



採購規範書

(A522001790)

1. 目的/用途說明：

網路詐騙通報查詢網為是依「詐欺犯罪危害防制條例」所開發之系統，為確保系統維運的資訊安防護，規劃委託通過認證之資訊安全驗證機構（Certification Body，以下簡稱驗證機構）針對系統辦理正式驗證前之階段審查（Stage Review）並提出查核報告。

本案受查之資訊安全管理制度（ISMS）尚在建置中，廠商應依入場時之實際建置現況執行查核，以鑑別本單位掌握已建置部分之符合情形及正式驗證前尚須完成之事項，作為後續正式驗證審查之參考。

2. 品名：網路安全及資安維運相關服務(系統資訊安全驗證前階段審查)

3. 採購服務規格：

No	品項	需求說明
1	系統資訊安全驗證前階段審查	- 由驗證機構針對網路詐騙通報查詢網民眾端網站辦理 ISO/IEC 27001:2022 正式驗證前之階段審查作業，並提供階段審查報告。受查 ISMS 尚在建置中，查核範圍以入場時已完成之制度、文件與控制措施為準。 - 提供階段審查服務，並包含以下項目： - 文件審查：審閱資通安全法規遵循情形、計畫負責單位之資訊安全規範及現有 ISMS 文件化資訊，包括資安政策、程序書、SOP、範圍書、適用性聲明（SoA）、資產清單、風險評鑑報告等，就已完成之文件確認其符合性。 - 符合性查核與落差認定：依 ISO/IEC 27001:2022 條文 4 至 10 及附錄 A 控制措施，逐項查核現行管理制度與控制措施之符合情形，列明查核發現（Findings）與觀察項目，並依其對正式驗證之影響程度區分優先等級。 - 現場抽樣查證：就系統之資產管理、風險評鑑與處理、存取控制、營運持續、事件管理等已實際運作之領域進行現場抽樣查證，透過訪談與紀錄查閱確認制度落實情形；就尚未建置或尚未累積執行紀錄之領域，列舉查核發現。

4. 執行期間：簽約日至115年11月30日止。

5. 廠商交付文件：■有 □無

(1) 階段審查報告一式（以電子檔方式提供），須經主導稽核員簽署

(2) 說明會議簡報(以電子檔方式提供)

6. 驗收標準：依「需求說明」、「廠商交付文件」及合約期間業主交付之需求事項與相關交付成果等進行驗收。



7. 付款標準：交付完相關文件及說明會議完成後，支付100%款項。
8. 訓練：☒有 ☐無
 - (1) 報告提供後需辦理差異查核結果說明會議一場，就審查發現、待辦事項清單及正式驗證審查流程進行說明。
9. 保固：☐有 ☒無
10. 服務：☐有 ☒無
11. 廠商資格：投標廠商須為資通安全管理法中經財團法人全國認證基金會（TAF）認證的ISMS公正第三方驗證機構，並應檢附有效認證證書影本；執行本案之審查人員(須為本案驗證機構的全職員工並檢附勞、健保證明文件)須具備 ISO/IEC 27001 主導稽核員（Lead Auditor，具備由ISO 17024人員驗證機構核發的人員驗證證書）資格及CISSP、CCA或同等或以上的資通安全專業證照(共二張)，並檢附資格證明。廠商應於投標文件中聲明本案之執行不影響其依 ISO/IEC 17021-1與ISO 27006-1 承接本系統後續正式驗證之資格。