證券期貨市場相關公會

新興科技資通安全管控指引

第一章 總則

第一條 （目的）

為協助證券期貨業者安全有效的管理及應用新興科技，特針對新興科技風險議題，擬定資通安全管控指引。

第二章 雲端服務運作安全

第二條 （雲端服務相關定義）

一、雲端服務：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。如下列雲端服務模式：

(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。

二、雲端服務提供者：係指提供雲端服務之業者，以及透過雲端平台對客戶提供應用軟體服務、工具或解決方案之業者。

三、風險基礎方法（Risk Based Approach, RBA）：組織應確認、評估及瞭解其使用雲端服務之風險，採取適當控制措施，以有效降低此類風險。依該方法，組織對於較高風險情形應採取加強措施，對於較低風險情形，則可採取相對簡化措施，以有效分配資源，並以適當且有效之方法，降低經其確認之使用雲端服務風險。

四、互通性：係指系統或資料可從原本受委託之雲端服務提供者，移轉至其他雲端服務提供者或移回組織。

五、所屬業別作業委託他人處理應注意事項：證券業係指「證券商作業委託他人處理應注意事項」；期貨業係指「期貨商作業委託他人處理

應注意事項」;投信投顧業係指「證券投資信託事業證券投資顧問事業作業委託他人處理應注意事項」。

六、重大性：應參考所屬業別作業委託他人處理應注意事項之定義。

第三條 （雲端服務指引適用範圍）

一、本指引適用之範圍，以組織對於涉及營業執照所載業務項目或客戶資訊之相關作業委外，並涉及使用雲端服務者，應符合本指引控管建議。

二、組織如於非屬前項範圍使用雲端服務者，得參照本指引控管採納必要之雲端服務資安控管。

三、外資集團在臺子公司或分公司，辦理作業委外涉及雲端服務，如係透過外國母公司或總公司辦理者，可依外國母公司或總公司所訂管控措施辦理，惟須不低於本指引規範之規定，外資集團在臺子公司或分公司仍應就其在臺業務建立妥適內部控制制度及風險管理機制，充分掌握對在臺作業涉及雲端委外事項之控管情形。

第四條 （雲端服務風險管理）

一、組織使用雲端服務應建立使用雲端服務治理制度，規劃並確認以下事項：

(一)應制定雲端服務管理政策，至少每年檢視一次。

(二)專責單位及相關單位對雲端服務使用之角色權責與責任劃分，專責單位應包含雲端財務、成本或資源管理之角色。

(三)應針對雲端服務採取風險基礎方法評估潛在風險與管理風險議題，評估項目宜包含：

1、 雲端服務使用模式與情境；

2、 雲端服務所涉及之業務與資料；

3、 組織對於雲端服務可用性與互通性之要求；

4、 組織對於雲端服務之管理能力與經驗。

(四)使用雲端服務與控管其風險事項應注意風險適度分散，惟採取多雲或其他分散策略時，應同時考量營運複雜性提升之風險。

(五)如將作業項目委託至境外處理，應評估雲端服務提供者之客戶資

料處理地及其儲存地之資料保護法規，不得低於我國要求。如有高風險之情形者，組織應採行妥適之風險控管措施。

(六)組織應針對使用雲端服務之風險建立適當監控機制，如：監控雲端資源負載、安全防護與服務可用性，以健全業務持續性運作。

二、董事會應認知及監督組織使用雲端服務之風險，確保對於控管雲端服務風險事項具備充足之資源、專業及權限。

三、應確保組織相關人員具備應有之專業知識與技能，於使用雲端服務期間定期辦理人才教育訓練並驗證教育訓練之有效性，訓練內容可包含資訊安全、風險認知和雲端知識技能等議題，以提升人員對雲端服務導入、使用及管理之能力，並能以風險為基礎方法做出適當之決策與監督。

第五條 （雲端服務提供者選擇與盡職調查）

一、組織應依所使用之雲端服務模式，對雲端服務提供者執行盡職調查及定期審查程序，評估雲端服務提供者之服務水準、備援機制、資料銷毀機制、資源邏輯區隔機制、日誌留存機制、資通安全防護能力、資通安全事件通報責任管理、業務持續運作與災難復原能力、受託業務之專業知識與資源、財務健全、內部控制及符合法規要求等項目是否可符合需求，若有不符合需求之處，應考量其他補償性措施。

二、委由雲端服務提供者處理之資料，組織應保有完整所有權，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。

三、組織為確保於服務結束時，可將系統遷移或資料遷出雲端服務，應評估雲端服務提供者可滿足下列雲端互通性和可移植性需求：

(一)雲端服務提供者可提出應用程式及資訊處理之互通性與可移植性需求說明文件供組織參考。

(二)雲端服務提供者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)雲端服務若涉及應用程式介面存取服務，雲端服務提供者宜使用

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。

第六條 （雲端服務查核）

一、就雲端服務委外作業，組織對雲端服務提供者負有最終監督義務，應落實定期對雲端服務提供者之查核，宜依風險基礎方法規劃查核頻率、查核內容、時間及方式，並得視需要委託專業第三人以輔助其監督作業，且應遵循所屬業別作業委託他人處理應注意事項之規定辦理。

二、組織應確保其本身、主管機關、同業公會及其指定之人能取得雲端服務提供者執行作業之相關資料或報告，包括客戶資訊及相關系統之查核報告，並進行查核。

三、涉及重大性之雲端委外作業者，對雲端服務之查核重點項目宜包含：

(一)雲端服務所在機房之實體安全控管機制。

(二)雲端服務提供者處理作業相關之重要系統及控制環節。

(三)盡職調查過程中雲端服務提供者所提供之報告內容。

(四)雲端平台資料刪除與災難復原流程。

(五)雲端服務提供者之營運持續性控制措施。

(六)雲端服務作業內容執行之妥適性並符合相關國際資訊安全標準及隱私保護標準。

四、應持續追蹤雲端服務提供者之查核改善情形，確保其採取適當和及時之替代性措施。

第七條 （雲端服務供應鏈管理）

一、雲端服務委外作業之供應鏈管理事項，應參酌「資通系統與服務供應鏈風險管理參考指引」辦理。

二、如涉及重大性自然人客戶業務資訊系統委託由雲端服務提供者處理，契約或協議應包括委外作業移轉至其他雲端服務提供者或移回組織之情況，原雲端服務提供者有關系統遷移、資料處理之義務，及雲端服務提供者服務中斷之賠償責任。

三、契約或協議內容如無法符合本條第一項及第二項要求，應採取適當

評估，並依風險規劃替代措施，以確保對雲端服務提供者之最終監督義務之執行。

第八條 （雲端服務資安控管）

組織使用雲端服務應依風險基礎方法採取適當之控管措施，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。

一、 加密與金鑰管理

(一)傳輸及儲存客戶資料至雲端服務提供者時，應採行客戶資料加密或代碼化等有效保護措施，並訂定妥適之加密金鑰管理機制。

二、 身分識別與存取控制

(一)雲端服務存取權限管理應採權限最小化原則，輔以適當安全控管措施，如：透過多因子認證、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。

(二)若透過網際網路直接存取雲端服務者，應強化身分、設備與來源 IP 識別等存取控制措施。

(三)應針對特權帳號實施多因子身份驗證機制，如：具備調整雲端服務組態設定權限之帳號。

三、 稽核軌跡與監控

(一)應留存雲端服務平台操作之稽核軌跡與監控資料。

(二)應有威脅與弱點檢測及管理流程，持續關注雲端服務相關威脅與弱點，定期評估相關威脅與弱點對雲端服務使用之影響及網路安全防禦措施之有效性。

(三)宜針對雲端安全事件場景制定監控與分析之關聯規則，以即早發現潛在資安風險。

(四)宜考量集中管理稽核軌跡與監控資料。

(五)應避免雲端平台之稽核軌跡內容含有未加密之營運或客戶重要資料。

(六)如組織之雲端服務係採與其地端資訊環境介接之雲地混合模式，宜考量雲地間邊際防護，並建立日誌與監控分析相關機制。

四、 基礎架構安全

(一)應確保採用可信任來源之映像檔，管理映像檔之完整性，並保留映像檔異動紀錄。

(二)應確保採取適當措施管理使用中的虛擬機和容器。

(三)應確保雲端服務提供者依據需求，提供虛擬機隔離性(isolation)說明，隔離性失效時應立即通知組織。

(四)應實施資料外洩、跨服務攻擊防護及持續性威脅防護等進階威脅防禦策略，以保護對雲端環境的存取。

五、 組態安全

應實施雲端服務組態管理機制，妥善管制對雲端服務組態之變更紀錄。

六、 資料安全

(一)涉及組織資料(含客戶資料)之登錄、處理、輸出或儲存時，組織應確認雲端服務提供者辦理設備維護更換時(如硬碟更換)，具備相關機制可確保資料遷移過程安全性及完整性，且須對汰換設備內之組織資料進行全數刪除或銷毀，並留存刪除或銷毀之紀錄。

(二)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。

(三)涉及委託雲端服務提供者處理之客戶資料及其儲存地應依下列規定辦理：

1、 組織須保有其指定資料處理及儲存地之權力。

2、 境外當地資料保護法規不得低於我國要求。

3、 涉及重大性自然人客戶業務資訊系統之客戶資料儲存地以位於我國境內為原則。如位於境外，除經主管機關核准者外，客戶重要資料應在我國留存備份。

(四)宜依據雲端服務使用之目的控管雲端服務存取方式。

七、 涉及重大性之雲端委外作業，組織宜評估採行以下資安控管措施：

(一)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。

(二)定期評估雲端服務之基礎架構安全管理機制，以確保使用雲端服務符合組織資訊安全政策等相關規範要求。

(三)使用自行管理之加密金鑰，以提升對金鑰的控制權。

(四)加密工具及金鑰儲存於隔離且安全的網路環境，並限制存取來源。

(五)避免使用營運資料執行雲端服務測試與驗證。

(六)監控與定期查核雲端資料使用情形，預防客戶隱私及營運機密外洩。

第九條 （雲端服務持續性及退場管理）

一、 組織應針對涉及雲端服務使用之資訊系統辦理營運衝擊分析，評估雲端服務之韌性及復原能力，並考量雲端服務所涉及資產、資源與資料所在位置，以及雲端服務提供者可提供之復原能力規劃營運持續管理計畫。

二、 涉及重大性之雲端委外作業，組織規劃雲端服務營運持續之測試或演練計畫時，應以風險基礎方法，決定測試或演練執行頻率與方式。宜考量與雲端服務提供者共同合作擬訂建立使用雲端服務之營運持續測試或演練計畫，並得於情況允許下與雲端服務提供者進行聯合測試或演練。

三、 組織應建立雲端資料備份機制，並留存備份清冊，備份媒體或檔案應妥善防護，確保資訊之可用性及防止未授權存取。

四、 組織應建立使用雲端服務之資訊安全事件通報與管理機制。

五、 組織應於採用雲端服務前，建立終止使用雲端服務之轉移策略及計畫，以確保終止或結束作業委託能順利移轉至另一雲端服務提供者或移回自行處理。

六、 組織應確保終止委外契約或終止使用雲端服務時，刪除雲端服務提供者留存之資料(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)，並要求雲端服務提供者出具資料完全刪除之證明。

第三章 社群媒體安全控管

第十條 （社群媒體定義）

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。

第十一條（社群媒體指引適用範圍）

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。

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（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

第十五條（行動裝置定義）

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。

第十六條（行動裝置指引適用範圍）

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應採行以下安全控管措施：

(一)行動裝置應建立身分識別機制。

(二)行動裝置之作業系統環境設定應由被授權者進行變更。

(三)行動裝置之作業系統與防毒軟體應定期檢查，避免持有者私自異動設定，如：越獄(Jailbreaking)或提權(Rooting)。

(四)行動裝置應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)行動裝置應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，應採加密或資料遮蔽方式進行保護。

(七)行動裝置應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。

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、 涉及客戶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。未涉及客戶使用之行動應用程式，組織應於開發設計時，參考前述資安檢測基準。

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。檢測範圍以最新 OWASP MOBILE TOP 10 之標準為依據，並留存相關檢測紀錄，且由資安專責單位（或資安專責人員）確認完成改善，如因故需緊急上線者（經適當層級核准）仍應於1個月內完成。

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，覆核紀錄應送資安專責單位（或資安專責人員）監控，並由資安專責單位（或資安專責人員）確認完成改善。

第五章 物聯網設備安全控管

第二十一條 （物聯網設備定義及指引適用範圍）

本指引所稱物聯網設備係指具網路連線功能並連線於Internet或Intranet之嵌入式系統（具有小型作業系統）設備（以下簡稱設備），包含自動化辦公設備（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）及不具備遠端操控介面功能之感測器。

第二十二條　（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（含網路 IP、連線方式及使用之通訊埠等）、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。

第二十三條　（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。

第二十四條　（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。

第二十五條　（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。

第二十六條　（設備採購控管）

組織於採購物聯網設備前應依據二十三條至二十五條進行評估及測試，宜優先採購取得資安標章之物聯網設備。

第二十七條　（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。

第二十八條　（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。

第二十九條　（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二十三條至二十五條之規範，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，仍應遵循本規範第二十二、二十五、二十六、二十七、二十八、二十九條之要求辦理。

第六章 電子式交易身分驗證安全控管

第三十一條　（電子式交易身分驗證定義）

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。

第三十二條　（電子式交易型態）

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、「財團法人中華民國證券櫃檯買賣中心證券商營業處所買賣有價證券業務規則」第六十二條、「財團法人中華民國證券櫃檯買賣中心興櫃股票買賣辦法」第二十三條、「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。

第三十三條　（電子式交易身分驗證指引適用範圍）

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。

第三十四條　（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。

第三十五條　（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；採用加密演算法者，其金鑰應儲存於經第三方認證(如 FIPS 140-2 Level 3 以上）之硬體安全模組內並限制明文匯出功能。

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）；加密金鑰應儲存於符合 FIPS 140-2 Level 3 以上或其他相同安全強度認證之設備，以防止該私鑰被匯出或複製。

四、 組織直接驗證該生物特徵時應依據其風險承擔能力，建立其錯誤接受率及錯誤拒絕率之標準，並於上線前與每年定期檢視。若不符合組織要求時，應建立補償措施；針對間接驗證生物特徵技術，應每年定期檢視並蒐集資安威脅情資，建立補償措施；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，應為經濟部核定或許可之憑證機構所核發之憑證，並強化憑證換發之驗證機制（如採用 OTP 機制），以確保為客戶本人登入。

第三十六條 （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 5 次者應予帳號鎖定，帳號解鎖應確實辨識本人身份後始得解鎖。

六、 組織應提供客戶定期更新密碼之機制並使用長度 6 個字元（含）以上，且具有文數字或符號之優質密碼（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。

第三十七條 （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，相關軌跡資料、證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

二、 組織應就帳號登入及交易時，記錄並通知帳號所有者，並留存相關紀錄。

第七章 深度偽造防範安全控管

第三十八條 （深度偽造定義）（Deepfake）

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。

第三十九條 （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，初始密碼應隨機產生，或為與當事人約定與身分無關之資訊）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。

第四十一條 （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，應涵蓋深度偽造認知及防範議題。

第八章 運用人工智慧安全控管

第四十二條 （人工智慧定義）

一、 人工智慧(AI)系統：係指透過大量資料學習，利用機器學習或相關建立模型之演算法，進行感知、預測、決策、規劃、推理、溝通等模仿人類學習、思考及反應模式之系統。

二、 生成式人工智慧（Generative AI）：為人工智慧的一種；係指通過大量資料學習，從而可以生成模擬人類智慧創造之內容的相關人工智慧系統，其內容形式包括但不限於文章、圖像、音訊、影片及程式碼等。

第四十三條 （人工智慧指引適用範圍）

一、 組織運用人工智慧，作為與消費者直接互動並提供金融商品建議、或提供客戶服務且影響客戶金融交易權益、或對營運有重大影響者，應符合本指引控管建議。

二、 本條所稱之營運重大影響可參考「證券商作業委託他人處理應注意事項」、「期貨商作業委託他人處理應注意事項」、「證券投資信託事業證券投資顧問事業作業委託他人處理應注意事項」之重大性定義。

三、 外資集團在臺子公司或分公司，如係透過外國母公司或總公司提供之人工智慧系統辦理第一項服務者，可依外國母公司或總公司所訂管控措施辦理，惟須不低於本指引規範之規定，外資集團在臺子公司或分公司仍應就其在臺業務建立妥適內部控制制度及風險管理機制，充分掌握對在臺作業涉及人工智慧服務之控管情形。

第四十四條 （法令遵循）

組織運用人工智慧系統時，應確認資料來源的合宜性，並確實遵循資通安全、個人資料保護、智慧財產權及營業秘密等議題之金融及其他法律

規範。

第四十五條 （治理及組織權責）

一、 組織應指定高階主管或委員會負責人工智慧相關監督管理並建立內部治理架構，指派單位或人員負責人工智慧之推動及管理，並提供相應資源。

二、 組織應落實辦理人才培育，提供適當之培訓資源，以提升人員對人工智慧系統導入、使用及管理之了解與能力、適應人工智慧系統的快速發展與變化，並能以風險為基礎做出適當之決策及監督。

第四十六條 （風險管理及定期審查）

一、 運用人工智慧系統應以風險基礎為導向，就個別使用情境，考量是否提供客戶服務或對營運有重大影響、使用個人資料程度、人工智慧自主決策程度、人工智慧系統複雜性、影響不同利害關係人的程度及廣度、以及救濟選項之完整程度等因素進行風險評估。

二、 組織應依據風險評估結果視風險大小、特性或範圍，建立適當之風險管控措施及定期審查機制。

三、 組織辦理定期審查時，應評估人工智慧系統是否符合原先運用目的及風險程度。就風險程度較高之人工智慧系統，得由具人工智慧專業之獨立第三人進行審查，審查內容宜包括資料品質、模型品質、系統安全性，以及公平性、永續發展、透明性及可解釋性等，並根據審查結果調整和改進相關策略和措施。

四、 組織運用人工智慧系統於提供與消費者直接互動之金融服務前，應針對系統所使用之資料的治理方式、資通安全、監督機制、消費者權益保障及發生非預期事件時之應變措施等，就資安、法遵及風控等層面進行評估。

第四十七條 （作業委外管理）

一、 組織委託第三方業者導入人工智慧系統時，宜評估該第三方業者是否具備相關知識、專業及經驗。

二、 組織應考量委外項目與範圍，於合約中增訂資訊安全、資料保護、複委託、責任範疇、罰則之條款，並就停止委託之情形訂定適當之

資料或系統遷移機制。

三、 組織運用第三方業者開發或營運之人工智慧系統提供金融服務時，應執行監督作業，並確保第三方業者留存執行受託辦理事項之書面或數位作業紀錄，俾利後續追蹤、驗證及管理。

四、 對於涉及營業執照所載業務項目或客戶資訊之相關人工智慧作業委外時，應遵循「證券商作業委託他人處理應注意事項」、「期貨商作業委託他人處理應注意事項」、「證券投資信託事業證券投資顧問事業作業委託他人處理應注意事項」之規定辦理。

第四十八條 （公平性原則）

一、 組織運用人工智慧時，在演算法設計、開發、資料蒐集、訓練資料選擇、處理、模型建置/生成/優化，及後續應用於金融服務過程中，應採取以人為本及人類可控措施以符合金融服務業公平待客原則。

二、 組織對於數據資料之蒐集及處理，宜盡量使用多元、包含各種背景與特徵且具代表性之資料，而非僅依賴單一類別或群體之數據，以減少對某些群體的偏見與歧視。

三、 如使用以下資料參數納入演算法判斷，如: 姓名、居住所、族群、宗教、國籍、法律無限制或禁止之年齡、所有生理特徵（包含但不限於身高、體重、性別、膚色、髮量、肢體障礙等），或所有非涉及心神喪失致無法自主理解該金融商品判斷能力之疾病，應就資安、法遵及風控等層面進行必要性評估。

四、 運用人工智慧系統提供金融服務宜評估提供救濟選項，可能包括申訴或補救管道、爭議處理機制等。若所運用之人工智慧系統如與洗錢防制或詐騙偵防有關，而不適合提供救濟選項者，得不提供。

第四十九條 （保護資料隱私）

一、 組織運用人工智慧時，處理、儲存、傳輸與使用資料的過程中，應注意保護個人和組織的資料隱私權，具備適當的保護措施確保其系統和資料的安全，避免資料未經授權存取、修改或洩露。

二、 組織應以資料最小化之原則蒐集與處理必要之客戶資料，並避免蒐集過多或不必要之敏感資訊。

第五十條（安全性與穩健性原則）

一、 組織運用人工智慧系統於模型建立及驗證階段中(包括進行預訓練、優化訓練等)，在選擇模型或演算法等相關工具時，應注意其安全性，並採取有效措施，包含但不限於資料品質處理、模型驗證與監控等，以提高訓練品質防止生成不適當資訊，提升人工智慧系統的輸出或生成內容的準確性與可靠性。

二、 組織應遵循資訊安全相關規範，建立適當之資安防護或管控措施，防範各種安全威脅及攻擊，如駭客攻擊、惡意軟體等，並持續監控運作結果，確保人工智慧系統之安全性。

第五十一條（透明性與可解釋性原則）

一、 組織運用人工智慧系統與消費者直接互動時，應告知該互動或服務係利用人工智慧系統自動完成，或揭露該互動或自動化金融服務適用的人群、場合、用途。另宜由消費者自行選擇是否使用，並提醒消費者該項服務有無替代方案，但法令另有其規定者，從其規定。

二、 組織運用人工智慧系統技術，若涉及金融交易者應理解其如何做出決策並提高可解釋性，以確保對人工智慧系統運作之有效管理。

第五十二條（紀錄留存）

組織自行或委外開發、優化人工智慧系統時，應保存人工智慧系統生命週期必要之技術文件及相關紀錄，包括開發者在設計、開發和實施過程中，如為可能影響決策的重要資料、模型或演算法等紀錄，以確保其在必要時可被查驗。

第五十三條（生成式人工智慧）

一、 組織運用生成式人工智慧產出之資訊不可完全信任，應就該資訊之風險進行客觀評估與管控，亦不得以未經確認之產出內容直接作成決策之唯一依據。

二、 組織在無適當管控機制下，人員不得向生成式人工智慧提供涉及應保密、未經個人或未經組織同意公開之資訊，亦不得向生成式人工智慧詢問可能涉及機密業務或個人資料之問題。但封閉式地端部署之生成式人工智慧模型，於確認系統環境安全性後，得考量資訊機

密等級提供。

三、 組織使用第三方業者開發之生成式人工智慧系統，如無法掌握訓練過程及確保其數據或運算所得出之結果符合公平性原則時，應對該系統產出之資訊由人員就風險進行客觀且專業管控。

四、 組織導入生成式人工智慧系統，應重視公平性及以人為本的價值觀評估是否對特定群體產生偏見或歧視之情況，並降低可能之不公平情況。

第五十四條 （永續發展原則）

一、 尊重並保護一般受僱員工的工作權益，包括在數位轉型過程中，提供適當的教育及培訓以助其適應新的工作環境。

二、 組織運用人工智慧系統之策略及執行方向，應依據國際永續發展目標及自訂之永續發展原則，適當列入永續發展綜合指標。