建立證券商資通安全檢查機制-分級防護應辦事項附表

實收資本額分級表

等級 應辦事項	第一級證券商 實收資本額200億(含)以上	第二級證券商 實收資本額100億(含)以上，未達200億	第三級證券商 實收資本額40億(含)以上,未達100億	第四級證券商 實收資本額未達40億	對應項目
一、資訊安全管理系統之導入及通過公正第三方之驗證	初次受核定或等級變更後之二年內，全部核心資訊系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。	初次受核定或等級變更後之二年內，全部核心資訊系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。	初次受核定或等級變更後之二年內，全部核心資訊系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入，於三年內完成公正第三方驗證，並持續維持其驗證有效性。		2. 資訊安全政策(CC-12000)、(8)
二、資通安全專業證照(參考資安法資通安全專業證照清單含管理類及技術類)	初次受核定或等級變更後之一年內，資通安全人員總計應持有四張以上，並持續維持證照之有效性。	初次受核定或等級變更後之一年內，資通安全人員總計應持有三張以上，並持續維持證照之有效性。	初次受核定或等級變更後之一年內，資通安全人員總計應持有二張以上，並持續維持證照之有效性。	初次受核定或等級變更後之一年內，資通安全人員總計應持有一張以上，並持續維持證照之有效性。	3. 安全組織(CC-13000)、(6)
三、資訊系統分級	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	4.資產分類與控制(CC-14000)、(3)

等級 應辦事項	第一級證券商 實收資本額200億(含)以上	第二級證券商 實收資本額100億(含)以上，未達200億	第三級證券商 實收資本額40億(含)以上,未達100億	第四級證券商 實收資本額未達40億	對應項目
四、網路防火牆	建置網路防火牆	建置網路防火牆	建置網路防火牆	建置網路防火牆	7.通訊與作業管理 (1)網路安全管理(CC-17010)、b.(a)
五、防毒軟體	導入防毒軟體	導入防毒軟體	導入防毒軟體	導入防毒軟體	7.通訊與作業管理 (1)網路安全管理(CC-17010)、f.
六、電子郵件過濾機制	具有郵件伺服器者，應備電子郵件過濾機制。	具有郵件伺服器者，應備電子郵件過濾機制。	具有郵件伺服器者，應備電子郵件過濾機制。	具有郵件伺服器者，應備電子郵件過濾機制。	7.通訊與作業管理 (1)網路安全管理(CC-17010)、f.(e)
七、系統滲透測試	全部核心資訊系統每年辦理一次。	全部核心資訊系統每二年辦理一次。	全部核心資訊系統每二年辦理一次。		7.通訊與作業管理 (1)網路安全管理(CC-17010)、j.(a)
八、資通安全健診	第一類系統每年辦理一次；第二類系統每三年辦理一次；第三類系統每五年辦理一次。	第一類系統每年辦理一次；第二類系統每三年辦理一次；第三類系統每五年辦理一次。	第一類系統每二年辦理一次；第二類系統每三年辦理一次；第三類系統每五年辦理一次。	第一類系統每二年辦理一次；第二類系統每三年辦理一次；第三類系統每五年辦理一次。	7.通訊與作業管理 (1)網路安全管理(CC-17010)、j.(b)
九、資通安全威脅偵測管理機制	建置資通安全威脅偵測管理機制。(SIEM)	建置資通安全威脅偵測管理機制。(SIEM)	建置資通安全威脅偵測管理機制。(SIEM)		7.通訊與作業管理 (1)網路安全管理(CC-17010)、 j.(c)
十、入侵偵測及防禦機制	建置入侵偵測及防禦機制	建置入侵偵測及防禦機制	建置入侵偵測及防禦機制	建置入侵偵測及防禦機制(註1)	7.通訊與作業管理 (1)網路安全管理(CC-17010)、j.(d)
十一、應用程式防火牆	具有對外服務之核心資訊系統者，應備應用程式防火牆。	具有對外服務之核心資訊系統者，應備應用程式防火牆。	具有對外服務之核心資訊系統者，應備應用程式防火牆。	具有對外服務之核心資訊系統者，應備應用程式防火牆。(註1)	7.通訊與作業管理 (1)網路安全管理(CC-17010)、j.(e)
十二、進階持續性威脅攻擊防禦措施	建置進階持續性威脅攻擊防禦措施				7.通訊與作業管理 (1)網路安全管理(CC-17010)、j.(f)

等級 應辦事項	第一級證券商 實收資本額200億(含)以上	第二級證券商 實收資本額100億(含)以上，未達200億	第三級證券商 實收資本額40億(含)以上,未達100億	第四級證券商 實收資本額未達40億	對應項目
十三、公司不得使用危害國家資通安全產品。	公司交易相關網路直接連線之設備不得~~應避免~~使用危害國家資通安全產品。	公司交易相關網路直接連線之設備不得~~應避免~~使用危害國家資通安全產品。	公司交易相關網路直接連線之設備不得~~應避免~~使用危害國家資通安全產品。	公司交易相關網路直接連線之設備不得~~應避免~~使用危害國家資通安全產品。	4.資產分類與控制(CC-14000)、(5)
十四、業務持續運作演練	全部核心資訊系統每年辦理一次	全部核心資訊系統每二年辦理一次	全部核心資訊系統每二年辦理一次	全部核心資訊系統每二年辦理一次(註：自115年12月底生效)	10.營運持續管理(CC-20000)、(4)
十五、網路活動異常監控	公司應對異常及不明來源 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： (a)同一來源 IP 登入不同帳號達一定次數以上。 (b)同一帳號在一定時間內由不同國家登入。 (c)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。	公司應對異常及不明來源 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： (a)同一來源 IP 登入不同帳號達一定次數以上。 (b)同一帳號在一定時間內由不同國家登入。 (c)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。	公司應對異常及不明來源 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： (a)同一來源 IP 登入不同帳號達一定次數以上。 (b)同一帳號在一定時間內由不同國家登入。 (c)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。	公司應對異常及不明來源 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： (a)同一來源 IP 登入不同帳號達一定次數以上。 (b)同一帳號在一定時間內由不同國家登入。 (c)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。	7.通訊與作業管理 (1)網路安全管理(CC-17010)、1.
十六、核心系統重要組態設定檔案加密	對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。	對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。	對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。		7.通訊與作業管理 (2) 電腦系統及作業安全管理(CC-17020).b.(g)

等級 應辦事項	第一級證券商 實收資本額200億(含)以上	第二級證券商 實收資本額100億(含)以上，未達200億	第三級證券商 實收資本額40億(含)以上,未達100億	第四級證券商 實收資本額未達40億	對應項目
十七、核心系統帳號之使用管控	應訂定對核心系統之閒置時間或可使用期限與核心系統之使用情況及條件(如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等)。	應訂定對核心系統之閒置時間或可使用期限與核心系統之使用情況及條件(如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等)。	應訂定對核心系統之閒置時間或可使用期限與核心系統之使用情況及條件(如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等)。		7.通訊與作業管理 (2) 電腦系統及作業安全管理(CC-17020).b.(h)
十八、建置異地備援機房	依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統(註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自116年12月底生效。)	依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統(註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自116年12月底生效。)	依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統 (註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自116年12月底生效。)	符合設置資安長條件之證券商，依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統。(註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自116年12月底生效。)	10.營運持續管理(CC-20000)、(3)

註1：須建置 IPS 及 WAF 二項網路資安防禦機制，若無提供網頁下單服務者，可不須建置 WAF 機制。

經紀業務規模市占率暨自然人客戶數比率分級表

等級	A 級證券商(註2) (市占率1%以上且自然人客戶數達公司客戶數50%以上)	B 級證券商 (市占率未達1%或自然人客戶數未達公司客戶數50%以上)
應辦事項	核心系統可容忍中斷時間為1小時	核心系統可容忍中斷時間為2小時

註2：資格每年檢視乙次，首次適用由證交所通知所有證券商其所在級別，次年後則僅通知調整為 A 級之證券商，已列為 A 級者將不再變更級別。