國泰金融控股股份有限公司
區塊鏈聯盟自律公約
銀行業技術暨資訊安全規範與訂定說明

中華民國　　年　　月　　日

編號	條文內容	訂定說明
一、	**技術暨資訊安全規範目的：**各參與聯盟之聯盟成員於聯盟鏈平台上進行數據交換及商業合作時，須配合本公約訂定之技術暨資訊安全內部標準，以確保聯盟成員系統具有一致性安全防護基準。	
二、	**本基準用詞定義如下：** 一、關鍵資訊系統：支持核心區塊鏈生態圈業務持續運作必要之系統或設備。 二、資訊資產：係指軟體、硬體、文件、資料及人員等與資訊處理相關之資產皆屬於資訊資產範疇。 三、稽核軌跡：包含但不限於登入帳號、系統功能、時間、系統名稱、查詢指令或結果。 四、持續營運控制措施：保護重要營運過程不受重大資訊系統失效管控措施，包含但不限於模擬測試或災害的影響，仍然可以繼續運作。 五、尖峰作業：短時間內進行大量資料傳輸之情況。 六、資料交換政策、程序及控制措施：包含但不限於區塊簽名驗證機制、多重簽名機制、告警機制等。 七、惡意攻擊：包含但不限於 51 攻擊、雜湊衝突、共識機制妥協、重入攻擊、DoS 攻擊等惡意攻擊手段。 八、雲端服務：公約聯盟成員承租雲端服務業者之網路、伺服器、儲存空間、基礎設施、資安設備、系統軟體、應用程式、分析與計算等資源，以達資源共享之服務。	

遵循性		
三、	公約聯盟成員應確保區塊鏈生態圈所在之司法管轄區之法律、法令、法規未禁止區塊鏈及分散式帳本技術(Blockchain/Distributed Ledger Technology)，且應每年或法令法規進行變更時，定期確保、盤點檢閱並避免違反區塊鏈生態圈(The Network)相關資訊安全之法律、法令、法規或契約義務，及任何安全要求事項，以持續確保其合宜性、適切性及有效性。	參酌 ISACA Blockchain Framework and Guidance G-1 、 G-1.01 ； ISO 27001 A.18.1.1;金融機構資通安全防護基準第三條第四項及第十九條。
四、	公約聯盟成員應依據前述所盤點檢閱之資訊安全相關法律、法令、法規或契約義務，及任何安全要求事項，與內部控制制度結合，定期進行法令遵循自評，以確保資訊安全之法令遵循性。	參酌 ISO 27001 A.18.1.1 及金融機構資通安全防護基準第十九條。
五、	公約聯盟成員應透過內部控制制度進行定期檢核，並應於每年依據前述所盤點檢閱之資訊安全相關法律、法令、法規或契約義務，及任何安全要求事項，提出資訊安全評估報告。	參酌 ISO 27001 A.18.1.1 及金融機構資通安全防護基準第十九條。
六、	公約聯盟成員應確保區塊鏈生態圈無法於高風險或受制裁之區域維運。	一、參酌 ISACA Blockchain Framework and Guidance G-1.02；ISO 27001 A.18.1.1。 二、高風險及受制裁地區應循法務部公告之「防制洗錢與打擊資助恐怖份子有嚴重缺失之國家或地區」及「其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區」。
七、	公約聯盟成員應針對涉及資料上鏈之客戶進行客戶盡職調查(KYC)或防制洗錢(AML)審查作業。	參酌 ISACA Blockchain Framework and Guidance G-5.03 及 ISO 27001 A.18.1。
系統維運人員管理		
八、	公約聯盟成員之區塊鏈生態圈維運人員，應依執行業務之必要，設定相關	參酌金融機構資通安全防護基準第五條第三項。

	人員接觸客戶資料之權限及控管其接觸情形,並與所屬人員約定保密義務,以維護所保有客戶資料之安全。	
九、	公約聯盟成員應確認區塊鏈生態圈相關維運人員超過十五分鐘未操作個人電腦時，應設定密碼啟動螢幕保護程式或登出。	參酌金融機構資通安全防護基準第四條第四項。
十、	區塊鏈生態圈相關維運人員帳號應採一人一號管理，避免多人共用同一個帳號為原則。如有共用需求，申請及使用須有其他補強管控方式，並留存操作紀錄且應能區分人員身份。	一、參酌金融機構資通安全防護基準第四條第六項。 二、補強管控方式係指包含但不限於使用後更換密碼、代登入機制、密碼拆分保管等措施。
十一、	區塊鏈生態圈相關維運人員帳號如採用固定密碼進行身份確認者，應符合下列要求： 一、 訂定密碼檢核邏輯。 二、 提供給維運人員使用之帳號於使用後三個月內應變更密碼。 三、 提供給系統使用之帳號應採取適當之管控措施(包含但不限於限制人工登入、監控告警)。	一、參酌金融機構資通安全防護基準第四條第七項。 二、公約聯盟成員已具相關內部規範，可優先遵循其內部規範；如無則應符合公約條款之最低要求。 三、固定密碼強度可參酌「金融機構辦理電子銀行業務安全控管作業基準」第七條相關控管措施。
十二、	公約聯盟成員區塊鏈節點角色之定義，應遵循已議定之區塊鏈協議、合約、共識機制或其他相關協議之基本要求，並指派其資訊安全責任，且衝突之角色及其權限範圍應予以區隔。	參酌 ISACA Blockchain Framework and Guidance I-1.10； ISO 27001 A.6.1.1 及 A.6.1.2；金融機構資通安全防護基準第三條第六項。
十三、	公約聯盟成員應依據區塊鏈生態圈作業風險及專業能力，選擇適當人員擔任節點角色並定期提供必要教育訓練。	參酌金融機構資通安全防護基準第三條第七項。
	資訊資產	
十四、	公約聯盟成員應依據區塊鏈生態圈之作業流程，識別人員、表單、設備、軟體、系統等資產，並建立資產清冊、作業流程、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確	參酌金融機構資通安全防護基準第三條第五項。

	性。	
	系統生命週期管理	
十五、	公約聯盟成員應透過正式變更管理程序，以控制區塊鏈生態圈新增及變更作業(包含但不限於網路代碼、智能合約、共識機制等作業)，以確保區塊鏈生態圈內進行任何變更時，皆依循已議定之共識機制並產生適當稽核軌跡紀錄。	參酌 ISACA Blockchain Framework and Guidance G-3.03、G-7.02、I-1.03、I-1.11、I-2.05、SC-2.03； ISO 27001 A.12.1.2、A.12.2、A.14.1.1、A.14.1.3、A.14.2.2。
十六、	區塊鏈生態圈生命週期管理應符合下列要求： 一、 應訂定相關關鍵資訊系統開發設計規範並落實執行。 二、 應監督委外開發之應用軟體，並確保其有效遵循本基準規定。 三、 應確保相關關鍵資訊系統軟體和應用軟體安裝最適安全修補程式。 四、 應針對相關關鍵資訊系統架構重大變更或異動時，訂定復原程序，並於上線前進行程序演練或實際演練。 五、 應分別從技術、功能、情境等建立測試案例並進行端點對端點測試。 六、 對於測試用之機敏資料，應先進行資料遮蔽處理或管制保護。 七、 於開發階段起至營運階段，應遵循變更控制程序處理並留存相關紀錄；營運環境變更(包含但不限於執行、覆核)應由二人以上進行，以相互牽制。 八、 相關關鍵系統軟硬體變更應先進行技術審查並測試；套裝軟體不應自行異動，並應先進行風險評估。程式不應由開發人員自行換版或產製比對報表，應建立程式原始碼管理機制，以符合職務分工及牽制原則。	參酌 ISO 27001 A.14.1.1、A.14.2 及 A.14.3；金融機構資通安全防護基準第十四條。
十七、	各公約聯盟成員應針對其區塊鏈生態圈維運人員，制定正式之使用者註冊、異動、註銷及存取權限配置程序，其	一、參酌 ISACA Blockchain Framework and Guidance G-5.04；ISO 27001 A.9.2.1 及

	應包含最小權限(least privilege)及僅知原則(need-to-know)，並定期審查帳號及權限之合理性，以在所有系統及服務中，對所有型式之使用者，指派或撤銷存取權限，並確保已註銷使用者無檢視或存取區塊鏈生態圈內任何交易之權限。	A.9.2.2；金融機構資通安全防護基準第四條第一項、第二項、第三項及第四條第十二項。 二、已取得權限之各公約聯盟成員內部權限管理，若公約聯盟成員已具相關內部規範,可優先遵循其內部規範;如無則應符合公約條款之最低要求。 三、核發公約聯盟憑證單位應依公約聯盟相關申請作業辦法進行憑證授予，並經聯盟大會決議。
十八、	公約聯盟成員應依據下列要求管理區塊鏈生態圈正式營運環境： 一、 應評估避免於正式營運環境安裝程式原始碼。 二、 應建立定期備份機制及備份清冊，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。 三、 應驗證備份資料之完整性、可用性及儲存環境的適當性。 四、 應留存相關紀錄並建立適當保護機制及管理程序，相關紀錄至少留存一年。 五、 應訂定區塊鏈生態圈相關安全強化標準，建立並落實資訊安全設定。 六、 應避免區塊鏈生態圈維護人員未經申請使用最高權限帳號。	參酌金融機構資通安全防護基準第八條。
十九、	公約聯盟成員應依據下列要求管理區塊鏈生態圈測試環境： 一、應避免於使用測試環境時共用其他環境(包含但不限於營運環境、測試環境、辦公環境)之設備、憑證金鑰、資源存取帳密及使用者配置檔(User Profiles)。 二、應限制連接網際網路，並應遵循	參酌金融機構資通安全防護基準第十一條。

	銀行公會所訂定之相關電子銀行相關自律規範辦理。	
	網路管理	
二十、	公約聯盟成員應針對區塊鏈生態圈及相關網路備妥資料交換政策、程序及控制措施，並依各公約聯盟成員內部作業程序核定，以管理及控制區塊鏈生態圈及相關網路之安全性，並防止惡意人士或未經授權節點存取已核准區塊鏈或其他聯盟鏈。前述核准之政策、程序及控制措施，應對所有公約聯盟成員、其員工及供應商公布或傳達。	參酌 ISACA Blockchain Framework and Guidance G-5.01、I-2.01、I-2.02、I-2.03、KM-2.05 ； ISO 27001 A.9.2.3、A.10.1.2、A.12.3.1、A.13.1.1、A.13.2.1、A.14.1.1；金融機構資通安全防護基準第三條第一項、第三條第二項及第三條第三項。
二十一、	公約聯盟成員應依據下列要求進行區塊鏈生態圈網路管理： 一、 網路應區分網際網路、非武裝區(Demilitarized Zone)、營運環境及其他(如內部辦公區)等區域，並採用防火牆規則、路由器存取控制列表(Access Control List，ACL)保護區塊鏈平台維運環境，以確保其流量皆經過授權，降低系統未經授權存取或變更的風險。 二、 使用遠端連線進行系統管理作業時，應使用加密通訊協定。	參酌金融機構資通安全防護基準第十三條。
二十二、	公約聯盟成員應監控網路傳輸，以確保可滿足資料傳輸流量與共識過程速度，並實踐聯盟鏈使用效能目標。	參酌 ISACA Blockchain Framework and Guidance I-1.01 及 ISO 27001 A.13.1.1。
二十三、	公約聯盟成員應針對網路傳輸之安全性與正確性進行風險評估，以識別區塊鏈生態圈相關威脅情境。	一、參酌 ISACA Blockchain Framework and Guidance I-1.02 及 ISO 27001 A.14.2。 二、依照聯盟大會訂定之風險等級相關規範進行風險評估及風險緩解措施。
	智能合約安全	
二十四、	智能合約 (Smart Contracts, SC)治理：應針對智能合約之架構設計及維運作	參酌 ISACA Blockchain Framework and Guidance

	業相關固有潛在監管或法律風險，制訂對應治理目標及控管程序，以避免合規風險。	SC-1。
二十五、	公約聯盟成員應確保智能合約(包含但不限於資料傳輸技術、程式碼撰寫之已議定條款及已核准共識機制)符合直接或間接維運作業所在地之司法管轄區相關法律、法令、法規及其他要求事項；且公約聯盟成員應依據前述法律、法令、法規及其他要求事項，執行相關法令遵循作業(包含但不限於內部稽核報告、主管機關要求之報告等)。	參酌 ISACA Blockchain Framework and Guidance SC-1.01、SC-1.02、SC-1.03；ISO 27001 A.18.1。
二十六、	公約聯盟成員應針對智能合約相關維運作業，指定權責單位及人員，並依前項條款執行相關法令遵循作業(包含但不限於內部稽核報告、主管機關要求之報告等)。	參酌 ISACA Blockchain Framework and Guidance SC-1.04 及 ISO 27001 A.18.1。
二十七、	公約聯盟成員應針對智能合約設計之相關程式漏洞風險，制訂相關管理程序及處置措施(包含但不限於修復或風險緩解措施)。	參酌 ISACA Blockchain Framework and Guidance SC-2。
二十八、	公約聯盟成員應確保所有於區塊鏈生態圈中運作之智能合約已經共識機制核准，且具適當資料傳輸大小限制，以預防潛在超量資料傳輸或未被檢測到之資料遺失。	參酌 ISACA Blockchain Framework and Guidance SC-2.02 及 ISO 27001 A.17.1。
二十九、	公約聯盟成員應確保智能合約符合資訊安全相關要求事項(包含但不限於存取權限控管)，並針對惡意攻擊建立適當風險緩解及處置措施。	參酌 ISACA Blockchain Framework and Guidance SC-3.01、SC-3.02、SC-3.03、SC-3.04、SC-3.06、SC-4、SC-4.05；ISO 27001 A.8.2.3、A.9.2、A.14.1、A.18.1。
三十、	公約聯盟成員應針對智能合約建立確保資料完整性與不可否認性之機制，以避免相關風險。	參酌 ISACA Blockchain Framework and Guidance SC-4.02；ISO 27001 A.8.2.3、A.13.2 及 A.18.1。
三十一、	公約聯盟成員應明確定義智能合約程	參酌 ISACA Blockchain

	式碼函式之存取權限，包含但不限於透過適當加密保護措施，以防止外部人員未經授權之存取。	Framework and Guidance SC-4.03；ISO 27001 A.8.2.3 及 A.18.1。
	節點安全	
三十二、	公約聯盟成員應確保區塊鏈生態圈之資料格式與系統架構符合公約聯盟成員相關資訊安全要求事項或標準，且資料上傳至聯盟鏈應符合聯盟鏈開發者所制定之相關規定，以達到區塊鏈生態圈之互通性。	參酌 ISACA Blockchain Framework and Guidance G-3.05 及、D-1.05；ISO 27001 A.13、A.14.1.1。
	作業安全	
三十三、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統產生之稽核紀錄(內容包含但不限於事件類型、發生時間、發生位置、使用者身分識別等資訊)應有保留機制及存取管理。	參酌 ISACA Blockchain Framework and Guidance G-6.01 及 G-6.02； ISO 27001 A.12.4.1 及 A.12.7.1；金融機構資通安全防護基準第四條第五項。
三十四、	公約聯盟成員應確保區塊鏈之架構設計或網路協定已遵循資料傳輸時間順序，以防止網路效能或完整性毀損。	參酌 ISACA Blockchain Framework and Guidance I-1.05 及 ISO 27001 A.12.6.1。
三十五、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統進行校時，以確保生態圈之時間戳記與相關關鍵系統時間之誤差不超過議定範圍，並防止時間戳記誤差值導致區塊鏈生態圈內之濫用與詐欺行為。	參酌 ISACA Blockchain Framework and Guidance I-1.09；ISO 27001 A.12.4.4、A.12.6.1。
三十六、	公約聯盟成員應確保無論是直接或間接操作情境下，區塊鏈生態圈維運人員無法變更區塊時間戳記，以避免惡意人士對區塊鏈進行濫用或詐欺，並確保資訊安全。	參酌 ISACA Blockchain Framework and Guidance I-2.04 、 D-1.04 ； ISO 27001 A.13、A.14.2。
	個人資料保護	
三十七、	公約聯盟成員應確保區塊鏈生態圈維運作業所在司法管轄區客戶個人可識別資訊之隱私符合相關法律、法令、法規中之要求。	一、參酌 ISACA Blockchain Framework and Guidance G-1.04、SC-1.06、SC-4.09；ISO 27001 A.8.2.3 、 A.9.2 、 A.13.1.3、A.18.1.2、A.18.1.4、A.18.1.5。

		二、客戶個人可識別資訊可參酌「個人資料保護法」第2條第1款針對「個人資料」之定義：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。"
三十八、	公約聯盟成員應針對區塊鏈生態圈涉及之資料處理(包含但不限於客戶資料)採取下列資料安全管理措施： 一、 訂定各類資訊資產或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施，以確保任何敏感性資料已被妥適移除或覆寫。 二、 針對區塊鏈生態圈所涉及之資料處理(包含但不限於客戶資料)，可依各公約聯盟成員內部作業規範，於蒐集、處理或利用時，採用加密技術、資料區隔、網路安全及相關處置計畫等控制措施。 三、 區塊鏈生態圈作業過程有備份資料(包含但不限於客戶資料)之需要時，對備份資料予以適當保護。 四、 保有區塊鏈生態圈相關資料(包含但不限於客戶資料)存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施： 1. 實施適宜之存取管制。 2. 訂定妥善保管媒介物之方式。	參酌 ISACA Blockchain Framework and Guidance G-1.04、G-3.04；ISO 27001 A.11.2.7;金融機構資通安全防護基準第五條第一項第一款、第五條第一項第二款、第五條第一項第三款、第五條第二項第一款、第五條第二項第二款、第五條第二項第三款、第六條第一項。

	3. 依媒介物之特性及其環境，建置適當之保護設備或技術。	
三十九、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統，其相關之資訊資產及客戶資料進行風險評估及控管。	參酌金融機構資通安全防護基準第五條第四項。
四十、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統，建置留存客戶資料使用稽核軌跡及建立資料外洩防護機制，以利客戶資料外洩時得以追蹤個人資料使用狀況。	參酌金融機構資通安全防護基準第五條第五項、第六項。
	加密及金鑰管理	
四十一、	公約聯盟成員應建立金鑰管理程序，且應包含但不限於以下要求： 一、應確保金鑰設計及產製具有適當複雜度。 二、應防止並針對加密金鑰外洩事件或潛在情境進行應變。 三、應針對加密金鑰擁有者建立並實施適當權限授予與移除之相關程序。 四、當金鑰使用期限將屆或有洩漏疑慮時，應進行金鑰替換。 五、應針對加密金鑰及種子制訂相關存取控制及備份程序，並定期針對其備份資料進行測試。 六、應確保加密金鑰及種子之備份儲存位置，應與主加密金鑰存放於不同伺服器或地理位置。 七、公約聯盟成員應避免加密金鑰及種子之備份之環境風險，包含但不限於火災、洪水、盜竊及其他不可抗力因素。	一、參酌 ISACA Blockchain Framework and Guidance KM-1、KM-1.01、KM-1.02、KM-1.03、KM-2.01、KM-2.02、KM-2.03、KM-3.02、KM-3.03；ISO 27001 A.9.2.3、A.10.1.2、A.11.1、A.12.3.1、A.17.1；金融機構資通安全防護基準第六條第四項、第六條第五項。 二、公約聯盟成員已具相關內部規範，可優先遵循其內部規範；如無則應符合公約條款之最低要求。
四十二、	區塊鏈生態圈機敏資料如儲存於雲端者，公約聯盟成員應遵循銀行公會所訂定之雲端服務相關自律規範辦理相關管理措施。	參酌金融機構資通安全防護基準第六條第六項。
	實體安全	
四十三、	公約聯盟成員應依據下列要求管理區塊鏈生態圈正式營運環境之實體安	參酌金融機構資通安全防護基準第七條。

	全： 一、 應避免主機房及異地機房同時在地震斷層帶、海岸線、山坡地、海平面下、機場飛航下、土石流好發區域、百年洪水氾濫區域、核災警戒範圍區域、工安高風險區域其中之一，並應有相關防護措施，以避免受到地震、海嘯、洪水、火災或其他天然或人為災難之損害。 二、 應建立機房門禁管制，並將營運設備集中於機房內，以確保僅允許經授權人員進出；非授權人員進出應填寫進出登記，並由內部人員陪同及監督；進出登記紀錄應定期審查，如有異常應適當處置。 三、 應於主機房及異地機房內建立全天候監視設備並確保監視人員操作範圍無死角。 四、 應有足夠營運使用之電力、供水、用油等供應措施，當發生供應措施中斷時，應至少維持七十二小時運作時間，並應介接二家以上網際網路電信營運商，或本地與異地二線以上互為備援。 五、 油槽儲存及消防安全應符合相關法規規定。 六、 應設置環境監控機制，以管理電信、空調、電力、消防、門禁、監視及機房溫濕度等，並自動告警及通知。 七、 應具備與機房相當之操作環境，或獨立可管制人員操作系統及設備之監控室，該監控室應符合下列要求： 1. 應具門禁及監視設備，且必須留存連線及使用軌跡，並定期稽核管理。 2. 系統維運人員應經授權進入監控室使用監控室內專屬電腦設備；或應使用指定設備由內部網路以	

	一次性密碼登入並經服務管控設備(如防火牆)使用監控室內專屬電腦設備。 3. 連線過程須以內部網路、專線或虛擬私有網路進行。 4. 監控室之網路設備及電腦設備應符合本基準相關規定。	
四十四、	公約聯盟成員應依據下列要求管理區塊鏈生態圈辦公環境： 一、 異地辦公之 VPN 使用管理 1. 應將 VPN、網路基礎架構設備之主機更新至最適版本，並使用安全設定。 2. 應提醒用於連入遠端作業環境之主機，應先安裝安全修補程式、更新病毒碼後再進行連線。 3. 應確認 IT 及資安人員已完成準備，包含日誌檢視、攻擊偵測、事件應變及事件復原機制。 4. 應採用高強度密碼或多因子進行身份驗證。 5. 應確認 VPN 資源足以應付大量使用，若情況允許，可以透過設定流量管制，以讓有高流量需求的員工有充足的資源能夠使用。 二、 異地辦公之虛擬桌面(VDI)使用管理 1. 應針對伺服器及虛擬桌面軟體進行妥善設定，避免員工可以將虛擬桌面連接到本機印表機印出檔案內容，透過虛擬桌面存取本機主機檔案，連接可卸除裝置或透過剪貼簿於兩端剪貼資料。 2. 應適時進行軟體更新以修補最適漏洞，並向員工宣導不應安裝可疑程式避免中毒。 3. 應設定虛擬桌面在一段閒置時間後將螢幕鎖定或中斷連線，以免	一、參酌金融機構資通安全防護基準第十二條。 二、公約聯盟成員已具相關內部規範，可優先遵循其內部規範；如無則應符合公約條款之最低要求。

	遭到被入侵之本機主機操控。 4. 應禁止員工使用自動抓取關鍵字之鍵盤軟體,以免機敏資訊外洩。 5. 應採用高強度密碼或多因子進行身份驗證。 6. 建議使用全硬碟加密機制或限制下載，以防止虛擬桌面之檔案遭誤存於本機裝置中。	
事件與營運持續管理		
四十五、	公約聯盟成員應依據區塊鏈生態圈現有網路協定與資源使用狀況及未來容量需求，進行以下作業： 一、 應針對資源使用狀況及容量定期分析/模擬，以確保區塊鏈生態圈系統效能可滿足目前及未來容量和雜湊需求。 二、 應確保共識機制之驗證速度滿足資料傳輸流量，以實現區塊鏈生態圈營運持續目標。 三、 應考量軟體更新、生命週期、軟硬體運作相容性等因素，評估採用多重備援或冗餘配置(Redundancies)等方式，適時進行資源調整及擴充。 四、 應進行營運衝擊分析，定義最大可接受系統中斷時間，設定系統復原時間及資料復原時點。 五、 應依區塊鏈生態圈業務性質及設備功能等對關鍵資訊系統訂定相關負載量要求，以強化系統穩定性，確保業務持續運作不中斷(包含但不限於採取適當措施以限縮或封存區塊鏈生態圈)。 六、 應針對區塊鏈生態圈相關關鍵資訊系統特性、風險因素及所需效能，設定監控項目(包含但不限於效能，容量空間，負載量、頻寬等)、規則(包含但不限於警示種類)、程序或規範。 七、 應監控批次作業(包含但不限於	參酌 ISACA Blockchain Framework and Guidance G-3.02、G-4.01 及 G-4.03；ISO 27001 A.12.1.3、A.14.2.8 及 A.17.1.1；金融機構資通安全防護基準第九條及第十八條第一項。

	監控資源使用情況，並應注意是否已執行完成所有作業程序，以避免影響正常交易)，並定期將監控結果適時通知相關權責單位，於完成相關處理及應變後，留存紀錄由權責單位核示。	
四十六、	公約聯盟成員應建立對於重大區塊鏈生態圈相關關鍵資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。	參酌 ISO 27001 A.17.1.1 及金融機構資通安全防護基準第十八條第二項。
四十七、	公約聯盟成員應每年驗證及演練其營運持續性控制措施，以確保其有效性，並應保留相關演練紀錄及召開檢討會議。	參酌 ISO 27001 A.17.1.3 及金融機構資通安全防護基準第十八條第三項。
四十八、	公約聯盟成員應針對區塊鏈生態圈尖峰作業或例行業務處理量較大等時段，應特別注意各類異常情形之監控並加強檢核系統資源，俾事先提出因應措施。	參酌 ISO 27001 A.17.2 及金融機構資通安全防護基準第十八條第四項。
四十九、	公約聯盟成員應確保區塊容量大小(Block size)、區塊高度(Block height)和區塊間隔時間(Block interval time)符合區塊鏈生態圈目前及未來資源需求，以實現區塊鏈生態圈營運持續目標，並維持其運算完整性及穩定性。	參酌 ISACA Blockchain Framework and Guidance G-4.02、I-1.06、I-1.07 ；ISO 27001 A.12.6.1、A.17.1.1。
五十、	區塊鏈生態圈之資訊安全事件管理，應符合下列要求： 一、 應將區塊鏈生態圈相關各作業系統、網路設備、資安設備之日誌，及稽核軌跡集中管理，進行異常紀錄分析，設定告警指標並定期檢討修訂。 二、 應建立資訊安全事件通報、處理、應變及事後追蹤改善作業機制，並應留存相關作業紀錄；另應定期辦理演練，以確保資安事件發生時相關通報、處理及應變作業之有效性。 三、 如有資訊安全事件發生時，其系統交易紀錄、系統日誌、安全事件日	參酌 ISO 27001 A.16 及金融機構資通安全防護基準第十七條。

	誌應妥善保管，並應注意處理過程中軌跡紀錄及證據留存之有效性。	
	脆弱性管理	
五十一、	公約聯盟成員應確防止區塊鏈生態圈傳輸之資料(包含但不限於客戶資料)，遭受未經授權揭露、修改，或透過區塊鏈生態圈進行惡意攻擊。公約聯盟成員亦應進行預防性分析、實施安全功能性之測試及驗收測試計畫及準則、網路服務安全監控及分析等，以降低區塊鏈中演算法之存取漏洞，並避免區塊鏈生態圈損害之惡意行為。	參酌 ISACA Blockchain Framework and Guidance G-5.02、I-3.01、I-3.02、I-4.02、I-4.03、I-5.01、SC-4.06；ISO 27001 A.8.2.3 、 A.9.2 、A.12.6.1、A.13.1.2、A.14.1.1、A.14.1.2、A.14.2.8、A.14.2.9、A.18.1。
五十二、	公約聯盟成員應針對區塊鏈技術之脆弱性實施預防性控制措施，並採取適當措施以因應相關風險，以確保區塊鏈生態圈每一區塊之資料傳輸量總和不超過議定之區塊大小，以防止網路效能或完整性毀損。	參酌 ISACA Blockchain Framework and Guidance I-1.04 及 ISO 27001 A.12.6.1。
	供應商管理	
五十三、	公約聯盟成員應依據下列要求監督並管理區塊鏈生態圈之第三方單位(包含但不限於委外供應商)： 一、關鍵資訊系統應具備以下管理機制： 1. 應先對受託廠商進行適當之安全評估，並依據最小權限及資訊最小揭露原則進行安全管控設計。 2. 應定期針對可存取銀行內部網路之駐點廠商人員，辦理電子郵件社交工程教育訓練。 二、關鍵資訊系統之委託契約或相關文件(包含但不限於諒解備忘錄)中，應明確約定下列內容： 1. 應要求受託廠商遵守本基準及其他適當資訊安全國際標準要求，確保資料安全。 2. 應與受託廠商就服務品質、水準、	一、參酌 ISO 27001 A.15 及金融機構資通安全防護基準第十六條。 二、第三方服務供應商由各公約聯盟成員遵循其內部規範自行管理與監督。

	效能等方面訂定服務要求。 3. 應依本基準內容對受託廠商進行適當監督。 4. 當發生資安事件時，受託廠商應主動、即時通知委託人。 5. 應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。 三、 關鍵資訊系統應定期針對供應商辦理資訊安全訪視，亦可委由第三方提出報告(如 ISO/CNS 27001 有效證書)。	