NATIONAL CHENGCHI UNIVERSITY

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

開放銀行Open API 第二階段合規說明
- 合規第三方服務者 (QTSP) -

Part 1 – Compliance

報告人：謝叡憲 (Clement) 顧問

日期：2020/04/18

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

聲明

- 本報告係依銀行公會與財金公司相關規範，由政治大學金融科技研究中心研讀提出之解決方案。

- 解決方案如與規範在未來應用上如有衝突之處，以主管機關的解釋為依據。

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

報告大綱

1. 第二階段的現況與挑戰
2. 現行技術與資安標準說明
3. 合規項目說明：
   - (1). 法遵要求 – Compliance
   - (2). 資安要求 – Conformance
4. 輔導時程

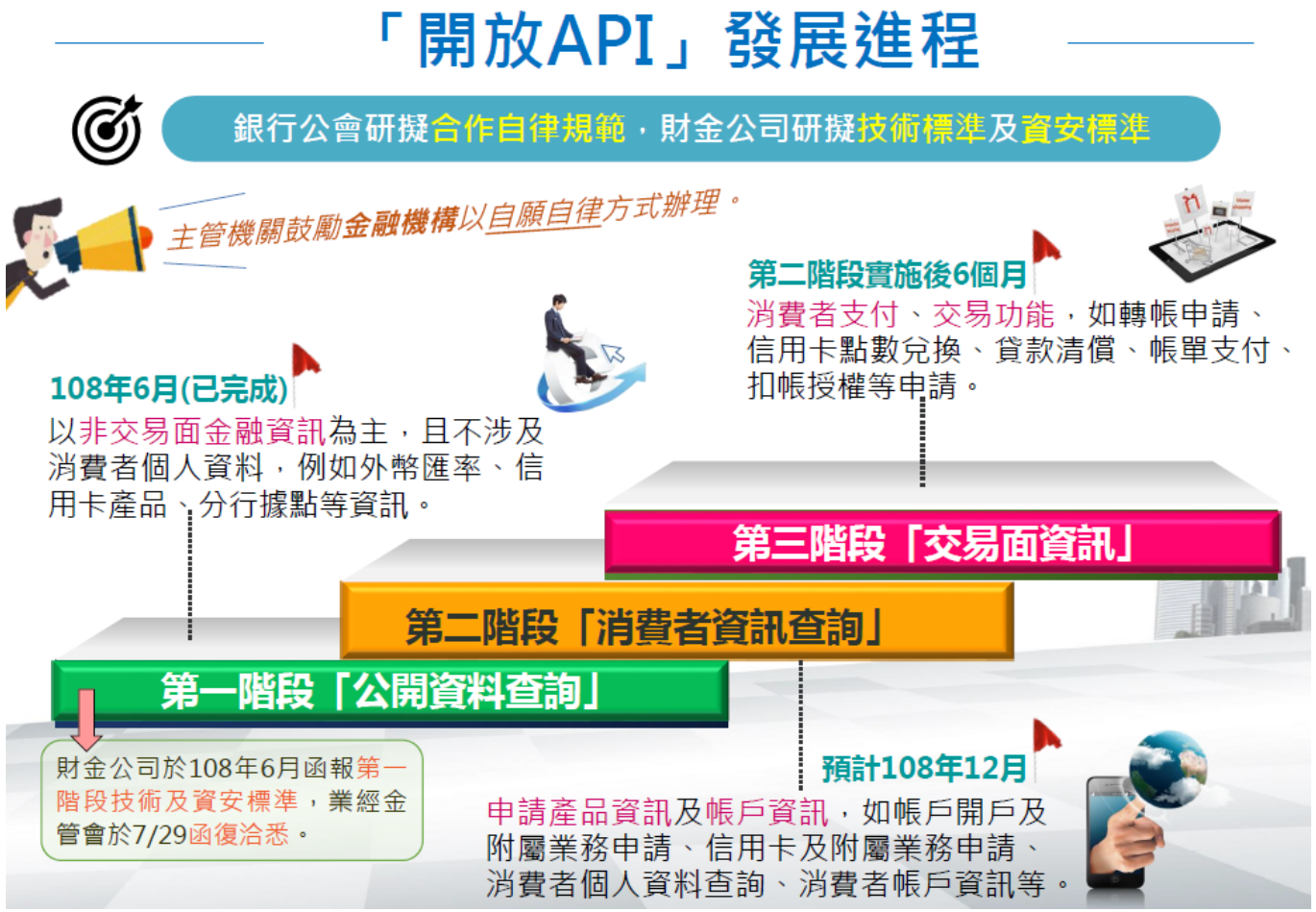
國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

Open API第二階段現況

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

Open API 預定進展

- 法源
  - 銀行與TSP 自律規範
  - 技術與資安標準
- API
  - 原先規劃以唯讀資料先讀寫資料其次
  - 現調整為以產品與業務相關API先開放
- 進程：
  - 108/10/16 – 第一階段啟動
  - 109/Q1 – 第二階段審核中



國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

TSP/銀行端現在的問題

業務面

- TSP商業模式
  - 個金/消金
- TSP規範大小

資訊面

- API管理平台
  - API上架
  - 連線安全
- 中後台整合
  - 交換資料
- 測試標準

法遵面

- 契約規定
  - 技術規範
  - 營運標範 (ISO 27001)
- 未來TSP稽核

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

政大方案：選擇合規TSP (QTSP)

法遵面

技術層面

營運層面

監理層面

業務面

互補性

生態圈經營

行動服務

資訊面

API標準

資料交換格式

資訊安全

....

先求合規
再求合作

合規TSP
Qualified
TSP
(QTSP)

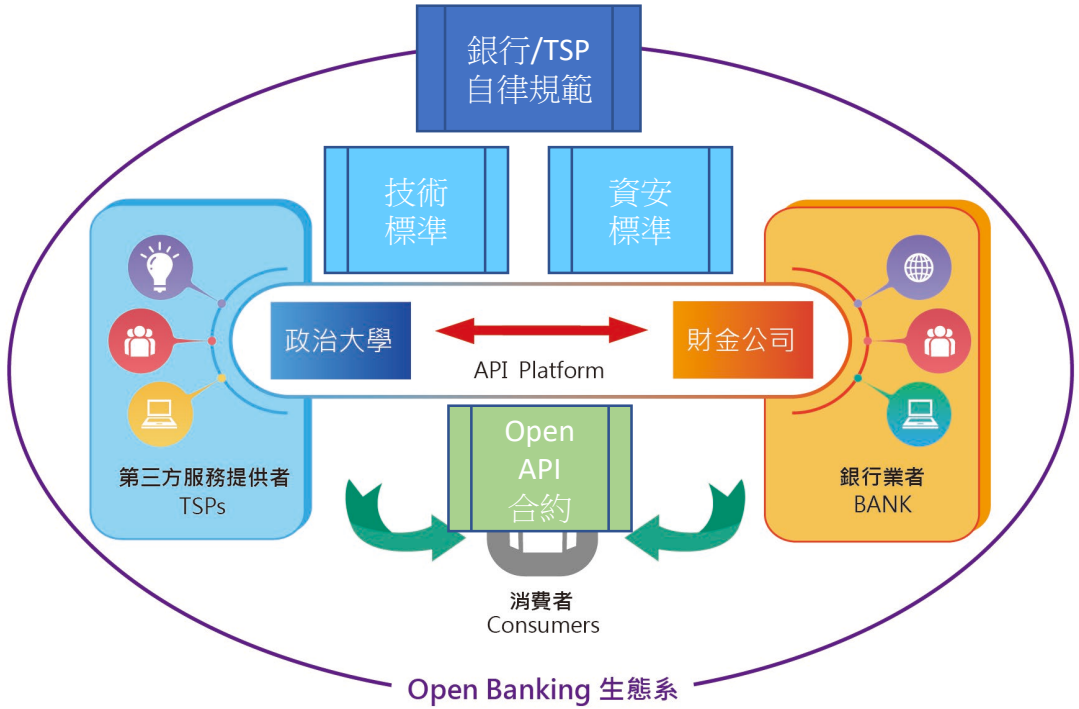
國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

法遵合規性介紹

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

Open API的法令架構

- 銀行與TSP合作，基於：
  - **銀行與TSP合作自律規範**
- 自律規範中提到
  - TSP必須和銀行簽定**合約**
  - TSP必須符合技術與資安標準
  - TSP必須符合ISO 27001或相當認證
- 二個標準
  - 技術標準：**Open API技術規格文件**
  - 資安標準：**業務安全控管作業規範**



國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

合規重點在資安標準文件

- 第二階段的技術與資安規範已經在12/26財金Open API委員會後，準備送金管會備 查中
- 合規重點在於銀行公會提出的資安標準文件

章節	內容摘要
一	明定本作業規範之法源依據、適用對象與範圍、用詞定義。
二	(安全控管要求) 消費者註冊時之身分確認安全設計、消費者資訊查詢之身分確認安全設計、網路型態與其安全設計、設計原則之共通要求與各類安全要求。
三	(資訊系統標準) 應訂定組織、人員及設備安全之相關管理措施；應就機房、營運、網路、金鑰、系統生命週期、資安事故、營運持續管理等採取資訊安全維護措施。
四	(配套監理措施) 應於業務申請時及其後每年由[redacted]進行檢視，提出「資訊系統及安全控管作業評估報告」。
五	明定本作業規範施行日期。

公正第三方

後續查核
- TSP年度查核
- 銀行內稽抽查

見下張示意圖
- TSP 端架構
- 銀行端架構
- 連線安規

ISO/CNS 27001: 建議
- 四大輔導
- 由TAF的廠商指定認證

合規項目

合作前

資格

- 聲明書
- 相關文件

技術

- 連線安全
- API檢驗

營運

- ISO27001
- 資安檢查

合作後

稽核

- TSP年度自評
- 銀行抽查

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

QTSP的範圍

QTSP

法遵合規 Compliance

技術合規 Conformance

- 資格 Qualification
- 營運 Operation
- 稽核 Auditing
- 技術 Info. Tech

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

合規項目說明

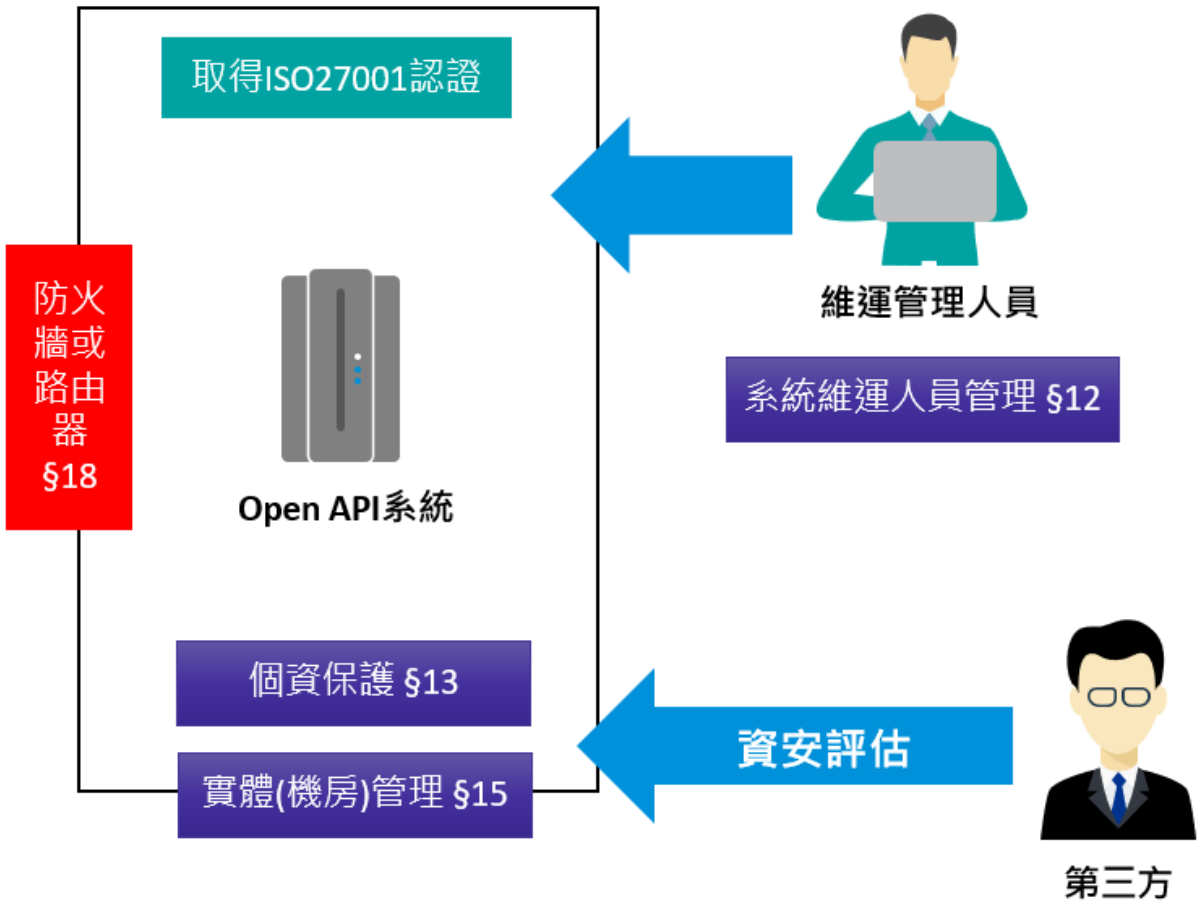
一、資格層面

合法登記	穩健經營	聲明文件	資安營運	介接標準
◘ 經濟部商業司商工登記網站查詢結果頁面。 ◘ 最近三個月內之公司變更登記表。 ◘ 最近一次修訂之公司章程。 ◘ 誠信經營聲明書(應擔保現在及未來均無經營非法事業之情事)。 ◘ 負面新聞審查紀錄(由銀行透過KYC程序、網路檢索查核該第三方服務提供者是否曾有經營非法事業之事實)。	◘ 最近三期經股東同意或股東常會承認之財務報告；如屬資本額達一定金額以上依法其財務報表應經會計師簽證者，應提供最近三期經會計師簽證之財務報表。 ◘ 董監事及高階管理人(含總經理、副總經理、執行/財務長、協理或其他具相當職務之人)學經歷資料表。	◘ 最近一個月內負責人及經理人之「警察刑事紀錄證明」（良民證）。 ◘ 最新票據信用查詢紀錄（包含最近三年退票（清償）紀錄、拒絕往來資訊等），如已出具「當事人綜合信用報告」者，得予免徵。 ◘ 財團法人金融聯合徵信中心「當事人綜合信用報告」（揭露期限至少五年）。 ◘ 經第三方服務提供者負責人及經理人簽署聲明未發生有「銀行負責人應具備資格條件兼職限制及應遵行事項準則」第三條第一項除第十三款外之各款聲明書。	◘ 第三方服務提供者應提供下列文件之一，以佐證具備資訊安全風險管理能力： ①**ISO27001標準認證**或相同等級之認證；如涉及支付卡業務者，並應出具PCI DSS認證； ②**資安防護能力經第三方驗證之證明**。 ◘ 最近三年未曾發生個人資料外洩或資通安全事件之聲明書，如曾發生者，應提供改善完成之證明。 ◘ 負面新聞審查紀錄(由銀行透過KYC程序、網路檢索查核該第三方服務提供者是否曾有發生個人資料外洩或資通安全事件)。	◘ 業務合作契約書應訂有下列條款： ①第三方服務提供業者承諾採用經主管機關核定或銀行公會決議通過之應用程式介面相關「技術及資安標準」之契約條款。 ②第三方服務提供業者或其委託開發廠商**所開發應用程式介面上線前應經安全性測試合格**。

註1：依銀行公會的”銀行與第三方服務業者自律規範”建議與TSP合作之審查資料與文件 (2019/07/03)
註2：各銀行可依銀行內部稽核制度另外要求

ISO 27001 驗證範圍

二、營運層面



三、稽核層面

條款	條文	作法
第23條	本規範所訂之資訊系統及安全控管項目，TSP業者應透過內部控制制度進行定期檢核，並應於依規定申請許可時及其後每年四月底前，由公正第三方驗證單位進行檢視，提出資訊系統及安全控管作業評估報告。	為TSP內部稽核措施，由原ISO27001驗證單位進行檢視，並提供報告。
	金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得TSP業者辦理開放應用程式介面業務之相關資訊，包括個人金融資料及相關系統之查核報告，及實地查核權力。	由銀行視必要性委任其它單位，對TSP做外部稽核檢視。 →銀行可請現行配合會計師事務所查核 →可依政大研究的 IASME 項目進行外部查核*

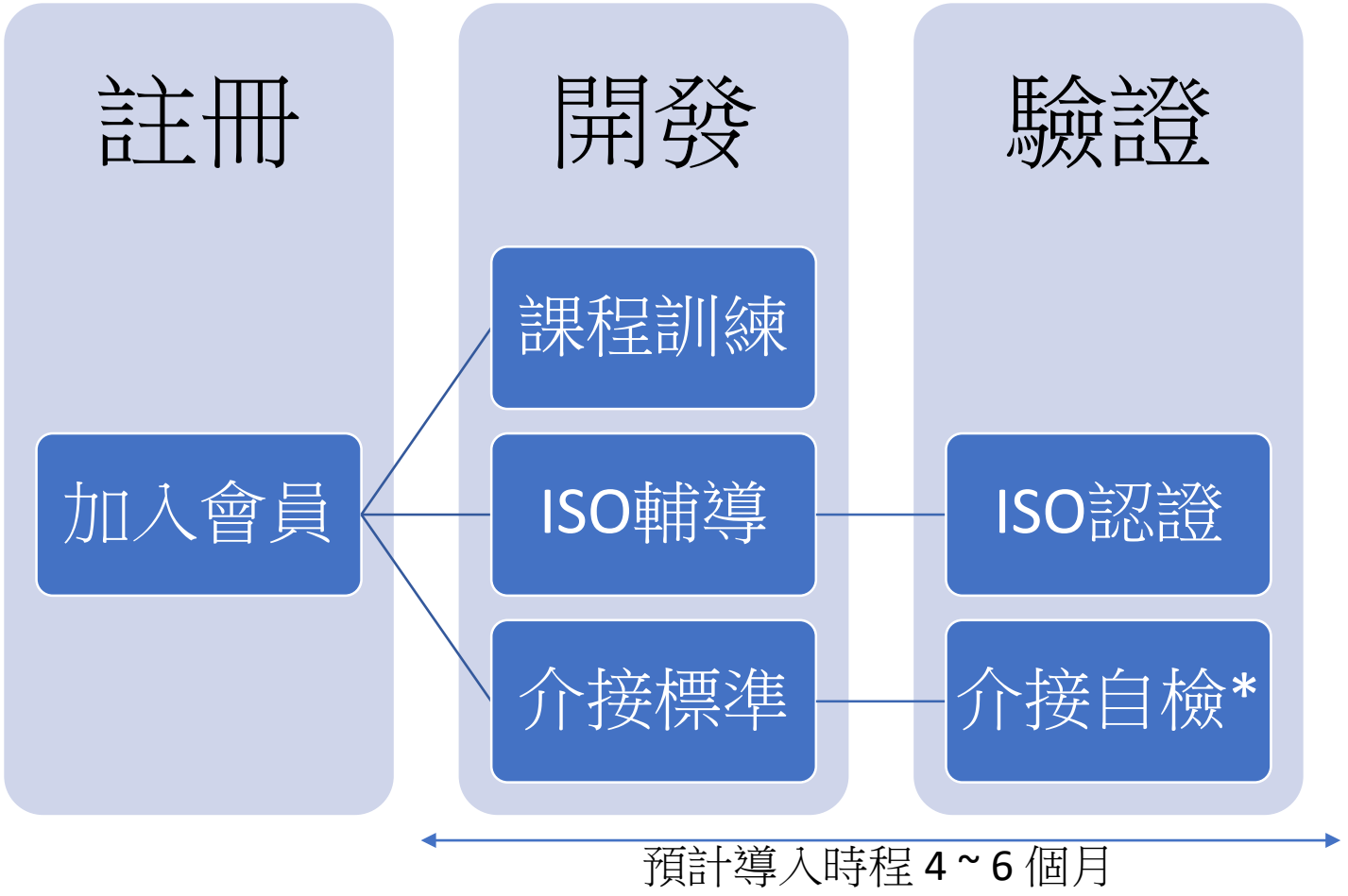
- IASME 為英國開放銀行驗證/稽核機構之一，但在台灣驗證單位必須國家核可，因此可做為銀行內部稽核時的標準
- 銀行如果想了解 IASME 內容，可洽政大金融科技中心

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

政大輔導計劃與時程

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

輔導的時程



* 由政大提供自檢工具或由銀行委託進行

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

輔導目標

項目	目的	作法
教育訓練	協助TSP了解與銀行合作上必要的法令與技術規範	• 提供商模、法令、技術、檢驗等四類課程，協助TSP降低與銀行合作門檻
ISO認證	TSP在輔導期間必須取得由銀行認可的第三方資安認證，由符合未來上線的法遵要求。	• 由政大協同第三方輔導與認證單位一起協助TSP。 • 未來TSP稽核可以銀行認的第三方單位執行。
測試檢驗	建立銀行間共用交換資料格式，並公開讓銀行與TSP使用。 建立標準測試項目，加速TSP與銀行測試速度與效率。	• 與SI廠商合作 • 建立測試標準項目 • 建立標準版API templates • 開發資料驗證小工具 • 開發API測試小工具 • 與SI合作進行API平台測試

* 可參考政大開放銀行網站有關以上資訊

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

課程訓練

商業

- OpenBanking 應用與發展
- OpenAPI 平台與運用

法令

- OpenAPI 法令與監理
- 個資法令與監理

技術

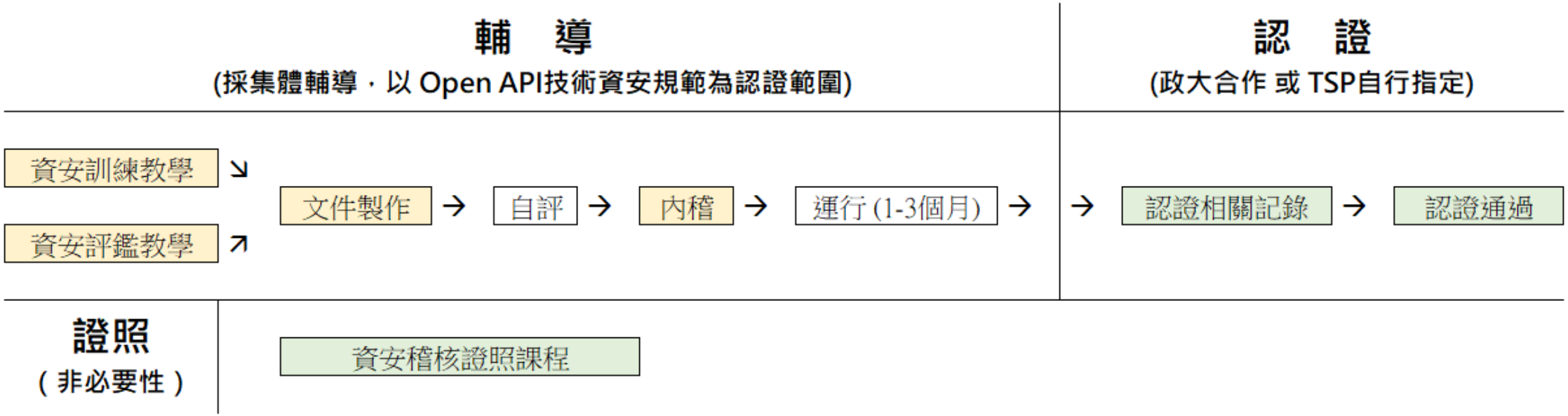
- API資安原理與應用
- OAuth原理與應用

檢驗

- 連線測試標準
- OAuth測試標準

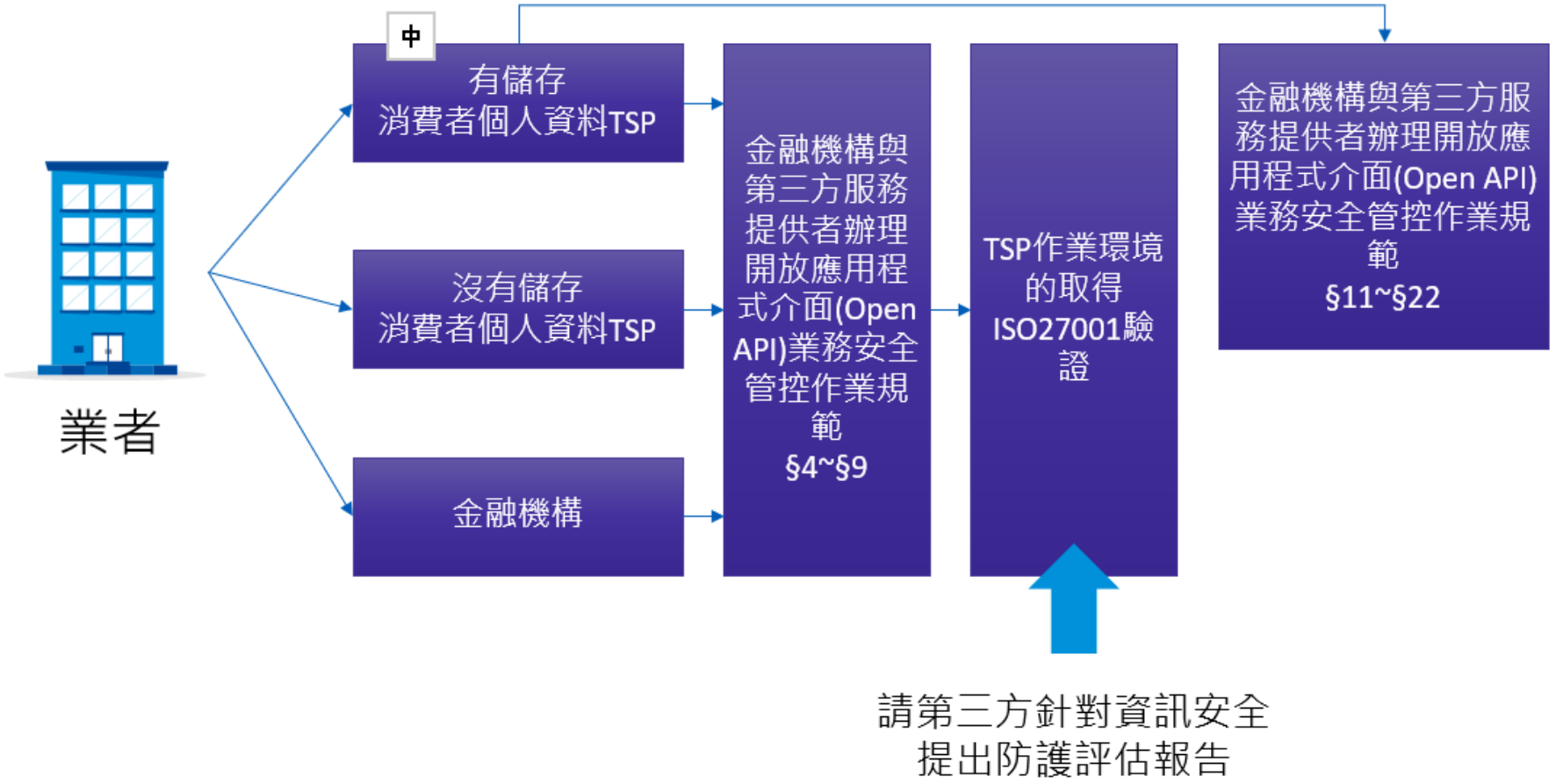
ISO 27001輔導作業

--ISO 27001 – 資訊安全認證--



國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

ISO 27001 驗證程序



國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

ISO 27001 驗證證書

證書樣本

管理系統驗證證書

環奧國際驗證有限公司授與
管理系統驗證證書予下列機構：

[Client's Logo]

[受稽客戶Client Name]
[登記地址Client Address]

驗證位址 Sites：

驗證範圍：
.....
.....
，並與適用性聲明(version XX)一致。

獲證單位將透過年度定期複核及每三年的重新驗證稽核，以維持本證書之有效性。

環奧國際驗證有限公司
統一編號：80160703
地址：台北市信義區松德路 161 號 12 樓之 2
電話：(02) 2726-0262 傳真：(02) 2726-0663
電子信箱：office@mail.tcicgroup.com

管理系統驗證證書證明有效應用且發展：

資訊安全管理系統
符合下列標準要求
ISO/IEC 27001:2013、CNS 27001:2014

證書編號：Q-NNN-YYYY-ISMS
初次驗證：YYYY 年 MM 月 DD 日
有效期限：YYYY 年 MM 月 DD 日

台北市，YYYY 年 MM 月 DD 日

驗證機構：環奧國際驗證有限公司

Class: Controlled

僅供TSP輔導與合規說明會參考使用

ISO 27001 細部輔導作業說明

KPMG/TCIC 介紹