|  |  |  |
| --- | --- | --- |
| 階段 | 評估項目 | 評估結果 |
| 需求 | 是否將資訊系統依資訊風險程度分級？ |  |
| 是否於資訊系統開發規格要求文件中載明相關資訊安全要求？ |  |
| 是否於保固維護合約中載明廠商之安全維護責任？ |  |
| 設計 | 是否進行資訊系統之風險分析？瞭解資訊系統之資產、威脅與弱點？ |  |
| 是否依據風險分析結果產出相關安全防護機制之安全設計文件？ |  |
| 開發 | 是否針對開發人員進行安全程式撰寫與安全防護機制設計文件之說明與訓練？ |  |
| 是否已將安全程式撰寫之指引文件化，並隨時供開發人員參考？ |  |
| 測試 | 在測試計畫中是否包含安全弱點及防護機制的安全測試項目？ |  |
| 安全測試項目是否包含所有安全需求與安全防護機制所提及的項目？ |  |
| 是否進行源碼檢測？ |  |
| 是否進行滲透測試？ |  |
| 是否清楚定義安全防護功能的驗收標準？ |  |
| 維運 | 是否針對應用系統執行之作業環境執行安全組態檢測？ |  |
| 是否定期更新及修補應用系統所執行之作業環境相關元件？ |  |
| 在程式變更後是不否確認其程式碼仍符合安全程式撰寫指引？ |  |
| 是否主動監控應用程式異常訊息？ |  |

SSDLC安全控制措施評估表