行動應用資安防護制度

中華民國資訊安全學會 理事長
中山大學資訊工程學系 教授

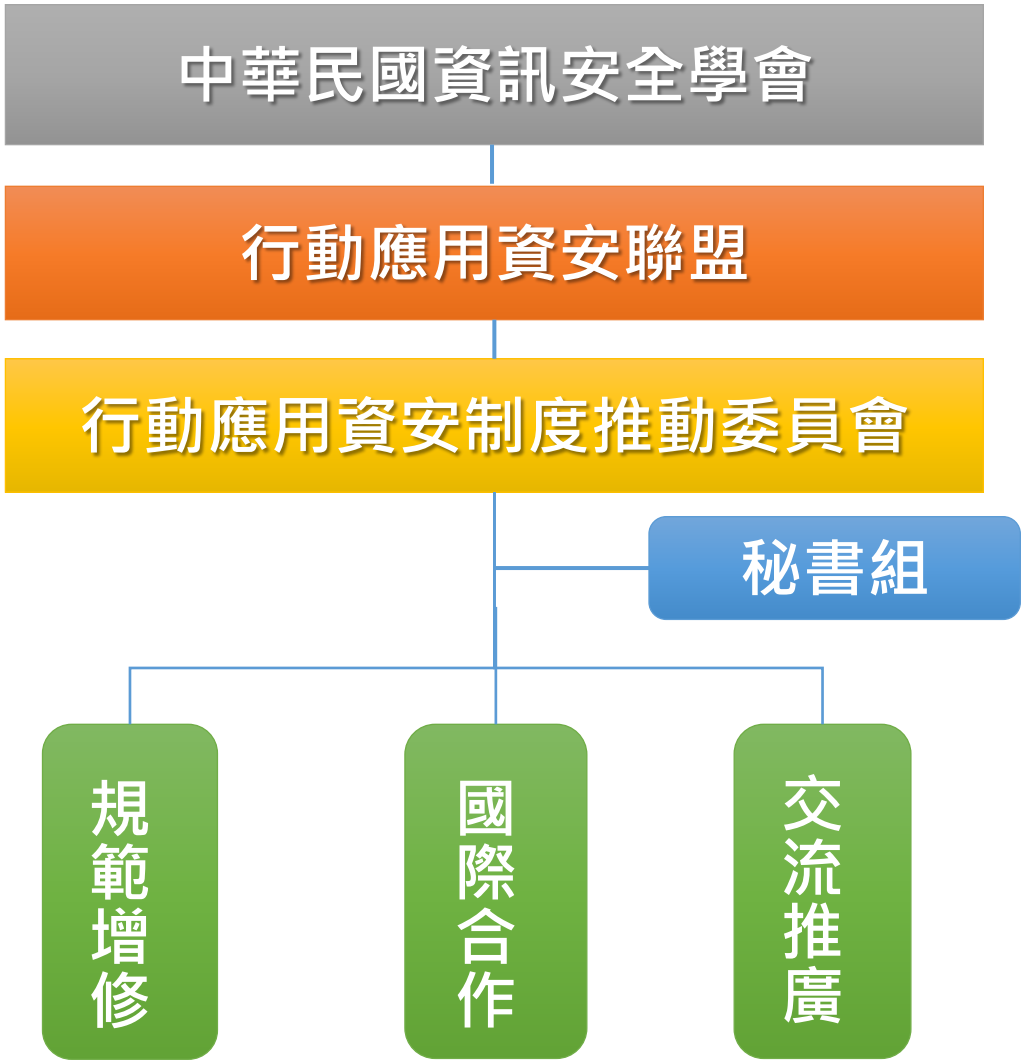
官大智

APP 資訊安全問題

- 安全的 APP
  - 軟體系統多少會有漏洞, 沒有絕對安全的 APP
  - 經由 APP 資安檢測, 降低 APP 的風險

- 推動方式
  - 建立制度與規範
  - 檢測實驗室認證
  - 發放安全標章

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

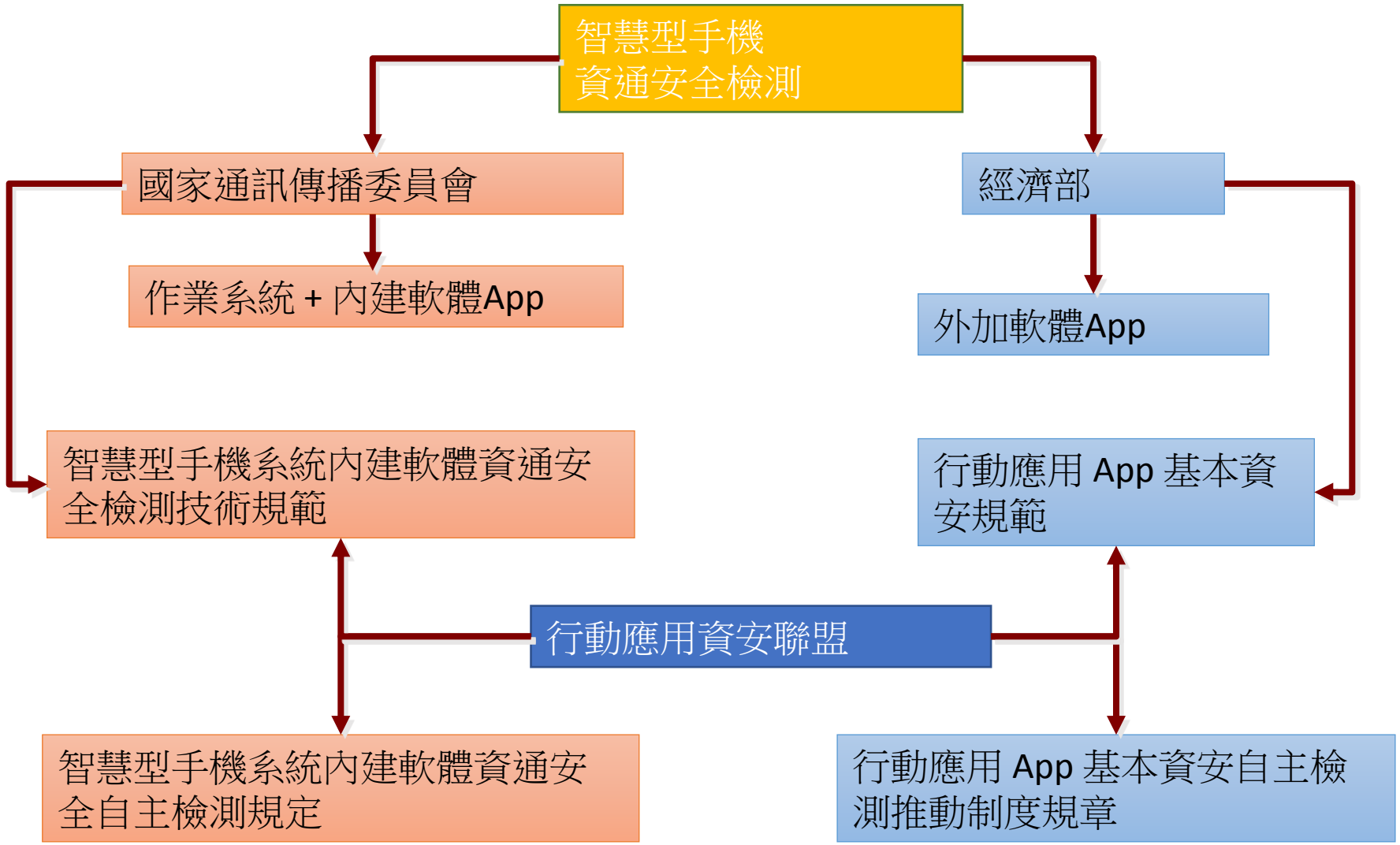
-財團法人資訊工業策進會
-財團法人全國認證基金會
-財團法人電信技術中心

手機資安之主管機關權責分工

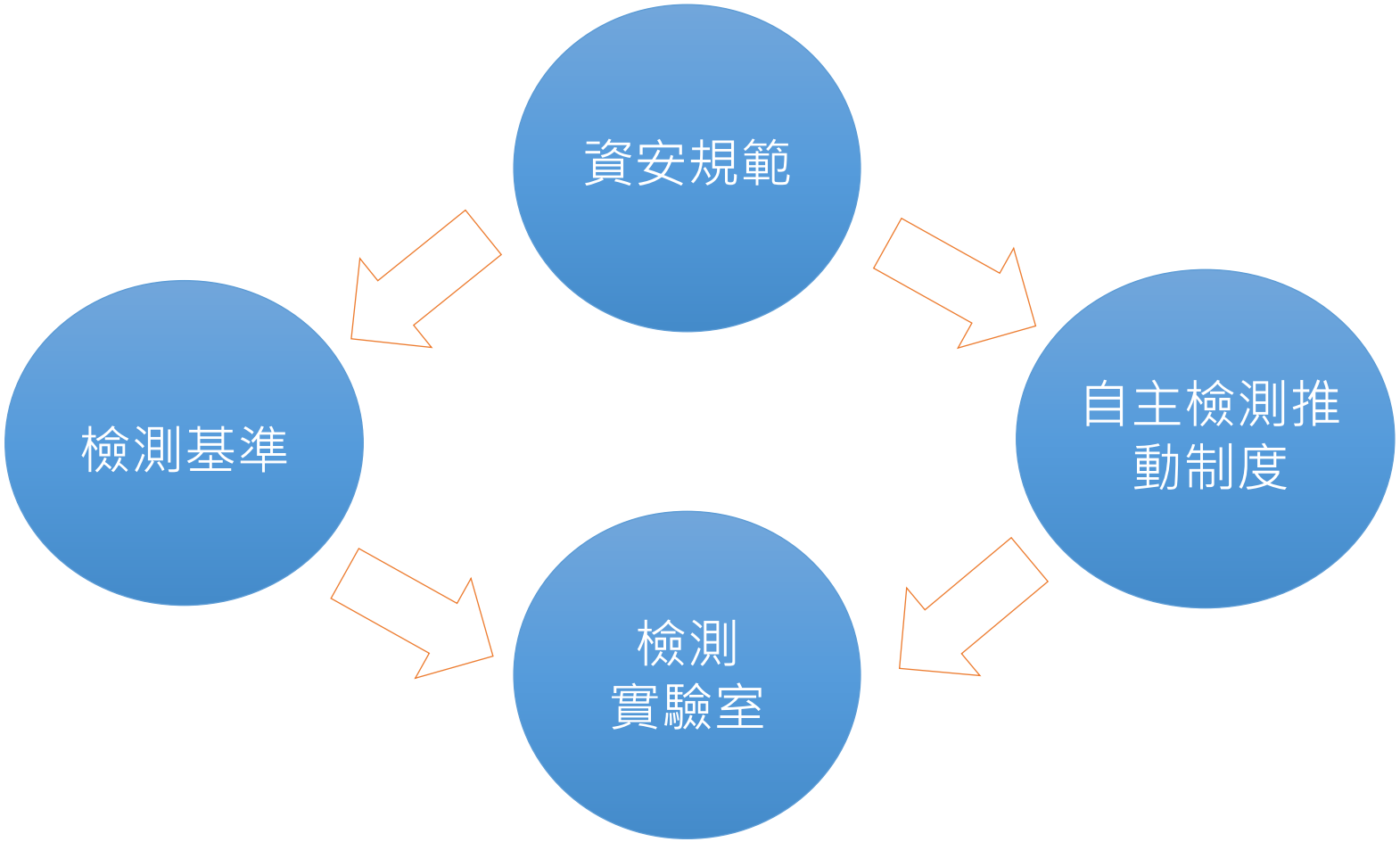
- 依據行動裝置軟硬體、App 類型及犯罪防治，分別由主管機關各司其職
- 使用者自行下載 App，依其應用類型由各目的事業主管機關負責管理

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)

智慧型手機安全檢測推動作業



資安檢測推動作法



自主檢測推動制度運作架構

主管機關

經濟部
工業局

App基本資安

通傳會
(NCC)

手機內建軟體

運作檢測制度及標章管理

行動應用資安聯盟
(行動應用資安制度推動委員會)

TAF：財團法人全國認證基金會

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 / E.S.S 檢測單位
通過認證，受理 App開發者或手機業者之檢測申請，檢測 App/手機是否符合資安檢測基準

行動應用資安聯盟官網

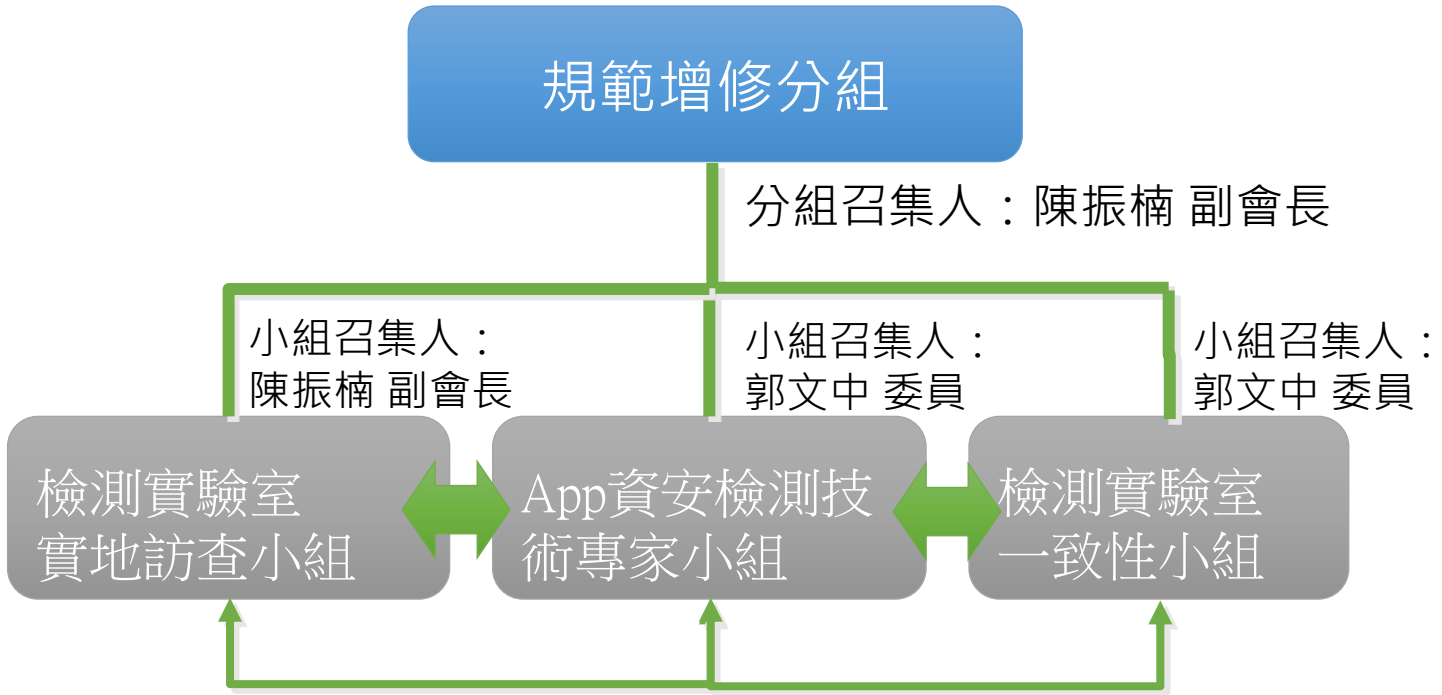
App基本資安/E.S.S 檢測制度推動

各項相關規範文件下載與活動公告網址

http://www.mas.org.tw

聯盟「規範增修組」各相關工作小組

- 制度推動委員會之「規範增修組」下設立各相關工作小組，由「規範增修組」召集人陳振楠副會長督導執行。
- 各相關工作小組如下：



聯盟「規範增修組」各相關工作小組

工作小組 名稱	檢測實驗室 實地訪查小組	App資安檢測 技術專家小組	檢測實驗室 一致性小組
工作小組 任務	進行檢測實驗室實地訪查App檢測實施現況並進行稽核，確保檢測品質	針對檢測基準或制度、作法、實驗室提出技術需判定議題，進行討論及審議	針對檢測實驗室或App開發商提出檢測相關議題，檢測一致性作法研討及布達
工作小組 召集人	陳振楠副會長	郭文中委員	郭文中委員
專家成員	孫宏民教授、 林金城教授	孫宏民教授、 林金城教授、 查士朝教授	視情況邀技術專家參加
參與者	郭文中秘書長、 秘書組	秘書組	TAF認可檢測實驗室、 秘書組
活動/ 會議名稱	App資安認證檢測實驗室實地訪視活動	App資安檢測技術專家會議	App資安檢測實驗室一致性會議
辦理時間	半年一次、 或特定需求辦理	每月一次、 或特定需求辦理	每月一次、 或特定需求辦理

聯盟各項收費項目及優惠方案

各收費項目於106年 5 月 16 日經委員會通過
自106年8月1日起收費(優惠期間至106年12月31日止)

類型	收費項目	子項目	金額(元)	優惠方案
入會費	會員入會費	團體會員(500萬含以上)	2,000	優惠期免費
		團體會員(500萬以下)	1,000	
		個人會員	500	
常年會費	會員年費	團體會員(500萬含以上)	4,000	優惠期優惠 5 折
		團體會員(500萬以下)	2,000	
		個人會員	1,000	
事業費	App 合格證書	-	1,000	106 年免費
事業費	標章規費	含書面行政審查費用	3,000	優惠期會員 8 折
事業費	實驗室規費	-	10,000	可折抵年費
其他收入	教育訓練	-	500	會員 5 折
其他收入	研討會	-	0	

行動應用App基本資安(MAS)標章樣式

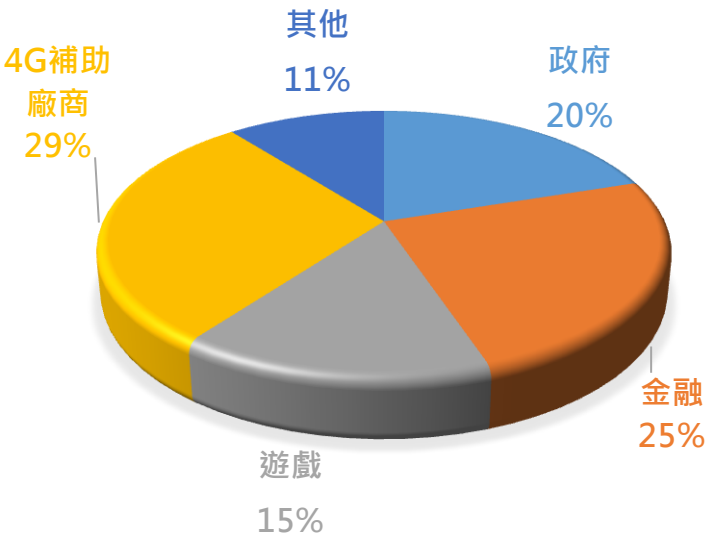
App基本資安檢測推動情形(1/3)

- 截至11月22日「行動應用App基本資安檢測實驗室」推動近況說明：
  - 7家實驗室通過TAF認證，成為TAF認可之「行動應用App基本資安檢測實驗室」(本年度新增4家)
    - 鑒真數位有限公司（105/7/7通過認證）
    - 勤業眾信聯合會計師事務所（105/7/7通過認證）
    - 中華電信股份有限公司電信研究院（105/8/2通過認證）
    - 安華聯網科技股份有限公司（106/1/24通過認證）
    - 行動檢測服務股份有限公司（106/2/23通過認證）
    - 財團法人台灣電子檢驗中心（106/4/25通過認證）
    - 安碁資訊股份有限公司（106/7/21通過認證）
  - 2家實驗室申請TAF認證中(分別於106/9月及11月申請)

App基本資安檢測推動情形(2/3)

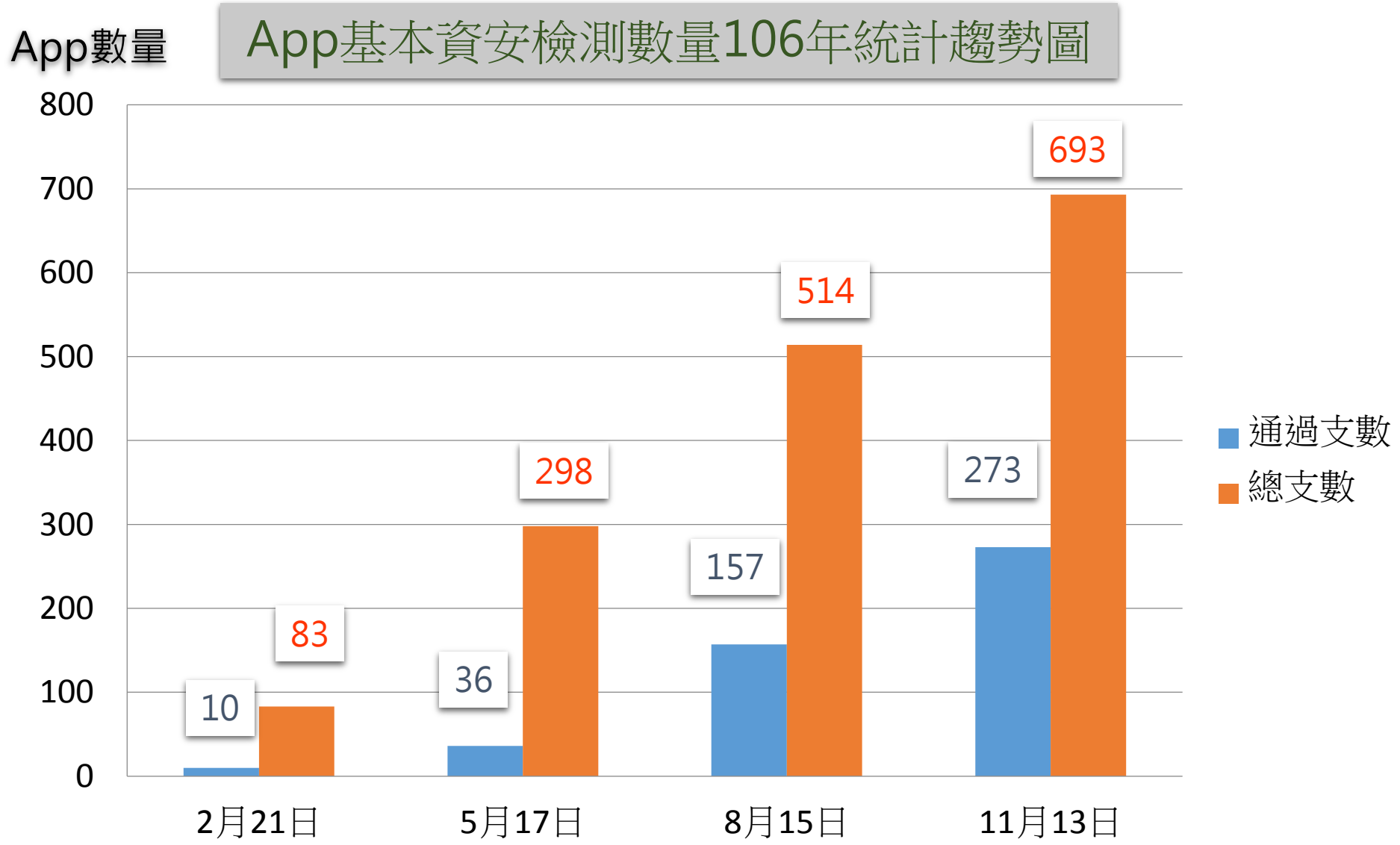
- 截至11月13日統計各檢測實驗室共收件693支，已通過檢測 273支 。
- 國發會委請行政院資安處(技服中心)，依據工業局App資安檢測基準，執行政府已上架之App基本資安檢測，抽檢共144支App。

受測數量				
類別	TAF認證檢測實驗室	技服中心	小計	佔比
政府	23	144	167	20%
金融	208	-	208	25%
遊戲(註)	129	-	129	15%
4G補助廠商	244	-	244	29%
其他	89	-	89	11%
小計	**693**	**144**	**837**	**100%**

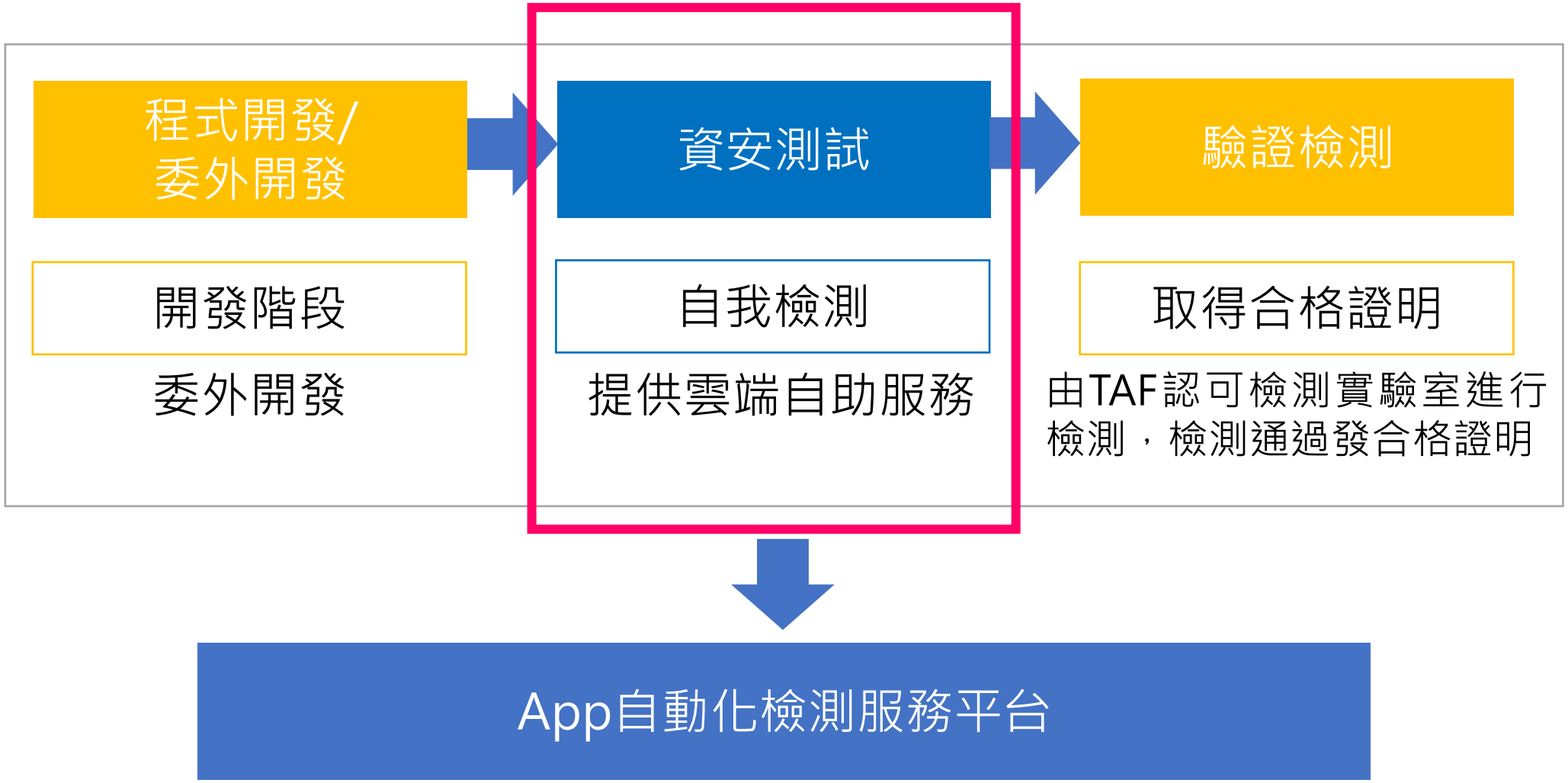


註：台灣代理大陸遊戲業者App，依據臺灣地區及大陸地區人民關係條例，大陸地區遊戲軟體未開放營運業務，主管機關要求台灣代理商提交資安檢測報告。

App基本資安檢測推動情形(3/3)



App資安自動化檢測服務平台(1/3)

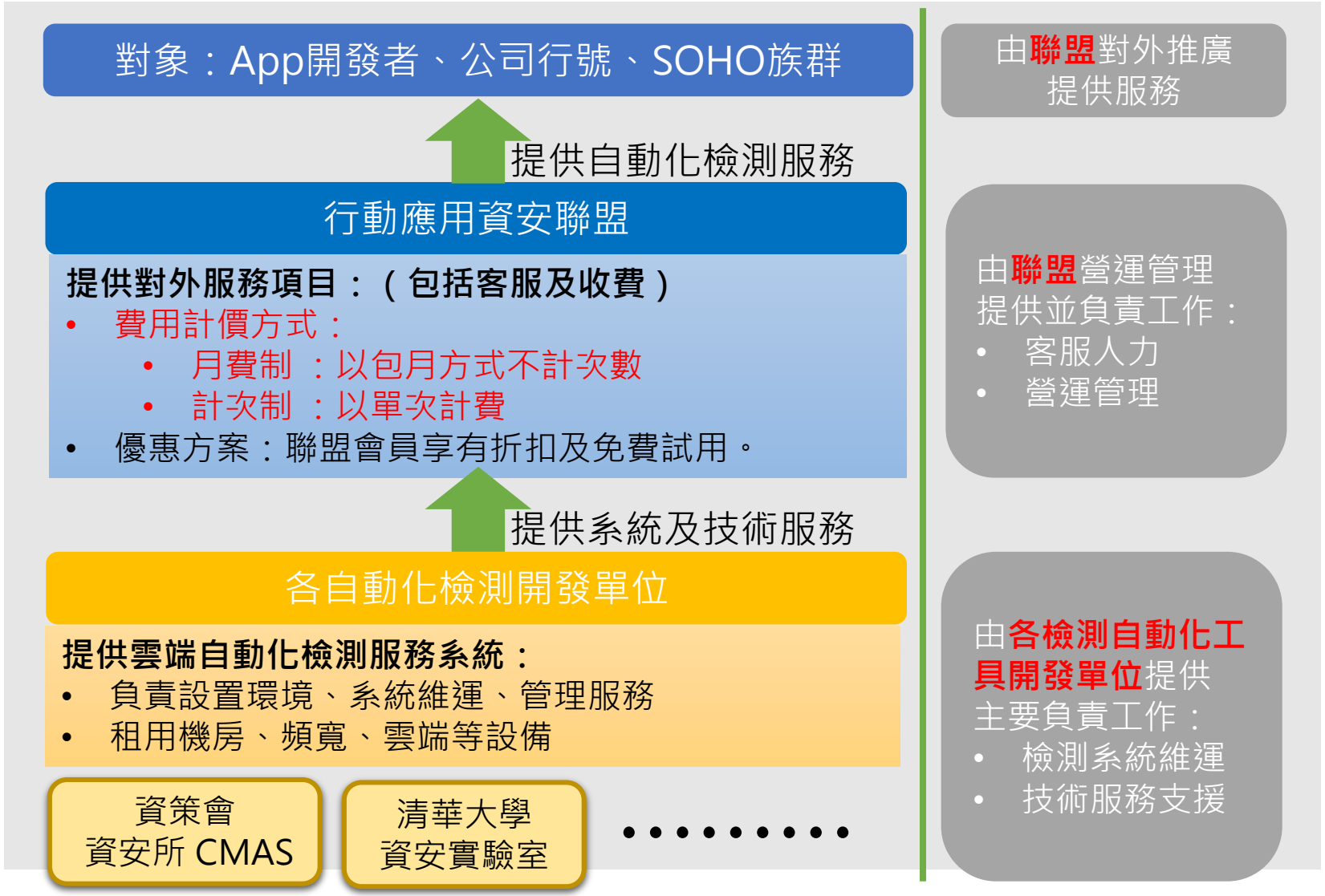


App資安自動化檢測服務平台(2/3)

- 提供App開發商自我檢測服務，於開發階段或測試階段，可供於送實驗室正式檢測及取得合格證明前，進行先期測試及資安改善。
- 僅提供測試報告，不提供檢測合格證明。
- 服務方式：
  - 以雲端自動化及自助服務方式實施。
  - 如需要額外提供檢測資安問題解說及改善建議等，擬另規劃App資安顧問服務及收費方式。
- 初期推廣以推廣帳號提供優惠使用「App基本資安自動化檢測服務平台」，推廣試用：
  - 期間：已於106年11月1日先試行開放至107年2月28日止
  - 次數：10次為限
  - 版本：僅Android

App資安自動化檢測服務平台(3/3)

- 由聯盟與自動化檢測開發單位合作，以聯盟名義對外提供服務



辦理 APP 快篩式自動化資安檢測工具競賽活動

❑ 執行方式

- 強化實驗室檢測能力並發展自動化檢測技術，**以提升自動化檢測技術準確度與涵蓋率**
- 規劃及設計APP檢測樣本軟體及資安檢測錯誤樣態
- 辦理「快篩式自動化資安檢測工具」競賽
- 由聯盟籌組技術專家進行競賽規劃與評選作業
- **透過公協會、學會廣邀產、學、研各界參與**
- 透過競賽活動**篩選出優秀檢測工具**

- 由聯盟與優勝之檢測工具單位合作，將其**納入App自動化資安檢測服務平台對外提供服務**，以強化自動化檢測服務平台能量。

APP 資安自動化檢測服務平台規劃

服務平台帳號規劃建議

免費帳號

初級5項免費

檢測級別：初級(部分項目)
檢測項目：5項
免費期間：試用一個月

推廣帳號

推廣期間免費，使用次數限制

檢測級別：初、中級為主(部分項目)
檢測項目：18項
推廣期間：106/11/01~107/02/28
免費次數：10次

企業帳號

收費帳號：計費方式提報經濟部及資安學會/聯盟審定後公告

檢測級別：初、中級為主(部分項目)
檢測項目：18項
啟用期間：預訂107/03/01 起
收費方式：分計時制與計次制

問題與討論