列管軍品廠商資格級別認證評鑑基準表

評鑑項目：柒、資通安全管理維護紀錄或稽核結果報告

<table>
<tr><th colspan="2">列管軍品廠商資格級別評鑑基準</th></tr>
<tr><td>評鑑項目</td><td>評　分　基　準　說　明</td></tr>
<tr><td>資通安全管理維護紀錄或稽核結果報告
（10 分）</td><td>
為符合行政院訂頒「資通安全管理法」及相關子法、國防部訂頒「國軍資訊安全政策」與保密及資安規定，以及台灣電腦網路危機處理暨協調中心(TWCERT/CC)所定「強化網路資安事件通報應變與橫向協調作業機制民間企業組織/產業公會 CSIRT 建置實務指引」等相關規範及程序，並參據「資通安全責任等級分級辦法」相關應辦事項，製訂下列評分方式。
※本評鑑項目分數計算方式及注意事項
一、依廠商所提出資料，本評鑑項目的第一款至第五款內，採計各項目之表格內所對應最高分數，各項目內之分數不重複計算或相加計算。再將各項目得分相加後，即為本評鑑項目原始得分。
二、依據「列管軍品廠商資格級別評鑑基準表」之級別規定，申請廠商於「科技水準」評鑑事項，其技術備便水準(TRL)等級，至少須達第六級，始得評鑑其級別為甲級、乙級或丙級。因此如果申請廠商於「科技水準」所提供之技術備便水準資料屬第一級至第五級(TRL1~TRL5)，或未提供技術備便水準佐證資料，應自本評鑑項目之原始總分中扣除 3 分，所得分數方為總得分。
三、本評鑑項目實際分數在 10 分為 A、未達 10 分為 B。

第一款、 內部資通安全防護規定及制度
視列管軍品相關系統（含資訊科技(IT)安全與作業科技(OT)安全）及維運管理，導入資通安全管理制度（ISO 27001 或 CNS27001），完成公正第三方驗證並持續維持其驗證有效性者，或自行訂定資通安全防護規範並檢附相關執行佐證資料等項目。

<table>
<tr><th>項目</th><th>配分</th></tr>
<tr><td>未訂定資通安全防護規範。</td><td>0</td></tr>
<tr><td>自行訂定資通安全防護規範及檢附執行佐證。</td><td>1</td></tr>
<tr><td>已導入資通安全管理制度，惟未完成第三方驗證者。</td><td>2</td></tr>
<tr><td>已導入資通安全管理制度及通過第三方驗證，惟未維持其驗證有效性者。</td><td>3</td></tr>
<tr><td>已導入資通安全管理制度，完成公正第三方驗證，並持續維持其驗證有效性。</td><td>4</td></tr>
</table>
</td></tr>
</table>

第二款、 資通安全維護設施建置及運用

檢視列管軍品相關系統，依是否連接網際網路、提供資訊網路及設備架構圖、訂定主機、個人電腦或儲存媒體（硬碟、USB 及磁帶等）相關管理規範、安裝防毒軟體及進行資安檢測等項目。

區分	項目	配分
系統未連接網際網路	未提供資通安全維護設施建置及運用資料。	0
	提供資訊網路及設備架構圖。	1
	訂定主機、個人電腦或儲存媒體(硬碟、USB及磁帶等)相關管理規範、安裝防毒軟體等。	2
系統連接網際網路	未提供資通安全維護設施建置及運用資料。	0
	提供資訊網路及設備架構圖，並訂有主機、個人電腦或儲存媒體(硬碟、USB及磁帶等)相關管理規範，以及安裝防毒軟體等。	1
	除前項並於年度內實施弱點掃描或資安健診者並對漏洞進行修補者。	2

第三款、 資通安全維護實際執行情形及成效

檢視「資通安全責任等級分級辦法」附件一資通安全責任等級 A 級之公務機關應辦事項相關執行佐證（含內部稽核、營運持續演練、安全檢測、資安健診、軍品相關系統人員資安內訓 3 小時、取得資安專業證照等）。

項目	配分
年度內上揭應辦事項執行未達 2 項者。	0
年度內上揭應辦事項 3 項（含）有執行佐證者。	1
年度內上揭應辦事項 6 項均有執行佐證者。	2

※有關資通安全事件分級係依據行政院訂頒「資通安全事件通報及應變辦法」第二條規定認列。

第四款、 歷史資通安全防護不良紀錄及後續維護紀錄，或政府機關（構）稽核報告結果

檢視近 3 年資安事件、或內、外部稽核改善作為、方式及成果佐證，或政府機關（構）稽核報告缺失改善已獲准備查等。

項目	配分
近 3 年資安事件、或內、外部稽核改善作為、方式及成果佐證，或政府機關（構）稽核報告缺失改善已獲准備查等佐證資料未改善。	0
近 3 年資安事件、或內、外部稽核改善作為、方式及成果佐證，或政府機關（構）稽核報告缺失改善已獲准備查等佐證資料完整。	1

	第五款、 其他與資通安全管理維護紀錄或稽核結果報告有關之重要事項 精進資通安全防護措施（如管理面、技術面或認知與訓練等）著有成效者 1 分；無相關事績者 0 分。

項目	配分
無資安防護特別措施或成效。	0
精進資通安全防護措施著有成效者。	1