行動應用資安聯盟
Mobile Application Security Alliance

行動應用 App 資安標章全攻略

「需求、開發到實驗室檢測的合規一體化實務」

L1 L2 L3

執行單位： TCA 台北市電腦公會

行動應用資安聯盟
Mobile Application Security Alliance

單元一 | 制度推動篇

行動應用 App 資安認驗證制度

從資安基本功，到臺灣產業的信任基礎建設

打造「全面性防禦」管理力

行動應用資安聯盟
施任峯 資深顧問

課程地圖

單元一｜制度推動篇 – 理解制度的「為什麼」

從制度緣起、制度架構、推動成果、到我們的期待，並對照國際，建立宏觀的制度全貌

三單元課程地圖

單元一　本單元

制度推動篇

打造「全面性防禦」管理力

制度緣起、架構、標章與市場價值

單元二

規範解析篇

建構「開發即合規」防護力

Security by Design，把規範化為開發控制點

單元三

基準說明篇

落實「實驗室實戰」檢測實務

檢測項目、常見盲點與送驗前 Checklist

課程主軸　**從「外部檢測」→ 到「開發即合規」**　以主動防禦貫穿 App 研發全生命週期

大綱

今天想和大家分享的四件事

1. **為什麼需要這套制度**
   App 資安品質看不見的問題，以及 AI 時代下正在加速的新風險。

2. **制度怎麼運作**
   治理架構、檢測執行流程、品質問責機制與檢測基準分級。

3. **制度帶來的效益**
   對 App擁有者、檢測實驗室、使用者與主管機關，各自代表什麼價值。

4. **國際對照與我們的期待**
   臺灣目前的位置，以及希望與夥伴們一起走的下一步。

在開始之前・分享的目的

打造能自我修正的資安生態系，而不是辦一次性檢測

這場分享想說明的，不是「多一項規定」，而是生態系裡每個角色如何彼此成就、持續進化：

1 **給 App 擁有者與開發商**

藉由送測過程了解常見資安威脅、持續精進，讓自己自然而然開發出更安全的系統。

2 **給檢測實驗室**

隨標準改版持續精進檢測能力，也能在眾多檢測機構中，與未受認證的實驗室做出明確區隔。

3 **給使用者與主管機關**

不需要自己判斷技術細節，也能更安心地使用、採用這些通過驗證的系統。

4 **給聯盟與 TAF**

扮演「第二道防線」：實驗室有收取開發商費用的壓力，聯盟與 TAF 站在更公正的位置督導檢測品質。

為什麼需要這套制度

App 無所不在，但資安品質看不見

1

行動裝置已是全民日常

各類 App 深入金融、醫療、政府服務，但使用者、企業甚至採購單位都難以自行判斷一款 App 的資安品質好壞。

2

各自為政、重複檢測

缺乏共通標準時，不同主管機關、不同採購案各自訂規則，同一支 App 可能被要求重複檢測，墊高開發與法遵成本。

3

風險不只是技術問題

資安漏洞牽動的是個資外洩、財產損失與社會對數位服務的信任，一旦出事，代價由全民承擔。

我們需要一個「看得懂、信得過」的第三方驗證機制

為什麼需要這套制度

AI 時代，破解 App 的門檻正在快速降低

App 一經上架，任何人都能下載安裝檔進行分析。
生成式 AI 工具，讓逆向分析與弱點挖掘變得更快、更容易上手。

App 公開上架

任何人都能下載安裝檔，取得分析素材。

AI 輔助逆向分析

自動化反組譯、比對已知漏洞樣態。

弱點更快被找到、被利用

過去要數週的分析，現在可能數小時完成。

檢測基準必須比攻擊手法更快進化，這正是制度十年來持續改版的原因

PART 1

制度怎麼運作

從治理架構、監督循環到檢測執行流程

看見機制背後看不見的把關

生態系全貌

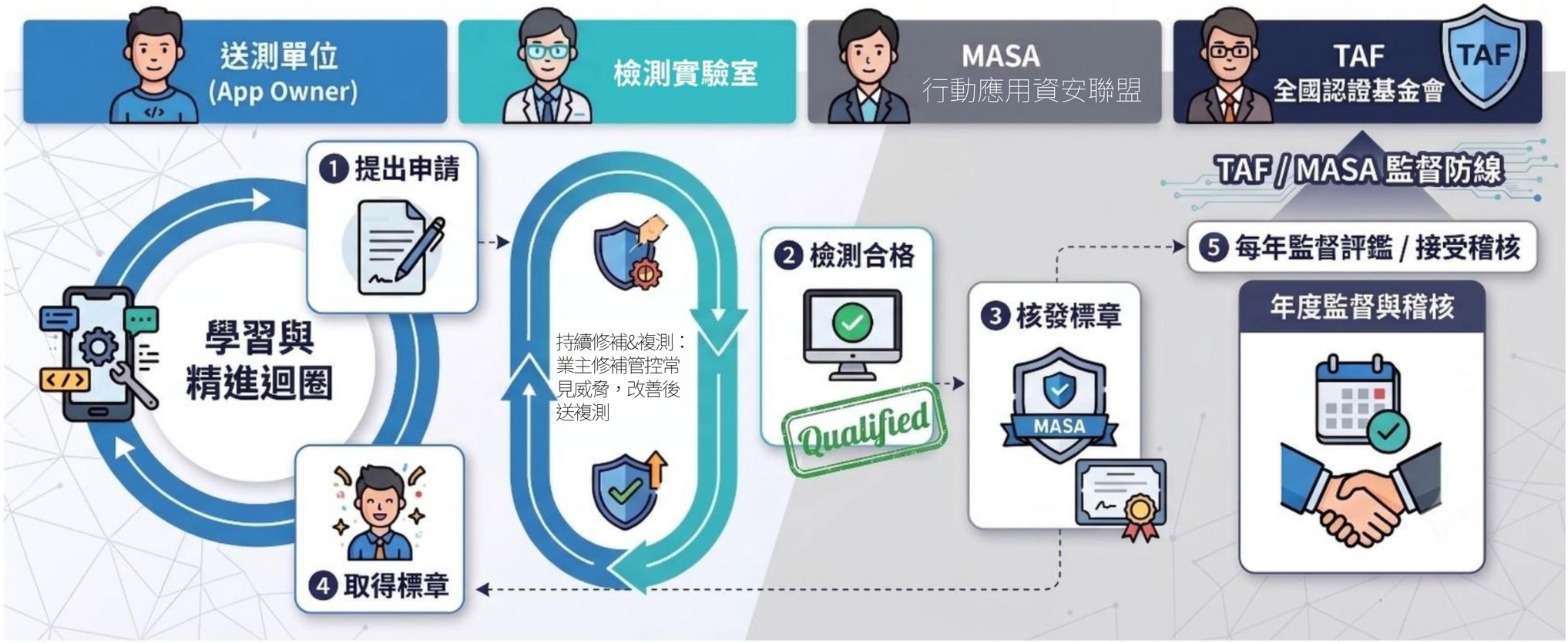
五方協作：從治理到使用者的完整鏈結

- 政府 (數位發展部 / 數位產業署)：政策支持 → 指定推動機構
- 行動應用資安聯盟 (MASA)：訂定規範／審核核發標章與證書
- 檢測實驗室 (TAF 認證 20 家)：執行第三方檢測
- App 擁有者 (App 開發商)：申請檢測 → 取得標章與證書
- 使用者 (消費者 / 企業 / 政府採購方)：安心下載 → 安心採購導入

公開透明：合格實驗室名單與通過檢測 / 驗證之 App，公告於行動應用資安聯盟網站 mas.org.tw 供社會大眾查詢

制度怎麼運作

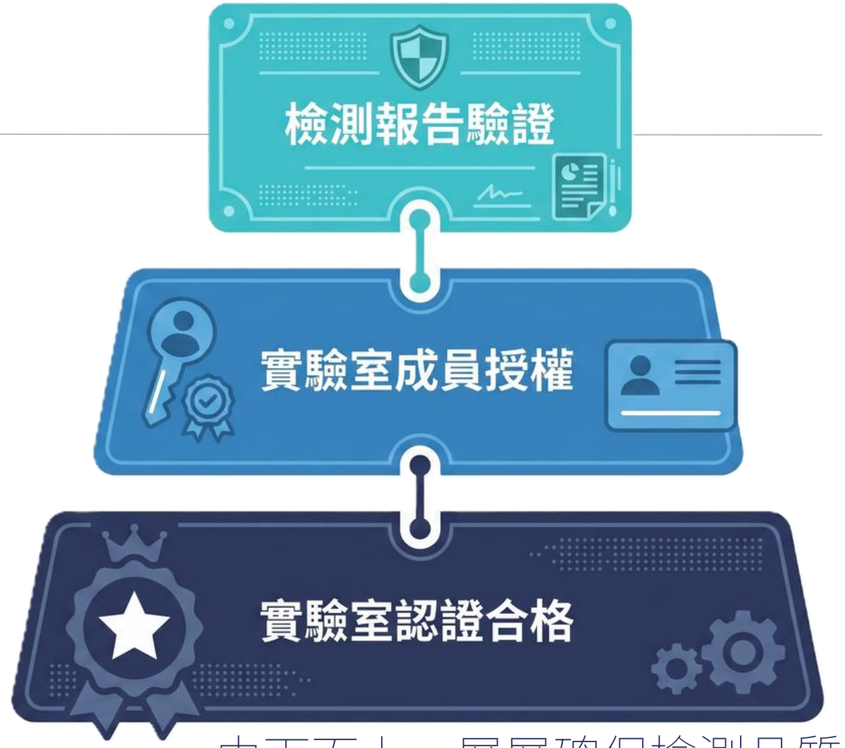
檢測/驗證執行流程： App擁有者在送測過程中持續學習精進



制度的公信力

品質怎麼把關：看得見的問責機制

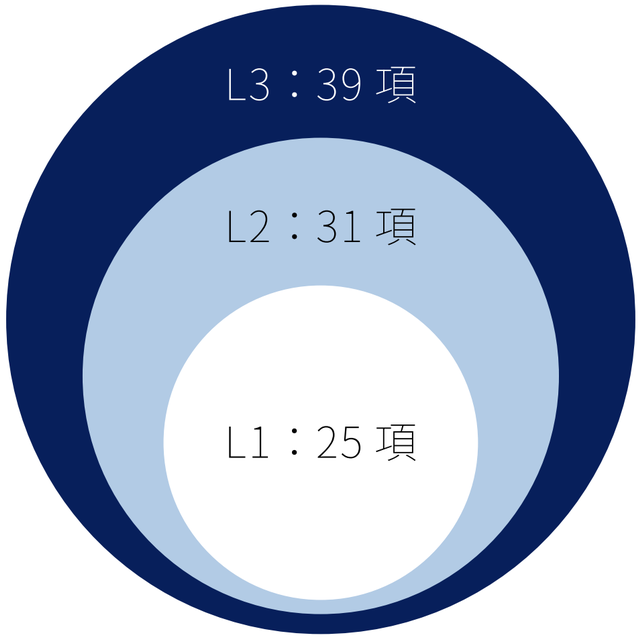
- 入場資格：須先取得 TAF「ISO 17025」認證，並配置實驗室主管、品質主管、報告簽署人等專職人員。
- 公正義務：須「公平、公正、獨立」執行檢測，不得與送測開發商有妨害公正性之關係，報告不得虛偽不實。
- 持續稽核：聯盟與 TAF 定期或不定期訪視、抽測比對；送測 App 須封存留存至少 1 年，供隨時複核。
- 獎優汰劣：違反規範者，聯盟得通知 TAF 撤銷認證證書；每年辦理績效評核，公開表揚優良檢測實驗室。



由下而上，層層確保檢測品質

制度怎麼運作

檢測項目涵蓋關係



L2包含L1的所有檢測項目
L3包含L2的所有檢測項目

資安等級	說明	等級標章
L1	無須使用者身分鑑別之行動應用程式。	
L2	須使用者身分鑑別之行動應用程式。	
L3	含有交易行為之行動應用程式。	
F	9 項選測：屬於安全性需求較高之行動應用程式，為加測項目。	

各類檢測基準採累計制：App 涉及的資料或交易風險越高，適用的等級也越高。

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

一 程式發布安全

二 敏感性資料保護

三 交易資源控管

四 身分鑑別、授權與連線管理

五 程式碼安全

六 伺服器端安全

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

一 程式發布安全

測什麼？

隱私權政策揭露與漏洞通報機制是否完備。

為什麼？

讓使用者知悉個資運用方式，並建立漏洞揭露與應變管道。

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

二 敏感性資料保護

測什麼？

個資、憑證等資料的儲存與傳輸方式。

為什麼？

防止資料外洩或遭側錄竊取。

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

三

交易資源控管

測什麼？

交易流程與重要操作的驗證機制。

為什麼？

防止交易遭竄改、重放或詐欺。

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

四

身分鑑別、授權與連線管理

測什麼？

登入、權限控管與連線加密機制。

為什麼？

防止帳號冒用、越權存取。

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

五

程式碼安全

測什麼？

程式碼是否存在漏洞、可否被反組譯。

為什麼？

防止關鍵邏輯外洩或遭竄改利用。

制度怎麼運作

六大類檢測範圍：測什麼？為什麼測？

六

伺服器端安全

測什麼？

後端 API 與伺服器的防護措施。

為什麼？

防止後端服務被入侵、API 遭濫用。

推動現況

十年扎根：量能與成果一次看

20 家
TAF認可檢測實驗室
涵蓋國際四大會計師事務所
與專業資安機構

9,445 件
App 資安標章累計核發
(105年至115年6月)

506 件
115年上半年通過檢測
政府107件・民間399件

四大類20家檢測實驗室已建立完整量能，涵蓋政府機關、金融、電信、資安專業機構，形成穩定運作十年的檢測生態系。

推動重點成果

已成為多個部會與採購之重要資安規範

工程會：須「公平、公正、獨立」執行檢測，不得與送測開發商有妨害公正性之關係，報告不得虛偽不實。

數發部數產署：委託行動應用資安聯盟（由台北市電腦公會執行）擔任制度的推動暨驗證機構，負責處理 App 資安認驗證標章的核發與推廣。

金管會 • 三大公會：銀行 / 證券 / 保險業 / App 須通過 MASA 檢測基準。

衛福部：行動應用 App 開發應依 MASA 基準辦理。

實際採購案：立法院、台電、中油等已於招標規範中納入本標準。

從採購規範到金融法遵，MASA 基準已是跨部會、跨產業共用的資安檢測共同語言。

PART 2

制度帶來的效益

對四個關鍵角色來說

這套制度各自代表什麼價值

效益

四個關鍵角色

一 給 App擁有者與開發商

二 檢測實驗室

三 使用者

四 目的事業主管機關

效益・給 App擁有者與開發商

從送測過程中學習，把資安內化成開發習慣

1

在送測中認識常見威脅、持續精進

檢測—修補—複測的來回過程，讓開發團隊實際掌握常見資安弱點，逐步內化為開發規範，而不是事後補救。

2

降低法遵與整改成本

檢測基準參考 OWASP MASVS 等國際規範，一次檢測、多方採信，免於重複驗證。

3

提升消費者信任與品牌價值

MASA 標章可於官網公開查詢，強化使用者下載與付費意願，也是企業資安治理成熟度的具體證明。

效益・給檢測實驗室

壯大本土能量，品質是我們的服務之本

產業能量與差異化

- 20 家檢測實驗室，涵蓋國際會計師事務所與本土專業資安檢測服務機構。
- 檢測基準逐版與 OWASP MASTG／MASVS 等國際規範同步，能量與國際接軌。
- 隨標準改版持續精進能力，在市場眾多檢測機構中，與未受認證者做出明確區隔。

想對實驗室夥伴說的話：

- 檢測品質，不該只是「形式合格」，而應該是「務實檢測」。
- 這也是聯盟持續投入訪視、抽測比對、績效評核與問責機制的原因。
- 希望與每一家夥伴實驗室一起把關品質，讓「拿到標章」等於「真正做到位」。

效益・給使用者

不必懂技術細節，也能安心採用

1

下載更安心

消費者只要認明 MASA 標章，就能判斷一款 App 是否通過第三方資安檢測，不必自己研究技術細節。

2

採購更省心

企業與政府採購方可直接以標章作為評選依據，降低自行評估資安風險的專業門檻與人力成本。

3

信任有依據

標章背後是十年運作、持續改版的檢測與問責機制，不是廠商自我宣稱，而是第三方公正驗證的結果。

效益・給目的事業主管機關

第二道防線：比實驗室更公正的督導者

1

分攤治理與稽核負擔

各目的事業主管機關無需逐案自行稽核，可仰賴具公信力的第三方檢測與問責機制。

2

扮演第二道防線

檢測實驗室收取開發商費用，難免有商業壓力；聯盟與 TAF 站在公正的角色，持續督導實驗室的檢測品質。

3

兼具「國際同步」與「產業公信」的檢測驗證量能

歷經十年運作、七次標準改版，建構與時俱進的常設資安防禦機制。

國際對照

臺灣不是在跟隨，部分面向已經領先

臺灣・MASA
2015 年（民國104年）推動至今

- 行動應用 App 基本資安規範 V1.5 。
- 檢測基準 V4.0，接軌 OWASP MASTG 。
- 20 家實驗室・近萬件標章實績。

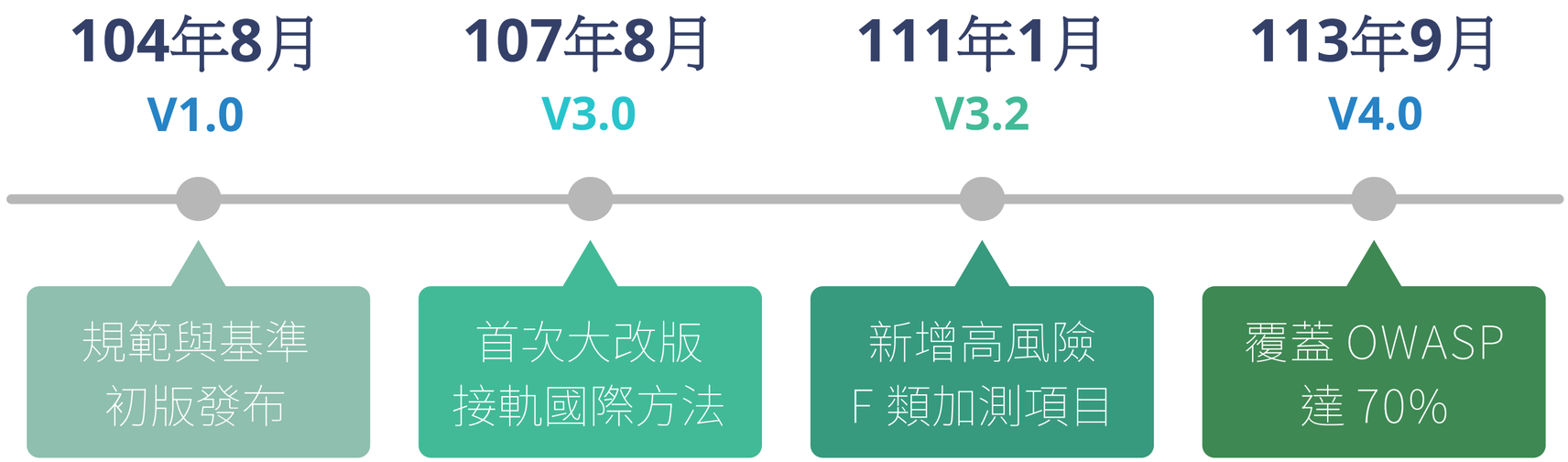
其他國家・參考做法
近年陸續推出 App 專屬資安指引

- 陸續發展 App 專屬資安指引與規範。
- 部分聚焦高風險交易類 App 防護。
- 多屬指引或建議性質，鼓勵業者自主導入。

臺灣行動應用 App 基本資安規範及檢測基準已參考 OWASP MASVS 等國際規範滾動式改版。

制度是活的

跟著威脅與國際標準，持續滾動修訂



＊ 制度自 104 年推動以來即持續滾動修訂，上列為近年之版本紀錄。

課程地圖

單元一回顧｜制度推動篇 - 理解制度的「為什麼」

從制度緣起、制度架構、推動成果、到我們的期待，並對照國際，建立宏觀的制度全貌

三單元課程地圖

單元一　本單元

制度推動篇

打造「全面性防禦」管理力

制度緣起、架構、標章與市場價值

單元二

規範解析篇

建構「開發即合規」防護力

Security by Design，把規範化為開發控制點

單元三

基準說明篇

落實「實驗室實戰」檢測實務

檢測項目、常見盲點與送驗前 Checklist

課程主軸　從「外部檢測」→ 到「開發即合規」　以主動防禦貫穿 App 研發全生命週期

行動應用資安聯盟
Mobile Application Security Alliance

十年淬一盾

打造「全面性防禦」管理力

讓每一個 App 標章，都值得被信任

感謝聆聽，敬請指教
行動應用資安聯盟
mas.org.tw

十年淬鍊．全面守護．值得信任