經 濟 部

行動應用App基本資安自主檢測制度介紹

指導單位：經濟部工業局

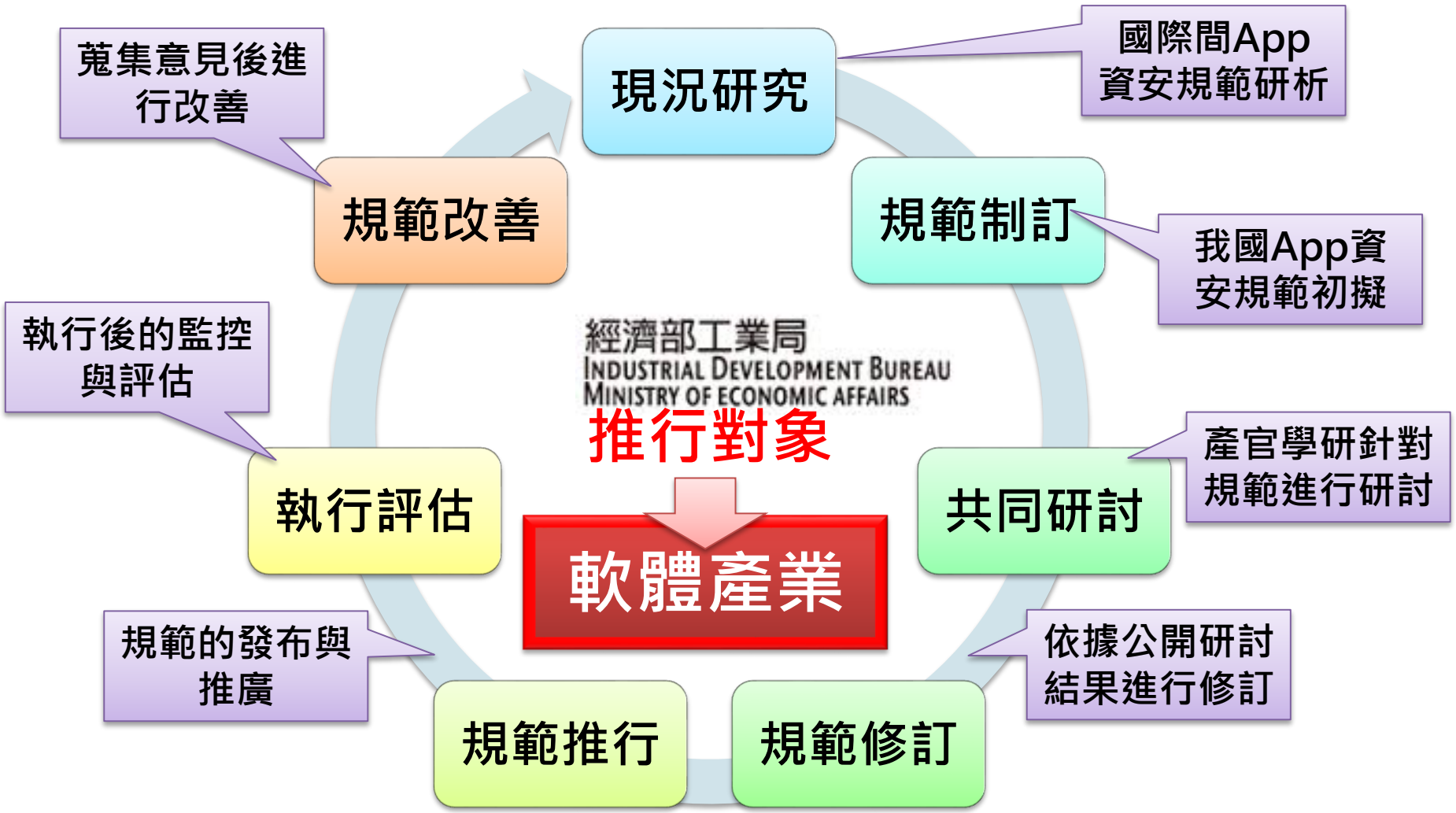
執行單位：行動應用資安聯盟

民國106年8月

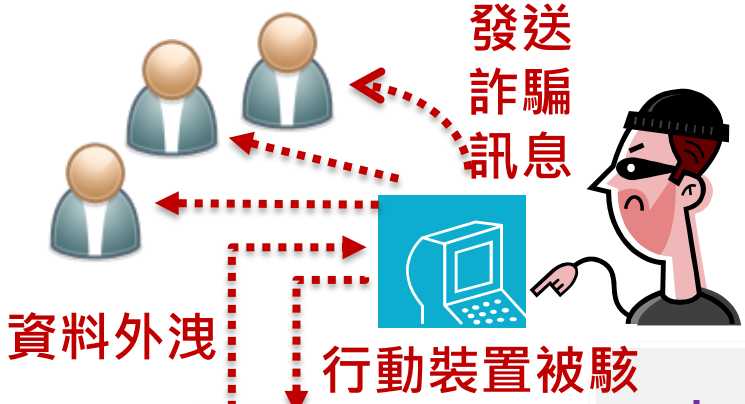
本案背景概述 – 緣起

- 國人日益關心智慧型手機(App)資訊安全
  - 台灣地區每天約有4000多部手機中毒遭駭
  - 嚴重者可能造成民眾的財務損失
- 依據「行政院國家資通安全會報第26次委員會議」決議應配合事項辦理
  - 103年6月24日，主持人張召集人善政、袁協同召集人桂笙
  - 決議事項：參考各國手機管制機制及我國相關業務分工，手機與電腦之應用軟體(包含LINE)基本資安規範由經濟部主管，惟手機屬電信法第42條規定之電信終端設備，其出廠時已內建之軟體仍併同硬體由通傳會主管；請前揭二部會依此分工原則積極研議相關管理作為，並規劃制訂資安檢測標準及鼓勵廠商自主驗證等業務

本案背景概述 - 推動策略


現況研究
國際間App資安規範研析
規範制訂
我國App資安規範初擬
共同研討
產官學研針對規範進行研討
依據公開研討結果進行修訂
規範修訂
規範推行
規範的發布與推廣
執行評估
執行後的監控與評估
規範改善
蒐集意見後進行改善
經濟部工業局
INDUSTRIAL DEVELOPMENT BUREAU
MINISTRY OF ECONOMIC AFFAIRS
推行對象
軟體產業

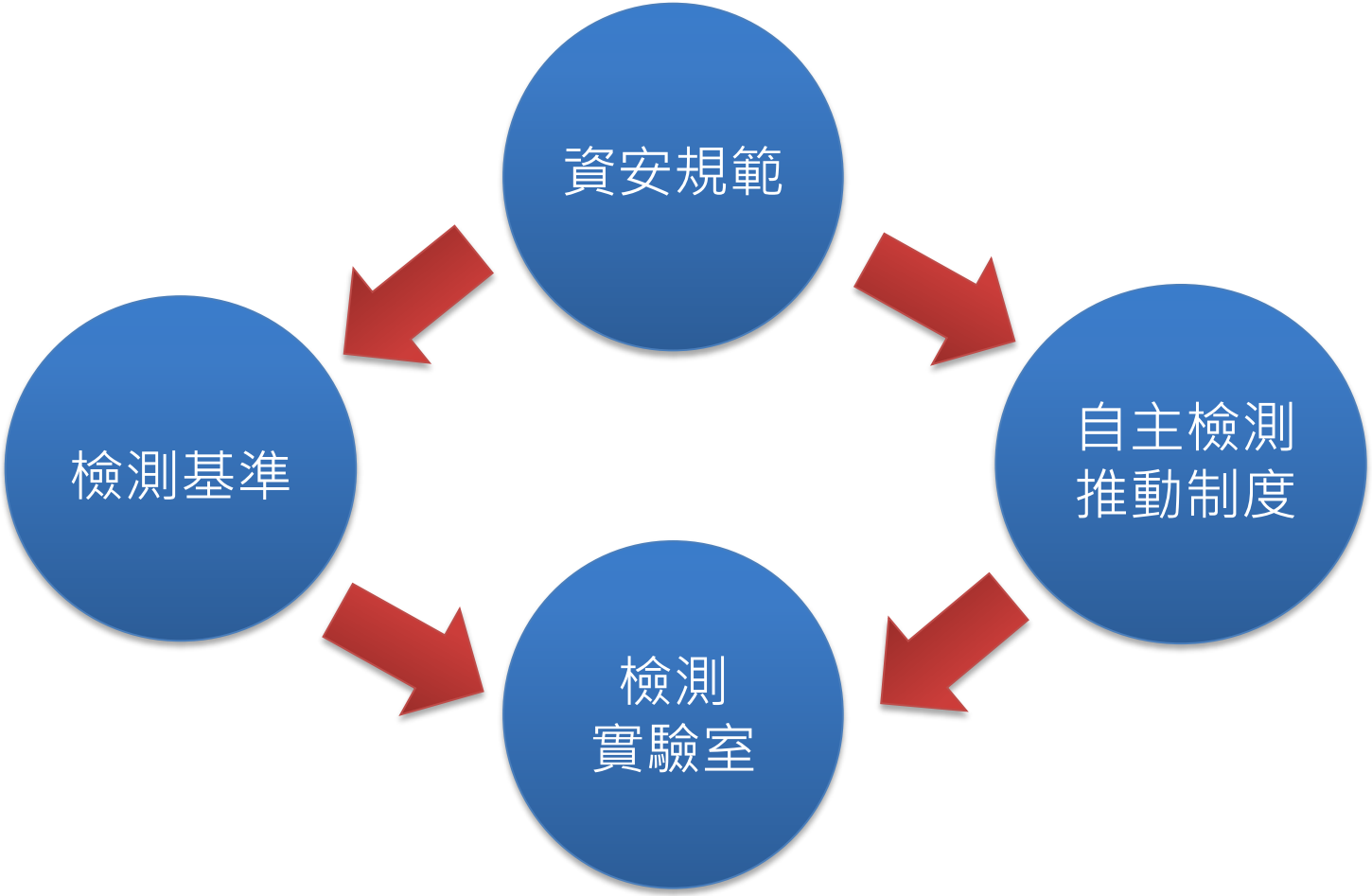
背景概述– 權責分工



- 依據行動裝置軟硬體、App類型及犯罪防治，分別由主管機關各司其職
- 使用者自行下載App，依其應用類型由各目的事業主管機關負責管理

Layer5：手機詐騙行為防範	內政部 警政署
4.2：特定領域應用App安全 (例：網路銀行App、健康照護App...)	各目的事業 主管機關
4.1：共通性及非特定領域App基礎安全要求 Layer4：第3方業者開發之App安全	經濟部 工業局
Layer3：手機預載App安全 Layer2：手機作業系統安全 Layer1：手機硬體安全	國家通訊傳播 委員會(NCC)

推動作法



行動應用App基本資安說明

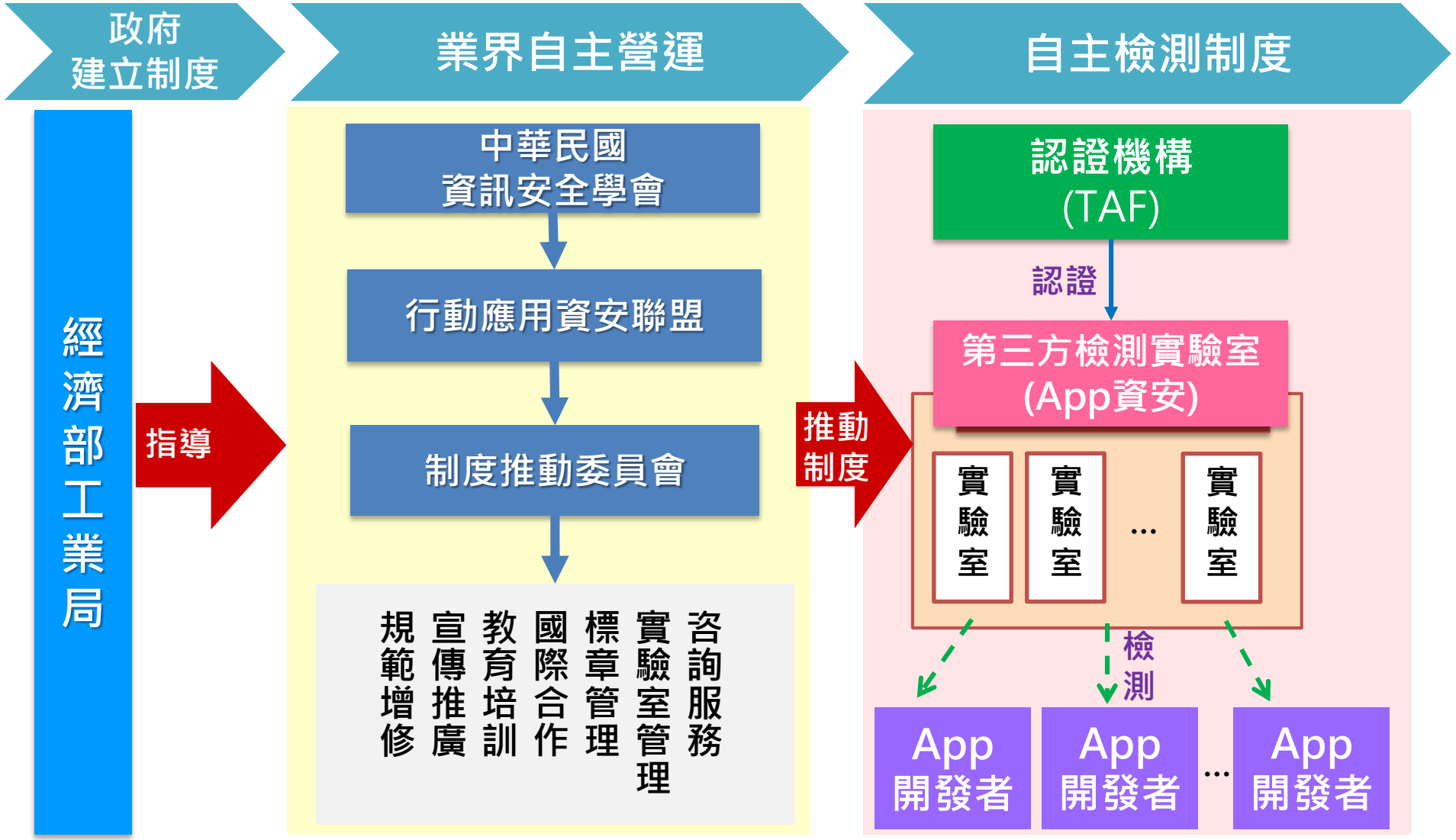
- 工業局規劃App基本資安規範，係針對非手機內建之共通性及非特定領域App，制定並推動國內第一個行動應用App基礎安全要求之資安規範，鼓勵行動應用App開發商自主管理。

- 本規範可提供各目的事業主管機關依據業管產業特性與需要，訂定各產業需要之App資安規範。

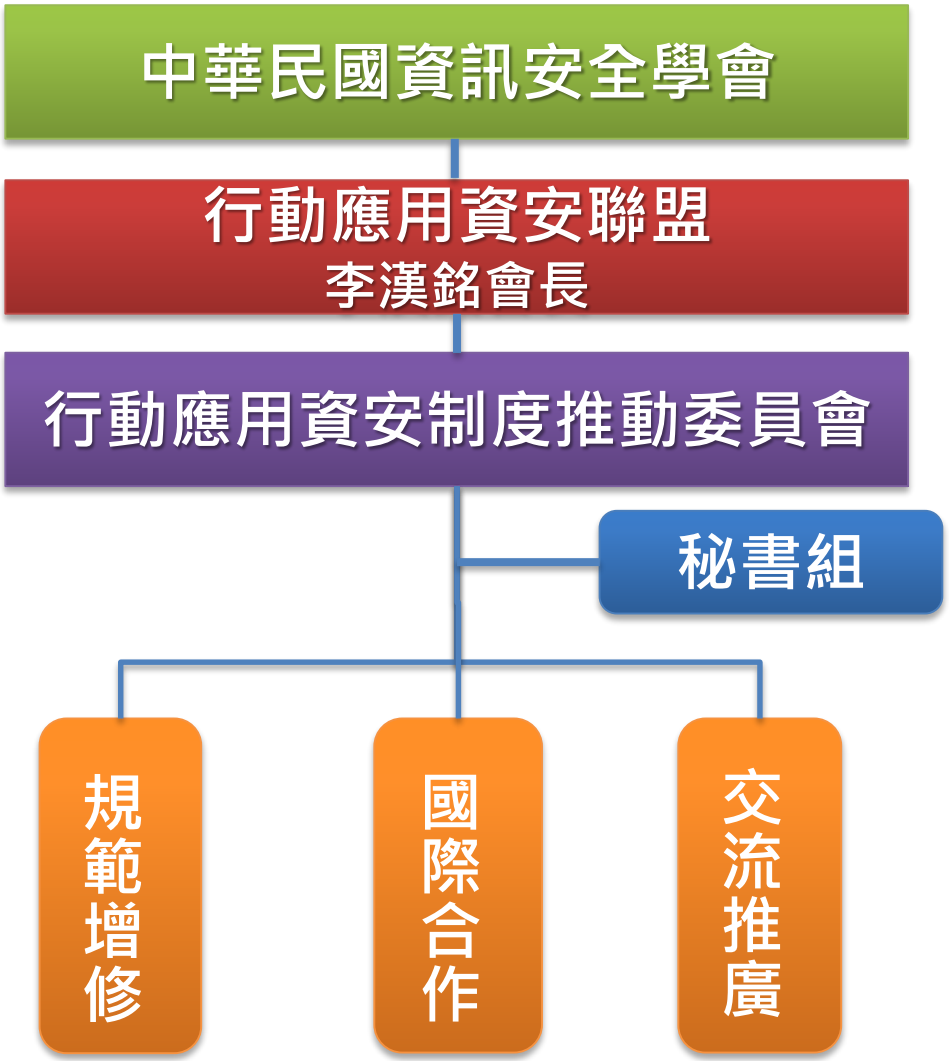
推動過程與現況

- 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V1.0」、「行動應用App基本資安自主檢測推動制度V1.0」**正式公告**於經濟部通訊產業發展推動小組網站
- 於104年10月28日「行動應用App資安檢測實驗室認證申請」**正式公告**於經濟部通訊產業發展推動小組網站
- 於105年2月19日「行動應用App基本資安檢測基準V2.0」、「行動應用App基本資安自主檢測推動制度V2.0」**正式公告**於經濟部通訊產業發展推動小組網站
- **最新版規格文件：於106年3月7日「行動應用App基本資安規範V1.1」、「行動應用App基本資安檢測基準V2.1」、「行動應用App基本資安自主檢測推動制度V3.0」、「行動應用App安全開發指引V1.0 」正式公告於經濟部通訊產業發展推動小組網站**

App基本資安自主檢測制度業界自主營運



行動應用資安聯盟-組織架構



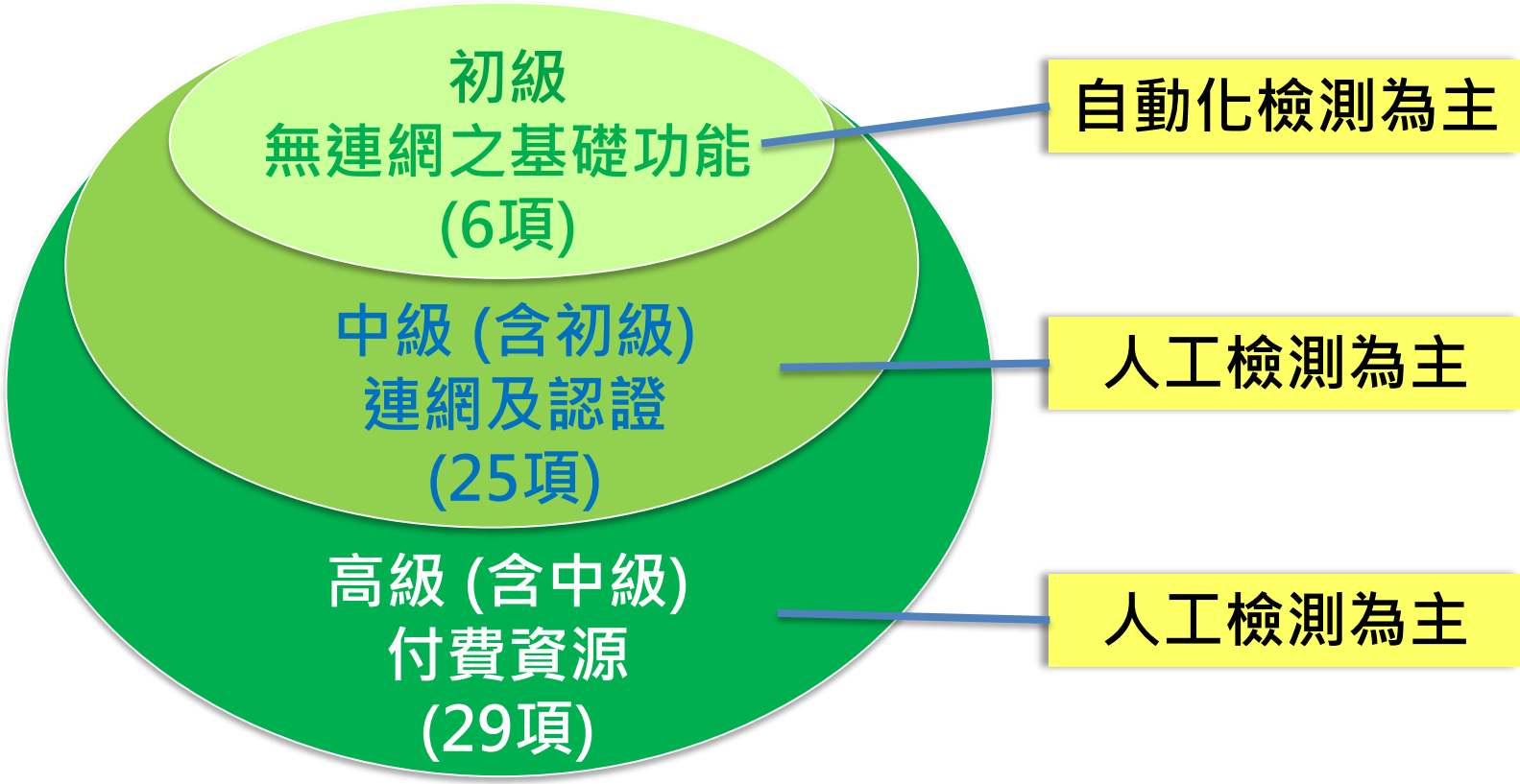
行動應用資安聯盟於105年11月29日成立，由中華民國資訊安全學會結合國內五大產業公協會設立：

-台北市電腦商業同業公會
-中華民國資訊軟體協會
-台灣雲端物聯網產業協會
-台灣雲端安全聯盟
-台灣駭客協會

參與法人單位包括：

-財團法人資訊工業策進會
-財團法人全國認證基金會
-財團法人電信技術中心

App基本資安檢測基準(V2.1版)



App基本資安檢測基準(V2.1版)
各級檢測項目表

INDUSTRIAL DEVELOPMENT BUREAU, MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

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6項，中級檢測項目新增19項，共計25項，高級檢測項目新增4項，共計29項

基本資安規範面向	資訊安全技術要求事項	初級項目	中級項目	高級項目
4.1.1.行動應用程式發布安全	4.1.1.1.行動應用程式發布	0	1	0
	4.1.1.2.行動應用程式更新	0	0	0
	4.1.1.3.行動應用程式安全性問題回報	0	1	0
4.1.2.敏感性資料保護	4.1.2.1.敏感性資料蒐集	0	2	0
	4.1.2.2.敏感性資料利用	0	0	0
	4.1.2.3.敏感性資料儲存	3	2	0
	4.1.2.4.敏感性資料傳輸	0	1	0
	4.1.2.5.敏感性資料分享	0	3	0
	4.1.2.6.敏感性資料刪除	0	0	0
4.1.3.付費資源控管安全	4.1.3.1.付費資源使用	0	0	2
	4.1.3.2.付費資源控管	0	0	2
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	0	2	0
	4.1.4.2.連線管理機制	0	4	0
4.1.5.行動應用程式碼安全	4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	2	1	0
	4.1.5.2.行動應用程式完整性	0	0	0
	4.1.5.3.函式庫引用安全	0	1	0
	4.1.5.4.使用者輸入驗證	1	1	0
	各級檢測項目小計	6	19	4
	各級檢測項目累計	6	25	29

App檢測實驗室資格

- **基本資格：凡國內合法登記之法人或學術研究機構所屬檢測實驗室，具備一定專業條件、依其管理系統從事有關行動應用App之測試、檢驗工作，並出具報告者，皆可由法人代表人或機構負責人提出申請**
- **專業資格**
  - **實驗室資格：**
    - 實驗室認證證明 ISO/IEC 17025
  - **人員資格：**
    - 員工3人以上，各需具備資歷與專業證照資格(如CEH、ECSA/CISSP等)
  - **執行實績：**於3年內有2件以上實際檢驗App資安經驗
- **認證單位：財團法人全國認證基金會(TAF)**

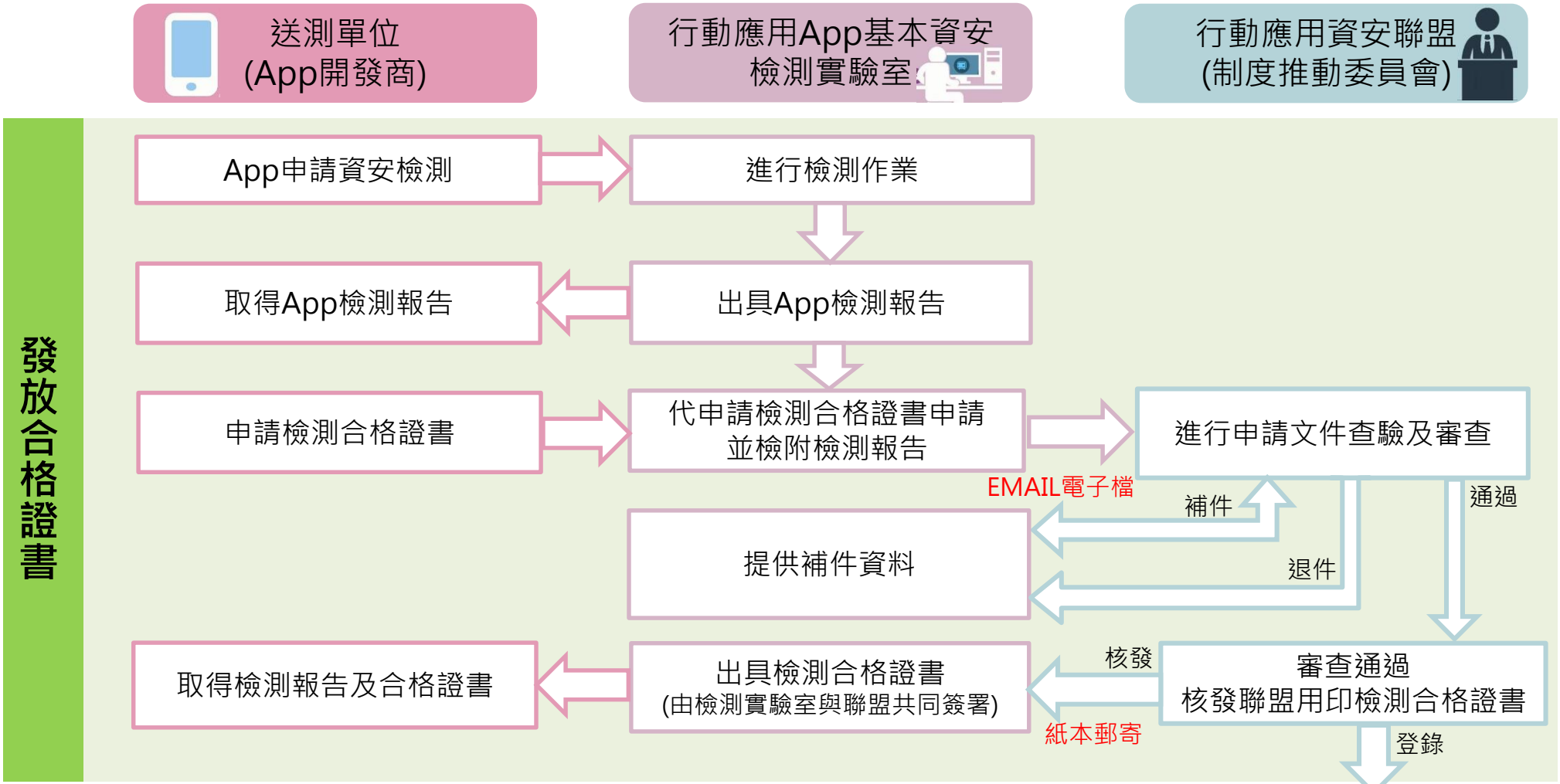
依據TAF公告之「行動應用APP基本資安檢測實驗室認證服務計畫」（TAF-CNLA-A24），成為TAF認可之「行動應用App基本資安檢測實驗室」

App檢測實驗室認證

- 財團法人全國認證基金會(TAF)於105年1月正式公告受理檢測實驗室申請，截至106/8/15止，已有7家實驗室通過TAF「行動應用APP基本資安檢測實驗室認證服務計畫」，成為TAF認可之「行動應用App基本資安檢測實驗室」，如下：
  - 勤業眾信聯合會計師事務所
  - 鑒真數位有限公司
  - 中華電信股份有限公司電信研究院
  - 安華聯網科技股份有限公司
  - 行動檢測服務股份有限公司
  - 財團法人台灣電子檢驗中心
  - 安碁資訊股份有限公司
- **實驗室認證通過名錄與連絡資訊：**

https://www.mas.org.tw/web_doc.php?cid=lab-2

申請App檢測合格證書流程



註：App檢測合格證書自106年8月起，由聯盟與檢測實驗室共同發證。

行動應用App資安標章

- 行動應用App資安標章(Mobile Application Security)

初級
(1顆星)

識別證號：
TM-1-OOOOO –VVV-YYYYMM

「初級」：檢測純功能之安全性

中級
(2顆星)

識別證號：
TM-2-OOOOO –VVV-YYYYMM

「中級」：檢測連網及認證安全性

高級
(3顆星)

識別證號：
TM-3-OOOOO –VVV-YYYYMM

「高級」：檢測交易相關之安全性

MAS標章圖示說明


MAS
MOBILE APP BASIC SECURITY
行動應用App基本資安標章
Mobile Application Basic Security
初級
Baseline level
TM-1-OOOOO –VVV-YYYYMM
行動應用資安聯盟
Mobile Application Security Alliance


MAS
MOBILE APP BASIC SECURITY
行動應用App基本資安標章
Mobile Application Basic Security
中級
Intermediate level
TM-2-OOOOO –VVV-YYYYMM
行動應用資安聯盟
Mobile Application Security Alliance


MAS
MOBILE APP BASIC SECURITY
行動應用App基本資安標章
Mobile Application Basic Security
高級
High level
TM-3-OOOOO –VVV-YYYYMM
行動應用資安聯盟
Mobile Application Security Alliance

申請MAS標章流程

INDUSTRIAL DEVELOPMENT BUREAU, MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

送測單位 (App開發商)	行動應用App基本資安 檢測實驗室	行動應用資安聯盟 (制度推動委員會)

發放資安標章

下載標章申請相關文件，填覆MAS標章申請書(含權利義務規章)簽署用印，送件申請

申請單及附件郵寄

收到申請書，進行審查作業(若不通過請申請者補件)

審核

E-mail通知補件

提供補件資料

郵寄補件資料

審查通過，通知申請者付款

E-mail通知繳款

進行繳費，匯款資訊：

銀行名稱：國泰世華銀行(013)
戶名：中華民國資訊安全學會
帳號：032-50-831131-1

※ 備註欄署名：公司名稱-合格證書編號

E-mail通知及檢附繳費證明(掃描檔)

確認付款後，發送MAS標章，並登錄於網站。

E-mail核發標章(電子檔)

取得MAS標章，並依據規定宣告標示

登錄

「行動應用資安聯盟」網站
https://www.mas.org.tw/

註：行動應用資安聯盟自106年8月起，開始受理MAS標章申請。

App基本資安自主檢測制度規範
相關文件下載網址

https://www.mas.org.tw/


THANK YOU