

# 「信用合作社資通系統與服務供應鏈風險管理規範」條文說明

本聯社第 15 屆第 3 次、第 5 次理事社務會議通過  
金管會 114 年 3 月 13 日金管銀合字第 1130234039 號函洽悉

條 文	說 明
<p>第一條 中華民國信用合作社聯合社(以下稱本聯社)為確保信用合作社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。</p> <p>信用合作社之核心資通系統或各類電腦系統，採委託本聯社南區聯合資訊處理中心(以下稱南資中心)處理本規範相關事務者，應依據本規範之規定辦理；並應要求南資中心於複委託供應商處理本規範相關事務時，亦須依據本規範之規定辦理。</p>	<p>一、奉金融監督管理委員會 113 年 1 月 22 日金管銀合字第 1120238657 號函，參照銀行公會「金融機構資通系統與服務供應鏈風險管理規範」內容訂定之。</p> <p>二、第一項說明本規範訂定目的，係依據金融監督管理委員會「金融資安行動方案」強化金融資通系統與服務供應鏈體系之風險評估與管理，以促進金融機構健全經營與管理，全體信用合作社均應遵循辦理。</p> <p>三、第二項明定南資會員社除應依據本規範之規定辦理外，並應要求南資中心於複委託供應商處理本規範相關事務時，亦須依據本規範之規定辦理。</p>
<p>第二條 本規範所稱信用合作社資通系統與服務供應鏈，係指提供信用合作社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。</p> <p>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以當次合約採購金額為新臺幣壹仟萬元以上者，適用本規範。</p>	<p>一、第一項說明本規範之適用範圍，以信用合作社「各類資通系統」之供應鏈為原則，並得考量資訊安全風險例外排除。前開「各類資通系統」包含：核心資通系統、第一至三類電腦系統。</p> <p>二、第二項所稱「資訊服務」，以信用合作社委託供應商負責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、維運管理及雲端服務類(可參照「政府資訊作業委外資安參考指引」說明)，與上述服務無涉者，不適用本規範。</p> <p>三、第三項明定各類系統之適用，惟考量第二、三類電腦系統遭受供應鏈攻擊而影響客戶權益之可能性，以</p>

<p>信用合作社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、中華民國銀行商業同業公會全國聯合會及本聯社所訂定之相關規範。</p>	<p>及此類電腦系統數量對信用合作社資安風管量能之衝擊，為符比例原則並達到簡化作業，設定適用本規範之一定金額門檻。採購金額門檻訂定參照「資通安全管理法施行細則」第四條第一項第五款、「政府資訊作業委外資安參考指引」2.3.1及銀行公會所訂定之金額。</p> <p>四、第四項說明參照「金融資安行動方案」說明，跨機構合作夥伴係指金融機構與其他非金融機構合作發展與提供金融服務之情形(如雲端服務、行動支付等)。</p>
<p>第三條 本規範用詞定義如下：</p> <p>一、核心業務：由信用合作社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、匯款業務等。</p> <p>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。</p> <p>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 自動化服務等系統）。</p> <p>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)。</p> <p>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：</p>	<p>一、說明本規範之名詞定義。</p> <p>二、第一款至第五款用詞定義參照「信用合作社資通安全防護基準」第二條。</p> <p>三、第六款說明供應鏈資訊安全風險來源，列舉常見資訊安全議題。</p> <p>四、第七款說明邊際防護係指管控信用合作社與供應商間之網路介接防護機制，以強化信用合作社防護邊界。</p> <p>五、第八款明定機敏資料之用詞定義；另登入帳號以涉及個人資料為限。</p>

<p>人資、財會、總務等系統、物聯網設備)。</p> <p>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)，可能對信用合作社資通系統與資訊服務的機密性、完整性或可用性造成衝擊。</p> <p>七、邊際防護：管控信用合作社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)。</p> <p>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。</p>	
<p>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：</p> <p>一、應針對擬委外之項目執行資訊安全可行性分析：</p> <p>(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。</p> <p>(二)將擬委外項目之資訊安全要求列入成本估算。</p>	<p>一、明定信用合作社於規劃委外作業前應進行分析，評估委外項目之資訊安全可行性與委外資訊安全風險，以確認委外之適切性。</p> <p>二、第一款說明委外實務中，信用合作社應先評估委外項目之資訊安全風險與委外可行性，依據評估結果擬訂資訊安全要求，依據資訊安全要求進行成本估算，並透過訪商過程中，探詢潛在供應商是否可遵循信用合作社之資訊安全要求。</p> <p>三、第二款說明信用合作社委託供應商提供核心資通系統與第一類電腦系統之應用系統開發案暨第二、三類電腦系統委外開發之供應商</p>

<p>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：</p> <p>(一)屬核心資通系統與第一類電腦系統。</p> <p>(二)屬第二或第三類電腦系統，且供應商於契約存續期間得存取信用合作社機敏資料。</p>	<p>若能存取信用合作社機敏資料，需配套其等專案成員應有資訊安全人員參與，以協助第一道防線管理資訊安全風險與評估資訊安全作業執行情形。</p>
<p>第五條 選擇供應商前，應執行下列事項：</p> <p>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：</p> <p>(一)供應商需符合之專業資格與資訊安全要求。</p> <p>(二)資訊安全要求之服務水準。</p> <p>二、選擇供應商過程，如涉及信用合作社資訊交換，信用合作社應備妥保密協議書，並於資訊交換前完成簽署。</p> <p>三、應執行安全評估以選任合適之供應商：</p> <p>(一)注意作業委託供應商對信用合作社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。</p>	<p>一、說明信用合作社於選擇供應商前，應制定供應商專業資格與資訊安全要求，以作為選任依據，確認供應商資訊安全量能符合信用合作社資訊安全要求。</p> <p>二、第一款說明應於需求書中明定供應商需符合之專業資格、資訊安全要求，以及資訊安全要求之服務水準(如：系統可用率、安全管控、資訊安全稽核要求等)，以做為選商之依據。</p> <p>三、信用合作社應注意供應商之選定是否存在服務集中度過高之疑慮。爰以第三款第一目說明，如單一供應商對信用合作社之服務集中度過高時，信用合作社應制定風險處理計畫，並將評估結果提報適當主管層級核准。</p> <p>四、考量地緣政治要求，爰以第三款第三目說明信用合作社應評估供應商與提供產品或服務之位置，確認其所適用之當地法令法規，對於資訊安全要求與委外契約關係是否存在不利衝擊。</p>

<p>(二)供應商對所委託項目之資訊安全管理機制。</p> <p>(三)供應商與其提供產品或服務位置。</p>	
<p>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：</p> <p>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。</p> <p>二、定義信用合作社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。</p> <p>三、非經信用合作社書面同意，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。</p> <p>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。</p> <p>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、</p>	<p>一、說明信用合作社於供應商之委託契約或相關文件中，應明確約定供應商應負之資訊安全責任。</p> <p>二、第一項第四款說明信用合作社應依據與供應商交換之資料類型、機密等級、資料處理流程與傳輸方式，規範資料存取(如：可攜式設備、行動裝置等)與傳輸安全管控機制(如：加密、代碼化、專線傳輸等)。</p> <p>三、第一項第五款說明信用合作社與供應商約定各項服務要求，應將資訊安全要求納入。</p> <p>四、第一項第六款說明信用合作社應保留對供應商稽核權之行使權利。</p> <p>五、第一項第七款說明信用合作社應針對委託供應商建置之資通系統訂定資訊安全功能之需求(如：網段區隔、環境限制、設備存取限制與密碼規範等)。</p> <p>六、第一項第十款說明信用合作社應要求供應商針對其交付之產品或服務提供安全性檢測報告(如：程式碼掃描或檢查、黑箱測試、弱點掃描等)，若無法提供檢測服務者，得提供安全性承諾替代。</p> <p>七、第二項說明若供應商之委託契約等文件，無法符合本條之要求進行約定者，應於風險評估程序中執行評估，並依評估結果執行風險處理計畫。</p>

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。
  - 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，信用合作社應執

<p>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或接受風險並取得適當管理階層核准。</p>	
<p>第七條 於供應商契約存續期間，應注意下列原則：</p> <ol style="list-style-type: none"> <li>一、信用合作社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。</li> <li>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。</li> <li>三、應識別供應商涉及之關鍵資訊資產，以加強風險管理。</li> <li>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。</li> <li>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。</li> <li>六、建立對核心資通系統、第一類電腦系統及於契約存續期間得存取信用合作社機敏資料之第二或三類電</li> </ol>	<ol style="list-style-type: none"> <li>一、說明信用合作社之供應鏈風險管理作業應遵循之原則，以監督及管理供應商契約存續期間契約內容與資訊安全責任之落實。</li> <li>二、第二款說明信用合作社與供應商間若涉及個人資料交換，應符合我國個人資料保護法相關規定，包含當事人告知或同意、資料儲存地點與安全控制措施等。</li> <li>三、第三款說明信用合作社應盤點供應商服務所涉及之關鍵資訊資產，惟建議信用合作社可考量整併現有制度，定期執行資訊資產檢視更新。</li> <li>四、第四款說明若供應商具備信用合作社資通系統之存取權限時，信用合作社應規範系統存取權限管理規範，包含區隔設置(如：網段區隔、環境區隔、設備區隔等)、供應商人員之行動裝置與可攜式設備之管理，以落實最小權限及資訊最小揭露原則。</li> <li>五、第五款說明信用合作社應定期針對具信用合作社邏輯存取權限之供應商辦理供應鏈風險評估。風險評估內容應考量威脅來源、弱點分析與風險發生之可能性，以強化系統安全性。</li> <li>六、第六款說明信用合作社應建立核心資通系統、第一類電腦系統及於契約存續期間得存取信用合作社機敏資料之第二或三類電腦系統</li> </ol>

<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>供應商資訊安全稽核之程序，定期或不定期對上述供應商執行資訊安全稽核，以監督供應商遵循信用合作社資訊安全要求。得自行辦理資訊安全稽核、委託獨立第三方執行資訊安全訪視作業，或不便於執行稽核，亦可審查由供應商提供公正第三方之驗證報告（如：ISO/CNS27001 資訊安全管理系統標準及其他具有同等或以上效果之標準）。</p> <p>七、第七款說明供應商應對其專案執行人員辦理適當之資訊安全教育訓練，以確保人員對於資訊安全風險與責任之認知，並落實應有之管控措施。</p> <p>八、第八款說明為確保供應商所交付之系統或程式安全，應由供應商提供安全性測試報告，若無法提供安全性測試報告者，得以安全性承諾聲明為之。</p>
<p>第八條 供應商服務變更與契約終止時，應符合下列事項：</p> <p>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），信用合作社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。</p> <p>二、供應商契約終止時，信用合作社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、</p>	<p>一、說明與供應商委任關係變更或結束時處理原則。</p> <p>二、第一款說明供應商契約服務變更應執行供應鏈資訊安全風險評估，並依據評估結果執行風險處理計畫。</p> <p>三、第二款說明供應鏈資訊安全風險管理契約終止應監督執行事項，包含服務移轉、交付驗收外，應確保委任期間所取得之資訊資產、資料與存取權限之返還、移交、刪除或銷毀。</p>



<p>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。</p>	
<p>第九條 本規範經本聯社理事會通過並 函報金融監督管理委員會核備 後實施，修正時亦同。</p>	<p>訂定本規範核定層級。</p>