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

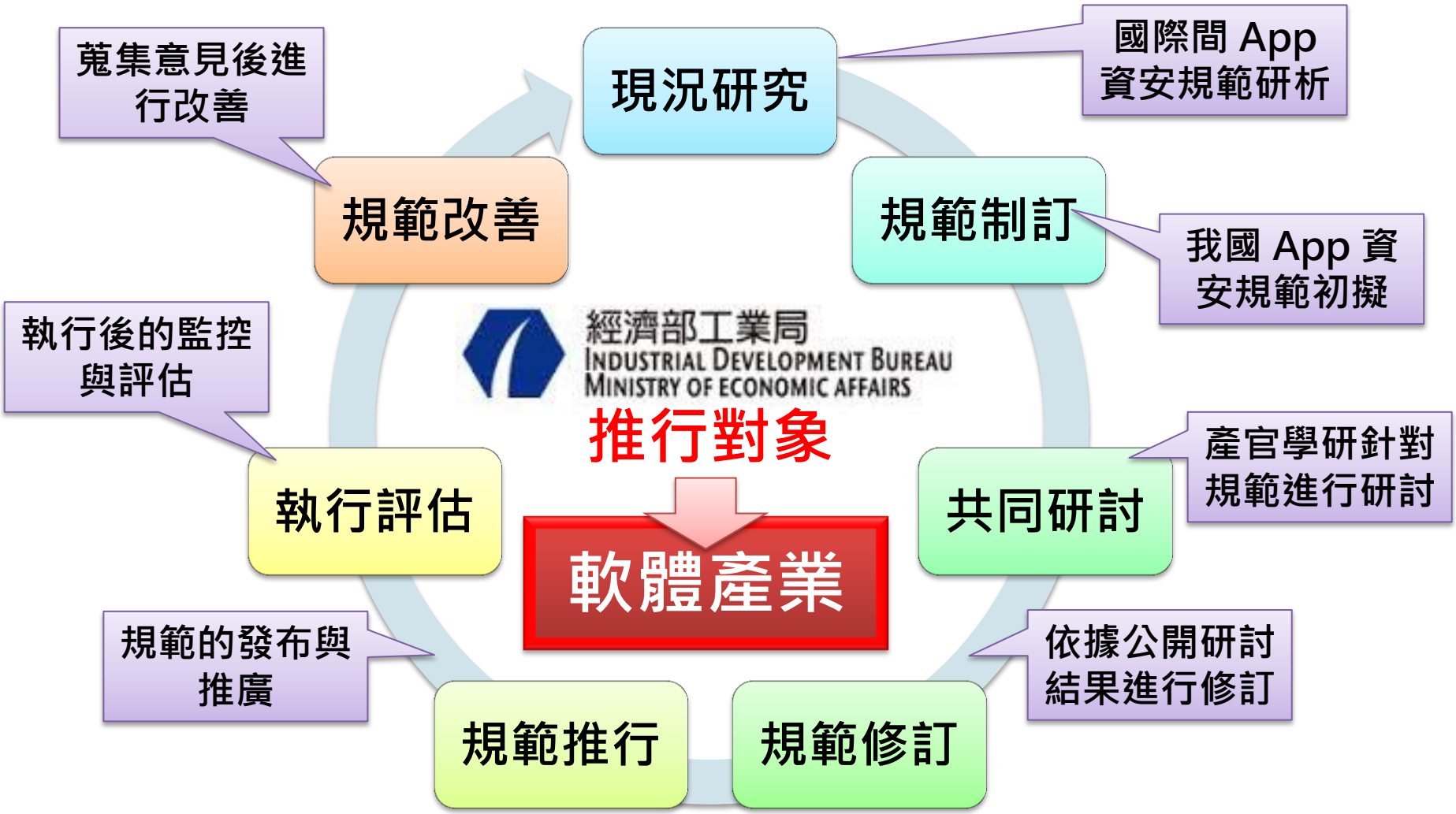
執行單位：行動應用資安聯盟

民國 106 年 10 月 25 日

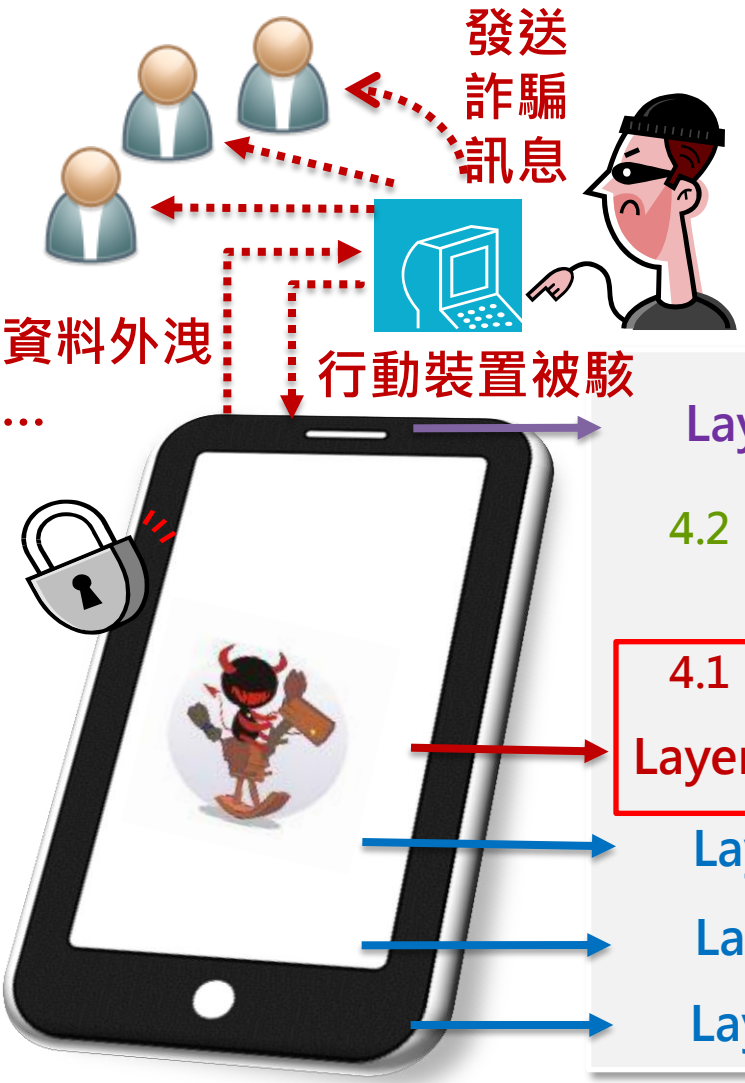
本案背景概述 – 緣起

- **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**
- 「行政院國家資通安全會報」於 103 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 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**

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
規範修訂
依據公開研討結果進行修訂
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

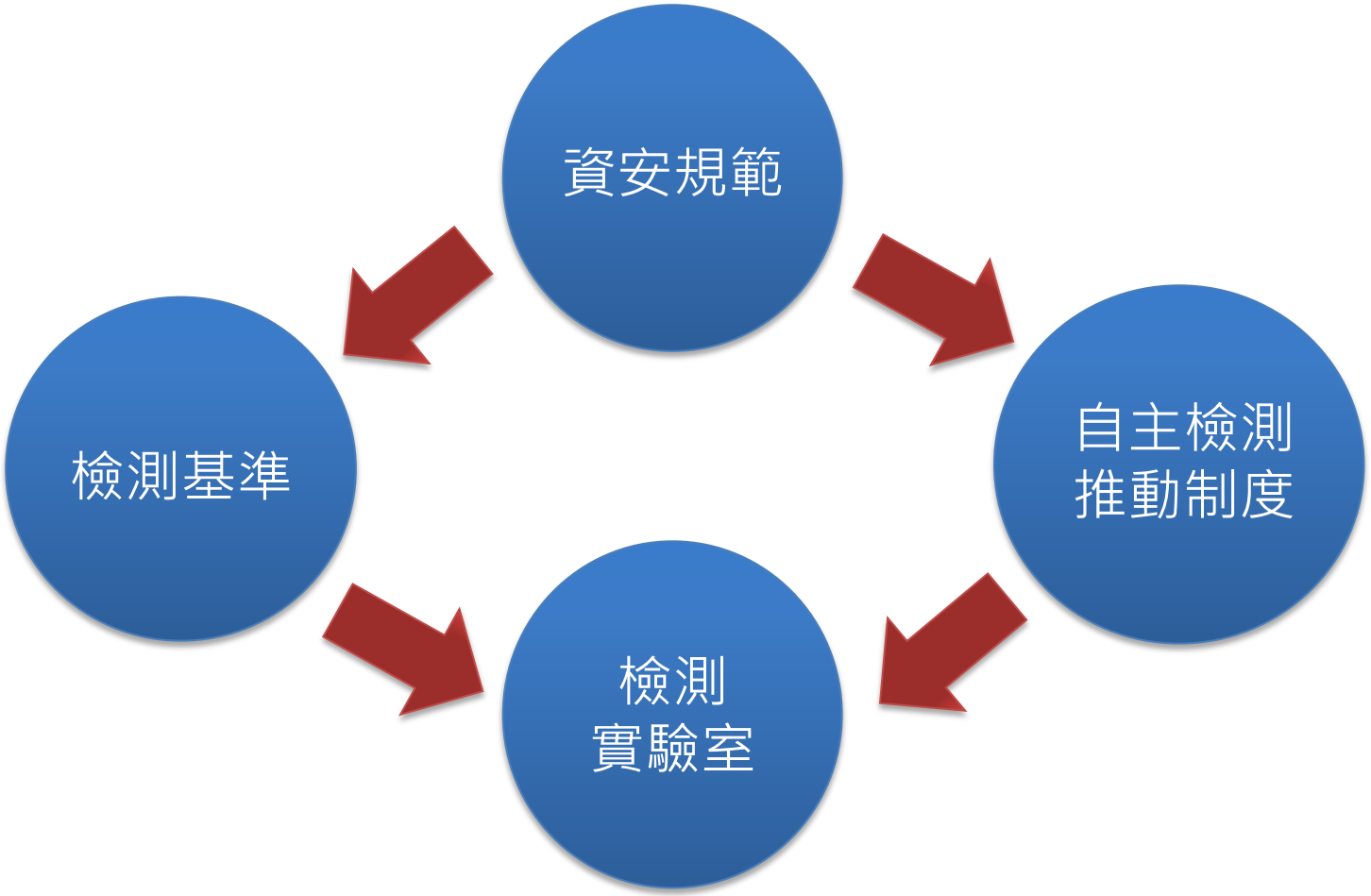
背景概述– 權責分工



- 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	經濟部 工業局
Layer4：第3方業者開發之 App 安全	
Layer3：手機預載App安全	國家通訊傳播 委員會(NCC)
Layer2：手機作業系統安全	
Layer1：手機硬體安全	

推動作法

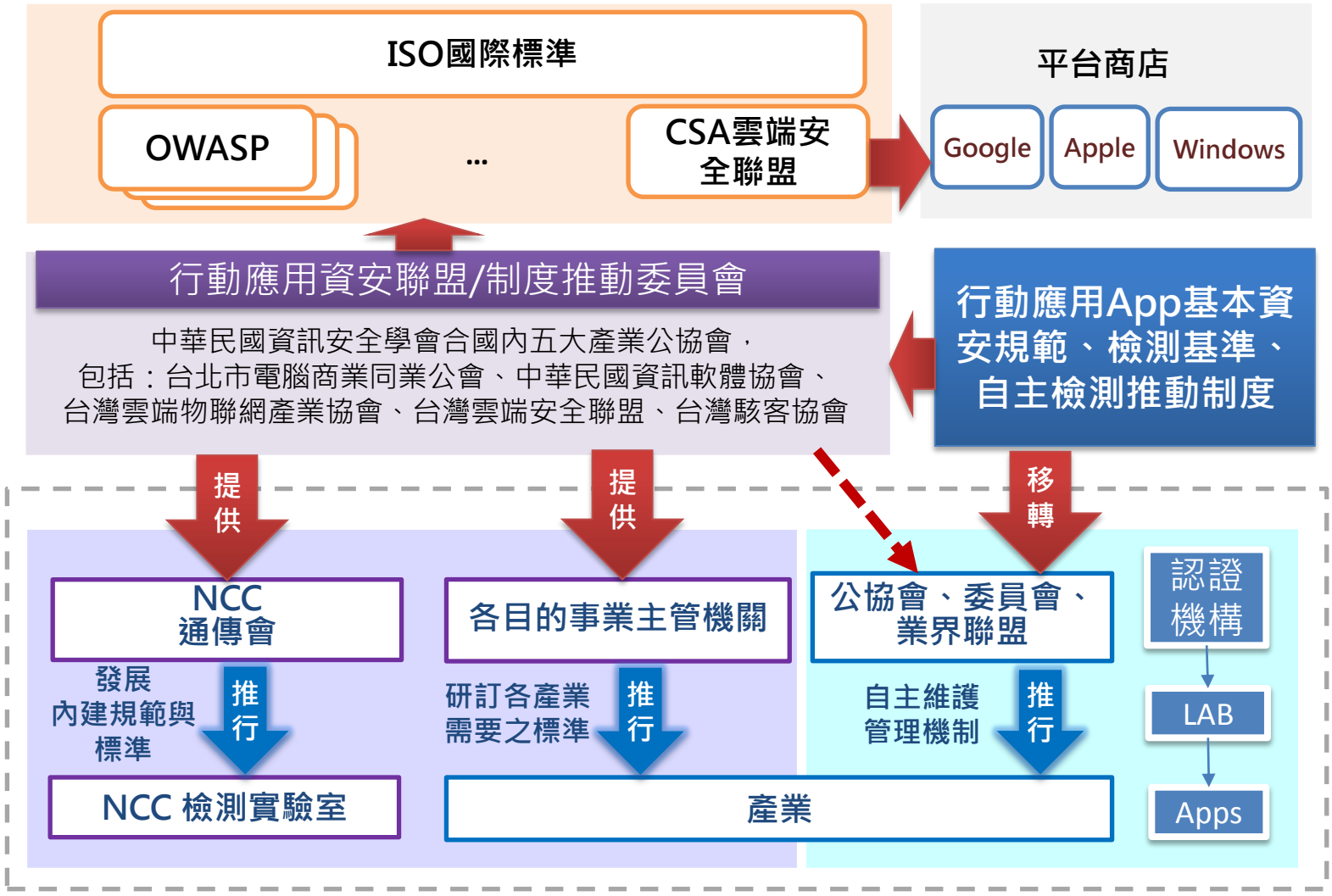


行動應用 App 基本資安說明

- 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。

App 基本資安自主檢測推動架構



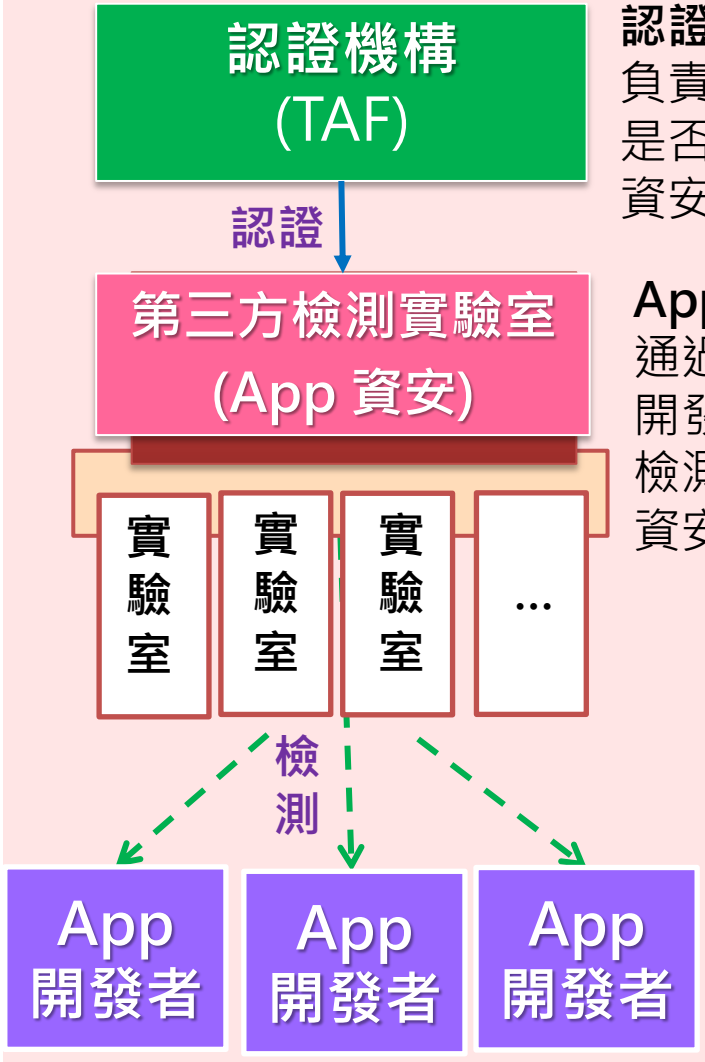
自主檢測推動制度 - 運作架構

主管機關

經濟部工業局

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)

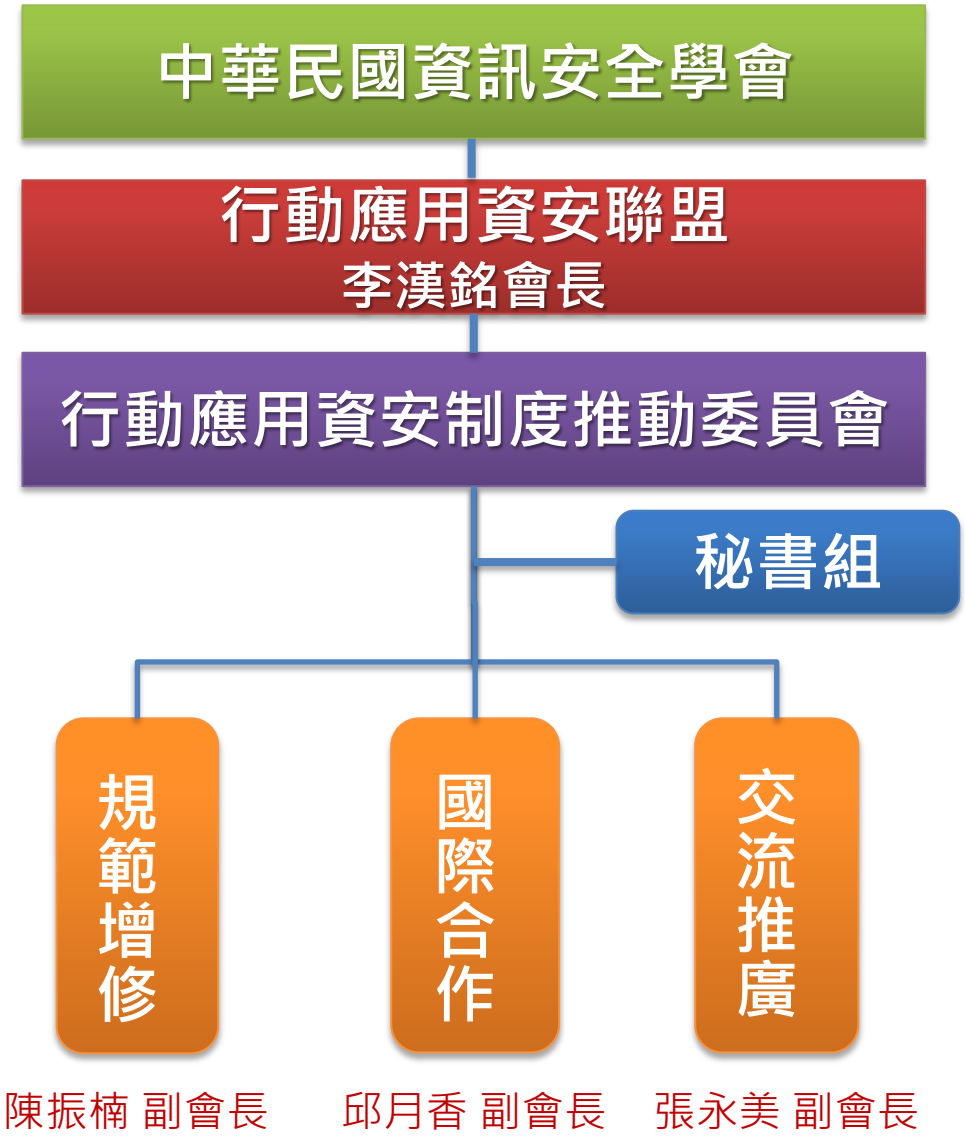


認證單位
負責認證檢測實驗室是否具備檢測 App 資安之能力

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

TAF：財團法人全國認證基金會

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

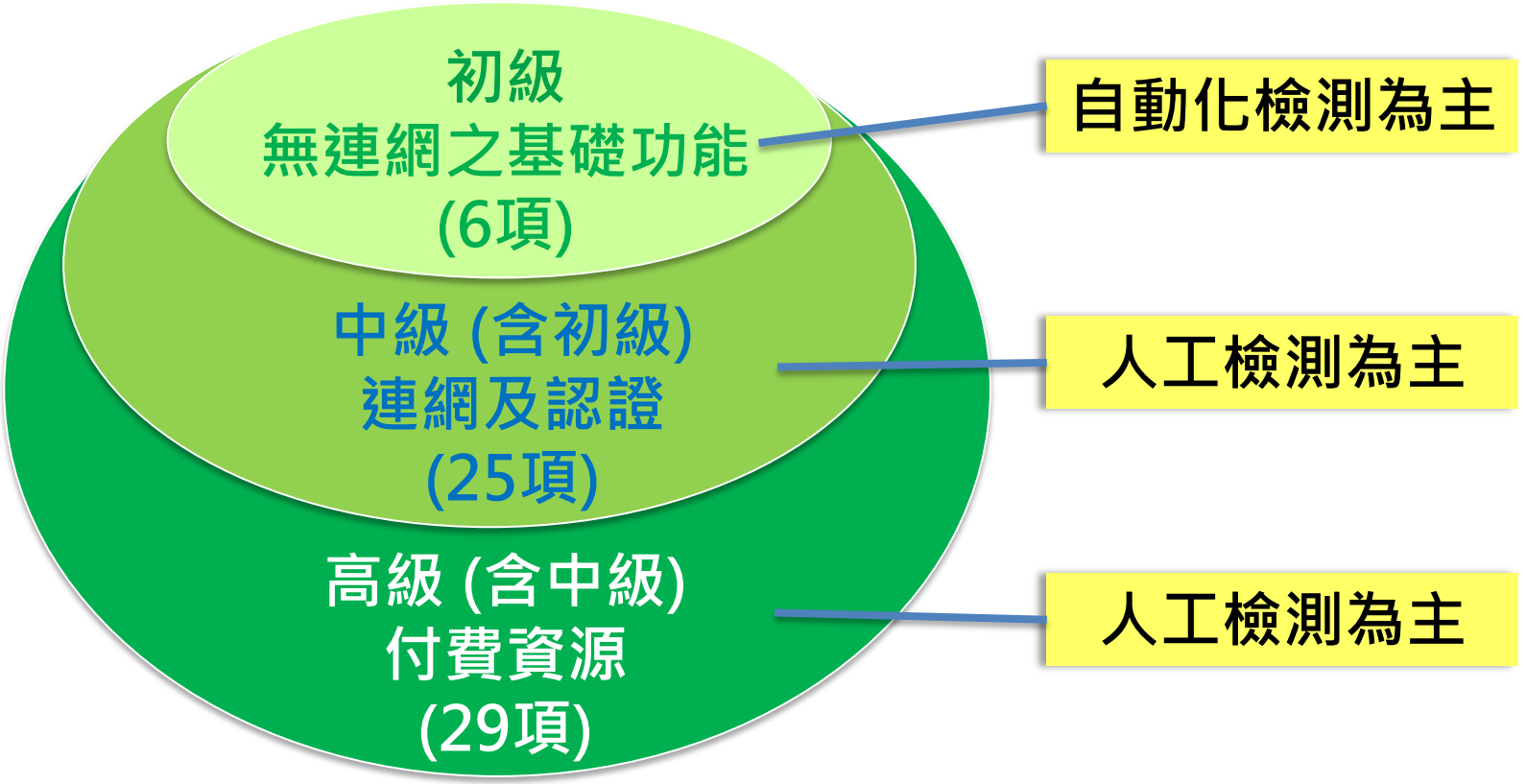
參與法人單位包括：

-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

行動應用資安制度推動委員會-委員名單

項次	姓名	資安聯盟-職稱	服務單位
1	李漢銘 教授	會長	台灣科技大學
2	陳振楠 教授	副會長	中國科技大學
3	邱月香 理事長	副會長	中華民國資訊軟體協會
4	張永美 副總幹事	副會長	台北市電腦商業同業公會
5	官大智 理事長	委員	中華民國資訊安全學會
6	孫宏民 常務理事	委員	中華民國資訊安全學會
7	郭文中 秘書長	委員	中華民國資訊安全學會
8	蔡一郎 理事長	委員	台灣雲端安全聯盟
9	陳逸萍 執行秘書	委員	台灣雲端運算產業協會
10	蔡松廷 理事長	委員	台灣駭客協會
11	許景行 執行長	委員	財團法人全國認證基金會
12	陳明義 技術長	委員	財團法人資訊工業策進會
13	林根煌 執行長	委員	財團法人電信技術中心
14	余遠澤 教授	委員	高雄師範大學
15	何英圻 董事長	委員	九易宇軒股份有限公司(91APP)
16	王炘 總顧問	委員	天龍安全科技公司
17	蔡以德 董事長	委員	行動檢測服務(股)公司
18	吳漢章 總經理	委員	華碩雲端股份有限公司
19	洪偉淦 總經理	委員	趨勢科技股份有限公司

App 基本資安檢測基準(V2.1版)



資安規範與檢測基準 V2.1 文件架構–各級檢測項目表

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(新增)	高級項目(新增)
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 106/10/20 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
- 財團法人台灣電子檢驗中心
- 行動檢測服務股份有限公司
- 安碁資訊股份有限公司

≡ 實驗室認證通過名錄

本名錄係登載由「行動應用App基本資安制度推動委員會」(以下簡稱本委員會)依據工業局公告之「行動應用App基本資安自主檢測推動制度」，經本委員會所認可之「行動應用App基本資安檢測實驗室」。

為確保測試報告之公信力，本委員會建議您，請於委託測試時，要求檢測實驗室出具合格證書，凡具有合格證書之檢測實驗室皆遵守「行動應用App基本資安檢測實驗室權利義務規章」(詳附件)。

實驗室認證編號	機構名稱	實驗室名稱	TAF認可日期	聯絡人姓名	聯絡人電話
3016	鑒真數位有限公司	鑒真數位鑑識實驗室	2016/07/07	藍先生	(02)2517-2532#15
2918	勤業眾信聯合會計師事務所	資安科技暨鑑識分析中心	2016/07/07	陳先生	(02)2545-9988#7807
0263	中華電信股份有限公司電信研究院	測試中心	2016/08/02	施先生	(03)424-4335
3102	安華聯網科技股份有限公司	資安檢測實驗室	2017/01/24	劉先生	(02)8911-5035#371
3302	行動檢測服務股份有限公司	APP檢測實驗室	2017/02/23	吳先生	(02)2226-6668
3325	財團法人台灣電子檢驗中心	資通訊檢測實驗室	2017/04/25	王先生	(03)328-0026#562
3334	安碁資訊股份有限公司	數位鑑識中心實驗室	2017/07/21	朱先生	(02)2784-1000#6015 0909-384076

※為因應個人資料保護法，故無法提供自然人之姓名。

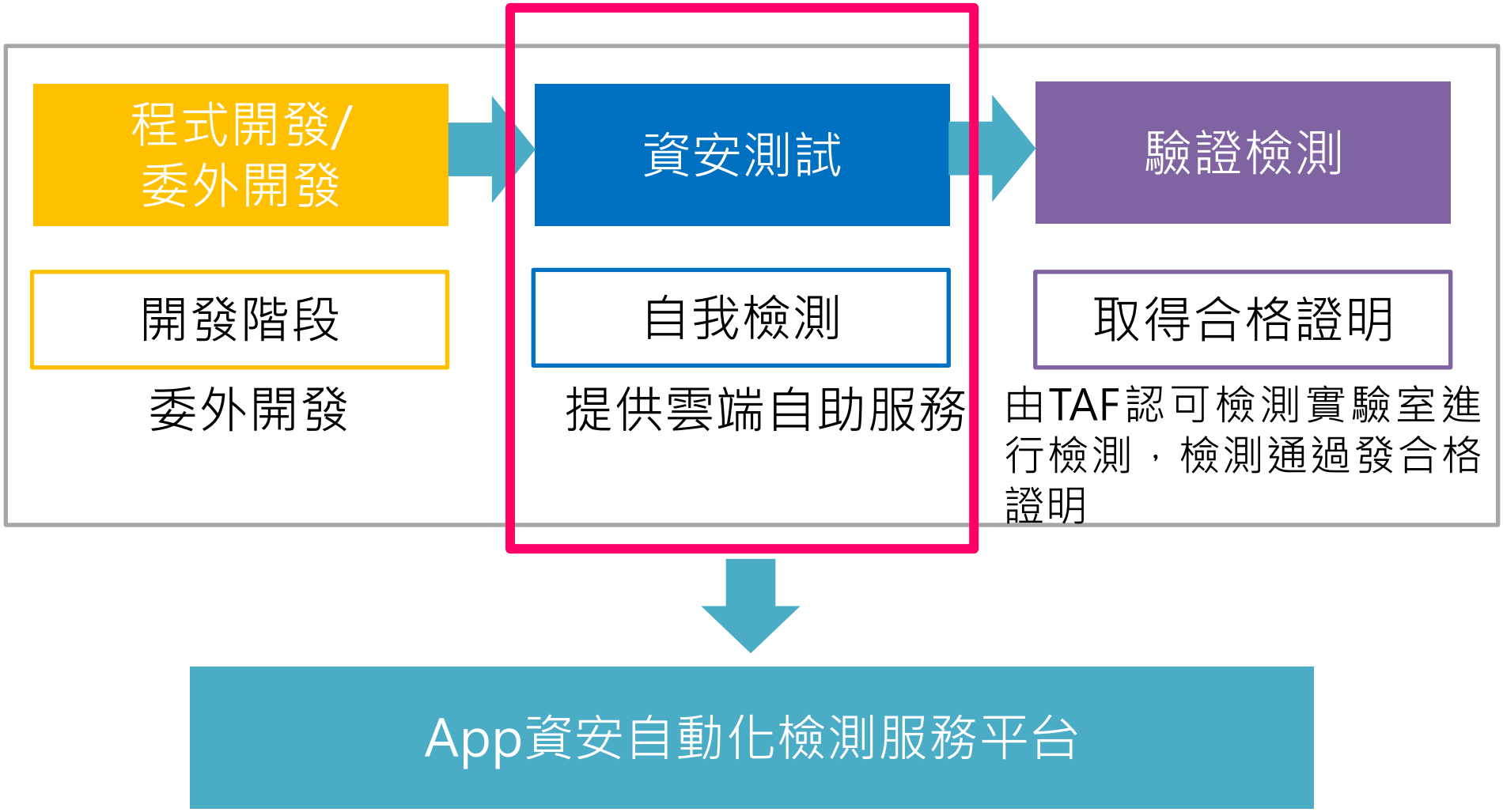
實驗室認證通過名錄與連絡資訊：

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

App 基本資安自主檢測制度推動計畫制度規範相關文件下載網址

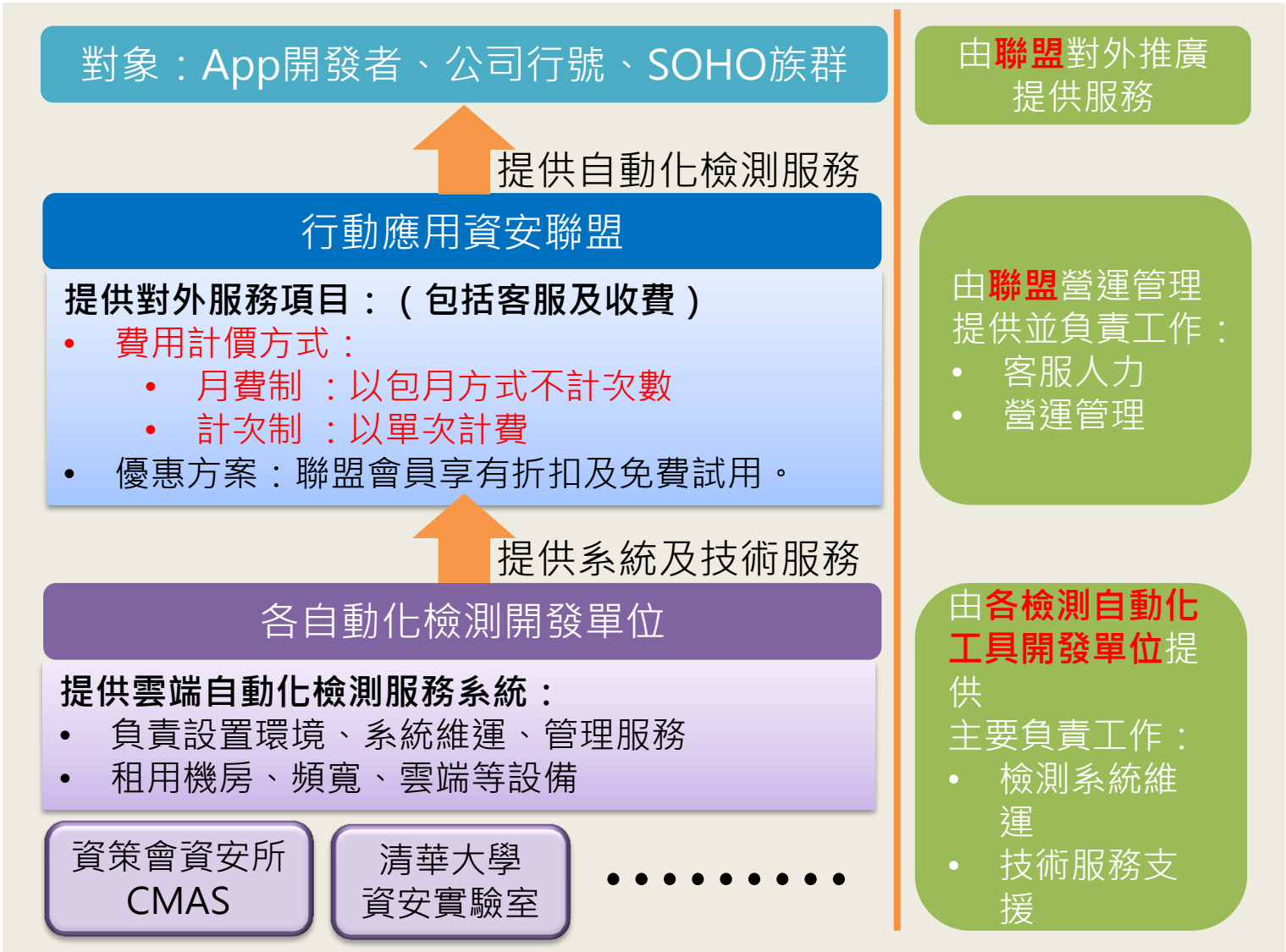
http://www.mas.org.tw

App資安自動化檢測服務平台規劃



App資安自動化檢測服務平台架構

- 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



聯盟各項收費機制及實施作業

- 各項收費於 5 月 16 日經委員會通過，於 8 月 1 日起實施。

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	

MAS 標章樣式

行動應用App基本資安標章
Mobile Application Basic Security

初級
Baseline level

TM-1OOOOO –VVV-YYYYMM

行動應用資安聯盟
Mobile Application Security Alliance

行動應用App基本資安標章
Mobile Application Basic Security

中級
Intermediate level

TM-2OOOOO –VVV-YYYYMM

行動應用資安聯盟
Mobile Application Security Alliance

行動應用App基本資安標章
Mobile Application Basic Security

高級
High level

TM-3OOOOO –VVV-YYYYMM

行動應用資安聯盟
Mobile Application Security Alliance


THANK YOU