證券商資安作業說明

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
- 近期修訂規範說明
- 重要事項宣導

TAIWAN
STOCK EXCHANGE

證券商資安查核與輔導

證券商資安查核與輔導

- 年度資安查核
  年度例查(約140項查核項目)
- 專案查核
  多因子驗證導入情形查核，主機共置服務專案查核
- 選案查核
  投資人檢舉、主管機關指示
- 強化輔導
  前一年度異常通報、前一年度有未通報之缺失、例查缺 失重複發生

證券商資安查核與輔導

發生缺失本公司相關處置

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

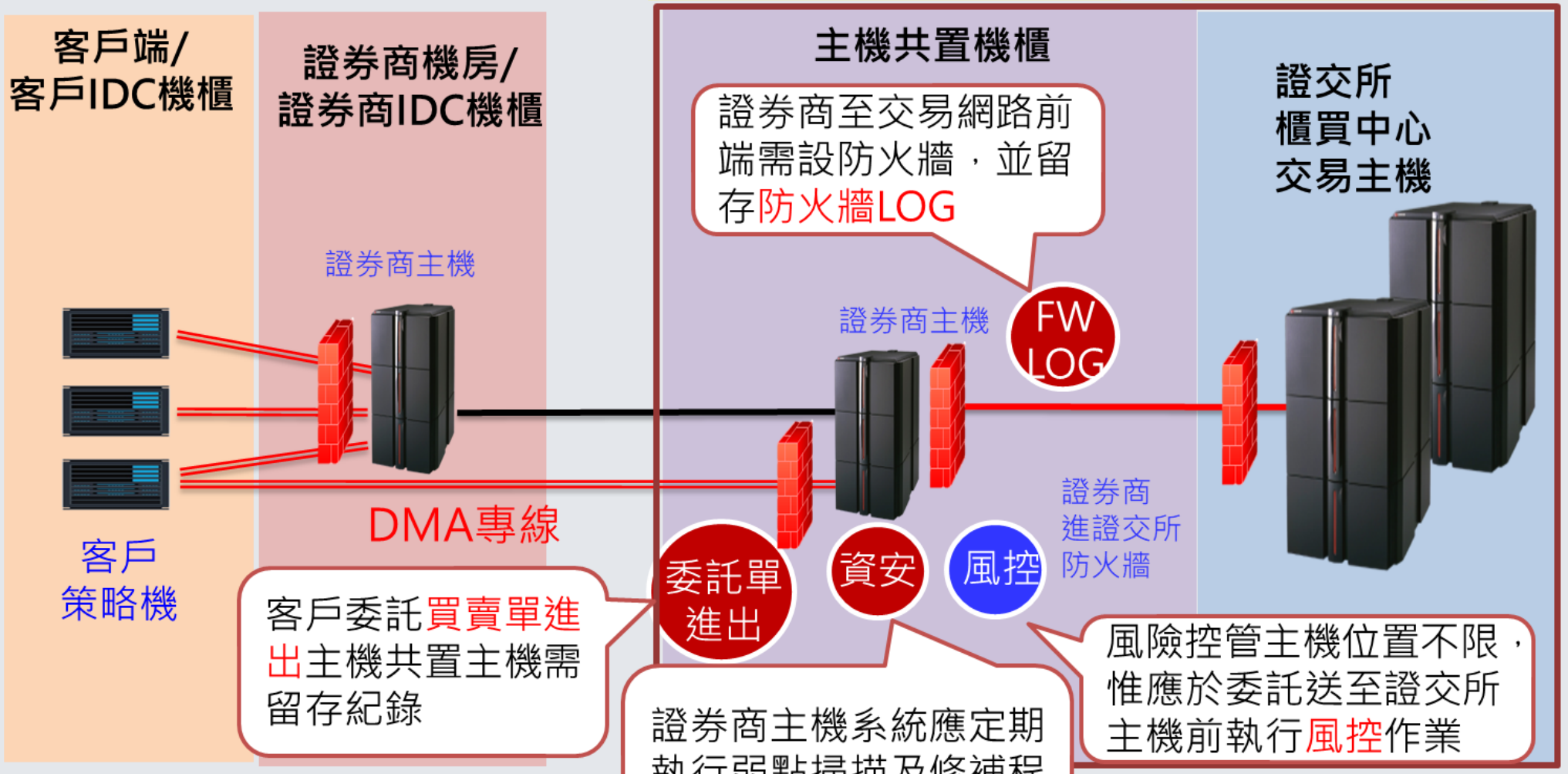
資安查核重點

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
個人資料保護情形	• 端點防護、個資事件發生處理小組
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

近期修訂規範說明

近期修訂規範說明

證券商內部控制制度標準規範—內部控制制度修訂對照表（111 年）

編號	作業項目	修訂後內容	修訂前內容	修訂說明
CC-12000	資訊安全政策	作業程序及控制重點： (一)~(五)略。 (六)、公司每年應將前一年度資訊安全整體執行情形，由**資訊安全長或**負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具**「證券暨期貨市場各服務事業建立內部控制制度處理準則」第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過，並將該聲明書內容揭露於主管機關指定之申報網站。** (以下略)	作業程序及控制重點： (一)~(五)略。 (六)、公司每年應將前一年度資訊安全整體執行情形，由負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具資訊安全整體執行情形聲明書，並提報董事會通過，於會計年度終了後三個月內將該聲明書內容揭露於公開資訊觀測站。 (以下略)	**依據主管機關 110 年 9 月 30 日金管證券字第 11003637894、11003637895 號令辦理。**

近期修訂規範說明

CC-17010(適用網際網路下單證券商，另(一)、(二)、(五)項並適用於所有證券商)	網路安全管理	(一)~(二)略 (三)、網路傳輸安全管理： 1、(略) 2、公司應每日針對核心系統之帳號登入失敗紀錄、非客戶帳號**嘗試**登入**嘗試**紀錄等進行監控及分析**，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，應即時了解異常原因**，並留存相關紀錄。 3. (略) (四)、CA 認證與憑證管理： 1、網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。**客戶申請或更新憑證下載，必須採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及 SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。**	(一)~(二)略 (三)、網際網路下單服務品質相關標準： 1、(略) 2、公司應每日針對核心系統之帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄等進行監控及分析，並留存相關紀錄。 3. (略) (四)、CA 認證與憑證管理： 1、網路下單應訂定憑證交付程序，避免非本人取得憑證。	**依據證交所 110 年 11 月 30 日臺證輔字第 1100503618 函辦理。鑑於駭客攻擊資通安全事件頻傳，為維護證券市場交易秩序及保障投資人權益，爰增修證券商強化網際網路下單之資通安全控管機制，並修訂證券商內部控制制度標準規範。**

近期修訂規範說明

		2、(略)	2、(略)
		(五)~(九)、(略)	(五)~(九)、(略)
		(十)、帳號登入或異常態樣通知： 公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣應即通知客戶，並留存紀錄，避免非客戶本人登入情事： 1. 密碼輸入錯誤或帳戶被鎖定。 2. 申請或更新憑證。 3. 變更基本資料。 4. 異常來源或行為嘗試登入等。 5. 密碼申請異動或補發時。 (112 年 2 月 28 日生效)	(十)、(新增)

近期修訂規範說明

		(十一)、異常 IP 登入之監控與預警： 公司應依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作： 1. 同一來源 IP 登入不同帳號達一定次數以上。 2. 同一帳號在一定時間內由不同國家登入。 3. 發現異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP)嘗試登入。 (111 年 9 月 30 日生效)	(十一)、(新增)	
		(以下略)	(以下略)	

近期修訂規範說明

CC-18000	存取控制	作業程序及控制重點： (一)~(二)略。 (三)、密碼管理： 1~2 略 3.密碼輸入錯誤次數達三次者，應予中斷連線**且鎖定該帳號，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，應確實辨認身分(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，並留存相關紀錄後，始得辦理之。(111 年 11 月 30 日生效)** 4、對因忘記密碼而無法登入系統之使用者**或客戶**申請核發原密碼時，應採取嚴格確認其身分及核發程序後**(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)**，方可開放其使用系統。	作業程序及控制重點： (一)~(二)略。 (三)、密碼管理： 1~2 略 3.密碼輸入錯誤次數達三次者，應予中斷連線。 4、對因忘記密碼而無法登入系統之使用者申請核發原密碼時，應採取嚴格確認其身分及核發程序後，方可開放其使用系統。	**依據主管機關 111 年 3 月 23 日金管證券字第 111033046 號函指示研議強化證券商對客戶帳號之密碼加強規範及管理，爰修訂(三)、(五)等相關項次，並修訂證券商內部控制制度標準規範。**

近期修訂規範說明

5.除**語音按鍵下單外**，~~輸入介面僅可輸入數字外(例如：語音按鍵下單)，~~公司應使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控，及加強宣導客戶定期更新**~~使用者~~**密碼以不超過三個月為宜，**如客戶密碼超過一年未變更或變更密碼與前一代相同，公司應做妥善處理。**除客戶外，公司其他使用者之密碼應至少每三個月變更一次。**(111 年 11 月 30 日生效)** 6.~8.(略) (四)略 (五)資料輸入管理： 1.~4.略 5.**密碼應使用公開安全且未遭破解之演算法(例如：雜湊演算法等不可逆運算式)產生亂碼並加密儲存。(111 年 11 月 30 日生效)** (以下略)	5、除輸入介面僅可輸入數字外(例如：語音按鍵下單)，公司應使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控，及加強宣導客戶定期更新使用者密碼以不超過三個月為宜。除客戶外，公司其他使用者之密碼應至少每三個月變更一次。 6.~8.(略) (四)略 (五)資料輸入管理： 1.~4.略 5.對隱密性高之重要資料，如通行碼之存放，應予亂碼後存放。 (以下略)

TAIWAN STOCK EXCHANGE

近期修訂規範說明

CC-19000	系統開發及維護	(一)~(十四)略。 (十五)、程式原始碼安全規範： 1~4 略 5.委外開發之行動應用程式如涉及機敏性資料傳送(如：客戶帳號密碼或交易資料等)應自行或委外檢視驗證傳遞對象是否適當並留存相關紀錄。 6. 公司應依上開安全事項檢驗程式原始碼並符合安全事項之要求；無法取得程式原始碼時，應要求程式提供者符合上開前五項安全事項之佐證。 (以下略)	(一)~(十四)略。 (十五)、程式原始碼安全規範： 1~4 略 5.(新增) 6. 公司應依上開安全事項檢驗程式原始碼並符合安全事項之要求；無法取得程式原始碼時，應要求程式提供者符合上開前四項安全事項之佐證。 (以下略)	依據主管機關指示研議檢討110年11月間證券商複委託遭駭客攻擊之原因並據以修訂相關資安規範，爰規範證券商須檢視及驗證行動應用程式機敏性資料傳輸對象之妥適性，並修訂證券商內部控制制度標準規範。

近期修訂規範說明

證券股份有限公司

作業週期：每月至少查核乙次

電腦作業與資訊提供查核明細表

項　　目	查　　核　　程　　序	查核結果 是	查核結果 否	查核結果 不適用	底稿索引
通訊與作業管理－網路安全管理（適用網際網路下單證券商，另一、二、五項並適用於全體證券商）	三、 網路傳輸安全管理： (一) 網路下單畫面是否採加密方式(例如：SSL)處理。 (二) 公司是否每日針對核心系統之帳號登入失敗紀錄、非客戶帳號**嘗試登入**紀錄等進行監控及分析，**發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，是否即時了解異常原因**，並留存相關紀錄。 (三) 網路下單登入時~~應~~**是否**採多因子認證方式(例如：下單憑證、綁定裝置、OTP、生物辨識等機制，以確保為客戶本人登入。 四、 CA 認證與憑證管理： (一) 網路下單是否訂定憑證交付程序，避免非本人取得憑證。**客戶申請或更新憑證下載，是否採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及 SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。** (二) 網路下單是否全面使用認證機制。 五、 電腦病毒及惡意軟體之防範： (一) 是否安裝防毒軟體，並及時更新程式及病毒碼。 (二) 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。				
備　　註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員　　日　期

近期修訂規範說明

電腦作業與資訊提供查核明細表

項　　目	查　　核　　程　　序	查核結果			底稿索引
		是	否	不適用	
通訊與作業管理－網路安全管理（適用網際網路下單證券商，另一、二、五項並適用於全體證券商）	七、公司提供 API 服務規範： 公司提供客戶使用應用程式介面(API)服務，是否於首次下單前就相關傳輸設定進行連線測試，並留存相關測試紀錄。 八、網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，是否訂定網際網路下單服務品質相關標準，並包含下列重點如：交易之安全性、交易之穩定及系統可用性、提供客戶服務。 **九、帳號登入或異常態樣通知：** **公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣是否即通知客戶，並留存紀錄，避免非客戶本人登入情事：(1)密碼輸入錯誤或帳戶被鎖定；(2)申請或更新憑證；(3)變更基本資料；(4)異常來源或行為嘗試登入等；(5)密碼申請異動或補發時。** **十、異常 IP 登入之監控與預警：** **公司應依其所屬資安分級對於嘗試登入帳號之異常及不明來源 IP，如發現下列情形，是否有警示機制，進行監控分析及留存紀錄，並定期檢視以確認機制有效運作：(1)同一來源 IP 登入不同帳號達一定次數以上；(2)同一帳號在一定時間內由不同國家登入；(3)發現異常 IP(如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單)或國外 IP 嘗試登入。**				

近期修訂規範說明

證券股份有限公司

作業週期：每月至少查核乙次　　電腦作業與資訊提供查核明細表

項　　目	查　　核　　程　　序	查核結果 是	查核結果 否	查核結果 不適用	底稿索引
存取控制	(二)密碼是否~~以亂碼方式儲存~~**使用公開安全且未遭破解之演算法(例如：雜湊演算法等不可逆運算式)產生亂碼並加密儲存。**。 (三)對於使用者**及客戶**忘記密碼之處理，**公司**是否有嚴格的身分確認程序**(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，並留存相關紀錄**，方可再次使用系統。 (四)初始密碼是否隨機產生，並與使用者**及客戶**身分無關。(本項不適用採自行訂定交付電子式交易密碼條之方式) (五)密碼輸入錯誤次數達三次者，是否予中斷連線**且鎖定該帳號。公司於接獲客戶聯繫時，是否確認客戶身分後(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，並留存相關紀錄，始得恢復使用**。 (六)除**語音按鍵下單外**~~輸入介面僅可輸入數字外（例如：語音按鍵下單）~~，公司是否使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控。 (七)**客戶密碼超過一年未變更或變更密碼與前一代相同，公司是否做妥善處理。**除客戶外，公司其他使用者之密碼是否至少每三個月變更一次。 (八)檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備是否設定使用密碼，且避免使用預設(如 administrator、root、sa)或簡易(如 1234)之帳號密碼及未設管理者存取權限。 (九)客戶申請採電子式交易型態者，如以一般電子方式交付電子密碼條時，是否傳送 OTP(One Time Password)密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信				

近期修訂規範說明

_____證券股份有限公司

作業週期：每半年至少查核乙次

電腦作業與資訊提供查核明細表

項　　目	查　　核　　程　　序	查核結果			底稿索引
		是	否	不適用	
系統開發及維護	十五、 如通過實驗室檢測後一年內有更新上架之需要，是否於每次上架前就重大更新項目進行委外或自行檢測；並留存相關檢測紀錄（適用網際網路下單證券商）。 十六、 對第三方檢測實驗室所提交之檢測報告，是否建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄（適用網際網路下單證券商）。 十七、 是否於發布前檢視應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵單位同意，並留有紀錄，以利綜合評估是否符合個人資料保護法之告知義務」（適用網際網路下單證券商）。 十八、 **委外開發之行動應用程式如涉及機敏性資料傳送(如：客戶帳號密碼或交易資料等)是否自行或委外檢視驗證傳遞對象之妥適性並留存相關紀錄。**				
備　　註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員 _____ 日　期 _____

FC-19000-S-3

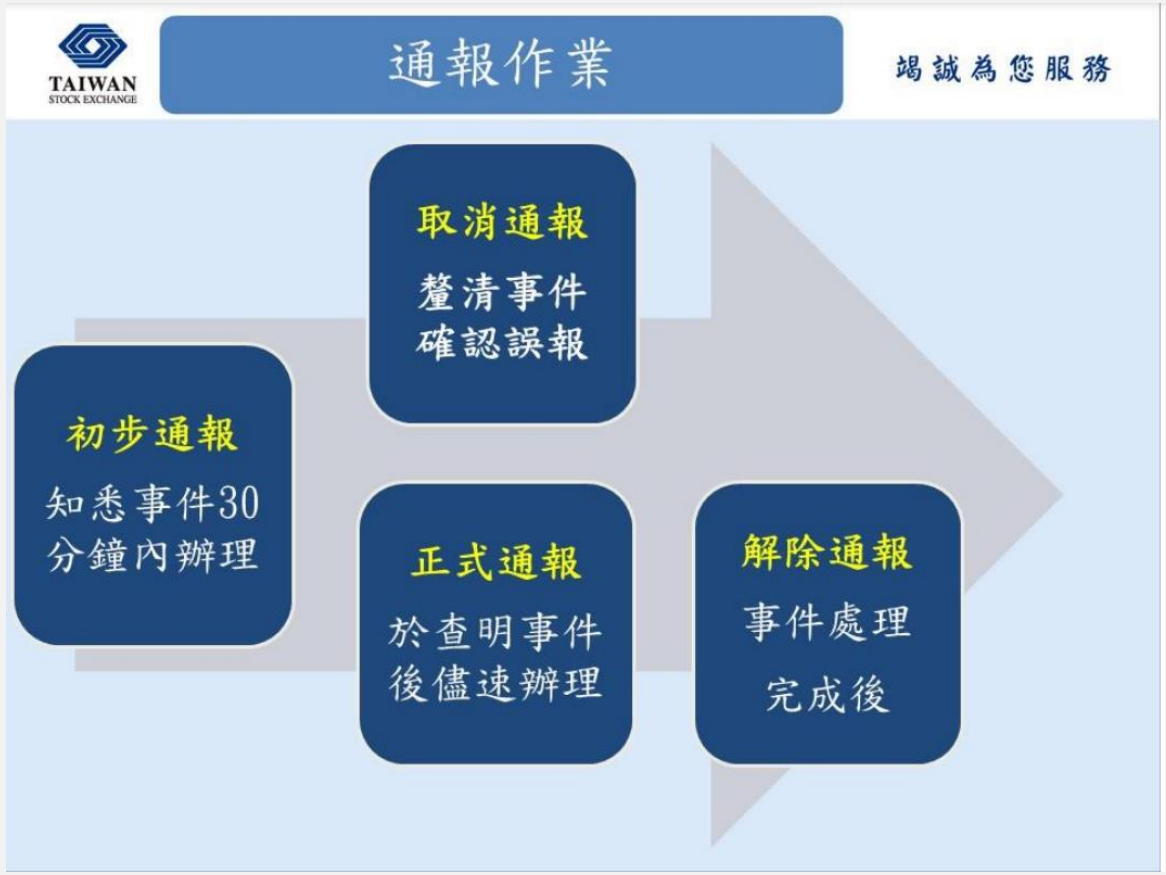
TAIWAN
STOCK EXCHANGE

重要事項宣導

明年實施

資本額分級標準	(規劃)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。

TAIWAN
STOCK EXCHANGE

簡報結束
敬請指導