金融業上雲委外實戰分享

金融機構將作業委託他人處理涉及使用雲端服務相關法規條款

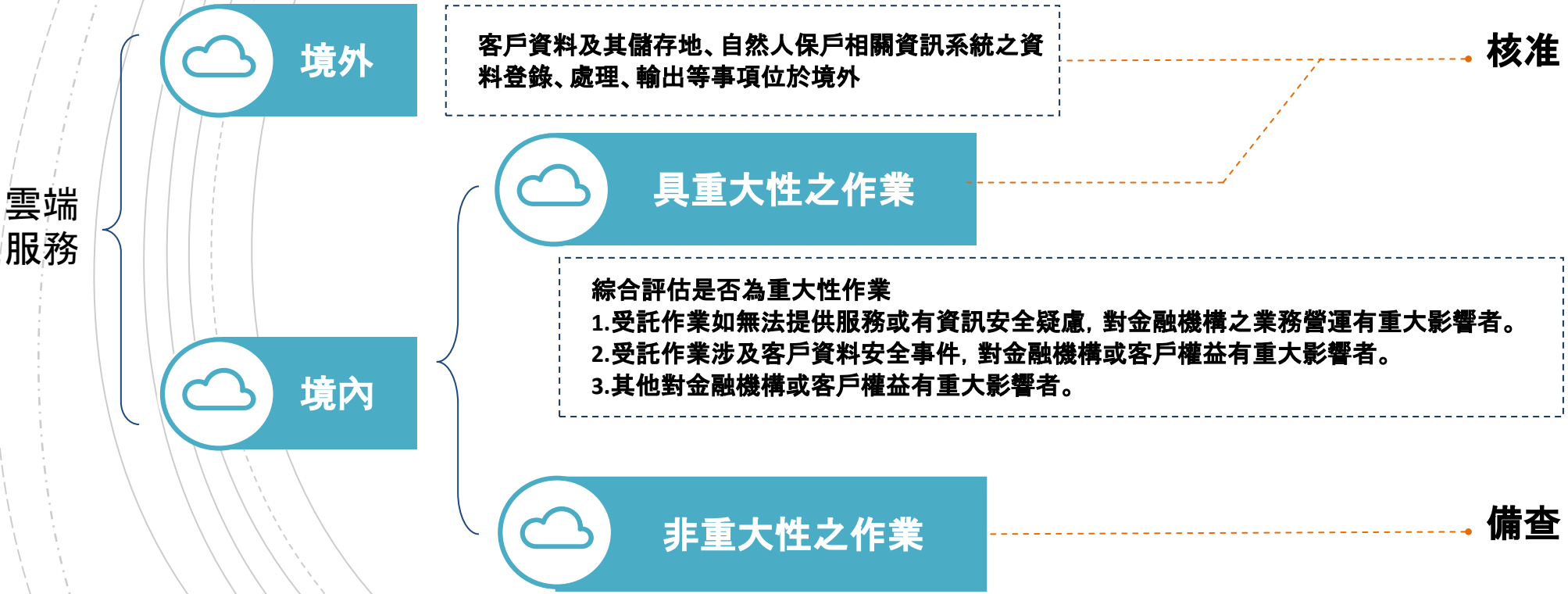
金融機構作業委託他人處理內部作業制度及程序辦法		保險業作業委託他人處理應注意事項
第3條	委外事項範圍	第3條
第10條	委外契約	第9條
第18、19條	境外委外作業	第16、17條
第19-1條	委外作業涉及使用雲端服務時	第17-1條
第19-2條	委外作業涉及雲端申請	第17-2條

金融機構將作業委託他人處理涉及使用雲端服務應辦理事項

- **委外服務之範圍與計畫**
- **作業委託之雲端服務業者，是否有適當風險管控措施，以避免服務中斷之風險**(緊急應變計畫)，及如何**適度分散風險。**
- **客戶資料及資料儲存地點及重要資料留存我國之說明，若境外儲存應說明**資料儲存地及當地資料保護法規
- **客戶資訊保護措施(如未涉及客戶資料可說明不適用)**
- **受委託機構(雲端服務業者)遵守我國客戶資料保護相關規定**
- **受委託機構(雲端服務業者)對於保於實地查核權之態度**

金融機構委外作業涉及雲端申請規定

金管會將依照雲端作業委外的重大性與否，區分為**「核准制」**以及**「備查制」**。作業委託他人處理涉及使用雲端服務，**具重大性**的委外作業，或將作業委託到**境外**者，應檢具書件向主管機關申請核准始得辦理，事先向金管會提出申請。非以上範圍的委外作業，得檢附簡化申請書件報請**備查**。



委外申請準備三步驟

★重點:確認範圍和分工, 成功邁出第一步

一、確認範圍階段

- 確認範圍與差異分析
- 與CSP溝通討論

★重點:充分溝通, 取得內部共識

二、文件準備階段

- 適法性分析
- 擬訂委外計畫
- 內部文件審閱
- 與金管會預先溝通
- 提報董事會審查

★重點:申請書件齊全

三、文件送審階段

- 彙整報部送件資料
- 正式遞件申請
- 文件審查
- 通過審查

委外申請文件準備建議分工權責

審查文件清單	資訊	資安	法遵	法務	風管	稽核	雲端服務商
申請表、自我檢核表	主要準備者	提供審閱意見與建議	提供審閱意見與建議			提供審閱意見與建議	
依委外辦法第4條第2項訂定之委外內部作業規範	主要準備者		主要準備者				
董(理)事會議事錄	主要準備者		提供審閱意見與建議		提供審閱意見與建議		
法規遵循聲明書		主要準備者	主要準備者				
委外作業之必要性與適法性分析	主要準備者	協助提供說明 提供審閱意見與建議	協助提供說明 提供審閱意見與建議	提供審閱意見與建議	提供審閱意見與建議	提供審閱意見與建議	協助提供說明
作業委外計畫書	主要準備者	協助提供說明 提供審閱意見與建議	協助提供說明 提供審閱意見與建議	提供審閱意見與建議		協助提供說明 提供審閱意見與建議	協助提供說明
客戶資訊保護措施及是否已取得客戶同意，以確保委外服務品質及客戶權益之說明	主要準備者	提供審閱意見與建議	協助提供說明 提供審閱意見與建議	提供審閱意見與建議	協助提供說明	提供審閱意見與建議	協助提供說明
受委託機構書面同意函	提供審閱意見與建議			提供審閱意見與建議			主要準備者
受委託機構之內部控制制度及相關作業程序	提供審閱意見與建議	提供審閱意見與建議				提供審閱意見與建議	主要準備者
法律意見書	提供審閱意見與建議			提供審閱意見與建議			主要準備者
受委託機構財務報告	提供審閱意見與建議						主要準備者
受委託機構出具聲明書	提供審閱意見與建議	提供審閱意見與建議		提供審閱意見與建議	提供審閱意見與建議	提供審閱意見與建議	主要準備者

主要準備者　協助提供說明　提供審閱意見與建議

獨立第三人查核之要求:金融機構除持續辦理定期獨立查核作業，可考量聯合查核

鑒於雲端科技具相當專業複雜度，金融機構對受託機構進行 查核，得自行或與其他金融機構聯合委託具資訊專業之獨立第三人查核為之;考量雲端業者委託之獨立第三人，對於我國相關法規，銀行公會資安標準以及委託銀行本身之相關要求，似未較銀行自行委託者熟稔，我國相關法規及制度，爰仍以自行委託或與其他金融機構聯合委託為限。

雲端委外服務提供商(CSP) 查核主要依據

- 台灣國內目前針對雲端應用之安全要求主要以金管會修訂之**《金融機構作業委託他人處理內部作業制度及程序辦法》**及銀行公會訂定之**《金融機構運用新興科技作業規範》**為主。其中CSP業者應遵循之事項如下:

金融機構作業委託他人處理內部作業制度及程序辦法

- 不得有存取客戶資料之權限，且不得為委託範圍以外之利用
- 資料保護措施
- 定期報告與操作紀錄
- 資料刪除/銷毀作業及其記錄
- 內部資訊安全管理作業(作業風險控管)
- 境外廠商特別規範

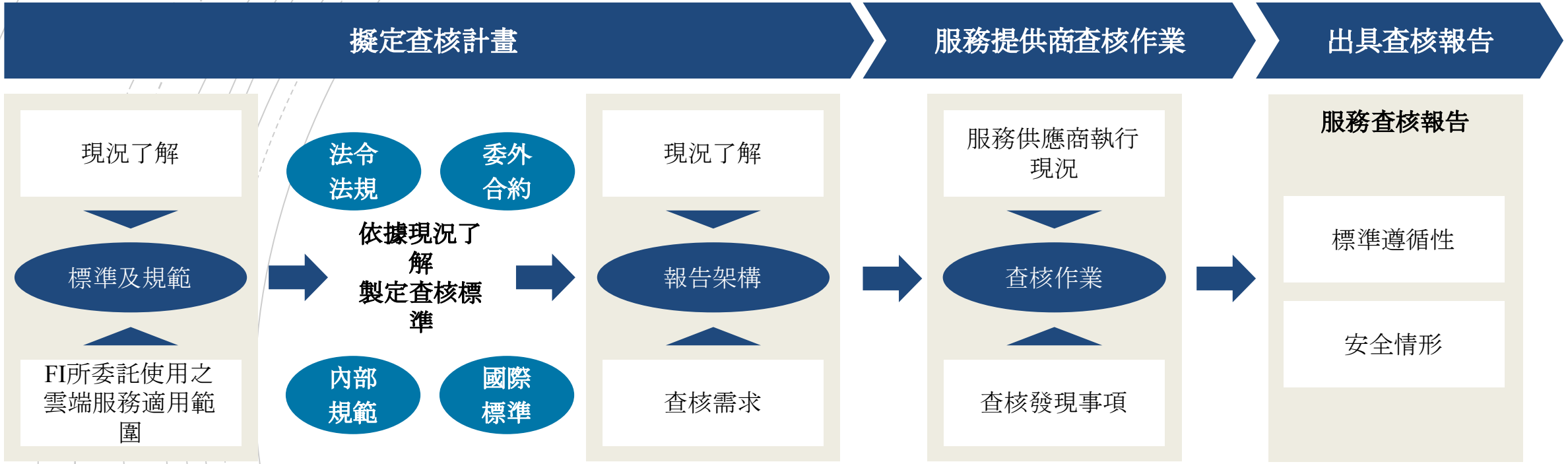
金融機構運用新興科技作業規範

- 服務協議簽訂
- 提供給委託者之雲端資源與其他委託者獨立
- 資料保護措施
- 緊急應變計畫
- 資料取得權力
- 資安事件通報程序
- 資料刪除
- 境外CSP作業要求

金融機構與CSP間的雲端服務合約

- 客戶資料保密
- 風險管理、內部控制及內部稽核制度
- 消費者爭端解決機制
- 聘僱人員之管理
- 契約終止或解約之條款
- 重大異常或缺失通知機制
- 複委託情況
- 其他契約重要約定事項

金融機構將作業委託他人處理涉及使用雲端服務，應對其受委託機構執行查核及監督



了解

確認服務供應商所適用之遵循標準，製定 查核標準。檢視服務供應商執行資訊安全遵循情況。

查核

對服務供應商提供之雲服務執行查核作業，確認其執行情形是否有符合相關要求。

結論

依據查核結果出具報告，確認服務供應商之服務資訊安全性，以確保廠商及交付服務品質。

如何完成有效的雲端委外稽核之關鍵

01 **雲端資安控管熟悉度**

熟悉雲端安全、國內外金融法規要求
熟悉雲端服務架構，了解金融機構與雲端業者之責任分工模型

02 **多方溝通之順暢度**

跨國、跨組織的溝通，需在語言、成本、時間多重壓力下，完成有效且完整之查核作業