「證券期貨業者資訊系統安全防護、網路安全防護、供應鏈風險管理」問卷填寫問與答(FAQ)

更新日期　　2021年7月16日

序號	問卷類別	題號	問項	選項	Q	A	更新日期
1	通則性問題	N/A	N/A	N/A	本次問卷的目的？	因應金融機構運用新興科技發展創新業務的趨勢，依金管會「金融資安行動方案」要求，爰增修訂證券期貨商資訊系統安全防護基準參考指引、證券期貨商網路安全防護基準參考指引以及證券期貨商供應鏈風險管理參考指引，以配合金融科技發展與業務開放，兼顧創新與風險之平衡。	6月30日
2	通則性問題	N/A	N/A	N/A	請問本問卷的核心系統與非核心系統定義為何?	本問卷的核心系統與非核心系統定義，係以是否為提供客戶交易或支持交易業務持續運作之必要系統進行判斷。	7月12日
3	通則性問題	N/A	N/A	N/A	請問本問卷目的為何?	因應金融機構運用新興科技發展創新業務的趨勢，依金管會「金融資安行動方案」要求，爰增修訂證券期貨商資訊系統安全防護基準參考指引、證券期貨商網路安全防護基準參考指引以及證券期貨商供應鏈風險管理參考指引，以配合金融科技發展與業務開放，兼顧創新與風險之平衡。懇請惠賜意見，作為相關指引修訂之參考。	7月12日
4	通則性問題	N/A	N/A	N/A	請問本問卷核心系統定義為何?	本問卷的核心系統與非核心系統定義，係以是否為提供客戶交易或支持交易業務持續運作之必要系統進行判斷。	7月12日
5	通則性問題	N/A	N/A	N/A	本公司為子公司，供應商由母公司選擇，請問本公司的狀況仍須填寫問卷嗎?	若貴司為子公司，且供應商由母公司選擇，本問卷供應商遴選問項可不必填寫，請於備註欄說明原因。其餘問項請就您所知的狀況盡量填寫	7月12日
6	通則性問題	N/A	N/A	N/A	本公司供應商包含提供軟體、硬體、網路等服務之供應商，請問該如何填寫問卷?	建議依照貴公司大致辦理情況填寫，如仍有疑慮可選擇「其他:請敘述」選項，並備註執行情形。	7月12日
7	通則性問題	N/A	N/A	N/A	請問網路安全防護問卷內容，是否跟核心系統有關?	本問卷跟核心系統無關，問卷設計僅針對網路相關的部分。	7月12日
8	(a)資訊系統安全防護	N/A	N/A	N/A	問卷填寫結果，可能作為未來稽核使用嗎？	本問卷結果使用純屬研究用途，僅供專案研究團隊了解目前業者實際作業狀況，以作為後續規範訂定參考，不會作為未來稽核使用。	6月30日
9	(a)資訊系統安全防護	N/A	N/A	N/A	問卷結果會如何使用？ 所有的問卷的項目都會變成未來的規範嗎？	本問卷結果使用純屬研究用途，僅供專案研究團隊了解目前業者實際作業狀況，將參考業者問卷結果，作為後續規範訂定參考。	6月30日
10	(a)資訊系統安全防護	N/A	N/A	N/A	如公司沒有應用系統，須要填寫哪些問卷項目？	針對無應用系統業者，無需填寫「(a)資訊系統安全防護基準問卷」、「(b)網路安全防護基準問卷」、「(d)核心系統供應商盤點」等3份問卷，其餘問卷設計皆已針對業者沒有應用系統的狀況，標示須填答/無須填答之問卷項目。	6月30日
11	(a)資訊系統安全防護	N/A	N/A	N/A	如公司沒有核心應用系統，須要填寫哪些問卷項目？	針對無核心應用系統業者，無需填寫「(d)核心系統供應商盤點」問卷，其餘問卷設計皆已針對業者沒有核心應用系統的狀況，標示須填答/無須填答之問卷項目。	6月30日

12	(a)資訊系統安全防護	N/A	N/A	N/A	問卷填寫上有疑問，諮詢的方式？	1.本案問卷填寫問與答(FAQ)(如附件2)，將於期間持續更新，如業者對問卷有任何填寫疑問，可至證交所「國內業務宣導網站」->「電腦資訊」->「宣導與講習」(https://dsp.twse.com.tw/advocacyWorkshop/list)路徑，取得最新版本問與答(FAQ)。 2.如前述問與答(FAQ)，仍無法解答填寫上的疑問，請利用下方管道聯繫專案窗口： (1)資訊系統安全防護基準問卷：丁先生；電子郵件：erting@deloitte.com.tw；電話：0919-419090 (2)網路安全防護基準問卷：王先生；電子郵件：nelswang@deloitte.com.tw；電話：0988-145130 (3)供應鏈風險管理問卷、核心系統供應商盤點：陳小姐；電子郵件：kaycchen@deloitte.com.tw；電話：0956-981226。	7月2日
13	(a)資訊系統安全防護	N/A	N/A	N/A	本問卷所稱之系統，是指公司所使用之系統、管理之系統或兩者皆是？	各控制措施評估以　貴公司所管理之系統為範圍。	6月29日
14	(a)資訊系統安全防護	N/A	N/A	N/A	本問卷評估之系統範圍，是否包含應用系統、資料庫(DB)、作業系統(OS)？	各控制項措施以應用系統為主要評估對象。	6月29日
15	(a)資訊系統安全防護	37	資訊服務供應商於貴公司使用遠端存取權限之比率?	(a)100% (b)75-99% (c)50-74% (d)25-49% (e)1-24% (f)無 (m)其他:請敘述	資訊服務供應商的遠端存取權限應如何計算?	請計算貴公司提供合約有效期間的資訊服務供應商的遠端存取權限比率。例如，今年貴公司總共有10家資訊服務供應商，貴公司允許提供其中3家遠端存取權限，比率即為30%。	6月29日
16	(a)資訊系統安全防護	15	貴單位採用哪些方式防止未經授權設備使用內部網路？（多選）	(a)綁定MAC位置 (b)強制系統更新 (c)強制防毒更新 (d)使用公司提供VPN (e)其他_____	請問未經授權設備的定義為何?	未經授權設備指不在組織預期內的設備（例如BYOD、非公司配發設備即是），但因特殊狀況允許存取內部網路的管控措施。	6月29日
17	(a)資訊系統安全防護	29	貴單位密碼原則有哪些？（多選）	(a)密碼輸入錯誤上限 (b)強密碼設定 (c)密碼需定期變更 (d)其他_____	請問密碼原則的範圍為何?	密碼原則主要範圍（包含但不限於）網域帳號密碼、網路設備特/高權帳號密碼…等。	6月29日
18	(a)資訊系統安全防護	N/A	N/A	N/A	本公司多數資訊系統由國外總公司統一採購並與供應商簽約，若簽約方非台灣公司，相關問題需如何填寫?	應先確認 貴公司之資訊服務供應商是否全數由國外總公司簽約管理。若資訊服務供應商非由台灣公司管理，則無須填寫相關問項，但應於備註欄註記並說明原因。	7月6日
19	(a)資訊系統安全防護	N/A	N/A	N/A	本問卷所涉資通系統稽核特定事件定義為何?	本問卷有關資通系統稽核特定事件定義，包含身分驗證失敗、存取資源失敗、帳號權限變更、重要資料異動、管理者帳號行為等。	7月14日
20	(a)資訊系統安全防護	N/A	N/A	N/A	本問卷所涉資通系統稽核處理失效定義為何?	本問卷所涉資通系統稽核處理失效之定義，包括儲存稽核紀錄空間不足或系統功能異常，造成產生的稽核紀錄無法存入或沒有內容等狀況。	7月14日
21	(a)資訊系統安全防護	N/A	N/A	N/A	若有滿足控制措施原則，但無滿足說明欄內全部描述項目，請問是否為已建立此控制項?	可以視為已建立此控制項，須於備註欄位註記說明滿足其問項要求的管控措施為何。	7月15日
22	(a)資訊系統安全防護	N/A	N/A	N/A	本問卷所涉核心系統與非核心系統定義為何?	請以系統是否為提供客戶交易或支持交易業務持續運作之必要系統，進行核心或非核心系統之判斷。	7月15日

23	(b)網路安全防護	N/A	N/A	N/A	本公司以代操服務為主，並無資訊服務供應商，對多數問題之業務(如:供應商遴選)沒有實際處理過，請問相關問題應如何填寫?	應先確認有無訂定相關供應商規範。若問項無法回答或與業務不相關則無須填寫，但應於備註欄說明原因。	7月6日
24	(b)網路安全防護	N/A	N/A	N/A	本公司網路皆由母公司管理，難以回答問卷題目。	若 貴公司為使用者角色，沒有進行網路管理，則無須填寫相關問項，但應於備註欄說明原因。	7月6日
25	(b)網路安全防護	N/A	N/A	N/A	本公司多數資訊系統由國外總公司統一採購並與供應商簽約，若簽約方非台灣公司，相關問題需如何填寫?	若資訊服務供應商非由台灣公司管理，則無須填寫相關問項，但應於備註欄說明原因。	7月7日
26	(b)網路安全防護	N/A	N/A	N/A	本公司今年六月方成立，僅有兩套系統且皆無涉及客戶交易，是否需要填寫問卷?	請以非核心系統的狀況進行問卷填答，另請協助於備註欄說明無核心系統的原因。	7月7日
27	(b)網路安全防護	N/A	N/A	N/A	本公司為外資，目前沒有對外服務和開發業務，有些問項無法填寫，應如何處理?	若 貴公司系統沒有對外服務，則無須填寫外部服務或外部使用者之相關問項，但應於備註欄說明原因。	7月7日
28	(b)網路安全防護	N/A	N/A	N/A	本次問卷的目的？	因應金融機構運用新興科技發展創新業務的趨勢，依金管會「金融資安行動方案」要求，爰增修訂證券期貨商資訊系統安全防護基準參考指引、證券期貨商網路安全防護基準參考指引以及證券期貨商供應鏈風險管理參考指引，以配合金融科技發展與業務開放，兼顧創新與風險之平衡。懇請惠賜意見，作為相關指引修訂之參考。	7月7日
29	(b)網路安全防護	N/A	N/A	N/A	因問卷問項多，填起來耗時耗工，是否有方法可以快速填寫?	問卷所涉資訊安全領域較廣泛故題目較多，懇請協助填寫， 貴公司提供的意見，將成為後續撰寫指引的寶貴資訊。	7月7日
30	(b)網路安全防護	N/A	N/A	N/A	公司為外資，網路由國外母公司管理，針對無法回答的問題應如何處理?	若單位為使用者角色，無進行網路管理，則無須填寫相關問項，但應於備註欄進行說明。	7月7日
31	(b)網路安全防護	18	依「金融機構辦理電腦系統資訊安全評估辦法」第五條資訊安全評估作業中所列舉之設備辦理網路安全檢測，請選擇有辦理的項目（多選）	(a)資訊架構檢視 (b)網路活動檢視 (c)網路設備、伺服器、端末設備及物聯網等設備檢測 (d)網路設備、伺服器及物聯網等設備且連線至Internet者 (e)客戶端應用程式檢測 (f)安全設定檢視 (g)合規檢視 (h)其他_____	[第18題]「金融機構辦理電腦系統資訊安全評估辦法」係銀行工會發佈規範銀行用，並不適用於證券業，惟本公司仍有就該辦法辦理自行檢視作業，請問本題應如何回覆?	請 貴公司協助回覆有依該辦法進行檢視的項目，並於備註說明並非依據此辦法，而係公司自行檢視。	7月14日
32	(b)網路安全防護	2	貴單位定期檢視網路設備存取控制清單（ACL）頻率為何？	(a)每月/次 (b)每季/次 (c)每年/次 (d)其他_____	[第2題] 網路設備由不同人管理（如防火牆是不同人管的)，是否都要回覆?	是的，網路設備若由不同人管理，皆必須回覆。	7月15日
33	(b)網路安全防護	3	貴單位目前有劃分哪些重要網路區域？（多選）	(a)非軍事區（DMZ） (b)正式區（Production） (c)測試區（UT） (d)驗收測試區（UAT） (e)災害復原區（DR） (f)辦公區（OA） (g)其他_____	[第3題] 本公司使用的名稱跟選項名稱有些微差異，是否以選項名稱為準?	若 貴公司使用的名稱跟選項名稱有些微差異，請以選項名稱為準。	7月15日
34	(b)網路安全防護	6	貴單位是否有已服務終止（EOS）網路設備？	(a)是 (b)否	[第6題] 本公司有EOS網路設備，係因廠商仍會維護，若回覆選項(a)是，是否會影響之後的政策?	本問卷係先調查各家現況，請照實回覆。	7月15日

35	(b)網路安全防護	18	依「金融機構辦理電腦系統資訊安全評估辦法」第五條資訊安全評估作業中所列舉之設備辦理網路安全檢測，請選擇有辦理的項目（多選）	(a)資訊架構檢視 (b)網路活動檢視 (c)網路設備、伺服器、端末設備及物聯網等設備檢測 (d)網路設備、伺服器及物聯網等設備且連線至Internet者 (e)客戶端應用程式檢測 (f)安全設定檢視 (g)合規檢視 (h)其他_____	[第18題] 請問經由Router連到Internet是否符合選項(d)網路設備、伺服器及物聯網等設備且連線至Internet的狀況?	是的，經由Router連到Internet已符合第18題選項(d)的狀況。	7月15日
36	(b)網路安全防護	20	貴單位提供交易之網際網路應用系統是否設有連線逾時機制？	(a)是 (b)否	[第20題] 此題指的是對外服務的系統?	是的，本問項所涉網際網路應用系統，係指對外服務的系統。	7月16日
37	(b)網路安全防護	23	貴單位針對遠端連線至內網是否限制系統/檔案存取範圍？	(a)是 (b)否	[第23題] 此題的遠端連線至內網包含哪些方式?	本問項所涉遠端連線至內網的方式，RDP(遠端桌面協定)和VPN都屬之。	7月16日
38	(c)供應鏈風險管理	N/A	N/A	N/A	公司為外資，網路由國外母公司管理，針對無法回答的問題應如何處理?	若單位為使用者角色，無進行網路管理，則無須填寫相關問項，但應於備註欄進行說明。	7月7日
39	(c)供應鏈風險管理	N/A	N/A	N/A	資訊系統皆由金控/證券母公司採購並與供應商簽約，相關問題需如何填寫?	若資訊服務供應商非貴公司管理，相關問項無須填寫，但應於備註欄進行說明。	7月8日
40	(c)供應鏈風險管理	N/A	N/A	N/A	請問本問卷用途為何?	因應金融機構運用新興科技發展創新業務的趨勢，依金管會「金融資安行動方案」要求，爰增修訂證券期貨商資訊系統安全防護基準參考指引、證券期貨商網路安全防護基準參考指引以及證券期貨商供應鏈風險管理參考指引，以配合金融科技發展與業務開放，兼顧創新與風險之平衡。懇請惠賜意見，作為相關指引修訂之參考。	7月9日
41	(c)供應鏈風險管理	N/A	N/A	N/A	本公司專案類型皆不一致，同一問項可能有不同的回答情形，這種狀況應如何填寫?	建議依照 貴公司各專案大致辦理情況填寫，如仍有填寫疑慮，可選擇「其他:請敘述」選項，並備註執行情形。	7月9日
42	(c)供應鏈風險管理	N/A	N/A	N/A	因部分資訊系統採購合約並非由本單位處理，這種狀況應如何進行填答?	建議請偕同其他單位，一同協助填答，若偕同其他單位共同填答在執行上有困難，盡量以您了解的情形填寫問卷。	7月9日
43	(c)供應鏈風險管理	N/A	N/A	N/A	請問本問卷的委外廠商是否包含維護廠商?	只要是委由外部供應商提供資訊服務，不論開發或是維護皆屬本問卷委外廠商的範疇。	7月9日
44	(c)供應鏈風險管理	28	核心系統之資訊服務供應商服務若有重大變更(組織調整、業務重大異動等，如:團隊變更、原定專案內容重新規劃)時，貴公司是否針對變更重新專案風險評估?	(a)是 (b)否 (c)其他:請敘述	[第28題] 若有專案發生重大變更不會重新跑風險評估流程，但會以實際工作情形判斷評估專案狀況，這種狀況應如何填答?	建議 貴公司留下正式文件紀錄證明確實評估專案風險，若不以正式流程或規範辦理，以實際狀況做評估，可考量勾選「其他:請敘述」並備註說明	7月9日
45	(c)供應鏈風險管理	29	貴公司是否要求資訊服務供應商服務提供安全性檢測報告?	(a)是 (b)否 (c)其他:請敘述	[第29題] 請問本問卷第29題的安全性檢測報告為何?	本問卷第29題的安全性檢測報告意指，針對系統及設備安全性問題進行檢測所產出的報告，如弱點掃描及滲透測試報告等。	7月9日

46	(c)供應鏈風險管理	35	貴公司進行資訊服務供應商於貴公司內部系統(作業系統、應用系統、核心系統)或設備之軌跡檢視頻率?	(a)每月一次 (b)每季一次 (c)每半年一次 (d)每年一次 (e)每二年一次 (f)無 (g)其他:請敘述	[第35題] 請問本問卷第35題的設備軌跡為何?	本問卷第35題的設備之軌跡，意指為設備連線及運作時所產生的紀錄，組織可藉由軌跡(log)了解系統運作狀態與使用者活動。	7月9日
47	(c)供應鏈風險管理	19	貴單位現行規範是否接受單一帳號多重登入？	(a)是 (b)否	[第19題] 本問項提到的單一帳號多重登入，是否指在同一網域的情形?	是的，此處單一帳號多重登入是指在同一網域的情形。	7月9日
48	(c)供應鏈風險管理	26	承上，是否有建立避免使用者（利用多個跳板機）使用蛙跳機制？	(a)是 (b)否	[第26題] 請問本公司應如何執行，才算做到符合第26題建立蛙跳機制的狀況?	顧問團隊僅針對問卷填寫相關問題進行說明，不便提供進一步建議。	7月9日
49	(c)供應鏈風險管理	32	承上，稽核日誌定期檢視頻率為何？	(a)每月/次 (b)季/次 (c)年/次 (e)其他_____	[第32題] 請問本問項檢視稽核日誌的意思為何?	本問項檢視稽核日誌的意思，即為log檢視。	7月9日
50	(c)供應鏈風險管理	N/A	N/A	N/A	請問本公司目前Windows系統有設定五分鐘自動登出，這樣是否算資通系統設有閒置時間?	不算，應以資通系統本身是否設置閒置時間，並具有帳號自動登出機制為準。	7月12日
51	(c)供應鏈風險管理	N/A	N/A	N/A	請問遠端桌面連線是否可定義為遠端連線?	是的，遠端桌面也是遠端連線方式之一。	7月12日
52	(c)供應鏈風險管理	N/A	N/A	N/A	請問本問卷系統總數量計算方式，應以系統數去盤點，還是以系統裡的伺服器數量進行盤點?	系統總數量計算方式，以系統總數進行盤點即可。	7月12日
53	(c)供應鏈風險管理	42	貴公司合約文件是否要求核心系統之資訊服務供應商於時限內完成資安事件處理?	(a)是 (b)否 (c)其他:請敘述	供應商可能有多種事件，此題只限資安事件嗎?	是的，供應商可能有多種事件，此題只限資安事件。	7月15日
54	(c)供應鏈風險管理	44	貴公司是否要求資訊服務供應商針對專案服務之應用系統及設備提供跡證保存機制?	(a)是 (b)否 (c)其他:請敘述	資訊服務供應商之系統之log皆會拋轉至公司系統，是否屬跡證保存?	是的，資訊服務供應商之系統之log皆會拋轉至公司系統，屬於跡證保存。	7月15日