

# FDIC 科技實驗室

## 「金融科技與第三方風險管理計畫指引」

### (Guide for Fintechs and Third Parties)

本公司國關室翻譯

#### 壹、前言

#### 貳、銀行決定採用第三方之考量點

- 一、 第三方風險管理計畫四要項
- 二、 風險評估及盡職調查注意事項

#### 參、第三方與銀行合作之注意事項

- 一、 瞭解銀行所適用之法律及規範
- 二、 維持良好管理及財務健全之營運
- 三、 預備銀行可能的提問及潛在補救方案
- 四、 證明第三方備有適當的監控體系
- 五、 銀行管理階層可能要求第三方提供之項目及文件

#### 肆、建模人員之特別注意事項

## 壹、前言

美國聯邦存款保險公司 (Federal Deposit Insurance Corporation, FDIC) 為逾 3,400 家州註冊銀行之主要聯邦銀行監理機關；每 12 至 18 個月對該類型銀行進行例行金融檢查。該金融檢查也包括銀行與第三方合作而產生的風險管理評估。

FDIC 科技實驗室 (FDiTech) 與銀行、民間企業、監理機構及其他團體合作為銀行業引進新科技，用以提升金融機構營運效能及推動滿足客戶需求之創新。該實驗室推出此首部指引，協助金融科技公司及第三方廠商與銀行間之合作。

---

本文中譯內容如與原文有歧義之處，概以原文為準。原文網址連結如下：  
<https://www.fdic.gov/fditech/guide.pdf>

## 貳、銀行決定採用第三方之考量點

### 一、第三方風險管理計畫四要項

銀行在不同營運層面使用第三方服務。然不論風險及營運活動係直接或間接源自於第三方，銀行管理階層最終仍須負責辨識及掌控。

爰此，銀行應建立風險管理計畫以管理與第三方合作相關之風險。雖各銀行皆有其獨特性，第三方風險管理計畫通常包括下列四個基本要項：

- (一) 評估與第三方合作廠商正進行之營運活動有關風險。
- (二) 挑選第三方廠商時，進行盡職調查 (due diligence)。
- (三) 擬定合約並由適當層級人員審視合約。
- (四) 持續監督及管理與第三方合作關係。

### 二、風險評估及盡職調查注意事項

銀行依據其自身風險概況與所銷售之商品與服務，客制第三方風險管理計畫。然風險評估及盡職調查注意事項一般應包括：

- (一) 評估是否遵循適用法律及規範：
  1. 所進行之營運活動皆為相關法律及規範所許可。
  2. 第三方持有相關執照、特許或登記，可進行該項營運活動。
  3. 第三方熟悉受監理之金融機構，並可證明其遵循適用之法律及規範。
  4. 是否有針對第三方之申訴、訴訟或監理措施。
- (二) 評估第三方之財務狀況：
  1. 從可取得的第三方財務資訊評估。
  2. 評估預擬合約對第三方財務的影響。
  3. 審視其保險涵蓋範圍。
  4. 評估第三方資本額、預估盈餘、資金來源，俾確保第三方可長期存續 (資金來源於評估新創廠商時，尤為重要)。

### (三) 檢視第三方經營所有權及組織管理架構

1. 其所有權架構，及其執行擬合作業務所需之相關資格及經驗。
2. 其組織架構、營業恢復策略、緊急應變及管理者繼任計畫。
3. 其策略及目標，包含服務宗旨、品質管控、效率改善及員工政策。

### (四) 評估第三方之內部風險管理及控制機制與運作

1. 其內部控制、管理資訊系統 (management information systems)、及資料安全、隱私權保護及稽核涵蓋範圍。
2. 其持續監控風險機制及風險降低 (risk mitigation) 策略。
3. 其風控模型、演算法及其他自動化決策系統之使用。
4. 第三方是否委外其業務。若是，第三方如何管理委外廠商及委外廠商可能暴露之風險，包括網路風險。
5. 第三方是否另僱用其他專業機構，定期測試及查核風險降低管控機制的有效性。
6. 其營運持續及突發事件回應計畫。

## 參、第三方與銀行合作之注意事項

銀行通常依據其需求及合約類型，量身制訂第三方審查作業要點。以下事項可供第三方為盡職調查程序預做準備。

### 一、瞭解銀行所適用之法律及規範

所有 FDIC 監理之金融機構均須遵循安全性及穩健性標準。這些標準包含內部控制、資訊系統、內部稽核、授信文件管理及核貸、資料與資訊安全計畫。

考量擬提供銀行之服務項目，第三方亦可能須熟稔關於消費者保護、隱私權及資料安全等法律與規範、銀行保密法 (Bank Secrecy Act) 及聯邦反洗錢法律。

### 二、維持良好管理及財務健全之營運

第三方藉由證明擁有良好的管理團隊及其營運足以因應變化或中斷，方可取

得較佳之優勢。第三方應預估為準備銀行其詳盡之財務及管理資訊，包括未來盈餘及股本預估。

### 三、預備銀行可能的提問及潛在補救方案

第三方應準備下列事項：

- (一) 擬提供之產品、服務或系統的詳細資訊及服務條款，包括使用者及帳戶合約；
- (二) 模型或服務驗證紀錄，以證明產品完整性以及降低風險管理措施與消費者保護政策；
- (三) 公司治理政策，包括內部控制及品質控制。

銀行在尚未與第三方建立業務關係前，因風險評估及盡職調查流程所需，可能要求第三方擬定新政策及流程，尤其是銀行可能要求合約內容明確定義資訊保密程度，包括任何共享的客戶資訊、銀行資料或智慧財產權與商業機密之必要保障。

### 四、證明第三方備有適當的監控體系

銀行與第三方建立業務關係後，將監督第三方提供之服務或活動，確保與銀行的商業模式、風險概況及策略相符，並要求第三方採取措施改正缺失。

此外，取決與銀行的業務關係，第三方可能需接受查核、進行網路安全及週邊測試 (perimeter test) 或定期實地檢查。另銀行也可能要求提供報告，確認第三方有遵循適用之法律及合約。

同時，第三方應準備其如何確保持續遵循適用法律及法規的證明。倘行業務往來涉及銀行客戶，應證明其如何確保遵循消費者保護法、資料安全及隱私權法等法規，以及如何追蹤、監控、補救及回應消費者申訴。銀行也可能限制第三方使用或揭露銀行資訊，及要求保護客戶個人所有可辨識資訊。

### 五、銀行管理階層可能要求第三方提供之項目及文件

銀行管理階層為盡職調查並作為合約管理流程之一部分，得向第三方索取相

關文件及條款清單。此清單並未必包含所有項目，得依據第三方提供之服務及其合作之金融機構而有所不同。

(一) 第三方之背景、新業務及所有權資訊

1. 第三方任務聲明 (mission statement)、服務宗旨及品質控管計畫。
2. 公司章程。
3. 營業執照和納稅識別碼。
4. 營業項目內容及範圍。
5. 從事所洽談之業務已有多久時間。
6. 負責人的經驗與資格。
7. 對於消費者保護法及規範之相關背景與經驗。
8. 其官方網站及社群媒體數位足跡之資訊與紀錄。
9. 針對第三方或其負責人過去任何及未解決之重大申訴、訴訟或法律行為等資訊。

(二) 政策、程序及基礎設施

1. 管理資訊系統的詳細資訊，包括網路及資料流程圖。
2. 內部控制、系統及資料安全、隱私權保護及稽核範疇。
3. 適用政策及程序，包括邏輯帳戶 (logical account) 管理政策、資料型別及資料處理、資訊安全、法律遵循、洗錢防制及突發事件管理。
4. 倘與銀行業務往來涉及客戶貸款，須有稽核或獨立審查參與計畫，包括稽核或審核人員的履歷及核貸條件。
5. 依據海外資產控管辦公室 (Office of Foreign Assets Control) 及其他相關控管清單核對客戶資料的程序。
6. 營業恢復策略及緊急應變計畫。
7. 滲透 (penetration) 測試及結果。
8. 品質保證報告。
9. 員工政策，包括背景調查及聘僱實務做法。
10. 與第三方合作之分包商及其他廠商清單
11. 申訴處理及申訴事件向上通報流程。

### (三) 財務資訊及行銷文件

1. 向美國證券交易委員會申報之文件。
2. 保險涵蓋範圍。
3. 三至五年經查核的財務報表、年報及其他可取得之財務資訊。
4. 涉及銀行名稱及產品的行銷文件。
5. 經由銀行提供產品或服務之手續費、利率及其條款的詳細資訊。

### (四) FDIC 監理之銀行可能要求訂定於商業合約內的條款

1. 要求第三方遵守適用之消費者保護法、規範及監理指引相關之條款。
2. 授權銀行及相關金融監理機關，得查看第三方評估其是否遵循適用之法律及規範之紀錄。
3. 授權銀行監控及定期檢視第三方之合約遵循狀況。
4. 客戶個人可辨識資訊之保護。
5. 銀行可查核第三方之權利。
6. 倘合約終止，第三方需妥適銷毀客戶資料。

### (五) 銀行可持續或定期檢視或要求的項目

1. 每年檢視第三方的執照或登記要項。
2. 每年檢視第三方財務報表、財務義務、年報，及所有權人與負責人的財務狀況。
3. 每年檢視第三方所投保險涵蓋範圍。
4. 第三方的審查報告 (audit report) 或其他相關報告。
5. 定期檢視其內部控制及安全環境，其中可能包括實地品質確認檢視。
6. 檢視第三方營業恢復緊急應變計畫及測試。
7. 檢視任何涉及第三方提供之產品及服務的客戶申訴。

## 肆、建模人員之特別注意事項

在提供銀行模型或使用模型提供銀行商品或服務時，第三方應特別注意及謹慎。使用模型、演算法或其他自動決策系統的銀行可能對模型風險管理有特定的要求。銀行的模型風險管理架構可能要求下列事項：

- 一、模型開發需自律並具相關知識，同時對模型開發作完整建檔及需有健全之邏輯。
- 二、確保模型適當運作的控制措施。
- 三、有效模型驗證的流程。
- 四、良好的模型治理、政策及控制。