# 經濟部工業局
# 行動應用App基本資安
# 檢測基準及自主檢測推動制度

執行單位：財團法人資訊工業策進會

民國104年9月

# 背景與概述

- 「行政院國家資通安全會報」於去年第26次委員會決議手機應用軟體由**經濟部工業局**主責：
  - 資安檢測**標準制訂**
  - 鼓勵廠商**自主驗證**
- 於103年10月經濟部工業局委託財團法人資訊工業策進會執行
- 於104年4月20日「行動應用App基本資安規範」**正式公告**於經濟部通訊產業發展推動小組網站
- 於104年8月14日「行動應用App基本資安檢測基準」、「行動應用App基本資安自主檢測推動制度」**正式公告**於經濟部通訊產業發展推動小組網站

# 主要參考依據

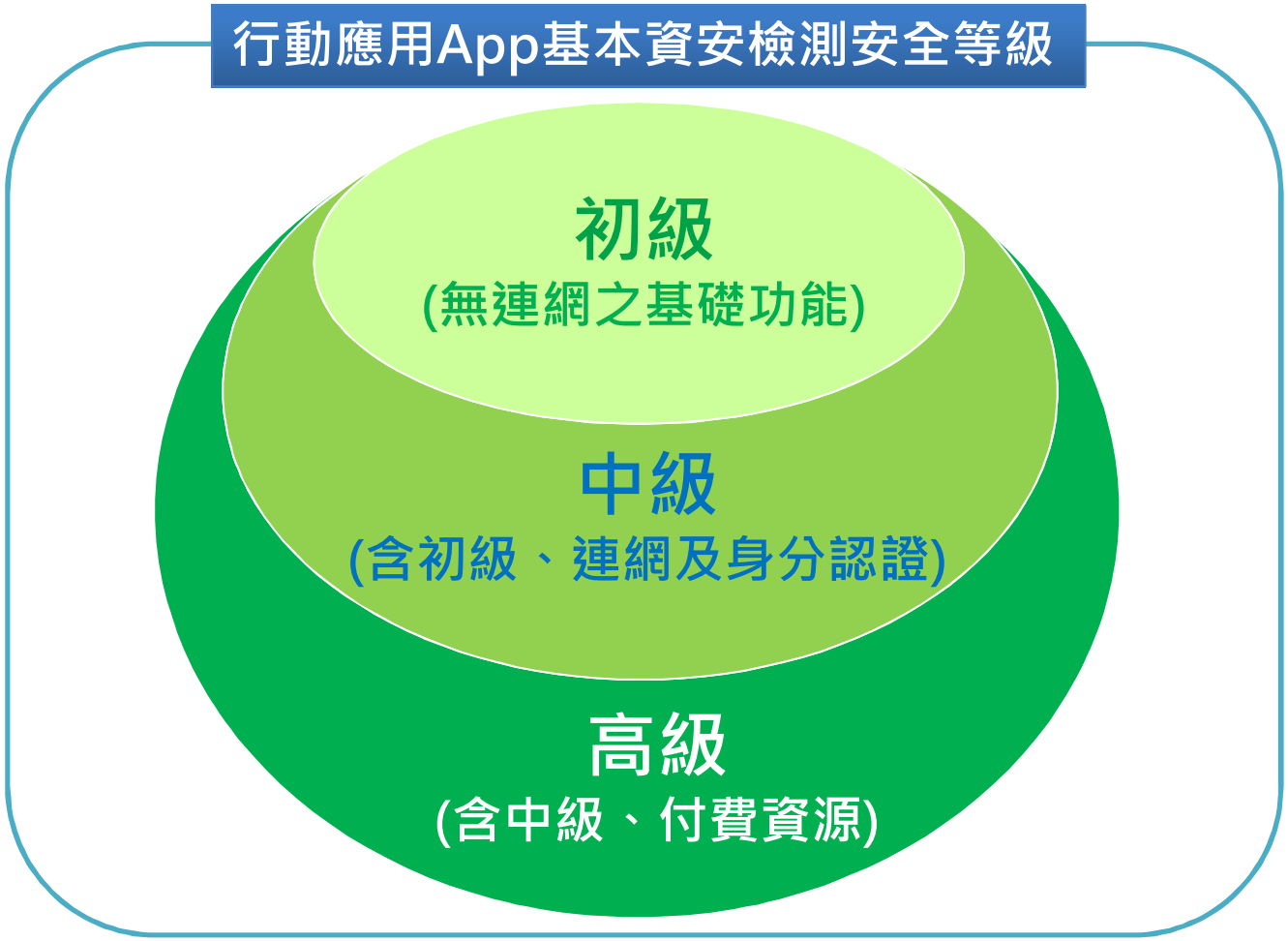
- **行動應用App基本資安規範**
  - 經濟部工業局，民國104年4月20日
- **NIST SP800-163**
  - National Institute of Standards and Technology (美國國家標準技術研究所)
  - Special Publication 800-163 Vetting the Security of Mobile Applications, January 2015
- **OWASP Top Ten Mobile Risks**
  - Open Web Application Security Project（開放Web軟體安全計畫）
  - Mobile Security Project - Top Ten Mobile Risks

# 適用範圍

- 適用範圍：行動應用程式**共通性**之安全檢測
- **特定領域**之行動應用程式其資安規範應由**各目的事業主管機關**訂定
- 資訊安全本質為**風險控管**概念，故
  - 通過檢測之行動應用程式，僅**對程式本身**具有安全水準保證
  - **使用者**亦需**善盡使用與管理**個人相關資料之責任，以降低因蓄意或個人行為疏失所造成之風險及危害

# 檢測基準安全等級

- 所有檢測項目依**功能安全性**分類**為初級、中級(含初級)及高級(含中級)三個安全等級**
- 原則上行動應用程式開發商可**自行決定**送檢之安全等級



# 檢測基準安全等級 – 架構

**檢測基準之安全等級依據資安規範技術要求事項，初級檢測項目共計29項，其中9項訂為必要檢測項目，其餘20項為非必要檢測項目**

| 資安基本規範面向 | 檢測基準安全等級 | 資訊安全技術要求事項 | 檢測項目 | 必要項 | 非必要項 |
|---|---|---|---|---|---|
| 4.1.1.行動應用程式發布安全 | 初級涵蓋規範11項要求 | 4.1.1.1.行動應用程式發布 | 2 | 2 | 0 |
| | | 4.1.1.2.行動應用程式更新 | 3 | 0 | 3 |
| | | 4.1.1.3.行動應用程式安全性問題回報 | 2 | 1 | 1 |
| 4.1.2.敏感性資料保護 | | 4.1.2.1.敏感性資料蒐集 | 2 | 2 | 0 |
| | | 4.1.2.2.敏感性資料利用 | 4 | 0 | 4 |
| | | 4.1.2.3.敏感性資料儲存 | 7 | 4 | 3 |
| | | 4.1.2.5.敏感性資料分享 | 3 | 0 | 3 |
| | | 4.1.2.6.敏感性資料刪除 | 1 | 0 | 1 |
| 4.1.3.付費資源控管安全 | | 4.1.5.1.防範惡意程式碼與避免資訊安全漏洞 | 2 | 0 | 2 |
| | | 4.1.5.3.函式庫引用安全 | 1 | 0 | 1 |
| | | 4.1.5.4.使用者輸入驗證 | 2 | 0 | 2 |
| | 中級（含初級）涵蓋規範14項要求 | 4.1.2.4.敏感性資料傳輸 | -- | 待訂 | 待訂 |
| 4.1.4.身分認證、授權與連線管理安全 | | 4.1.4.1.使用者身分認證與授權 | -- | 待訂 | 待訂 |
| | | 4.1.4.2.連線管理機制 | -- | 待訂 | 待訂 |
| 4.1.5.行動應用程式碼安全 | 高級（含中級）涵蓋規範17項要求 | 4.1.3.1.付費資源使用 | -- | 待訂 | 待訂 |
| | | 4.1.3.2.付費資源控管 | -- | 待訂 | 待訂 |
| | | 4.1.5.2.行動應用程式完整性 | -- | 待訂 | 待訂 |
| | | | 17 | 29 | 9 | 20 |

# 檢測基準安全等級 – 初級檢測必要項目

| 資訊安全技術要求事項 | 行動應用程式檢測項目 |
|---|---|
| 4.1.1.1.行動應用程式發布 | 4.1.1.1.1.應於可信任來源之行動應用程式商店發布 |
| | 4.1.1.1.2.應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途 |
| 4.1.1.3.行動應用程式安全性問題回報 | 4.1.1.3.1.開發者應提供回報安全性問題之管道 |
| 4.1.2.1.敏感性資料蒐集 | 4.1.2.1.1.應於蒐集敏感性資料前，取得使用者同意 |
| | 4.1.2.1.2.應提供使用者拒絕蒐集敏感性資料之權利 |
| 4.1.2.3.敏感性資料儲存 | 4.1.2.3.1.應於儲存敏感性資料前，取得使用者同意 |
| | 4.1.2.3.2.應提供使用者拒絕儲存敏感性資料之權利 |
| | 4.1.2.3.4.應避免將敏感性資料儲存於暫存檔或紀錄檔中 |
| | 4.1.2.3.6.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取 |

# 檢測基準安全等級 – 必要檢測項目

| | 試辦 | 研訂中（暫定） | |
|---|---|---|---|
| 技術要求(規範) ＼ 各安全等級必要檢測項目 ／ 安全等級 | 初級 | 中級 | 高級 |
| 4.1.1. 行動應用程式發布安全 | 3 | 3 | 6 |
| 4.1.2. 敏感性資料保護 | 6 | 8 | 15 |
| 4.1.3. 付費資源控管安全 | 0 | 0 | 4 |
| 4.1.4. 身分認證、授權與連線管理安全 | 0 | 6 | 6 |
| 4.1.5. 行動應用程式碼安全 | 0 | 0 | 5 |
| 必要檢測項目總數 | 9 | 17 | 36 |

註：「規範」為「行動應用App基本資安規範」之簡稱

# 檢測基準安全等級 – 標章之取得

- 第一類行動應用程式須通過初級安全檢測、第二類行動應用程式須通過中級安全檢測，第三類行動應用程式須通過高級安全檢測
- 於通過所有該等級**必要檢測項目**後，始取得該等級標章之資格

檢測實驗室提供之檢測項目

開發商參考之安全要求事項

| 檢測基準安全等級 / 行動應用程式分類 | 初級<br>檢測無連網之基礎功能安全性 | 中級(含初級)<br>檢測連網及身分認證安全性 | 高級(含中級)<br>檢測付費資源之安全性 |
|---|---|---|---|
| 第一類<br>純功能性 | ★ | V | V |
| 第二類<br>具認證功能與連網行為 | — | ★ | V |
| 第三類<br>具交易功能（包括認證功能及連網行為） | — | — | ★ |

★為必要通過之檢測等級　　V為可自由選擇通過之檢測等級

# 「行動應用App基本資安檢測基準」文件架構

# 基本資安檢測基準 – 檢測欄位範例

| | |
|---|---|
| **檢測編號** | 4.1.2.3.4 |
| **安全分類** | 「行動應用App基本資安規範」第一類、第二類、第三類 |
| **檢測項目** | 行動應用程式敏感性資料儲存限制 |
| **檢測依據** | 「行動應用App基本資安規範」4.1.2.3.敏感性資料儲存 |
| **技術要求** | 行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中 |
| **檢測基準** | 1) 檢查是否未將敏感性資料儲存於網頁暫存檔或自定義暫存檔。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 |
| | 2) 檢查是否未將敏感性資料儲存於系統日誌或自定義日誌。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 |
| **檢測結果** | 符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料<br>不符合要求：任一檢測基準不符合 |
| **備註** | 無 |

# 檢測方式

- 行動應用程式檢測性質屬黑箱測試，其檢測為滲透測試(攻與防)概念，故於本檢測基準僅提供檢測方式供參考
  - 考量行動應用程式開發商之行動應用程式原始碼屬**商業機密**
  - 「行動應用App基本資安規範」為**非強制性**，送測單位通常不會提供程式原始碼進行檢查
  - 各資安檢測業者所發展之檢測方法(Know-How)屬**商業機密**，難有標準一致性之檢測方法(SOP)
  - 檢測以**黑箱測試**方法論為主，主要以**未取得原始碼**之情況下進行測試
- 檢測方式
  - 採**靜態**分析與**動態**分析混合使用
  - 依實際檢測需要，進行行動應用App逆向工程(reverse engineering)或中間人(man-in-the-middle)測試等方法進行檢測

# 檢測結果與產出 – 參考項目

- 檢測結果與產出應包含但不限於以下內容
  - 檢測標的(含程式名稱、版本等)
  - 檢測範圍之宣告(檢測等級)
  - 檢測時程(含收件時程，檢測期間等)
  - 檢測方式、環境與使用工具
  - 檢測執行人員與負責項目
  - 檢測項目為「符合或不符合」之判定
  - 檢測過程紀錄及佐證資料

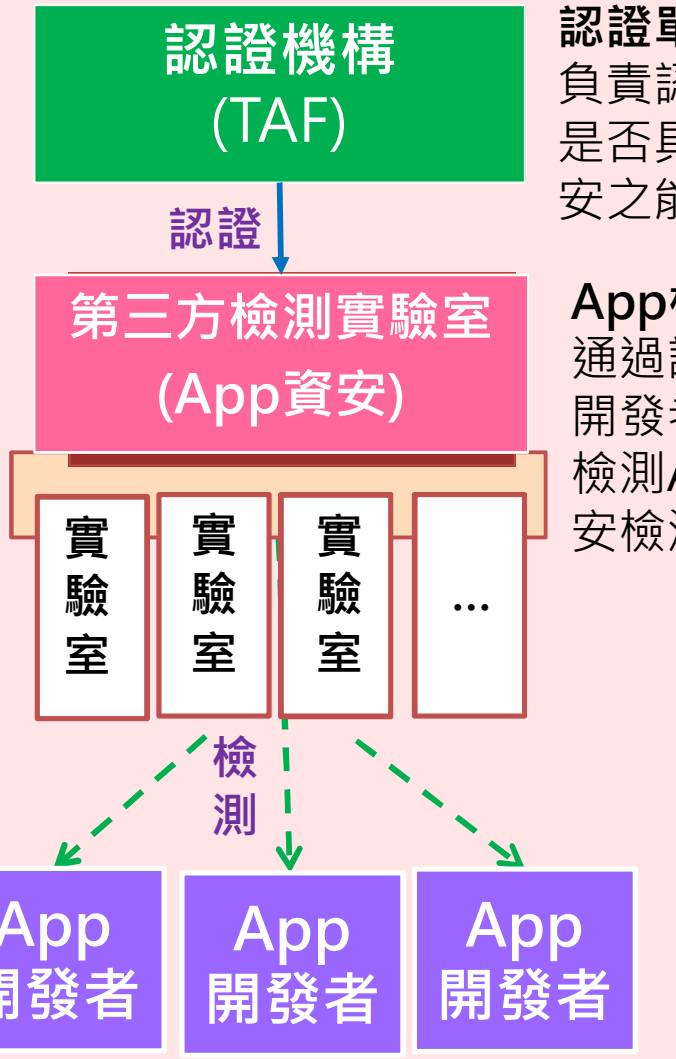
# 自主檢測推動制度運作架構

專案計畫委託單位

**經濟部工業局**

運作檢測制度及標章管理

**制度管理委員會**
(如資策會、公協會等共同籌組)




**認證單位**
負責認證檢測實驗室是否具備檢測App資安之能力

**App檢測單位**
通過認證，受理App開發者之檢測申請，檢測App是否符合資安檢測基準

# 檢測實驗室認證-時程規劃

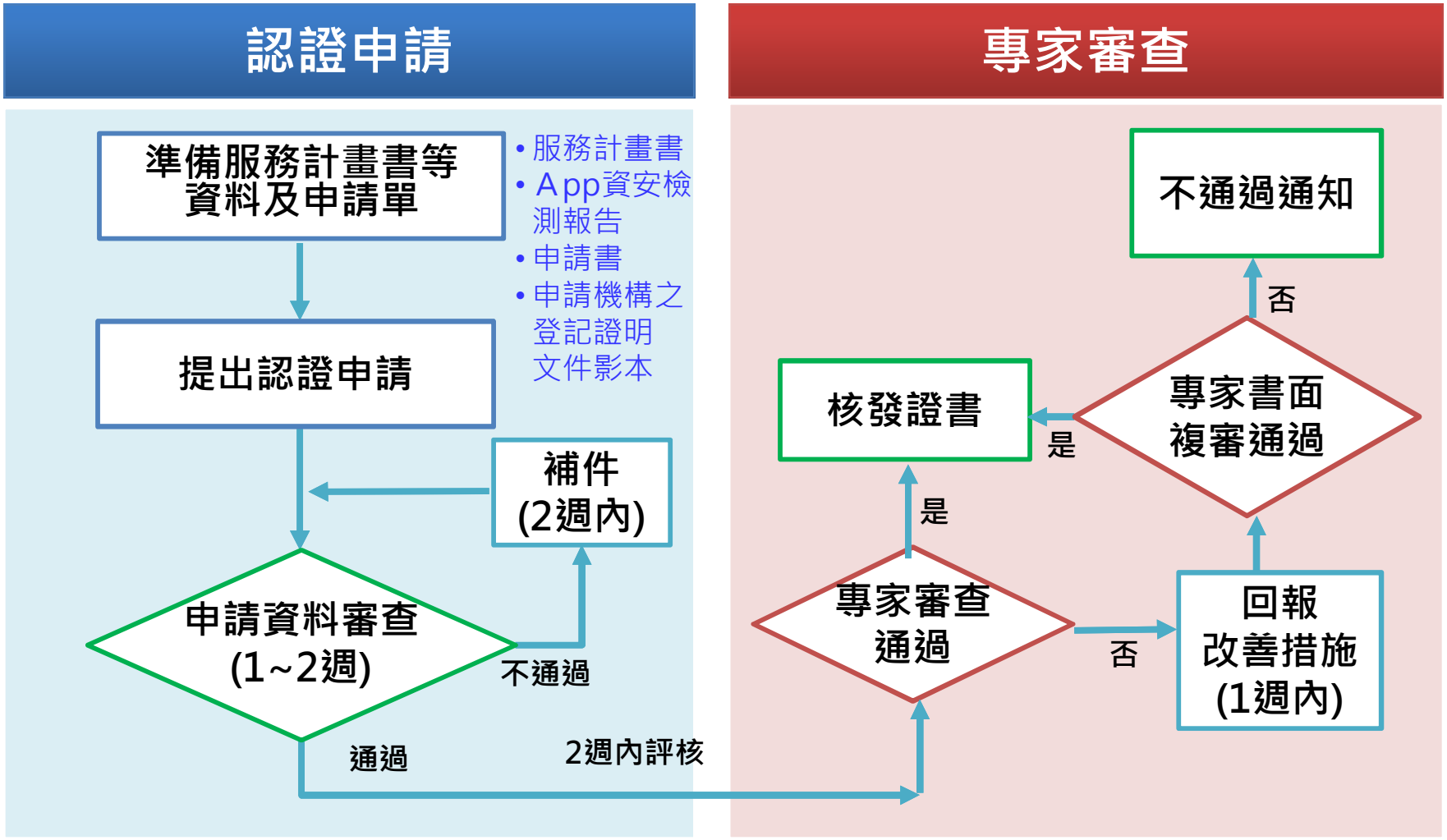
## 執行時程規劃

- 試辦期間：104/10/1~105/9/30
- 試辦檢測實驗室證書效期：至105/12/31(試辦期結束後3個月)

| 執行階段 | 試辦檢測實驗室認證 | | 正式檢測實驗室<br>TAF認證 |
|---|---|---|---|
| 梯次 | 第1梯次<br>104年度 | 第2梯次<br>105年度 | 不分梯次 |
| 1. 資訊公告 | 9/25 | 9/25 | 104/12/01 |
| 2. 認證申請 | 10/1~10/31 | 3/1~3/31 | 105/1/1 |
| 3. 專家審查 | 11/1~12/31 | 4/1~5/31 | 依據TAF審查流程 |
| 4. 能力試驗活動 | 無 | 無 | 依據制度管理委員會公告 |

# 試辦檢測實驗室認證 -限試辦期內

## 試辦檢測實驗室認證流程(1~2個月)



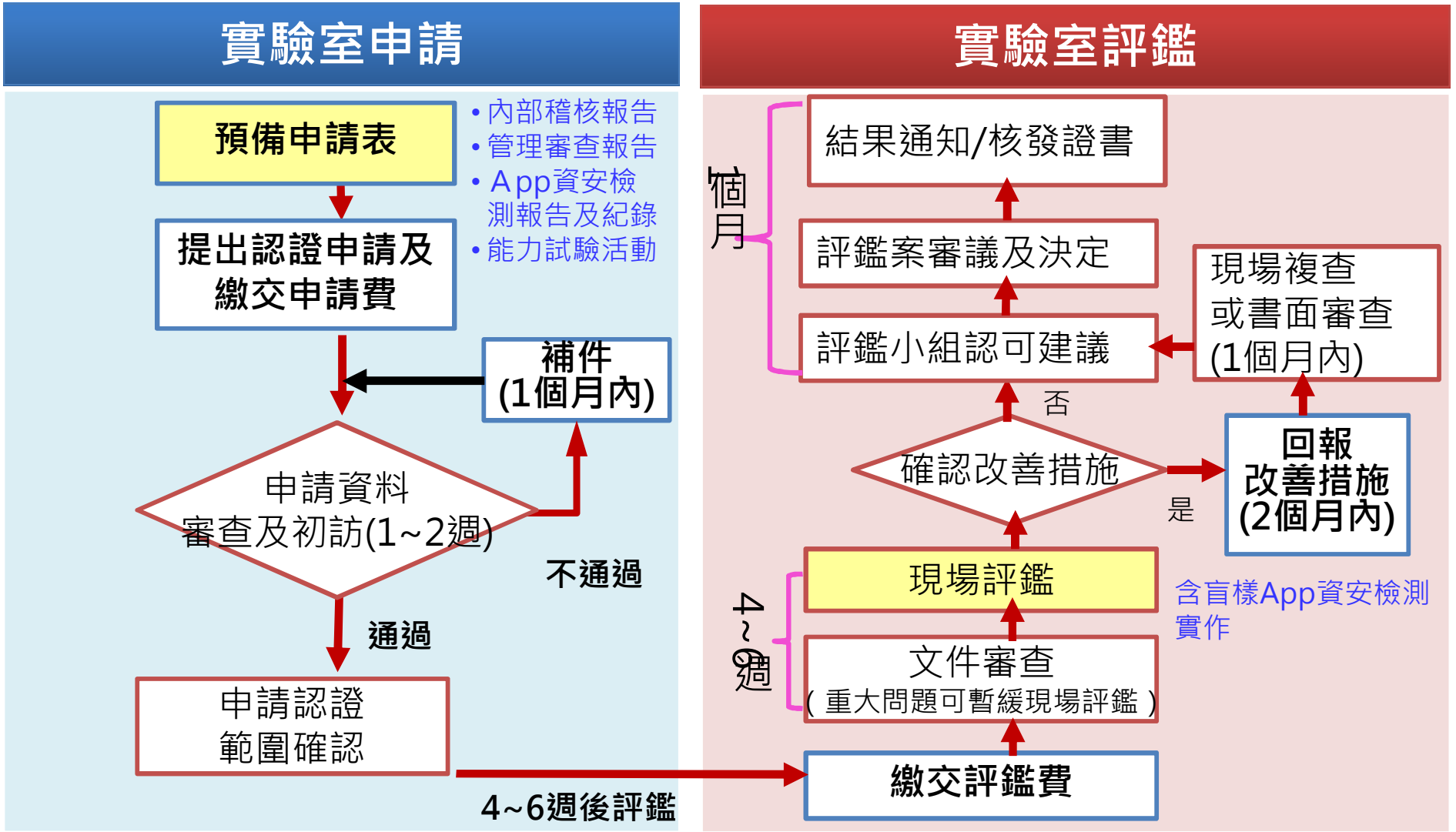
# 檢測實驗室認證-時程規劃

## 能力試驗活動時程規劃

| 執行階段 | 能力試驗活動 | | |
|---|---|---|---|
| 梯次 | 第1梯次<br>104年度 | 第2梯次<br>105年度 | 第3梯次<br>105年度 |
| 1. 資訊公告 | 104/11/1 | 104/11/1 | 104/11/1 |
| 2. 受理申請 | 104/12/1~12/31 | 105/5/1~5/31 | 105/11/1~11/30 |
| 3.能力試驗 | 105/1/1~1/31 | 105/6/1~6/30 | 105/12/1~12/31 |
| 4. 能力試驗結果通知 | 105/1/31 | 105/6/30 | 105/12/31 |

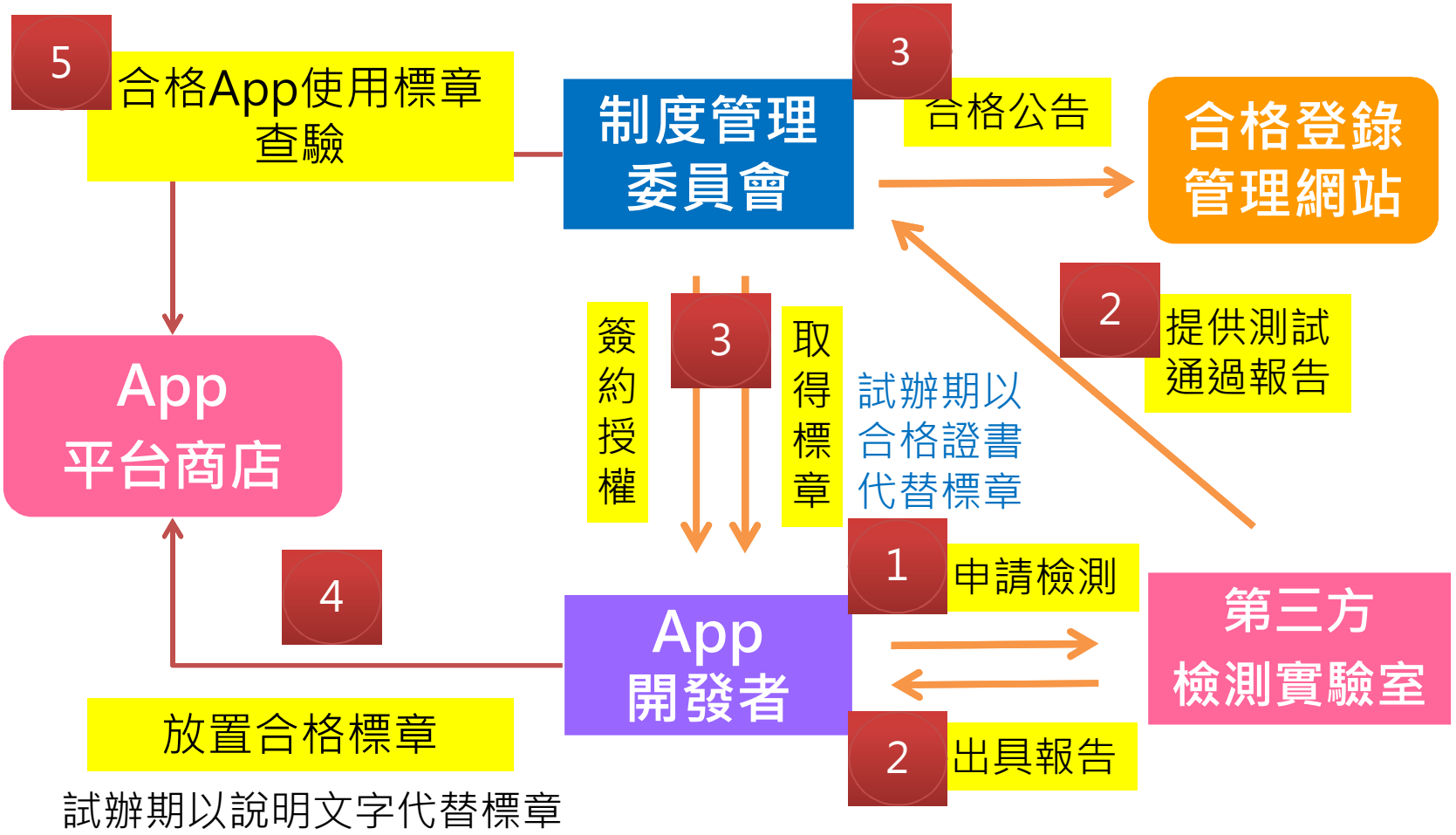
# 正式檢測實驗室認證 – 試辦期可申請

## TAF正式認證流程(3~6 個月)



# 標章申請流程

## 運作架構—App開發者申請標章流程



# THANK YOU


YES!
INSTITUTE FOR INFORMATION INDUSTRY
big data
SEED NET
Y2K
SMART TOURISM
CMMI
Living Lab
FIND
IDEAS SHOW
RFID
NII
DOC
e-TAIWAN
ME.168.COM
IA聯盟
雲端運算產業聯盟
台北港
聖多美號
ADOC
人才培育
SMART 101
ISO 10646
Best Link