禦措施	V	-	-	-

明年實施

資本額分級標準	資安單位暨人力編制
200億以上(1級)	應設資安專責單位，資安主管及至少3名資安人員
100億以上未達200億(2級)	資安主管及至少3名資安人員，但若已設專責單位，人員可維持2人
40億以上未達100億(3級)	資安主管及至少2名資安人員
未達40億(4級)	至少1名資安人員(維持)

資安事件通報



為確保資安通報之正確及有效性，資安事件通報應於初步通報後24小時內完成正式通報。

重要事項宣導

公司與資訊公司合作對外提供服務，應確實瞭解資訊公司具體業務內容，並就對外提供之服務有明確責任歸屬，且資訊公司如未經金管會許可及發給證券許可證照，不得涉及經營證券業務。

TAIWAN
STOCK EXCHANGE

簡報結束
敬請指導