## 資訊系統分級與防護基準作業規定

# 由資安法規與金融產業經驗掌握 SSDLC 機制

撰文 | 叡揚資訊 資訊安全事業處

行政院資安辦於 2015 年 7 月底頒佈「資訊系統分級與防護基準作業規定」，其中最矚目的重點就在於對安全應用系統開發周期（SSDLC）的要求。

### 政府單位法規對 SSDLC 的要求重點

在這份規定中，對應用系統發展生命周期主要著墨於「系統與服務獲得」與「營運持續計畫」兩章節中，在需求階段系統以檢核表確認系統安全需求到開發階段的 OWASP TOP10 控制事項及源碼檢測，再從測試階段的弱點掃描安全檢測，到部署與維運階段的版本控制與變更，其實都可以藉由變更管理軟體、源碼檢測白箱軟體與版本管理的整合，達到全自動化的系統開發流程！

對資訊委外一節，將 SSDLC 的安全要求均納入委外合約為必要條件，建議機關與企業由弱點稽核為起步，再以長期合作關係，逐步要求委外廠商強化開發系統資安觀念與習性。

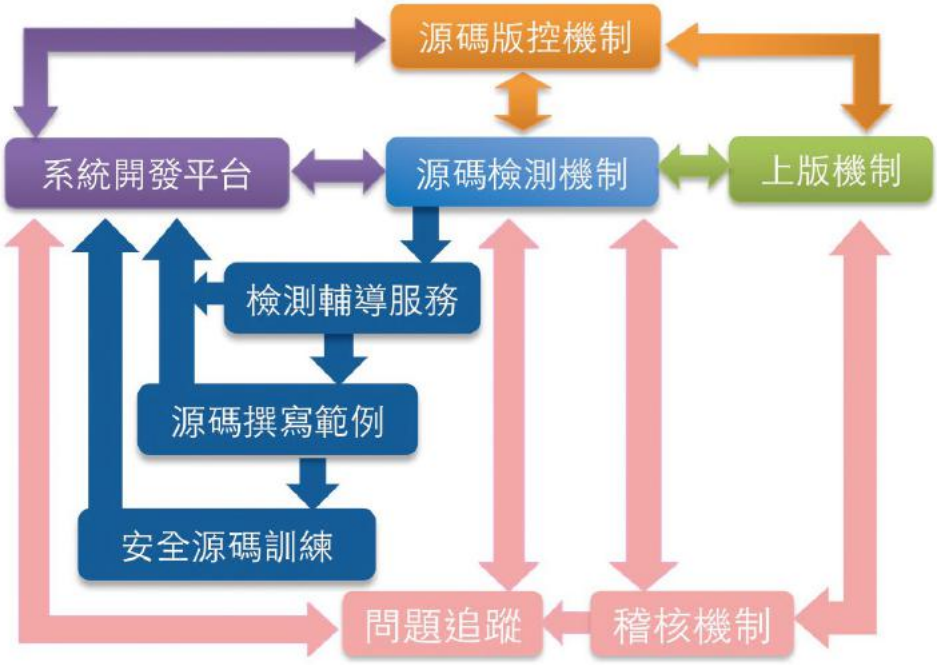
### SSDLC 的導入參考順序

雖然規定要求於維運階段須注意版本管理，其實版本管理機制貫穿全生命周期，從軟體開發初期到後續變更管理的不同版本差異分析，都與版控軟體脫不了關係。初期，除了導入應用系統弱點掃描（黑箱）工具與源碼檢測（白箱）工具，為不可或缺的資安把關工具外，源碼檢測工具與版控機制的整合，可以讓企業管控人員，清楚掌握源碼弱點修復的進度，同時確保上線軟體均經過完善資安體檢。


↑資訊系統防護基準分類：資訊系統安全等級分高、中、普 3 級；控制措施分為 7 大類 29 項。

政府機關委外發展或維護資訊系統規模不亞於民間企業，因此，委外廠商很可能為駭客頭號下手對象，再借道其應用系統漏洞著手破壞需求單位系統與竊取資料，需求單位對委外系統扮演稽核角色，當然機關部署的源碼檢測與版控機制，就是持續把關的最後一道防線。但應將防禦戰線延伸至委外廠商軟體開發流程中，

## SSDLC建議架構圖




委外廠商培養良好安全軟體開發習慣與源碼檢測機制，建立合作安全軟體供應鏈。

### 金融產業的導入經驗

因為主管機關合規要求，金融企業對資安機制的要求確實起步較早也較為嚴謹，惟不同企業導入 SSDLC 機制具些許差異性，仍可歸納出一致性的重點，摘述如下：

**SSDLC 整合骨幹** SSDLC 周期中，涉及許多工具，CI（Continuous Integration，持續整合）扮演核心整合平台的角色，Jenkins 為金融企業中普遍採用的一種 CI 工具。

**版本管理機制** 版本管理平台已為金融產業必備的平台，而政府機關這方面卻顯不足，採用 SVN 版控工具為較大宗，而近年 GIT 有明顯增加趨勢。

**源碼檢測（白箱）與弱點掃描（黑箱）工具** 黑白箱檢測工具已是金融企業必備的工具，同時整合上述工具，構成自動化檢測機制。由於近年來，對行動 APP 應用系統的黑白箱檢測需求有快速增加趨勢。

不分版本均可檢測：企業內部與委外廠商的應用系統開發環境版本差異，某些檢測工具與環境版本息息相關，造成系統檢測與建置時困擾，建議選擇不分版本均可檢測的工具。

**自動上版作法** 當應用系統風險已可完整監控時，上版流程自動化已成為精簡人力與減少人力疏失的利器，惟上版失敗復原及無瑕上版機制應謹慎規劃。

**變更管理** 營運期間，掌握需求變更項目對程式的衝擊程度，重要卻耗時耗力，金融銀行以需求變更系統與版控機制的整合，達成這個管理需求，同時利用版本系統的特性，動態掌握前後版程式更替情形，滿足主管機關合規要求。

更多客戶案例、資安資源 http://www.gss.com.tw/index.php/focus/security