

# 列管軍品廠商資格級別認證評鑑評分表

評鑑項目：資通安全管理維護紀錄或稽核結果報告(產製)

列管軍品廠商資格級別評鑑基準																			
評鑑項目	評 分 基 準 說 明																		
資通安全管理維護紀錄或稽核結果報告(10分)	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。 <b>※本評鑑項目分數計算方式及注意事項</b> 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，即為本評鑑項目得分。 二、本評鑑項目得分 10 分為 A、未達 10 分為 B。  第一款、 <u>內部資通安全防護規定及制度</u> 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)及維護管理，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 border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 10px;"> <thead> <tr> <th style="width: 70%;">項目</th> <th style="width: 10%;">配分</th> <th style="width: 20%;">勾選</th> </tr> </thead> <tbody> <tr> <td>未訂定資通安全防護規範。</td> <td style="text-align: center;">0</td> <td></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 style="text-align: center;">1</td> <td></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 style="text-align: center;">2</td> <td></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 style="text-align: center;">3</td> <td></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 style="text-align: center;">4</td> <td></td> </tr> </tbody> </table> 補充說明：		項目	配分	勾選	未訂定資通安全防護規範。	0		自行訂定資通安全防護規範及檢附執行佐證。	1		已導入資通安全管理制度，惟未完成第三方驗證者。	2		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。	3		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。	4
項目	配分	勾選																	
未訂定資通安全防護規範。	0																		
自行訂定資通安全防護規範及檢附執行佐證。	1																		
已導入資通安全管理制度，惟未完成第三方驗證者。	2																		
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。	3																		
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。	4																		

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	勾選
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	

補充說明：

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	勾選
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	

補充說明：

※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

檢視近三年資安事件、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	勾選
近三年資安事件、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	
近三年資安事件、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	
補充說明：		

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	勾選
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	
補充說明：		

評鑑委員：

簽 署

年 月 日