App基本資安規範推動成果報告

主辦單位：經濟部工業局

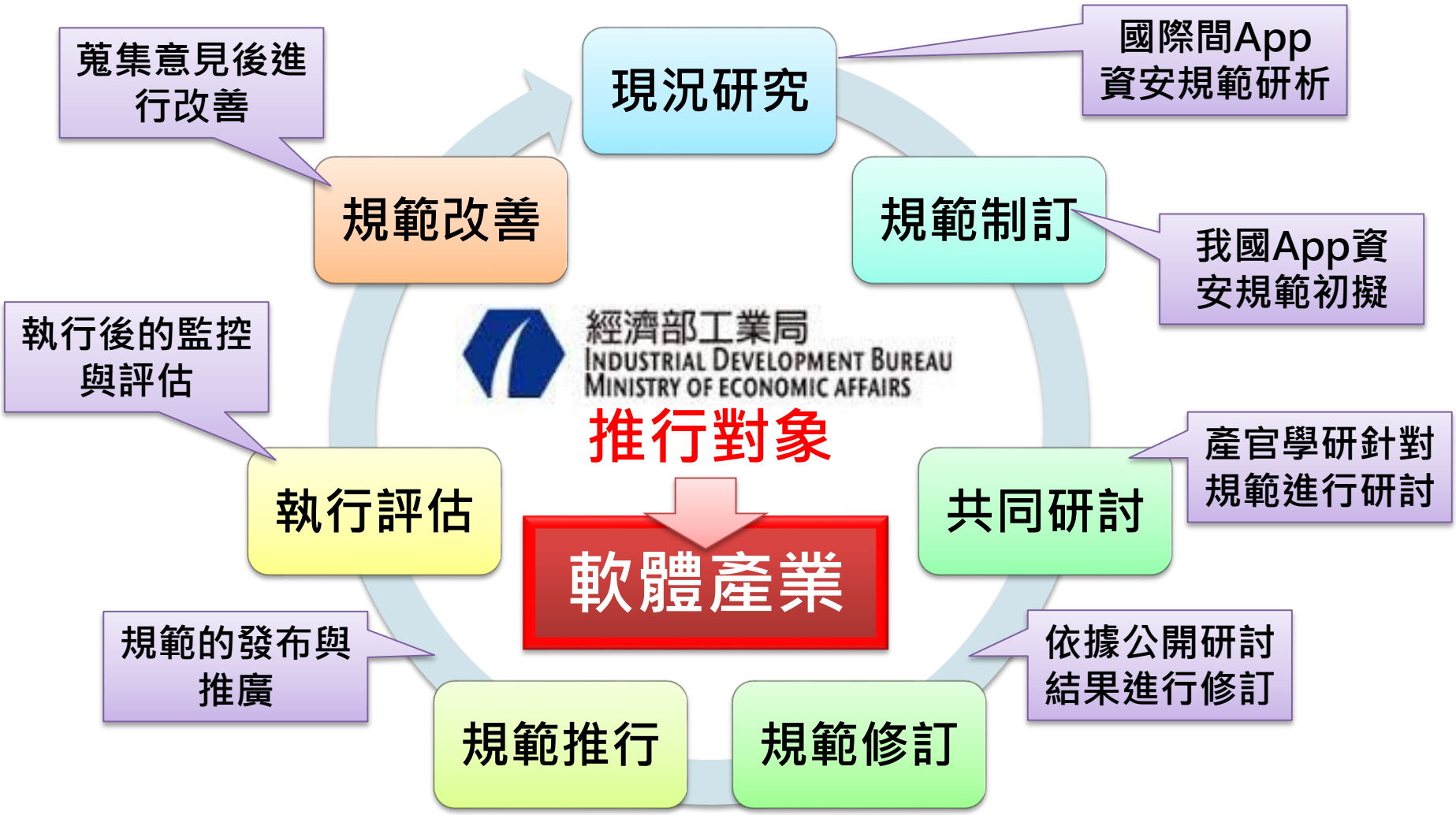
執行單位：財團法人資訊工業策進會

民國105年3月

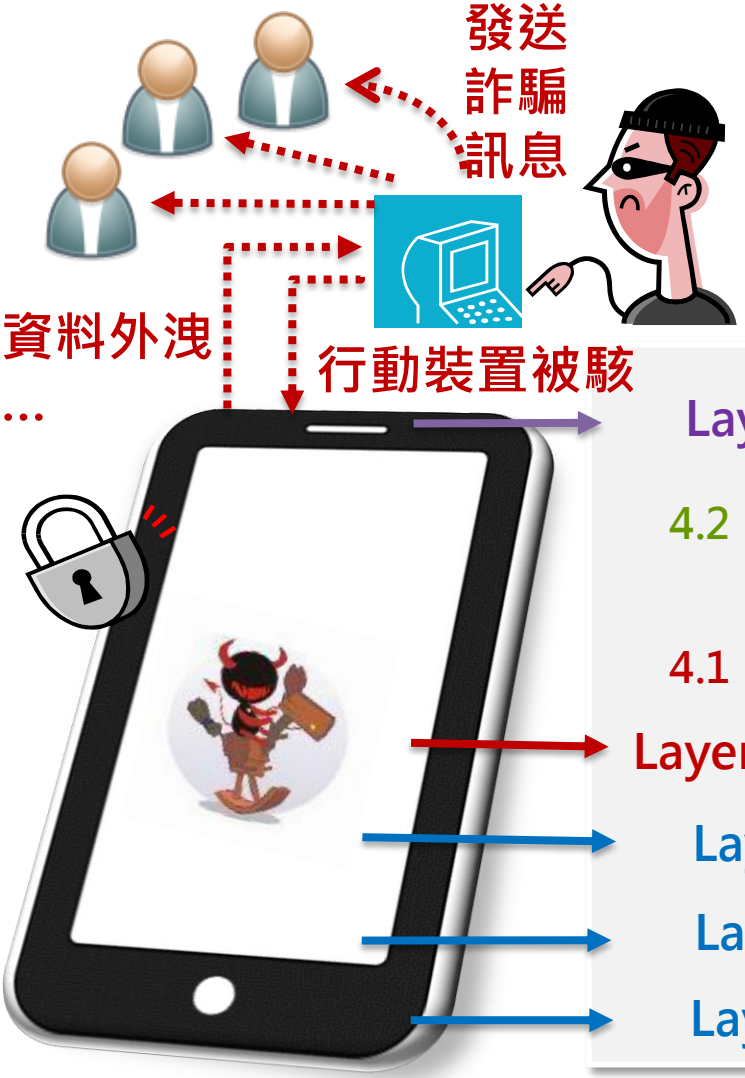
本案背景概述 – 緣起

- **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**
- 「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

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

本案背景概述 –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

4.2：特定領域應用App安全
(例：網路銀行App、健康照護App...)

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

Layer3：手機預載App安全

Layer2：手機作業系統安全

Layer1：手機硬體安全

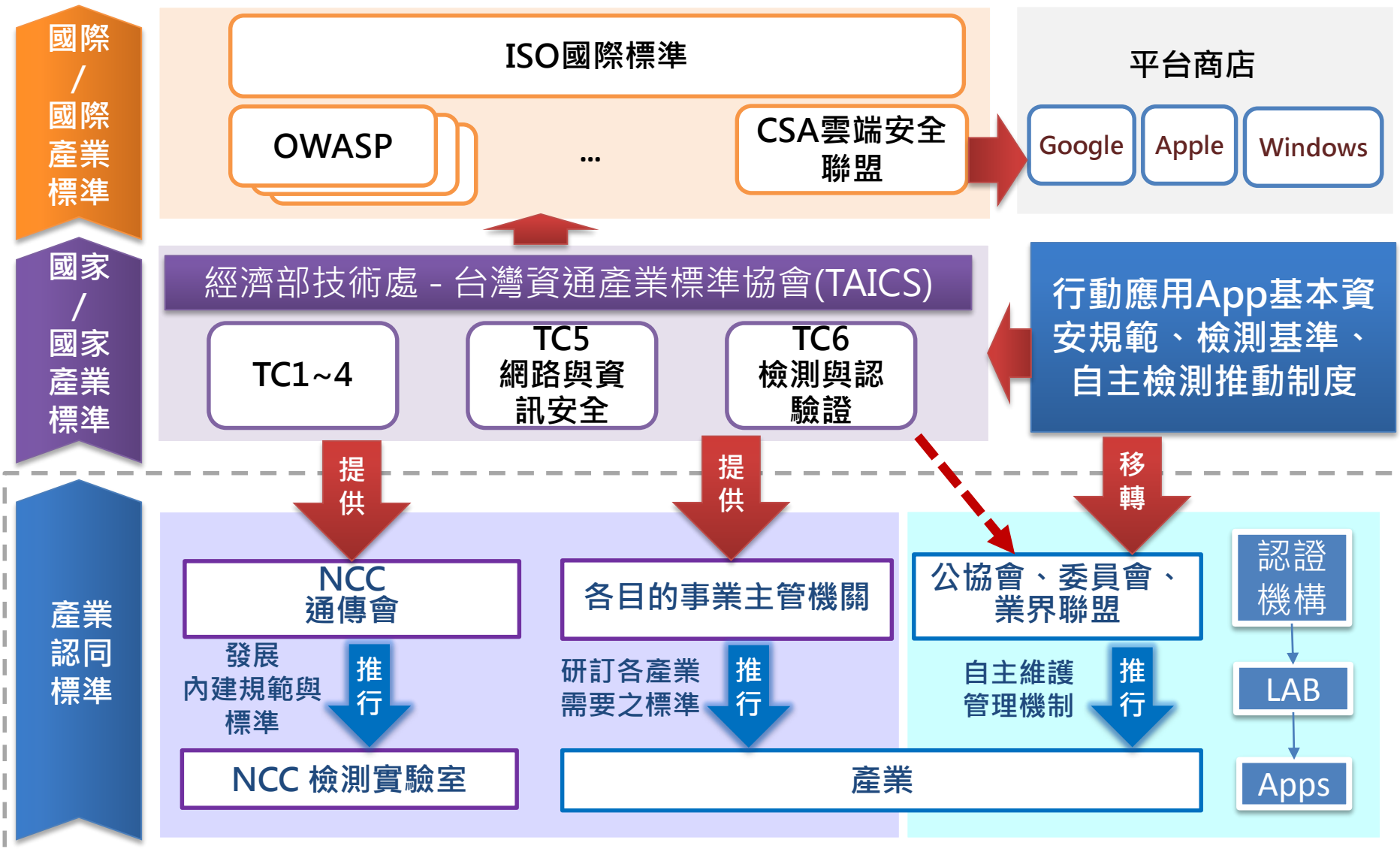
內政部
警政署

各目的事業
主管機關

經濟部
工業局

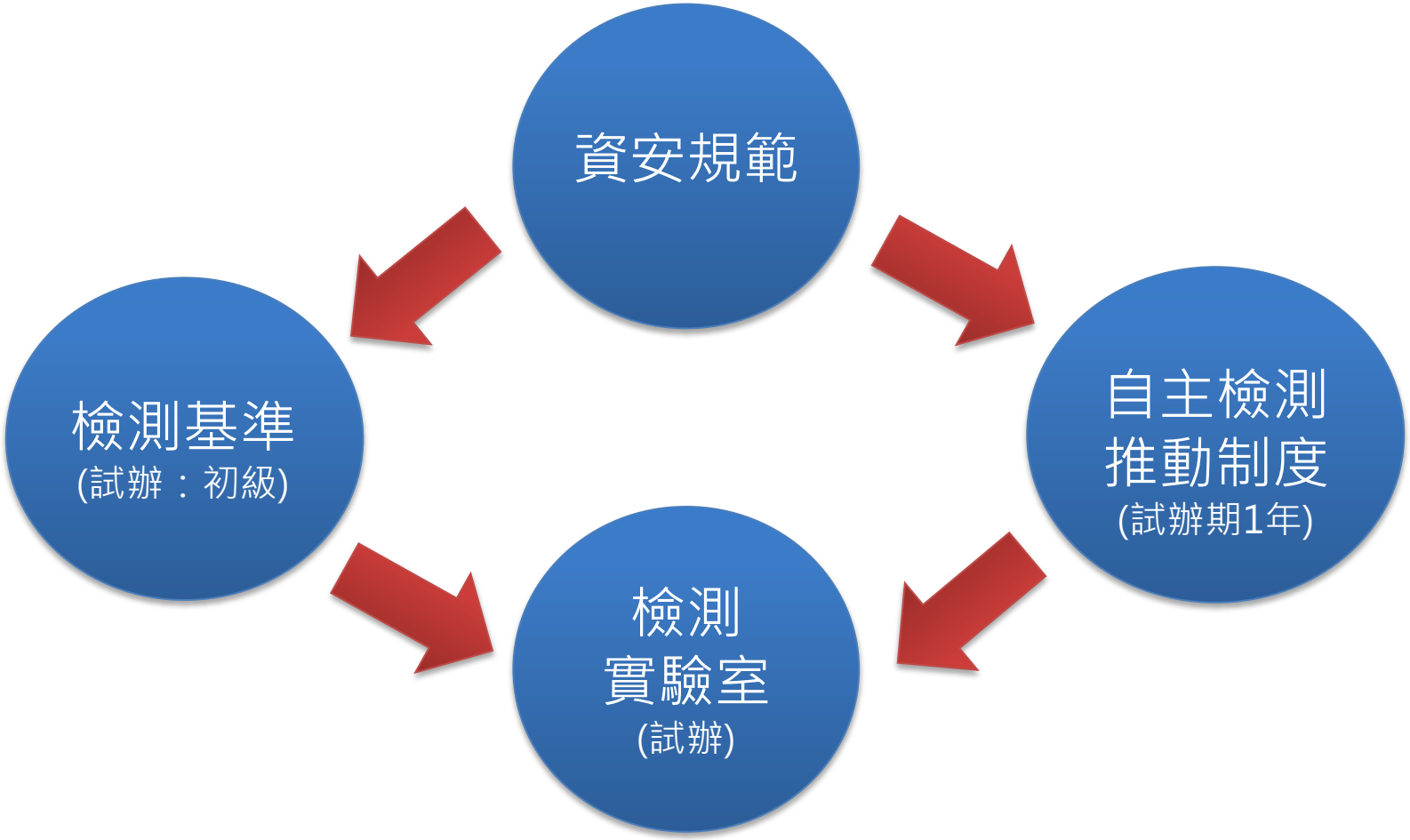
國家通訊傳播
委員會(NCC)

推動架構



TC：technical committees

推動作法



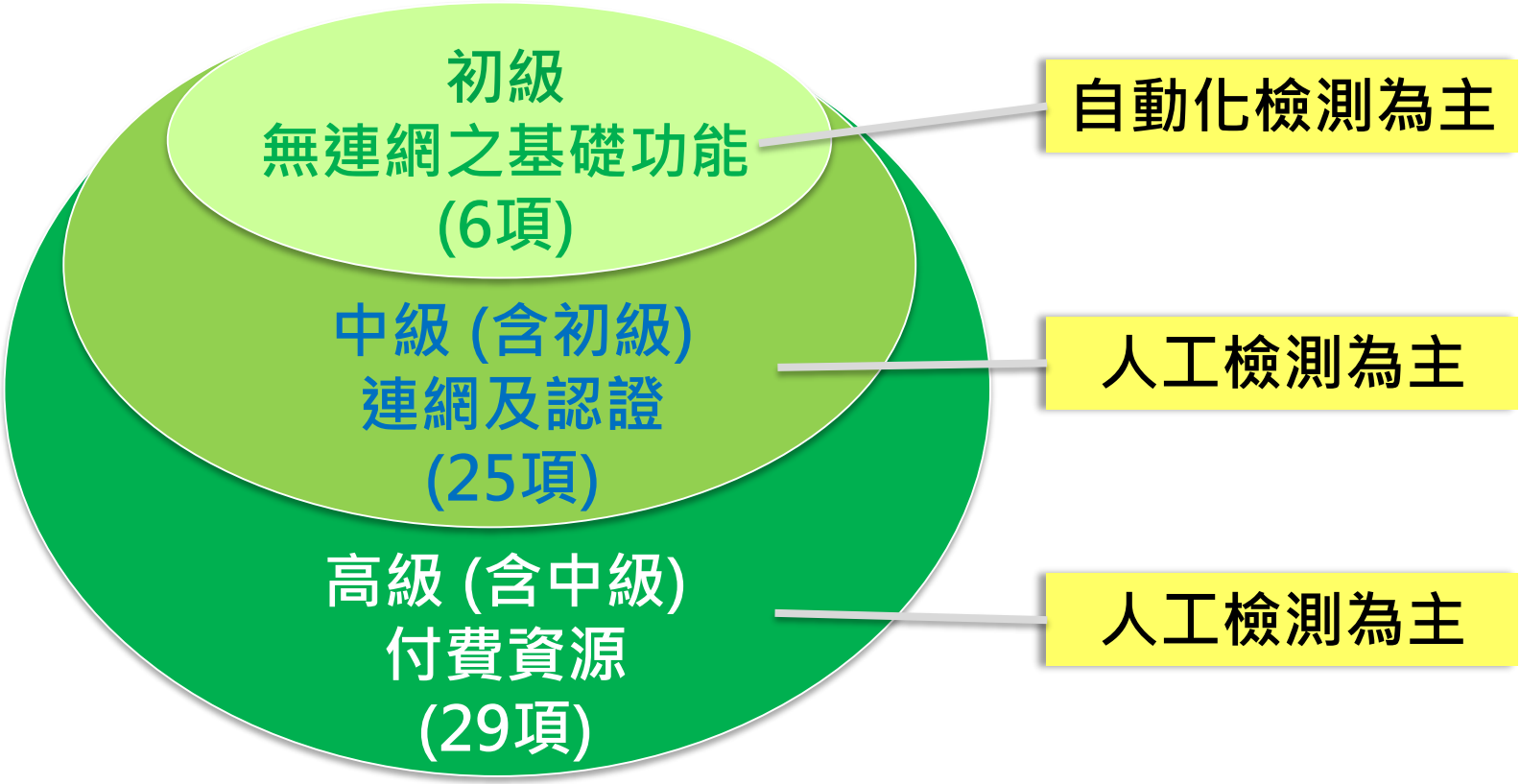
App檢測試辦

App基本資安規範說明

- 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，屬非強制性，係以輔導自主管理取代立法強制規範的精神，引導並鼓勵行動應用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。

行動應用App基本資安檢測基準V2.0

- 據App業者反應意見，考量App**改版頻繁**及**多數為小規模企業**等特性，故導入自動化檢測概念，主要針對初級檢測，以無連網之基礎功能安全性為主，並涵蓋惡意程式碼及可輕易洩漏之敏感性資訊

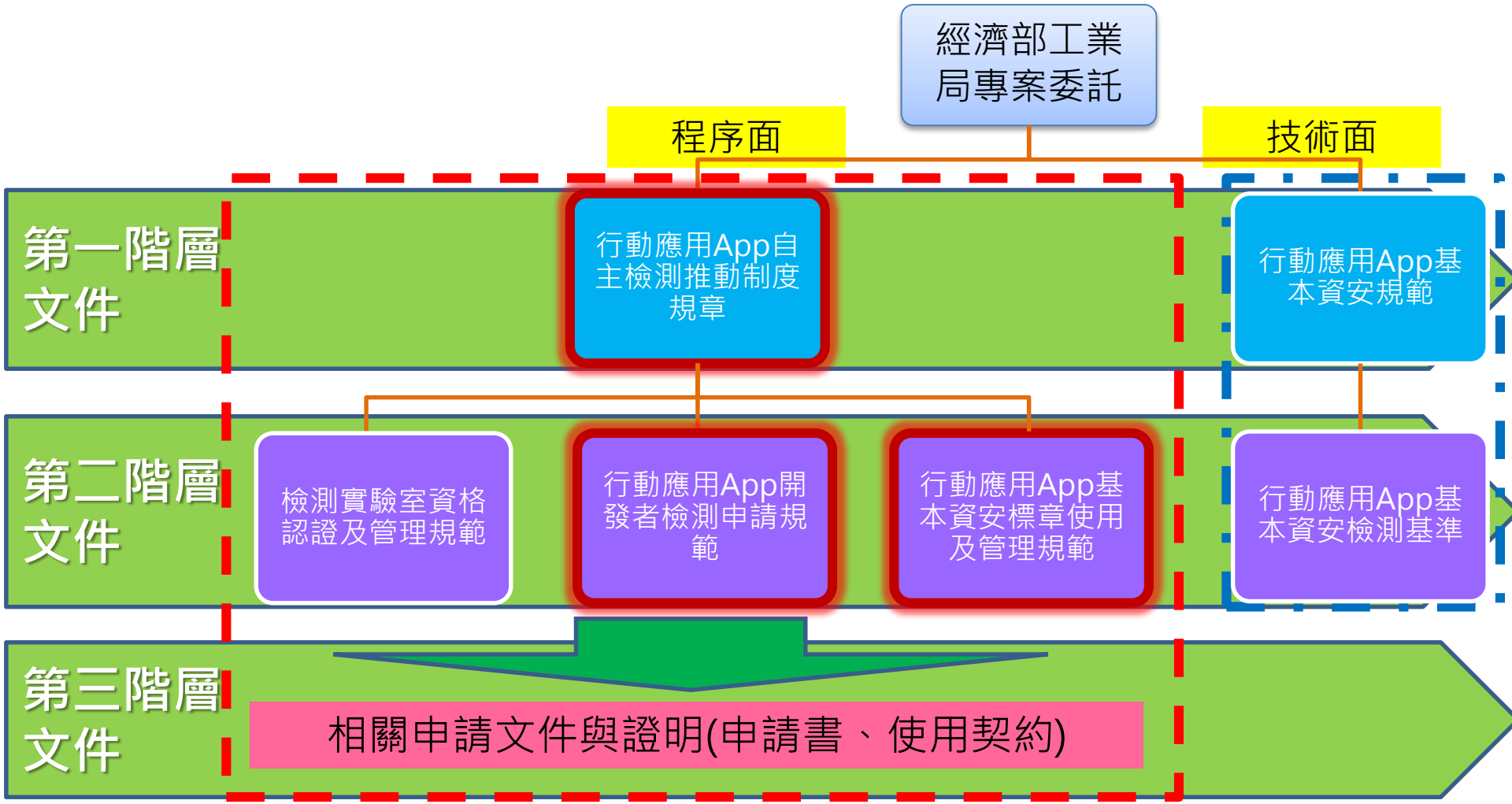


資安規範與檢測基準V2.0文件架構 – 各級檢測項目表

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，另12項為參考項目

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)	參考項目
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	1
	4.1.1.2.行動應用程式更新	0	0	0	3
	4.1.1.3.行動應用程式安全性問題回報	0	1	0	1
4.1.2.敏感性資料保護	4.1.2.1.敏感性資料蒐集	0	2	0	0
	4.1.2.2.敏感性資料利用	0	0	0	4
	4.1.2.3.敏感性資料儲存	3	2	0	1
	4.1.2.4.敏感性資料傳輸	0	1	0	0
	4.1.2.5.敏感性資料分享	0	3	0	0
	4.1.2.6.敏感性資料刪除	0	0	0	1
4.1.3.付費資源控管安全	4.1.3.1.付費資源使用	0	0	2	0
	4.1.3.2.付費資源控管	0	0	2	0
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	0
	4.1.4.2.連線管理機制	0	4	0	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	0
	4.1.5.2.行動應用程式完整性	0	0	0	1
	4.1.5.3.函式庫引用安全	0	1	0	0
	4.1.5.4.使用者輸入驗證	1	1	0	0
	各級檢測項目小計	6	19	4	12
	各級檢測項目累計	6	25	29	12

自主檢測推動制度 - 簡介


經濟部工業局專案委託
程序面
技術面
第一階層文件
行動應用App自主檢測推動制度規章
行動應用App基本資安規範
第二階層文件
檢測實驗室資格認證及管理規範
行動應用App開發者檢測申請規範
行動應用App基本資安標章使用及管理規範
行動應用App基本資安檢測基準
第三階層文件
相關申請文件與證明(申請書、使用契約)

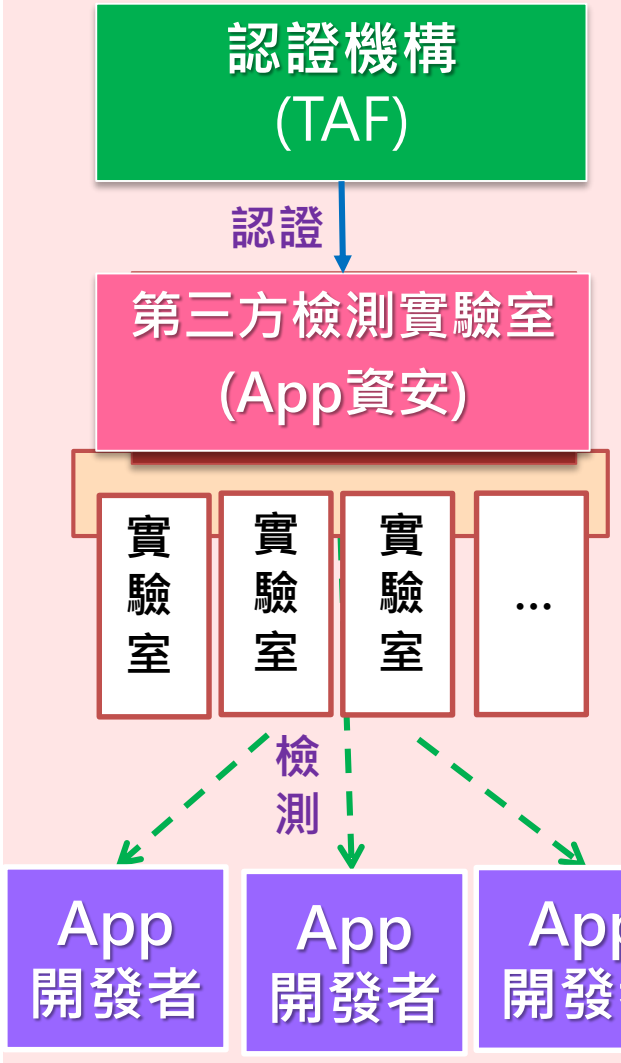
自主檢測推動制度 - 運作架構

主管機關

經濟部
工業局

運作檢測制度及標章管理

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

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：**
    - 正式：實驗室認證證明 ISO/IEC 17025
    - 試辦：檢測實驗室其具備之實驗室管理程序，包括：檢測方法及流程、檢測設備及軟體工具、檢測結果品質管理程序等，提出相關文件證明，由制度推動委員會選任專家審查。
  - **人員資格：**
    - 正式：員工3人以上，各需具備資歷與專業證照資格(如CEH、ECSA/CISSP等)
    - 試辦：員工3人以上，每一項專業要求需至少1人符合(不限同1人)，無資歷限制
  - **執行實績：於3年內有2件以上實際檢驗App資安經驗**

App檢測實驗室認證-推動進度

- **試辦檢測期(105/1/1~TAF正式授證)**
  - 首家檢測實驗室正式取得TAF(財團法人全國認證基金會) 認證時，試辦期自動截止。
  - 105年2月24日已完成5家試辦檢測實驗室認證申請、審查、認可與發證作業，可受理業者申請檢測。
    - 勤業眾信聯合會計師事務所
    - 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
    - 數聯資安股份有限公司
    - 行動檢測服務股份有限公司
- **正式檢測期(TAF正式授證~)**
  - 預計TAF 1月正式公告受理檢測實驗室申請，預計105年8月首家認證實驗室取得認證。

App檢測實驗室認證-執行時程規劃

- **試辦期間**：104年10月 28日至第一家行動應用App資安檢測實驗室通過TAF(財團法人全國認證基金會) ISO/IEC 17025認證止
- **試辦實驗室證書效期**：核發證書日起至第一家行動應用App資安檢測實驗室通過TAF ISO/IEC 17025認證止
- **正式實驗室(TAF認證)證書效期**：3年

執行階段	試辦檢測實驗室認證	正式檢測實驗室 TAF認證
梯次	批次作業	不分梯次
1. 資訊公告	104/10/28 http://www.communications.org.tw/news/policy/item/8768-app1028.html	104/12/11 http://www.taftw.org.tw/wSite/ct?xItem=11989&ctNode=30&mp=1
2. 認證申請	104/10/28~11/30	105/1/1
3. 專家審查	104/12/1~105/2/24	依據TAF審查流程(註) http://hr.taftw.org.tw/service/DocDownload.aspx?id=00003703
4. 能力試驗活動	無	依據制度管理委員會公告

註：行動應用APP基本資安檢測實驗室認證服務計畫(TAF-CNLA-A24)

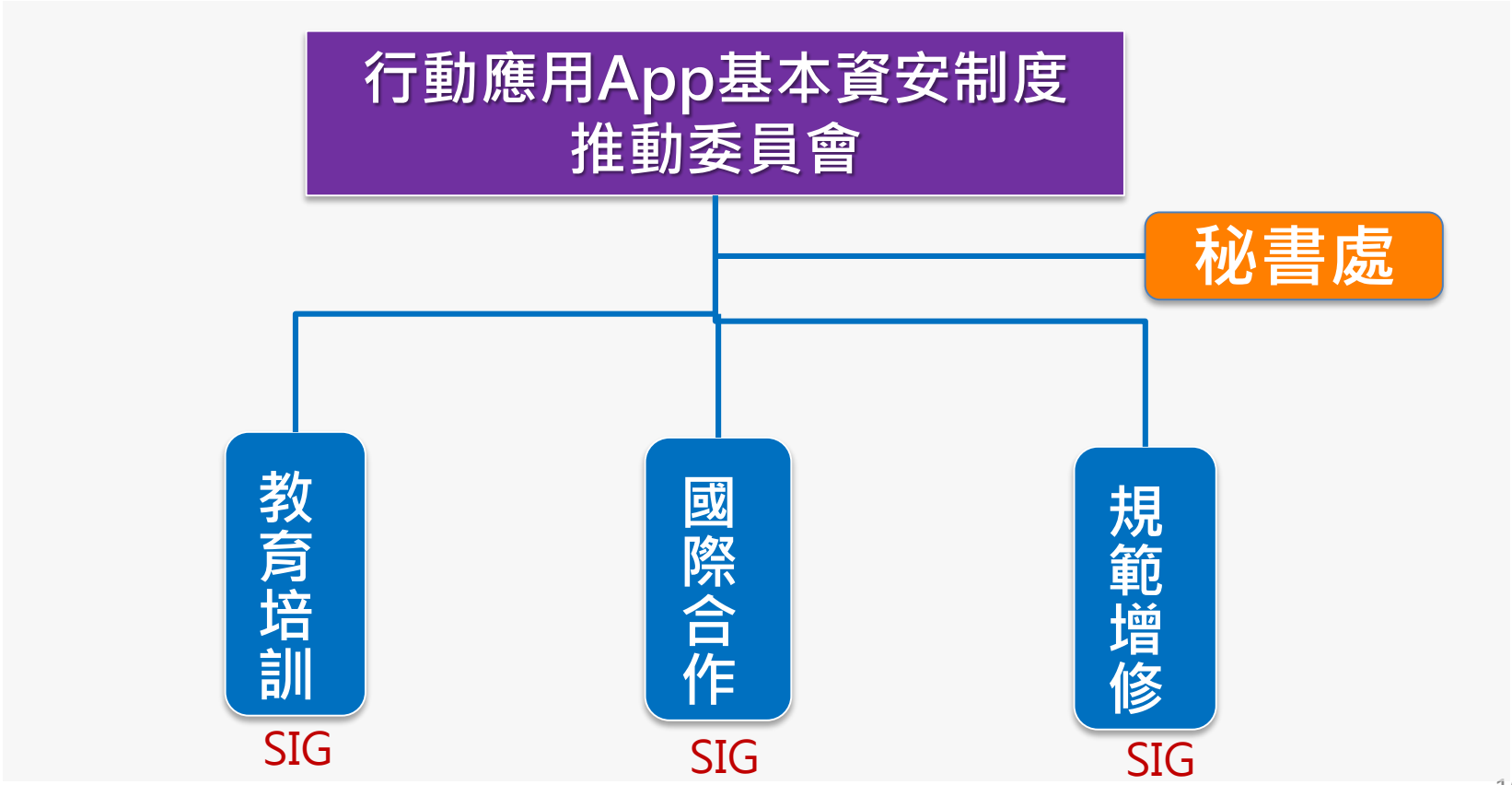
App檢測實驗室認證-能力試驗規劃

105年能力試驗活動時程規劃

執行階段	能力試驗活動	
梯次(105年度)	第1梯次	第2梯次
1. 資訊公告	105/1/30	預計105/7/1 (視正式公告而定)
2. 受理申請	105/2/1~2/29	預計105/8/1~8/31 (視正式公告而定)
3.能力試驗	105/3/1~3/31	預計105/9/1~9/30 (視正式公告而定)
4. 能力試驗結果通知	105/4/8	預計105/9/31前 (視正式公告而定)

籌組制度推動委員會

- 104 年底已籌組委員會，邀請相關公協會與業者參與，推動後續檢測實驗室、人才培育、國際合作，以及相關自主檢測機制維運與推展。



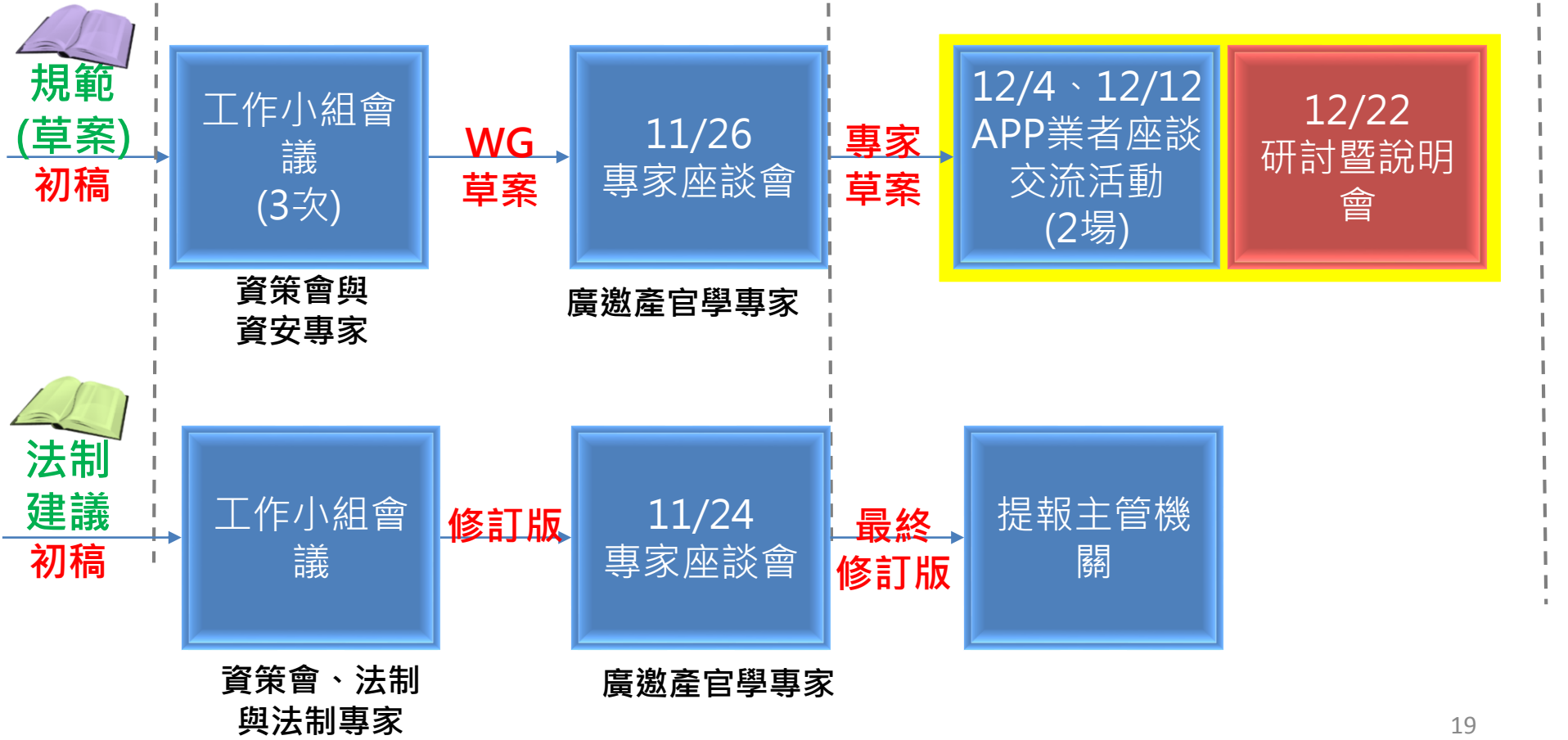
未來推動重點工作

APP標準 擴大普及	本規範係為App基本資安要求，各目的事業主管機關或公協會，可自行參酌此基礎，賡續研訂符合產業特性需要之標準。
企業廠商 自主管理	促成業界合格App資安檢測實驗室，推動業界資安檢測服務，協助App開發業者建立資安檢測能量，確保App基本資安檢測整體品質之一致性與完整性。
資安人才 專業培育	結合產業公協會能量，推動App基本資安檢測與安全開發相關課程，提昇資安檢測從業人員對行動資安檢測能力，強化產學合作培育相關人才。
產業標準 國際接軌	與Google、Apple 等國際行動應用程式商店洽談，推動App資安認證商店上架標示，另透過台灣資通產業標準協會與國際組織接軌，加速產業發展契機。

附件：執行方式與推動成果

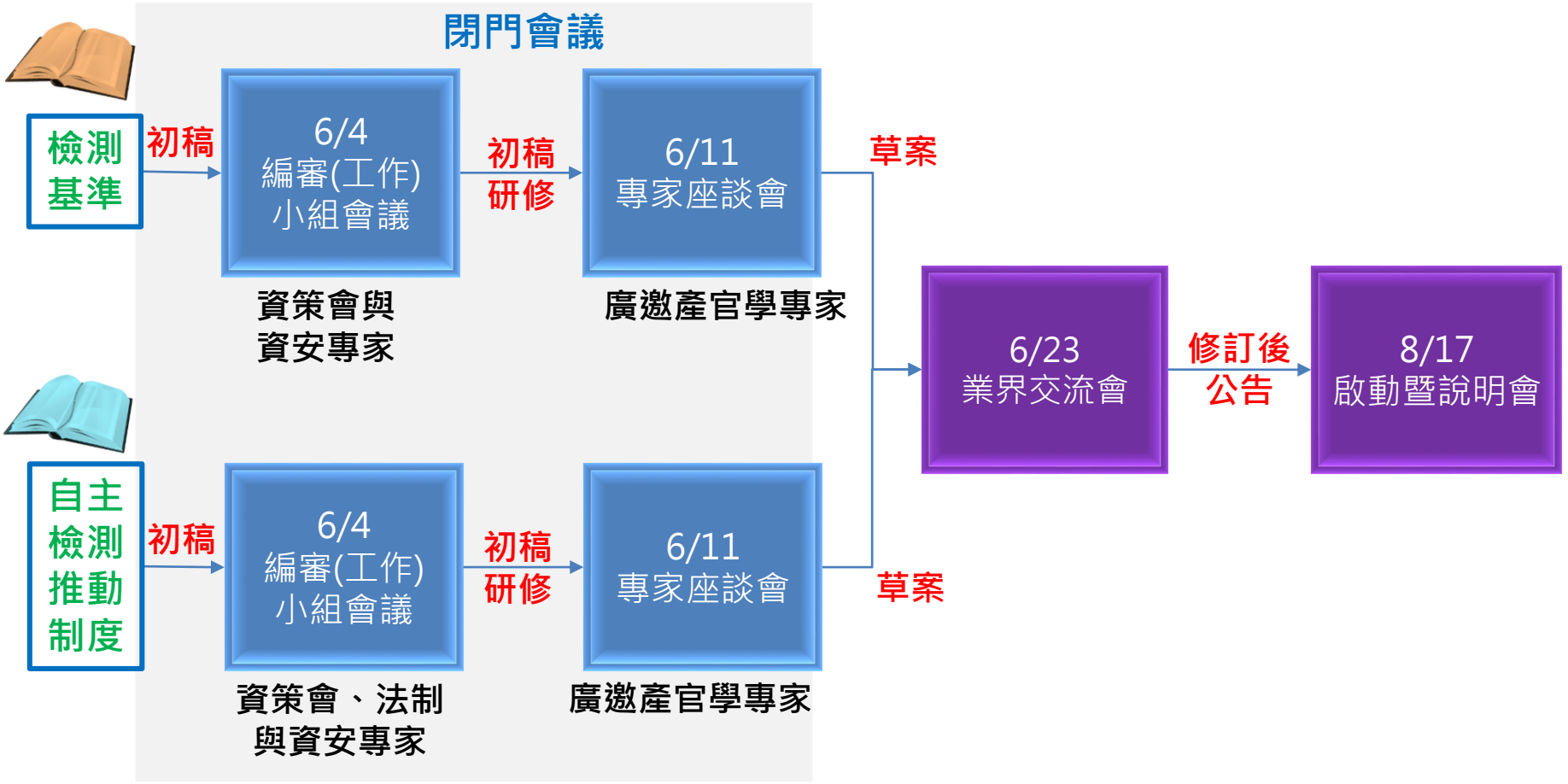
103年作業方式與時程 (1/3)

資安規範與法制建議作業方式與時程



104年作業方式與時程 (2/3)

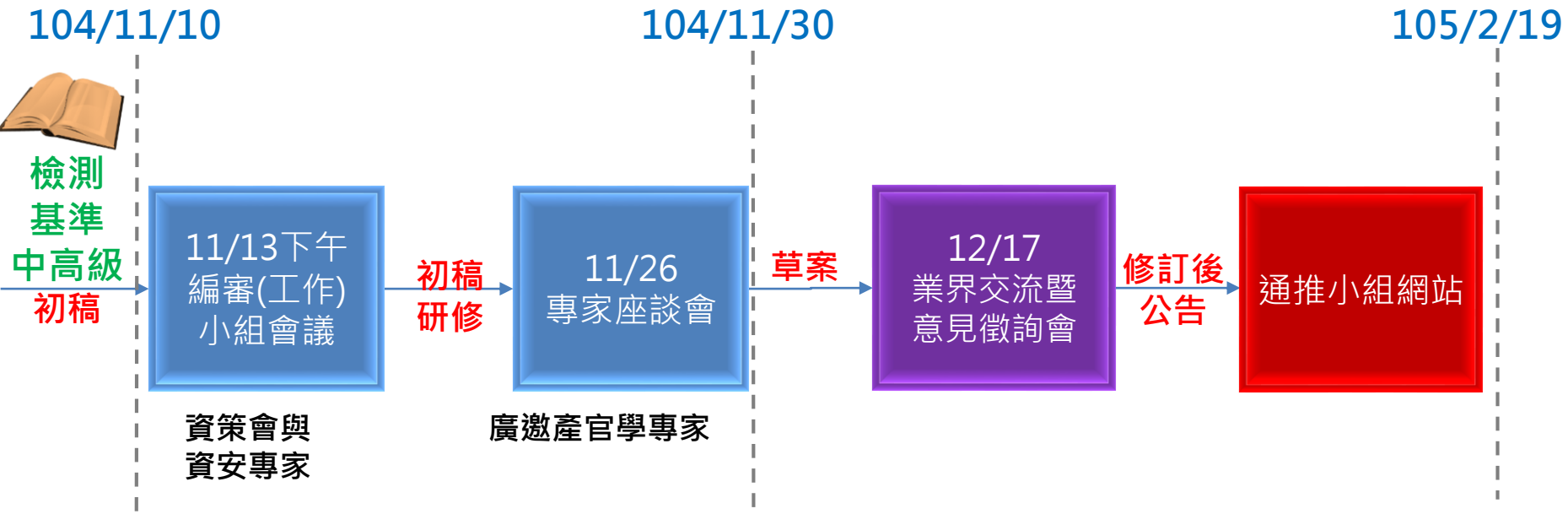
依據104年4月20日公告之行動應用App基本資安規範，進行下述文件研訂：



註：「檢測基準」為「行動應用App基本資安檢測基準」之簡稱
「自主檢測推動制度」為「行動應用App基本資安自主檢測推動制度」之簡稱

104年作業方式與時程 (3/3)

檢測基準作業方式與時程



103/12/22 App基本資安規範公開說明

- 工業局委託資策會於103年12月22日假台大集思會議中心，辦理「手機App軟體基本資安規範(草案)研討暨說明會」，邀請行政院資安辦公室、學界專家、公協會，與業界交流及凝聚規範共識，會後將「手機App軟體基本資安規範(草案)」公開審閱，採非強制性方式，鼓勵業者自主管理。

104/6/23 App基本資安檢測基準暨自主檢測推動業界交流

- 工業局委託資策會於104年6月23日假台大集思會議中心，辦理「行動應用App基本資安檢測基準暨自主檢測推動制度業界交流會」，邀集App開發者、檢測業者與資安業者，與各界交流制度面與技術面議題並凝聚共識，推動產業自主參與，促進國內App資安檢測深耕發展，提升台灣App產品在國際市場的競爭力。

104/8/17 啟動App基本資安規範

- 104年8月17日假空總創新基地由行政院張副院長、科技會報辦公室執秘鐘嘉德、 經濟部沈次長、相關產業公協會等，於空總共同啟動我國「行動應用App基本資安規範」，進行有關App基本資安自主檢測制度、基準與檢測試辦成果說明，共約150家業者出席活動。。

104/12/17 制度與基準修訂說明

- 為向業界說明 App 檢測基準之增修檢測項目、App基本資安標章管理與TAF認證檢測實驗室服務，特於**104年12月17日**假台大集思會議中心辦理**「行動應用App基本資安檢測基準及自主檢測推動制度修定版說明會」**，共**約100多家業者出席活動**。

104年度初級檢測試辦參與業者

ASUS WebStorage (資電類) 華碩雲端股份有限公司	LIVEhouse.in (資電類) 愛卡拉互動媒體股份有限公司	hicloud Box(e) (資電類) 中華電信數據通信分公司	雲端發票 (生活品味類) 雲端行動科技股份有限公司
M+ Messenger (通訊類) 台灣大哥大股份有限公司	The Lost Kids 貪吃的兄妹 (遊戲類) 樂陞科技股份有限公司	博客來快找 (電商類) 博客來數位科技股份有限公司	驅動城市 (交通類) 醬子科技股份有限公司
Juiker揪科 (通訊類) 源思科技股份有限公司	巨神之戰 (遊戲類) 雷爵網絡科技股份有限公司	全國繳費網 (eBill) (金融類) 財金資訊股份有限公司	友善台北好捷運 (公益類) 众社企股份有限公司

推動成果與情形–檢測輔導推動

- 搭配「4G智慧寬頻應用城市補助與推展計畫」，規範於計畫內業者所開發App，皆須通過App基本資安檢測。
- 推動政府軟體採購共同供應契約App軟體項目，納入App基本資安檢測要件(於試辦期104/12/31前統計，已輔導5家納入)。

M+ Messenger (通訊類)	team+ for Gov (通訊類)	Qmi (通訊類)
台灣大哥大股份有限公司	互動資通股份有限公司	中華電信數據通信分公司
Gorilla TV (資電類)	LIVEhouse.in (資電類)	
大猩猩科技股份有限公司	愛卡拉互動媒體股份有限公司	