<table>
<tr><td>項目</td><td colspan="3">(五) 資通系統或服務委外辦理之管理措施</td></tr>
<tr><td>5.4</td><td colspan="3">委外廠商執行委外作業時，是否確保其具備完善之資通安全管理措施或通過第三方驗證？開發維運環境之資通安全管理進行評估？</td></tr>
<tr><td rowspan="3">稽核依據</td><td colspan="2">資通安全管理法施行細則第 4 條</td><td>L1110082304</td></tr>
<tr><td colspan="2">資通安全管理法施行細則第 6 條：資通安全維護計畫應包括資通系統或服務委外辦理之管理措施</td><td>P11</td></tr>
<tr><td colspan="3">1. 資通安全管理法第 9 條：應考量、選任受託者，並監督其資通安全維護情形。
2. 通安全管理法施行細則
（1） 第 4 條第 1 項第 1 款：受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證
（2） 第 4 條第 1 項第 2 款：受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
（3） 第 6 條第 1 項第 11 款：資通系統或服務委外辦理之管理措施</td></tr>
<tr><td>稽核重點</td><td>資訊委外廠商之評選機制</td><td>佐證資料</td><td>投標廠商之資安管理要求、投標廠商專業能力或開發環境之需求資格、資訊作業委外安全管理程序文件、契約書</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 了解機關資訊作業委外安全管理程序。
3. 了解委外作業流程（委外前、中、後）之安全管理措施及監督內容。
4. 了解機關委外資訊業務項目，進一步抽樣檢視近 1 年訂定之契約，是否有相關要求。
5. 機關對委外廠商資安能力的評估機制及實際執行方式。[整併 5.7]
6. 重要資通系統之委外廠商，對其開發維運環境之資安管理進行評估，可參照資通系統籌獲各階段強化措施之廠商自我管理作業資安評估表。
7. 可參考行政院 111 年 5 月 26 日院臺護字第 1110174630 號函訂定「資通系統籌獲各階段資安強化措施」</td></tr>
</table>

FQA	1. [FAQ6.5]廠商的管理措施是否「完善」，係視機關委外業務之防護需求及等級而定。機關可在招標文件中述明，以作為選商的評判依據。另外，前述防護需求所需之「完善」管理措施，建議可參考資訊安全管理系統國家標準 CNS27001 或 ISO27001 之管理要求及相關資安法規之要求據以審視之；至於機關內部之單位權責分工議題，原則尊重各機關之內部行政作業與文化而定，但考量本項工作仍需仰賴資安專業，建議機關之資訊單位及資安專職人力應統籌扮演跨單位統籌及規劃之角色。
	2. [FAQ6.6]建議先查明廠商通過之第三方驗證範圍（包含人員、資安管理作業程序、資通系統、實體環境）是否已涵蓋貴機關委外之業務，另外以稽核方式確認受託業務之執行情形，確認前述第三方驗證通過及維運狀況。另外建議委託機關應先於招標文件敘明委託業務須通過第三方驗證及接受查核之要求，避免履約爭議。