# 資訊委外之資安應注意事項檢查表

業務項目：

| 執行階段 | | 執行事項 | | 適用狀況(Y/N) | 執行結果(Y/N/NA) | 執行說明與日期 |
|---|---|---|---|---|---|---|
| 資訊服務供應商遴選 | 計畫作業 | 資訊委外可行性分析 | 篩選適合委託辦理之業務項目，確定該項業務委外之資通安全可行性。 | | | |
| | | | 將資安列入成本估算項目，進行效益分析。 | | | |
| | | | 評估資訊委外資安風險與對策。 | | | |
| | | 資訊委外專案編成 | 重要資訊系統委外開發案，專案成員中應有資安人員參與。 | | | |
| | | 資訊委外資安需求識別 | 委外業務涉及敏感性或含資安疑慮時，應識別委外廠商之限制。 | | | |
| | | | 視需要邀請廠商提出資安對應措施方案。 | | | |
| | 招標 | 招標文件之制訂與發布 | 採購產品或服務之資安要求事項。 | | | |
| | | | 明定資安要求事項之服務水準(如系統可用率、安全管控機制、稽核作業)。 | | | |
| | | | 未符合資安要求事項或服務水準時，應訂定罰責標準，依損害程度向委外廠商進行求償或罰款。 | | | |
| | | 保密協議書之準備。 | | | | |
| | | 委外廠商遴選準則之定義與實作 | 委外廠商之資安能量，評估委外廠商過度集中之風險及因應措施。 | | | |
| | | | 委外廠商允許機關或經授權之第三方稽核，以確認所定義資安要求事項之遵循性。 | | | |
| | | | 委外廠商對其產品或服務之資安管理機制。 | | | |

| 執行階段 | | 執行事項 | | 適用狀況(Y/N) | 執行結果(Y/N/NA) | 執行說明與日期 |
|---|---|---|---|---|---|---|
| | | 評估委外廠商位置與提供產品或服務之位置，對資安是否有不利影響。 | | | | |
| 資訊服務供應商管理 | 決標 | 委外協議之最終確認與簽署 | 載明金融機構與委外廠商雙方之資安角色與責任。 | | | |
| | | | 確認資通事件之通報流程及處理程序。 | | | |
| | | | 確認軟體(含元件)之使用版權及安全性。 | | | |
| | | | 若有分包，確認分包計畫可能產生之資安風險。 | | | |
| | | | 廠商提供之優規產品或服務，仍需確認可能產生之資安風險。 | | | |
| | 履約管理 | 委外關係管理與監督 | 金融機構與委外廠商皆應指定專案負責人，負責督導及辦理各項資安要求事項。 | | | |
| | | | 持續識別資訊委外風險，並採取適當控制措施。 | | | |
| | | | 監督廠商於人員、實體環境及資訊委外管理等資安要求事項是否落實執行。 | | | |
| | | | 組織應適時確認委外相關作業人員具備適當之資通安全教育訓練，充分了解組織所要求之資安政策及責任。 | | | |
| | 驗收程序 | 顧問訓練類 | 確認使用檢測工具的安全性和教育訓練時安裝軟體的安全性。 | | | |
| | | 系統發展類 | 要求委外廠商揭露第三方程式元件之來源與授權。 | | | |
| | | | 要求委外廠商提供資通系統之安全性檢測證明(如源碼檢測、弱點掃瞄或滲透測試等)。 | | | |

| 執行階段 | | 執行事項 | | 適用狀況(Y/N) | 執行結果(Y/N/NA) | 執行說明與日期 |
|---|---|---|---|---|---|---|
| | | 維運管理類 | 每年定期執行系統弱點掃描。 | | | |
| | | 雲端服務類 | 確認雲端服務供應商宣稱之資安認證範圍(含功能及服務水準)。 | | | |
| | 保固 | 保固服務 | 組織應確認若發生系統異常之排除管道暢通，避免造成系統服務中斷或無法正常運作。 | | | |
| | | 異常管理 | 系統若有重大問題，應有變更計畫，評估潛在資安衝擊及提供變更及復原程序。 | | | |
| 資訊服務供應商終止與解除 | 委外關係終止 | 委外關係終止 | 產品或服務之移轉程序 | | | |
| | | | 資訊資產及資料之歸還、轉交或銷毀機制。 | | | |
| 其他 | 籌獲套裝軟體時，應確認可能產生之資安風險。 | | | | | |
| | 資訊委外服務案中，委外廠商有須結合第三方服務提供者(Third-party Service Provider,TSP)方能提供完整服務之情形，應將 TSP 可能產生之資安風險納入評估。 | | | | | |