

課程名稱：18695_行動應用 App 資安標章全攻略#2 - 規範解析篇 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- 適合族群：
 - 軟體開發廠商（PM 與工程師）：需要了解如何在需求、設計與開發階段提前納入資安控制點（Shift Left/左移策略），避免最後送測時花費高昂重修成本。
 - 發案單位 / 業主 / SIA 大 PM：需要知道如何在 RFP 需求書中列出資安檢核點，並在關鍵時程提醒廠商或跨部門協調（如 Webview 網域、IT 憑證管理）。
- 能力門檻：[入門至普通] 適合具備基本專案管理觀念或軟體開發/維護經驗者，不需要深刻的資安黑客技術，重點在於流程與規範管理。

2. 課程核心大綱與架構圖

- 章節架構：
 - 單元二：規範解析篇（本課核心） — Security by Design 把規範化為控制點，建立開發及合規防護力。
 - Part 1：為什麼要開發集合規 — 介紹「資安左移（Shift Left）」概念，說明越晚修正資安問題成本越高的道理。
 - Part 2：開發及合規的 Checklist — 彙整訪談、開發前盤點之清單範本（資料許可權、身份與連線、套件、Webview 等）。
 - Part 3：實務案例分享 — 分享 10 大常見資安陷阱與落地實作（如敏感資料儲存、憑證繫結、第三方套件 CVE、注入攻擊、蓋板/懸浮遮罩防護、背景快照遮罩）。

3. 必備前置知識清單

- 軟體專案開發生命週期（SDLC）：了解需求、設計、開發、測試、上架與維運等基本階段。

- **基礎 APP/Web 架構觀念**：對 API、WebView、憑證（TLS/SSL）、第三方 SDK 有基本概念即可。

4. 專有名詞與概念辭典

- **資安左移（Shift Left）**：將原本放在專案最後階段（送測驗收）的資安檢測，提前挪到專案一開始的需求與設計階段，以大幅降低修正成本與時間。
- **WebView**：APP 內嵌網頁的形式，常適用於客服中心或活動頁；在資安檢測中，所有 WebView 導向的網域皆需進行掃描與盤點。
- **CVE（Common Vulnerabilities and Exposures）**：通用漏洞揭露資料庫，用於衡量第三方套件的漏洞風險，若套件 CVE 風險分數大於 7 分則不符合合規標準。

5. 課程學習職能對照

- **對應職能名稱**：資安專案經理（Security PM）、行動應用程式開發工程師（Mobile App Developer）、軟體品質保證（QA）。
- **主要工作任務/能力指標**：
 - **流程規劃與溝通**：能在專案計畫書或 RFP 中列出各階段的資安控制點（退場條件），協調跨部門網域與憑證事宜。
 - **資安規範落地**：能落實開發階段的安全編碼、第三方套件 CVE 清查、敏感資料防護（加密儲存與背景遮罩）及懸浮蓋板防護機制。