附件 1　政府資訊委外資安注意事項或常見缺失

本附件說明政府資訊委外資安常見之疏漏與應注意之事項。將依據經常發生資安情事之「計畫作業」、「履約管理」及「驗收」階段分別描述。

1. 計畫作業階段

●專案編成

常見缺失在於專案編組不恰當或專業人力不足，此時應適時向資安主管反映，以明確律定各單位權責，並應儘量爭取經費以安排適當之教育訓練課程提升專業能力，或外聘顧問解決專業人力不足問題。

●資安風險評估

各單位經常未確實評估潛在風險或虛應故事，導致廠商提出對應措施建議方案未能解決資安風險，也產生資訊安全服務水準未能明確定義的現象，進而衍生後續的安全問題與採購作業之糾紛。建議參閱「資通系統風險評鑑參考指引」確實評估潛在風險。

●廠商提出對應措施方案

常見之缺失在於無法有效評鑑廠商提出對應措施建議方案是否符合需要，對於複雜或大型資訊專案之解決方法是遵循 RFI (Request for Information)、RFC(Request for Comment)、RFP(Request for Proposal)之作業程序，配合廠商相互競爭之實況提升對應措施建議方案之品質，對於簡單或小型資訊專案則宜外聘顧問協助審查。

●建立資訊委外資安管理制度

常見缺失在於建立資訊委外資安管控制度時，僅是抄襲 CNS/ISO/IEC 27001 內容或其他單位之文件，未能依據作業程序確實建立符合單位實況

之資通安全管理制度。

●資通安全服務水準定義

常見缺失在於資通安全服務水準定義不當或不明確。解決方法是先確實評估潛在風險，然後遵循 RFI、RFC 及 RFP 之作業程序辦理。

●資訊委外服務契約項目規劃：同上。

2. 履約管理

●執行契約規範項目

常見缺失在於未能依據合約與 RFP 要求，確實執行契約規範項目。

●採行控制措施 ：同上。

●新系統上線作業審查措施

常見缺失在於未能確實執行新系統上線作業審查，並依相關作業程序辦理。

●資安事件之反應與處理

常見缺失在於發生資安事件時隱匿不報，建議於單位資通安全管理規定中訂定適當獎懲措施，以建立資安作業紀律，並定期或不定期實施演練。

●營運持續管理

常見缺失在於營運持續管理計畫未依據實際狀況修訂，或事件發生時無法有效執行，建議定期或不定期實施演練。

●緊急應變計畫檢查缺失的改善

常見缺失在於未能確實追蹤管制缺失改善情形。

3. 驗收階段

- 定期評估與稽核廠商安全控管績效

  常見缺失在於未能確實執行定期評估與稽核廠商安全控管績效。

- 會議與文件資料

  常見缺失在於會議與文件資料建立不確實或不完整，建議委請第三方協助解決專業與人力不足問題。

- 軟體委外開發稽核

  常見缺失在於軟體委外開發稽核能力不足，建議委請第三方解決專業與人力不足問題。

- 異動稽核措施是否符合預期效能

  常見缺失在於未能確實執行異動稽核措施。

4. 綜合而言，完備政府資訊委外資通安全最重要的是：

- 確實評估潛在風險，才能找出資通安全需求。
- 依據資通安全需求建立資訊委外安全管控制度與資安計畫。
- 依據資通安全需求與單位現行 ISMS 制度，配合資訊委外作業程序之 RFI、RFC 及 RFP 各項步驟訂定適切之資通安全服務水準，並納入契約與 RFP 規範。
- 依據資訊委外資安管控措施確實執行稽核與改善措施。