金融機構資通系統與服務供應鏈風險管理規範

本會 111 年 11 月 14 日第 14 屆第 2 次理事會議討論通過
金管會 112 年 3 月 29 日金管銀國字第 1120270185 號函洽悉
本會 113 年 1 月 25 日第 14 屆第 13 次理事會議核議通過
金管會 113 年 5 月 6 日金管銀國字第 1130207638 號函洽悉
本會 114 年 6 月 26 日第 14 屆第 7 次理事會議核議通過
金管會 114 年 9 月 24 日金管銀國字第 1140222565 號函洽悉
本會 114 年 12 月 18 日第 15 屆第 3 次理監事聯席會議核議通過
金管會 115 年 2 月 13 日金管銀國字第 1150201525 號函洽悉

第一條　　中華民國銀行商業同業公會全國聯合會(以下稱本會)為確保銀行資通系統委外具有一致性之供應鏈資訊安全風險管理，特訂定本規範。

第二條　　本規範所稱金融機構資通系統與服務供應鏈，係指提供銀行資通系統之軟硬體產品開發、建置或維運服務的組織或個人(以下稱供應商)，包含其受託者與跨機構合作夥伴。

適用於本規範之資訊服務係指提供與電腦系統軟體或硬體有關之服務形態，包含系統發展類、維運管理類及雲端服務類。

核心資通系統及第一類電腦系統均適用本規範；第二類及第三類電腦系統如為提供網際網路連線服務、供應商於合約期間得存取銀行機敏資料，或當次合約採購金額為新臺幣壹仟萬元以上者，適用本規範。

銀行之資通系統供應鏈如為雲端服務、物聯網設備業者，除本規範外，亦應遵循金融監督管理委員會及本會所訂定之相關規範。

第三條　　本規範用詞定義如下：

一、核心業務：由銀行依業務運作中斷對客戶影響數等風險評估結果予以決定，評估範圍如：存款業務、放款業務、匯款業務、外匯業務等。

二、核心資通系統：支持核心業務持續運作必要之系統或設備。

三、第一類電腦系統：直接提供客戶自動化服務或對營運有重大影響之系統(如：電子銀行、分行櫃台、ATM 自動化服務、SWIFT 等系統)。

四、第二類電腦系統：經人工介入以直接或間接提供客戶服務之系

統(如：作業中心、客戶服務等系統)。

五、第三類電腦系統：未接觸客戶資訊或服務且對營運無影響之系統或設備(如：人資、財會、總務等系統、物聯網設備)。

六、供應鏈資訊安全風險：源自供應商的資訊安全議題(如：離職員工持有系統帳號、密碼及原始碼、對外服務系統管控不周或其他資訊安全事件等)，可能對銀行資通系統與資訊服務的機密性、完整性或可用性造成衝擊。

七、邊際防護：管控銀行與供應商之網路介接以限制未經授權之網路傳輸存取(如：內外網路架構、存取控制及資料傳輸等)。

八、機敏資料：係指如登入帳號、固定密碼、重要參數、晶片金融卡基碼、憑證私鑰、個人資料及製卡個人化資料等。

九、實質受益人：指對供應商提供之產品或服務具最終所有權或控制權之自然人。

十、控制權來源國：指直接、間接持有提供該產品或服務之供應商股份或資本超過百分之二十五者所屬國家。

第四條　資通系統與服務委外前，應分析及規劃下列供應鏈資訊安全事項：

一、應針對擬委外之項目執行資訊安全可行性分析：

(一)分析委外項目之資訊安全風險(如：可能受影響之資訊資產、流程及作業環境)與委外可行性，並依據分析結果擬訂資訊安全要求。

(二)將擬委外項目之資訊安全要求列入成本估算。

二、委外開發項目如有下列情形者，其專案成員應有資訊安全人員參與，以協助管理資訊安全風險：

(一)屬核心資通系統與第一類電腦系統。

(二)屬提供網際網路連線服務或供應商於合約期間得存取銀行機敏資料之第二或第三類電腦系統。

第五條　選擇供應商前，應執行下列事項：

一、應依據委外項目之性質訂定供應商需求建議書，內容應明列：

(一)供應商需符合之專業資格與資訊安全要求。

(二)資訊安全要求之服務水準。

二、選擇供應商過程，如涉及銀行資訊交換，銀行應備妥保密協議書，並於資訊交換前完成簽署。

三、應執行安全評估以選任合適之供應商：

（一）注意作業委託供應商對銀行服務集中度之適度分散，如存在集中度過高之疑慮，應依評估結果擬訂對應之風險處理措施。

（二）供應商對所委託項目之資訊安全管理機制。

（三）供應商與其產品或服務提供地、實質受益人或控制權來源國是否符合國內相關規範要求，以確保客戶資料安全，降低資通風險。

第六條　供應商之委託契約或相關文件中，應明確約定下列事項：

一、要求供應商遵守相關法令法規及其他適當資訊安全國際標準要求，並訂定供應商未符合資訊安全要求或服務水準時之罰責標準。

二、定義銀行與供應商之資訊安全權責，規範供應商應實施之資訊安全要求，應包含人員管理、資訊存取與傳輸安全管控機制等，以落實資通系統供應鏈邊際防護。

三、非經金融機構書面同意，不得將作業複委託他人。委外契約中應定義委託業務得否複委託、得複委託之範圍與對象，及複委託受託者應具備之資訊安全措施。

四、依據資料之機密等級、資料處理流程與傳輸方式，要求供應商實施資料安全管控。

五、與供應商約定各項服務要求，如：服務品質、水準、效能、供應商資訊安全事件應變與通報程序、資訊安全事件損害賠償責任、系統或程式定期檢測與修復要求、保固服務、異常管理等。

六、保留對供應商之稽核權。若供應商發生可能影響受託業務之資通安全事件時，應確保其本身、金融監督管理委員會及中央銀行，或其指定之人能取得供應商辦理受託業務之相關資訊，包括資通安全控管機制及相關系統之查核報告，及實地查核權力。

七、訂定資通系統功能需求或資訊建置要求，以及任何可能相關的開發方法、技術或實作，應包含資訊安全要求或控制措施。

八、訂定產品或服務之交付驗收程序和標準。

九、明確約定供應商應確保交付之產品及其服務組件來源為合法取得或經合法授權使用，且產品或服務提供地、實質受益人或控制權來源國符合國內相關規範要求。

十、要求供應商確保交付之資通系統或程式，包含供應商提供之產品及其服務組件，無惡意程式及後門程式，並取得相關安全性測試結果或供應商安全性承諾。

十一、訂定供應商契約終止時，資訊資產與資料返還、移交、刪除或銷毀之要求。

委託契約或相關文件與本規範規定不符者，銀行應執行供應鏈資訊安全風險評估，依評估結果擬訂對應之風險處理措施，包含供應商退場或替換機制，或接受風險並取得適當管理階層核准。

第七條　於供應商契約存續期間，應注意下列原則：

一、銀行與供應商應分別指定專人，負責督導及辦理各項資訊安全要求事項。

二、與供應商間如涉個人資料交換，應確認符合我國個人資料保護法相關規定，並確保僅授權者可存取資料及保留資料使用稽核軌跡，以利追蹤資料使用狀況。

三、應識別供應商涉及之關鍵資訊資產，以加強風險管理。

四、為落實資通系統供應鏈邊際防護，應訂定供應商存取權限管理規範，妥善管理供應商之實體與邏輯存取權限。

五、定期對具邏輯存取權限之供應商辦理供應鏈資訊安全風險評估，依據供應鏈資訊安全風險評估結果採取適當之資訊安全控管措施或提報適當主管層級核准可接受之風險等級。

六、建立對核心資通系統、第一類電腦系統，及提供網際網路連線服務或於合約期間得存取銀行機敏資料之第二或三類電腦系統供應商資訊安全稽核之程序，包含稽核結果之改善追蹤機制。依據供應鏈資訊安全風險評估結果選擇合適之資訊安全稽核之方式與頻率，包含自行辦理或委託獨立第三方執行資訊安全訪視作業，或由供應商提供公正第三方之驗證報告。

七、監督供應商針對其專案執行人員辦理資訊安全教育訓練。

八、依契約要求審查供應商所交付之系統或程式，包含供應商提供之產品及其服務組件之安全性測試結果或供應商安全性承諾。

九、依據與供應商約定各項服務要求定期審查供應鏈服務之品質及相關規範合規情形。如有違反要求情節重大且不能限期改善者，應執行供應商退場或替換機制。

第八條　供應商服務變更與契約終止時，應符合下列事項：

一、供應商提供之服務變更前(包含契約變更、供應商組織重大調整、業務重大異動或契約提前終止相關事宜)，銀行應執行供應鏈資訊安全風險評估，並依評估結果擬訂對應之風險處理措

施。

二、供應商契約終止時，銀行應於供應商依約完成產品或服務之移轉、交付驗收程序後，監督其完成資訊資產與資料返還、移交、刪除或銷毀，並移除供應商於服務期間所取得之實體與邏輯存取權限。

第九條　本規範經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。