Deloitte.

勤業眾信

證券期貨市場相關公會新興科技資通安全管控指引參考指引說明

Deloitte Risk Advisory、2022/05

Agenda

- 目的 & 總說明
- 修正現有章節說明
- 新增章節說明
- 問題與討論

目的 & 總說明

目的 & 總說明

目的

為協助證券商、期貨商及投信投顧業者強化新興科技資通安全管控之議題，依據金融監督管理委員會「金融資安行動方案」強化金融業資安防護能力，增修訂資安自律規範，納入行動應用程式(APP)、雲端服務、物聯網、網路身分驗證等新興科技安控規範。

總說明

本管控指引係參考以下法規，經蒐集實務做法併邀集業者共同研議相關參考指引，以有效的管理及應用新興科技之資通安全風險

1. 資通安全管理法及其子法
2. 金融機構運用新興科技作業規範、金融機構辦理電子銀行業務安全控管作業基準
3. 電子支付機構資訊系統標準及安全控管作業基準辦法
4. 經濟部工業局行動應用App基本資安檢測基準
5. 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、證券商作業委託他人處理內部作業制度及程序辦法
6. 臺灣證券交易所股份有限公司營業細則、臺灣期貨交易所股份有限公司業務規則
7. 臺灣證券交易所股份有限公司證券商受理線上開戶委託人身分認證及額度分級管理標準
8. 中華民國證券商業同業公會新興科技資訊安全自律規範
9. 中華民國證券投資信託暨顧問商業同業公會國內證券投資信託基金電子交易作業準則、中華民國證券投資信託暨顧問商業同業公會境外基金電子交易作業準則
10. 美國「H.R.3230 - DEEP FAKES Accountability Act」

修正現有章節說明
雲端運算服務、社群媒體、行動裝置、物聯網設備

概要說明

新興科技資通安全管控指引適用範圍

適用對象		
本指引適用對象包含證券商、期貨商、證券投資信託事業及證券投資顧問事業		
適用定義及範圍		
第二章、雲端運算服務運作安全	定義 (第二條)	透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務。如：IaaS(基礎架構即服務)、PaaS(平台即服務)、SaaS(軟體即服務)。 一. 基礎架構即服務(Infrastructure as a Service，簡稱IaaS)：雲端服務提供者通過網路向雲端服務使用者提供資訊科技基礎設施。 二. 平台即服務(Platform as a Service，簡稱PaaS)：雲端服務提供者向雲端服務使用者提供平台工具。 三. 軟體即服務(Software as a Service，簡稱SaaS)：雲端服務提供者利用網際網路向雲端服務使用者提供應用程式服務。
	範圍 (第三條)	一. 為確保組織使用雲端運算服務之安全，組織應事先評估使用雲端服務之風險，若雲端服務涉及**核心**系統、資料或服務者，應符合本指引控管建議。 二. 本指引定義之雲端服務，不包含建置組織內部且僅對內提供服務之私有雲。
第三章、社群媒體安全控管	定義 (第十條)	一種結合科技、社交互動與內容創造之網路應用，允許創造或交換使用者產出內容；且透過此高度互動的平台，個人及群體可以分享、共創、討論並修改使用者產出內容。
	範圍 (第十一條	本指引定義之社群媒體，不包含組織內部溝通使用之社群媒體或平台。

新興科技資通安全管控指引適用範圍

適用對象		
本指引適用對象包含證券商、期貨商、證券投資信託事業及證券投資顧問事業		
適用定義及範圍		
第四章、行動裝置安全控管	定義 (第十五條)	一. 行動裝置：一種具有資料運算處理、儲存與網路連線功能之可攜式設備，係指包含但不限於智慧型手機、筆記型電腦、平板電腦與PDA等裝置。 二. 員工自攜行動裝置(BYOD)：非屬組織行動裝置用於處理組織事務、直接連接組織網路設備或服務，並具備資料運算處理、儲存與網路連線功能之可攜式設備。
	範圍 (第十六條)	本指引定義之行動裝置，僅限於可用於處理組織內部定義之敏感性事務且可直接連接組織網路設備、服務之行動裝置。
第五章、物聯網設備安全控管	定義 (第二十一條)	指具網路連線功能之嵌入式系統設備及其周邊連網之裝置(如：感測器)。
	範圍 (第二十二條)	本指引定義之物聯網為具備網路連線功能且有連接外部或內部網路之自動化辦公(OA)設備，如：數位錄影機、電話交換機、傳真機、錄音設備、影印機、監視器等。

第二章、雲端運算服務運作安全條文說明

新興科技資通安全管控指引-第二章、雲端運算服務運作安全-第四、五條

條文	內容
第四條	（雲端服務提供者選擇） 一. 雲端服務使用者應**事先評估**雲端服務提供者之**服務水準(含資通安全防護)等風險**，採取適當風險管控措施。若有不符合需求之處，應考量其他補償性措施。 二. 雲端服務使用者應評估雲端服務提供者是否已**建立雲端服務備援機制**，並建議於**合約中明文規定雲端服務復原時間**之相關要求。 三. 雲端服務使用者就雲端服務提供者處理之資料應**保有完整所有權**，除執行受託作業外，應確保雲端服務提供者不得有存取客戶資料之權限，並不得為委託範圍以外之利用。 四. 雲端服務使用者就雲端服務委外作業，應落實定期對雲端服務提供者之查核。如雲端服務提供者已取得雲端安全國際認證(CSA-Star)銅牌以上者，則可視實際情況要求提供驗證報告或進行實地查核。
第五條	（雲端互通性和可移植性） 一. 雲端服務提供者應滿足雲端使用者對於應用程式及資訊處理之**互通性與可移植性需求**，並提出相關**說明文件**供使用者參考。 二. 雲端服務提供者宜使用業界常見之虛擬化平台、虛擬機檔案格式、資料檔案格式，以**確保互通性**。 三. 雲端服務提供者應依雲端服務使用者需求，使用標準化的網路協定。如涉及敏感性資料之傳遞，宜使用超文字傳輸安全協定(HTTPS)、安全檔案傳輸協定(SFTP)等加密之網路協定。 四. 雲端服務提供者提供之雲端服務若涉及應用程式介面存取服務，宜使用開放或已公開之應用程式介面(API)，以確保應用程式元件可以較容易地轉移。

新興科技資通安全管控指引-第二章、雲端運算服務運作安全-第六、七條

條文	內容
第六條	（雲端供應鏈管理） 一. 雲端服務使用者傳輸及儲存客戶資料至雲端服務提供者，應採行客戶資料加密或代碼化等有效保護措施，並**應訂定妥適之加密金鑰管理機制**。 二. 雲端服務提供者應根據與雲端服務使用者之**服務水準協議**，維持其服務水準，且**應定期提供協議中各項服務水準指標之報告與操作紀**錄(如系統變更紀錄、作業系統映像檔存取紀錄等)。 三. 雲端服務提供者應**負責檢視**雲端服務供應鏈中其他合作夥伴**可能影響服務品質的風險與錯誤**。 四. 雲端服務提供者應於雲端服務運作**發生資通安全事件**時，**及時通知**受影響的雲端服務使用者與供應鏈中的合作夥伴，並定期更新事件處理的相關訊息。
第七條	（雲端基礎設施與虛擬化安全，**適用於IaaS、PaaS服務**） 一. 雲端服務提供者**應確保虛擬機映像檔之完整性**，有關**映像檔的重要異動**，如：調整虛擬機記憶體大小、調整虛擬機硬碟容量等，都**應該被記錄**，並提供客戶檢視相關變更紀錄之機制。 二. 雲端服務提供者如有**設備維護更換時**(如硬碟更換)，所含組織之資料**須進行全數刪除或銷毀**，應依據其儲存媒介之性質，以消磁、銷毀、粉碎或其他適當之方式進行銷毀程序，並留存刪除或銷毀之紀錄。 三. 雲端服務提供者應依據雲端服務使用者需求，提供虛擬機隔離性(isolation)說明，**隔離性失效時應立即通知雲端服務使用者**。 四. 雲端服務提供者應就雲端作業系統，包含虛擬層 (hypervisor)與虛擬機的作業系統(guest operating systems)，輔以**適當的安全控管措施**，如：僅開放必要連接埠(Port)、通訊協定(Protocols)與服務(Service)、病毒防護、安全漏洞評估機制、檔案完整性監控等。 五. 雲端服務運作人員權限管理應採**權限最小化原則**，輔以適當安全控管措施，如：透過雙因子認證、稽核軌跡、IP地址過濾、防火牆，以及傳輸層安全性(TLS)封裝的通訊管理。 六. 雲端服務提供者提供IaaS服務(基礎架構即服務)時，應依雲端服務使用者需求將**含敏感資料之虛擬硬碟進行加密**，**限制快照或未授權存取**。

新興科技資通安全管控指引-第二章、雲端運算服務運作安全-第八、九條

條文	內容
第八條	（雲端服務之個人資料跨境傳輸） 涉及**個人資料跨境傳輸之雲端服務**，組織應建立加密傳輸機制且應就雲端服務提供者對客戶資訊之蒐集、處理、利用、國際傳輸及控管情形確認**符合我國個人資料保護法相關規定**，傳輸前應**取得當事人授權**且**不違反主管機關對國際傳輸之限制**，並**留存完整稽核紀錄**。
第九條	（雲端服務中斷及終止管理） 一. 雲端服務使用者應**訂定妥適之緊急應變計畫**，降低因雲端作業而可能有服務中斷之風險。 二. 雲端服務使用者**終止或結束作業委託**，應**確保能順利移轉**至另一雲端服務提供者或**移回自行處理**。 三. 雲端服務提供者於**提供終止後**，應**全數刪除或銷毀留存資料**(如虛擬機映像檔、儲存空間、快取空間、備份媒體、客戶資料或敏感資料)，並出具資料完全刪除之證明。

第三章、社群媒體安全控管條文說明

新興科技資通安全管控指引-第三章、社群媒體安全控管-第十二、十三、十四條

條文	內容
第十二條	（社群媒體使用政策） 一. 組織應擬定**社群媒體使用政策**，並**至少每年檢視一次**，以規範員工使用社群媒體行為，包含： (一)界定可**接受使用之社群媒體、功能及使用規則**。 (二)界定可於**社群媒體上分享之業務相關資料**。 (三)界定**私人與公務用社群媒體之區別**與應注意事項。 (四)界定各角色被**授予之發言權責**，並避免非授權之公務言論發表。 二. 組織應針對**開放**員工使用之**社群媒體類型評估其風險程度**，包含：資料外洩、社交工程、惡意程式攻擊等，並就高風險部分採行適當的安全控管措施，如：教育訓練或宣導、內容過濾及監控、防範惡意程式等防護機制。
第十三條	（組織經營官方社群媒體） 一. 組織應事先了解所經營之**社群媒體隱私政策**，並**定期檢視其隱私政策**之異動及評估其風險。 二. 組織於官方網站提供連結供使用者**連至組織外之社群媒體時**，應**出現提示視窗告知使用者**該連結非組織本身之網站。 三. 組織所經營之社群媒體應**標示組織名稱、聯絡方式及許可證字號**，以區別為官方經營之社群媒體。 四. 組織經營社群媒體時，應**建立帳號權限管理機制**，並對發布**內容制定過濾及監視政策**，其監視內容應至少包含防止客戶隱私及組織機密外洩、非授權或偽冒身分發言及不可有攻擊或詆毀同業之情事。
第十四條	第十四條（制定異常通報及申訴處理機制） 一. 組織應制定**社群媒體異常事件通報程序**，其經營官方社群媒體之管理單位，宜不定時監看該社群媒體之討論內容，並針對不適當言論或異常事件，進行必要之通報或處置。 二. 組織經營之**社群媒體應標示客戶申訴聯繫方式及處理窗口**。

第四章、行動裝置安全控管
條文說明

新興科技資通安全管控指引-第四章、行動裝置安全控管-第十七、十八條

條文	內容
第十七條	（公務用之行動裝置設備控管） 一.組織對於行動裝置**的申請、使用、更新、繳回與遺失應訂有相關規範**。 二.組織**人員異動**時，應進行**重新配置或清除配置程序**，以確保行動裝置環境安全性。 三.組織對行動裝置與行動裝置可存取的資源應**進行風險評估作業**，並依據風險評估結果採行適當的**安全控管措施**，如：螢幕鎖定、限制存取敏感資料、安裝防毒軟體、安裝行動裝置管理軟體等。 四.組織針對存有敏感性資料之行動裝置宜採行以下安全控管措施： (一)行動裝置宜**建立身分識別機制**。 (二)行動裝置之作業系統環境設定宜由**被授權者進行變更**。 (三)行動裝置之**作業系統與防毒軟體宜定期檢查**，避免持有者私自異動設定，如：越獄(Jailbreaking)或提權(Rooting)。 (四)行動裝置宜考量**遺失時資料清除方式**，如：以遠端方式刪除資料或透過身分認證錯誤超過規定次數後自動刪除機制。 (五)行動裝置宜**限制或關閉不需要之無線連線功能**，如：NFC、紅外線、Wifi或藍芽等。 (六)行動裝置傳輸敏感性資料時，宜採**加密或資料遮蔽**方式進行保護。 (七)行動裝置宜**限制敏感性資料儲存**於行動裝置上或將敏感性資料進行加密保護。 五.組織公務用之行動裝置應**避免安裝非官方發布之行動應用程式**，或僅安裝由組織列出通過檢測可安裝之行動應用程式。
第十八條	（員工自攜行動裝置管理）（BYOD） 一. 組織應**定期審核並限制**員工自攜行動裝置使用用途、使用期間及資料種類。 二. 組織應與持有人**簽署員工自攜行動裝置使用協議**，含：使用限制及雙方責任等。 三. 組織宜**限制內部資通設備**透過員工自攜行動裝置私接存取網際網路(Internet)之行為。

新興科技資通安全管控指引-第四章、行動裝置安全控管-第十九、二十條

條文	內容
第十九條	（行動應用程式安全控管）（Mobile App） 一. 組織透過行動應用程式發送簡訊或其他訊息通知方式告知使用者敏感性資料時，應進行**適當去識別化**。 二. 組織應**建立偽冒行動應用程式偵測機制**，以維護客戶權益。 三. 組織於啟動行動應用程式時，如偵測行動裝置疑似遭破解（如root、 jailbreak、 USB debugging等），**應提示使用者注意風險**。
第二十條	（行動應用程式發布控管） 一. 組織發布行動應用程式前應檢視行動應用程式所需**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。 二. 組織應於**可信任來源之行動應用程式商店或網站**發布行動應用程式，且應於**發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途**。 三. 涉及投資人使用之行動應用程式於**初次上架前及每年**，組織應委由經**財團法人全國認證基金會(TAF)認證合格之第三方檢測實驗室**進行並完成**通過資安檢測**，檢測範圍以經濟部工業局委託執行單位「行動應用資安聯盟」公布之行動應用程式基本資安檢測基準項目進行檢測。 四. 如通過實驗室檢測後一年內有更新上架之需要，組織應於**每次上架前就重大更新項目進行委外或自行檢測**；所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。檢測範圍以 OWASP MOBILE TOP 10 之標準為依據，並留存相關檢測紀錄。 五. 組織對第三方檢測實驗室所提交之檢測報告，應依經濟部工業局委託執行單位「行動應用資安聯盟」公布之行動應用程式基本**資安檢測基準項目建立覆核機制**，以確保檢測項目及內容一致，並留存覆核紀錄。

第五章、物聯網設備安全控管
條文說明

新興科技資通安全管控指引-第五章、物聯網設備安全控管-第十二、十三、十四條

條文	內容
第二十三條	（設備盤點評估） 組織應建立**物聯網設備管理清冊並至少每年更新一次**，以識別設備用途、網路設定、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制。
第二十四條	（設備軟體控管） 組織建置之物聯網設備應具備**安全性更新機制且定期更新**，以維持設備的可用性與完整性。
第二十五條	（設備權限控管） 組織建置之物聯網設備應具備**身份驗證機制或配對綁定機制**，並應進行**初始密碼變更**，且以**最小權限原則**針對不同的使用者身分進行授權，確保僅能由經授權之使用者進行資料存取、設備管理及安全性更新等操作。
第二十六條	（設備連線控管） 組織應**關閉物聯網設備不必要之網路連線及服務**，並避免使用對外公開的網際網路位置， 如設備採用**公開的網際網路位置**，應於設備**前端設置防火牆**予以防護，並採用**白名單**方式進行存取過濾。 如設備以**無線連接網路者**，應採用具**加密協定之無線存取點**連接網路，並以**網路卡卡號白名單**等機制進行設備綁定。
第二十七條	（設備採購控管） 組織於採購物聯網設備前應依據二十四條至二十六條進行評估及測試，宜優先採購取得**資安標章之物聯網設備**。

新興科技資通安全管控指引-第五章、物聯網設備安全控管-第十二、十三、十四條

條文	內容
第二十八條	（供應商管理） 組織如與**物聯網設備供應商簽定採購合約**時，其內容應包含**資通安全相關協議**，明確約定相關責任(如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案)，確保設備不存在已知安全性漏洞。
第二十九條	（物聯網認知控管） 組織應定期辦理物聯網設備使用及管理人員**資安教育訓練**。
第三十條	（例外控管） 組織知悉物聯網設備存在已知弱點且無法更新，或因設備功能限制無法落實第二十四條至二十六條之規範，應中斷設備網路連線，僅於必要時連接內部網路並**擬定汰換計畫**，汰換前應設置於獨立網段與內部網路進行區隔。
第三十一條	（不具備管理功能之感測器控管） 組織針對不具備管理功能之物聯網設備感測器，其功能雖較為單純且風險較低，仍應遵循本規範第二十三、二十六、二十七、二十八、二十九、三十條之要求辦理。

新增章節說明
電子式交易身分驗證、深度偽造防範

新興科技資通安全管控指引**適用範圍**

適用對象		
本指引適用對象包含證券商、期貨商、證券投資信託事業及證券投資顧問事業		
適用定義及範圍		
第六章、電子式交易身分驗證安全控管	定義 (第三十二條) (第三十三條)	指以組織同意之電子式委託買賣前對使用者身分驗證資訊進行確認。 電子式交易型態指委託人以「臺灣證券交易所股份有限公司營業細則」第七十五條、「臺灣期貨交易所股份有限公司業務規則」第四十八條、「中華民國證券投資信託暨顧問商業同業公會國內證券投資信託基金電子交易作業準則」第二條、「中華民國證券投資信託暨顧問商業同業公會境外基金電子交易作業準則」第二條所訂之電子式委託買賣方式。
	範圍 (第三十四條)	本指引定義之電子式交易身分驗證，僅適用於透過網際網路交易之系統，不包含電話語音、電子式專屬線路下單（Direct Market Access，簡稱DMA）、主機共置（Co–Location）等服務型態。
第七章、深度偽造防範安全控管	定義 (第三十九條)	指使用電腦合成或其他科技方法製作或散布涉及真實人物實際未發生的行為舉止影像紀錄、動態圖像、錄音、電子圖像、照片及任何言語或行為等技術表現形式。

第六章、電子式交易身分驗證安全控管條文說明

新興科技資通安全管控指引-第六章、電子式交易身分驗證安全控管-第三十五、三十六條

條文	內容
第三十五條	（電子式交易之訊息防護措施） **訊息防護措施應符合訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性之安全設計**，應符合下列要求： 一. 訊息隱密性：應採用AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同含以上之演算法進行加密運算，應採用TLS 1.2（含）以上之通訊協定並使用 Elliptic Curve Diffie-Hellman Exchange方式進行金鑰交換。 二. 訊息完整性：應採用SHA 256bits、AES 128bits、RSA 2048bits、ECC 256bits以上或其他安全強度相同含以上之演算法進行押碼或加密運算。 三. 訊息來源辨識性：應採用SHA 256 bits、AES 128bits、RSA 2048bits、ECC 256bits以上或其他安全強度相同 含以上之演算法進行押碼、加密運算或數位簽章。 四. 訊息不可重複性：應採用序號、一次性亂數、時間戳記等機制產生。 五. 訊息不可否認性：應採用SHA256以上或其他安全強度相同（含）以上之演算法進行押碼，及採用RSA 2048bits、ECC 256bits以上或其他安全強度相同含以上之演算法進行數位簽章。

新興科技資通安全管控指引-第六章、電子式交易身分驗證安全控管-第三十五、三十六條

條文	內容
第三十六條	（電子式交易身分驗證機制管理） 一. 除「金融機構辦理快速身分識別機制安全控管作業規範」另有規範之作業方式外，組織提供電子式交易登入時，其**安全設計應具有下列三項之任兩項以上技術**： (一)組織**所約定**之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等）。 (二)客戶**所持有**之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等），組織應確認該設備為客戶與組織所約定持有之設備。 (三)客戶提供給組織其**所擁有**之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），組織應直接或間接驗證該生物特徵。間接驗證係指由客戶端設備（如行動裝置）驗證或委由第三方驗證，組織僅讀取驗證結果，必要時應加驗證來源辨識；採用間接驗證者，應事先評估客戶身分驗證機制之有效性。 二. 組織使用**固定密碼為驗證機制**，於資料如為固定密碼者，於**儲存時應先進行不可逆運算（如雜湊演算法）**，另為防止透過預先產製雜湊值推測密碼，應**進行加密保護或加入不可得知之資料運算**。 三. 組織**直接驗證生物特徵且儲存生物特徵資料於組織內部系統**時，應將**原始生物特徵資料去識別化使其難以還原、將原始生物特徵資料及假名標識符進行加密儲存、將生物特徵資料分別儲存於不同之儲存媒體（如資料庫）**；儲存於組織提供之**端末設備**時，應儲存於**符合FIPS 140-2 Level 3標準**含以上之設備。 四. 組織**直接驗證該生物特徵**時應依據其風險承擔能力**調整生物特徵之錯誤接受度**，以能有效識別客戶身分；採用**間接驗證**者，**應事先評估客戶身分驗證機制之有效性**。 五. 組織使用憑證作為驗證機制，應為**經濟部核定之憑證機構所核發之憑證**，並強化憑證換發之驗證機制，以確保為客戶本人登入。

新興科技資通安全管控指引-第六章、電子式交易身分驗證安全控管-第三十七、三十八條

條文	內容
第三十七條	（電子式交易身分驗證控管） 一. 組織對於電子式交易身分的**申請、交付、使用、更新與驗證應訂有相關規範**。 二. 組織對電子式交易身分的驗證資訊於**網際網路傳輸時應全程加密**。 三. 組織對電子式交易身分的驗證資訊應**進行雜湊或加密儲存**。 四. 組織應於伺服器端驗證其電子式交易身分，避免因設置於客戶端而被繞過驗證機制之風險。 五. 組織應使用優質密碼設定並進行管控，確實執行**密碼輸入錯誤次數達3次者應予帳號鎖定**。 六. 組織應提供客戶**定期更新密碼之機制並使用優質密碼**（如：客戶逾三個月未更改密碼時應提供客戶更改密碼機制，提醒客戶更新密碼）。 七. 組織應**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。
第三十八條	（電子式交易稽核軌跡） 一. 組織應留存個人資料**使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）**或**辨識機制**，以利個人資料外洩時得以**追蹤個人資料使用狀況**。 二. 組織應就**帳號登入及交易紀錄時通知帳號所有者**，並留存相關紀錄。

第七章、深度偽造防範安全控管條文說明

新興科技資通安全管控指引-第七章、深度偽造防範安全控管-第四十、四十一、四十二條

條文	內容
第四十條	（電話交易身分驗證控管） 一. 組織如提供電話交易服務，應訂定**身分驗證程序(如語音密碼)**避免非本人之假冒。 二. 委託人以語音委託時，應配合**電信機構開放顯示發話端號碼之功能**，記錄其來電號碼。
第四十一條	（影像視訊身分驗證控管） 一. 組織使用影像視訊方式進行身分驗證時應**使用一次性密碼(OTP)**、**專人電訪**或**查驗本人並核對證件照片**等方式強化驗證。 二. 組織使用影像視訊時應確認**真實視訊環境（如隨機問答）**，以防止透過科技預先錄製影片。 三. 組織應留存**影像或照片**，以利後續查證。
第四十二條	（深度偽造防範控管） 組織每年定期辦理之**資訊安全教育訓練**，宜涵蓋**深度偽造認知及防範議題**。

問題與討論

Deloitte.

勤業眾信