風險值計算工具操作手冊 Excel 2007 版

一.請填入項次、部門、保管人、說明、資訊及資通系統資產、資產類別、數量、機密性、完整性、可用性、威脅、脆弱性、安控前的威脅等級及安控前的脆弱等級，分述如下：

1. 項次：請填註項次序。
2. 部門：請填註該項資訊及資通系統資產保管(擁有者)部門
3. 保管人：請填註該項資訊及資通系統資產保管人
4. 說明：請填註資訊及資通系統資產之用途、使用之系統，如 Windows 2000 應用系統伺服器。
5. 資訊及資通系統資產：請填註該項資訊及資通系統資產名稱。
6. 資產類別：請透過下拉式選單方式選取或自行鍵入。
7. 數量：請填註該項資訊及資通系統資產數量。
8. 機密性、完整性、可用性：請透過下拉式選單方式選取普、中或高。
9. 威脅及脆弱性：請透過下拉式選單方式選取或自行鍵入。
10. 資產類別、威脅及脆弱性選取方式：先選擇資產類別，再選擇威脅，最後選取脆弱性。如果沒有依此順序選擇，則下拉式選單將不會出現任何選項。例如必須先選擇資產類別中的資訊記錄，威脅下拉式選單才會出現資訊記錄的對應威脅項目，如火災；選擇威脅中的火災後，脆弱性才會出現火災的對應項目。

二.資訊及資通系統資產價值評定方式有相加、相乘、取最大值等等，本工具採取最大值，亦即資訊及資通系統資產價值為機密性、完整性與可用性之最大值。

1. 資訊及資通系統資產價值 = (機密性、完整性、可用性)最大值。
2. 機密性、完整性、可用性下拉式選單內容分為普、中及高，普的分數為 1、中的分數為 2 及高的分數為 3。

三.安控前的風險值為安控前的威脅等級、安控前的脆弱等級及資訊及資通系統資產價值之乘積，計算公式如下:

1. 安控前的風險值 = 安控前的威脅等級 * 安控前的脆弱等級 * 資訊及資通系統資產價值
2. 安控前的風險等級取決於安控前的風險值，分為普、中及高，分級基準如下：
   (1)安控前的風險值 小於等於 6 為普
   (2)安控前的風險值 大於 6，小於等於 12 為中

(3)安控前的風險值 大於 12，小於等於 27 為高

四.本工具對等級之劃分採 3 分法；資訊及資通系統資產價值採最大值法；風險值採乘積法，各單位可依需求修正本工具為符合貴單位之方式

五.各機關於執行安全控制措施後，請填註風險降低原因說明、安控後的威脅等級安控後的脆弱等級

六.安控後的風險值取決於安控後的威脅等級、安控後的脆弱等級及資訊及資通系統資產價值之乘積，計算公式如下:

1. 安控後的風險值 = 安控後的威脅等級 * 安控後的脆弱等級 * 資訊及資通系統資產價值
2. 安控後的風險等級取決於安控後的風險值，分為普、中及高，分級基準如下：

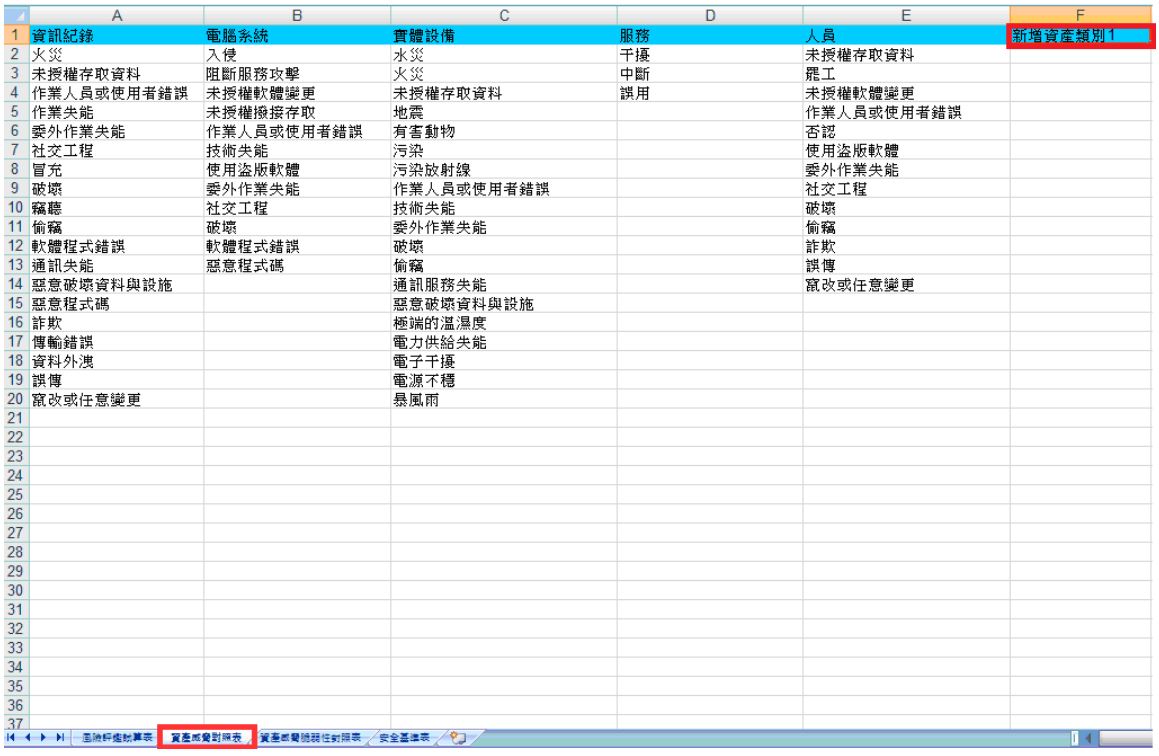
(1)安控後的風險值 小於等於 6 為普

(2)安控後的風險值 大於 6，小於等於 12 為中

(3)安控後的風險值 大於 12，小於等於 27 為高

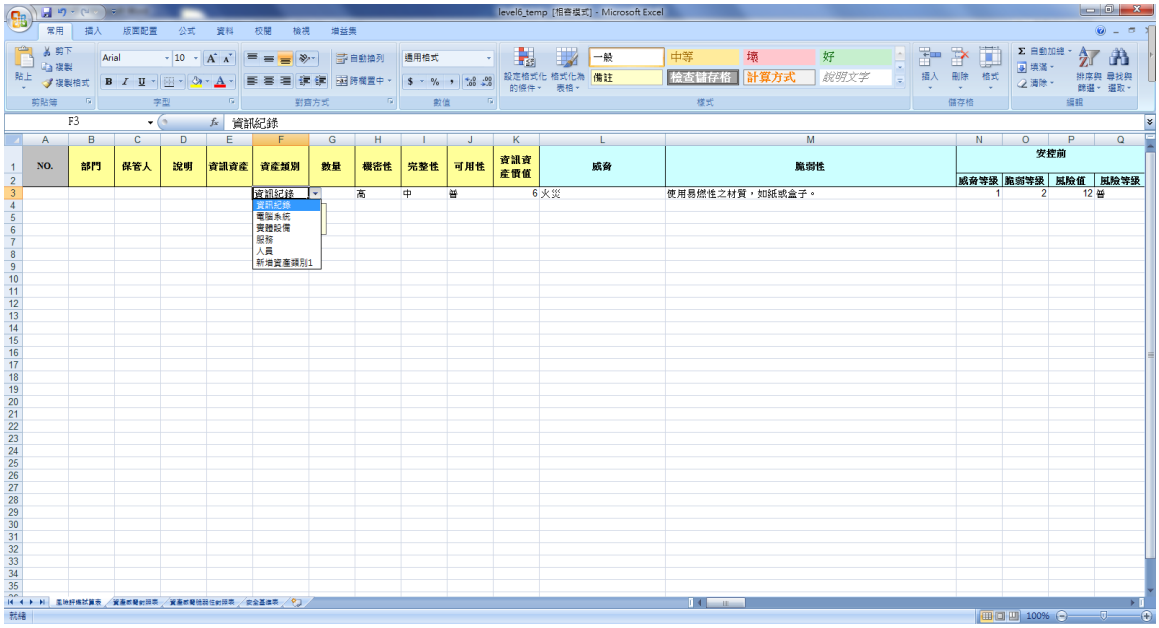
七.若風險評鑑試算表的資產類別不敷使用時，可以自行擴充。步驟如下：

1. 在資產威脅對照表之空白欄位，新增欲擴充的資產類別項目，如在 F1 欄位填註新資產類別項目”新增資產類別 1”，如下圖。



	A	B	C	D	E	F
1	資訊紀錄	電腦系統	實體設備	服務	人員	新增資產類別1
2	火災	入侵	水災	干擾	未授權存取資料	
3	未授權存取資料	阻斷服務攻擊	火災	中斷	罷工	
4	作業人員或使用者錯誤	未授權軟體變更	未授權存取資料	誤用	未授權軟體變更	
5	作業失能	未授權撥接存取	地震		作業人員或使用者錯誤	
6	委外作業失能	作業人員或使用者錯誤	有害動物		否認	
7	社交工程	技術失能	污染		使用盜版軟體	
8	冒充	使用盜版軟體	污染放射線		委外作業失能	
9	破壞	委外作業失能	作業人員或使用者錯誤		社交工程	
10	竊聽	社交工程	技術失能		破壞	
11	偷竊	破壞	委外作業失能		偷竊	
12	軟體程式錯誤	軟體程式錯誤	破壞		詐欺	
13	通訊失能	惡意程式碼	偷竊		誤傳	
14	惡意破壞資料與設施		通訊服務失能		竄改或任意變更	
15	惡意程式碼		惡意破壞資料與設施			
16	詐欺		極端的溫濕度			
17	傳輸錯誤		電力供給失能			
18	資料外洩		電子干擾			
19	誤傳		電源不穩			
20	竄改或任意變更		暴風雨			

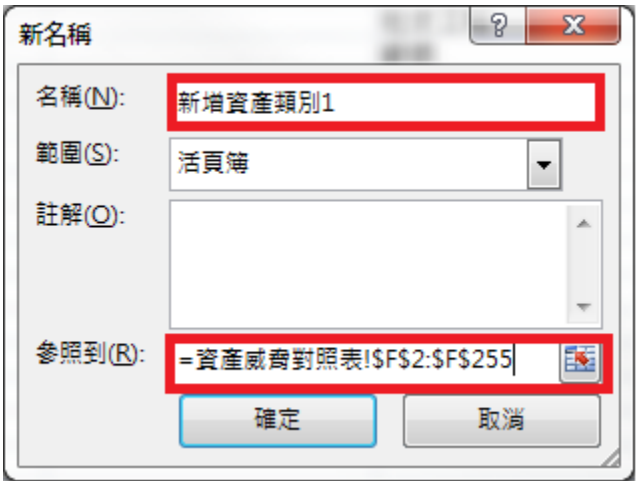
2. 完成新增資產類別項目後，風險評鑑試算表中的資產類別下拉式選單會列出新增的項目，新增資產類別 1。



3. 定義新增資產類別 1 之範圍。

(1)點選公式->定義名稱->定義名稱

(2)輸入名稱與參照範圍



(3) 在新增資產類別 1 下方擴充欲增加之項目，如新增威脅 1、新增威脅 2

	A	B	C	D	E	F
1	資訊紀錄	電腦系統	實體設備	服務	人員	新增資產類別1
2	火災	入侵	水災	干擾	未授權存取資料	新增威脅1
3	未授權存取資料	阻斷服務攻擊	火災	中斷	罷工	新增威脅2
4	作業人員或使用者錯誤	未授權軟體變更	未授權存取資料	誤用	未授權軟體變更	
5	作業失能	未授權撥接存取	地震		作業人員或使用者錯誤	
6	委外作業失能	作業人員或使用者錯誤	有害動物		否認	
7	社交工程	技術失能	污染		使用盜版軟體	
8	冒充	使用盜版軟體	污染放射線		委外作業失能	
9	破壞	委外作業失能	作業人員或使用者錯誤		社交工程	
10	竊聽	社交工程	技術失能		破壞	
11	偷竊	破壞	委外作業失能		偷竊	
12	軟體程式錯誤	軟體程式錯誤	破壞		詐欺	
13	通訊失能	惡意程式碼	偷竊		誤傳	
14	惡意破壞資料與設施		通訊服務失能		竄改或任意變更	
15	惡意程式碼		惡意破壞資料與設施			
16	詐欺		極端的溫濕度			
17	傳輸錯誤		電力供給失能			
18	資料外洩		電子干擾			
19	誤傳		電源不穩			
20	竄改或任意變更		暴風雨			

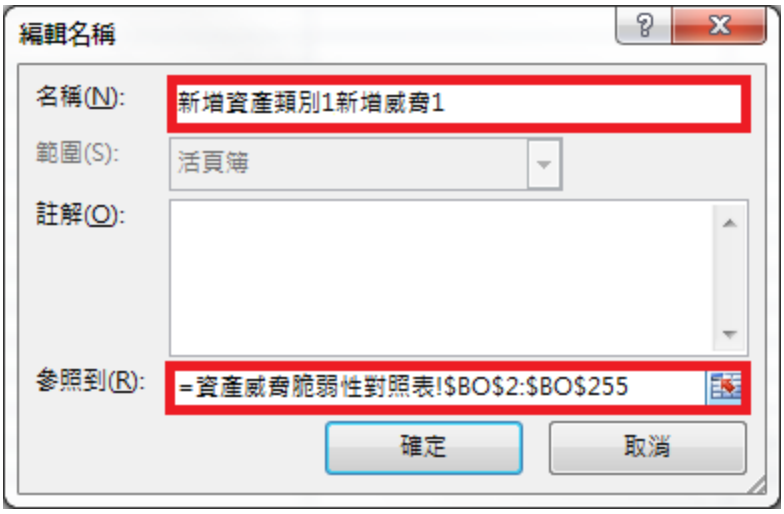
(4) 定義新增資產類別 1 之新增威脅 1 範圍。

A.請於資產威脅脆弱性對照表之空白欄位，如 BO1 輸入新增資產類別 1_新增威脅 1。

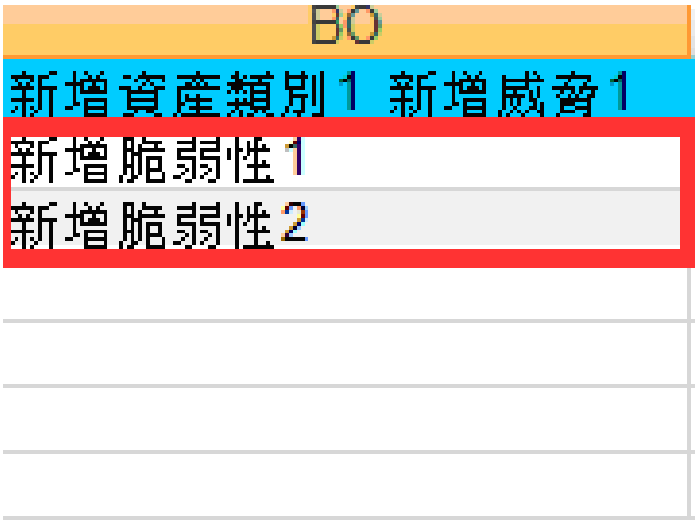
BO
新增資產類別1_新增威脅1

B.點選公式->定義名稱->定義名稱

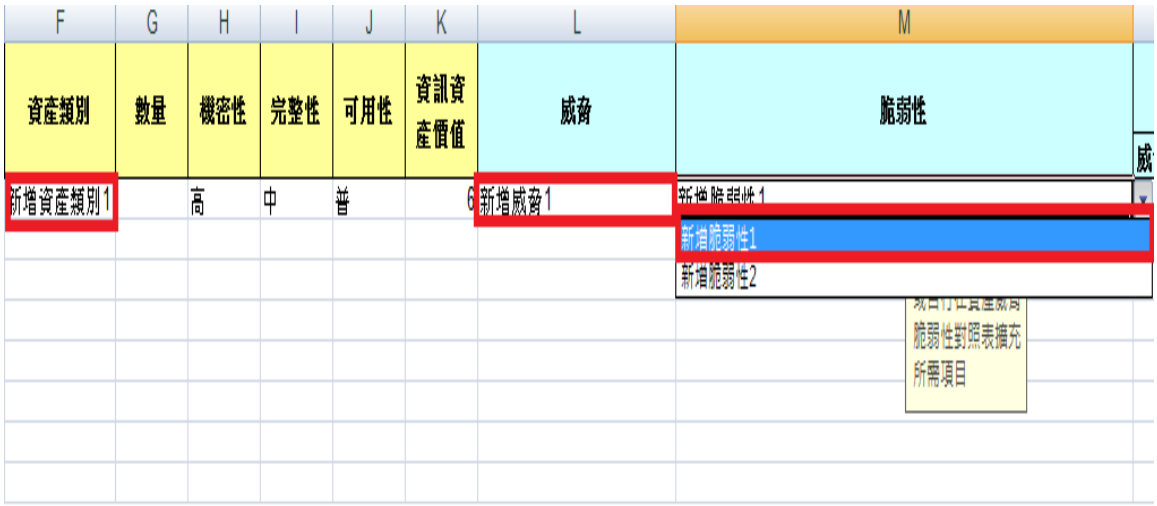
C.輸入名稱與參照範圍(名稱中請勿使用特殊符號)



D.在新增威脅 1 下方擴充欲增加之脆弱性，請於資產威脅脆弱性對照表之空白欄位，如 BO2 與 BO3 輸入新增脆弱性 1 與新增脆弱性 2。



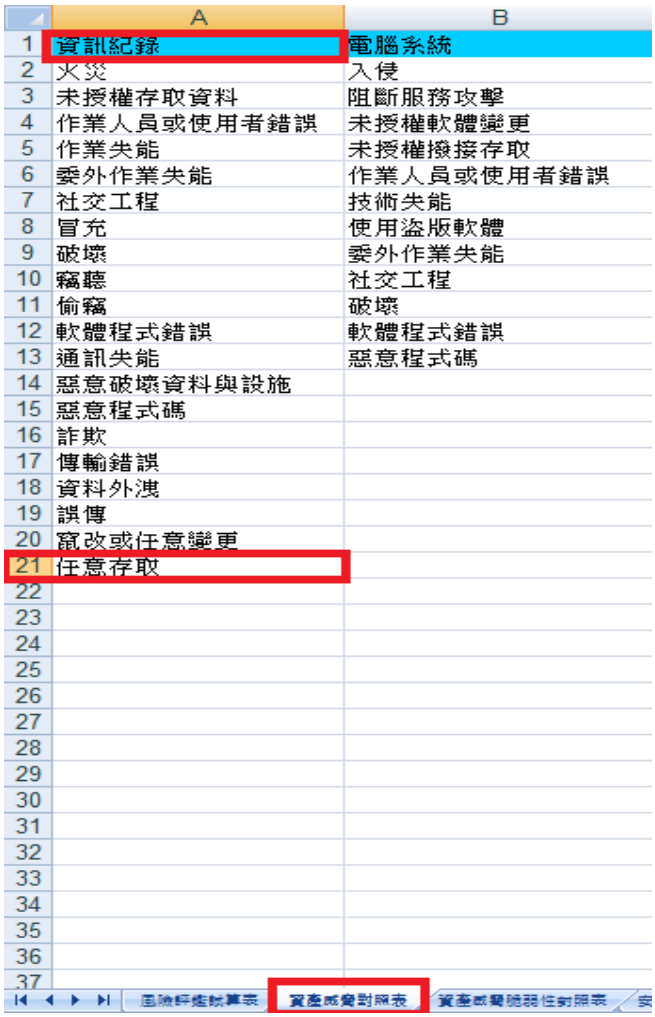
(4)選取已擴充之新增資產類別 1 之新增威脅 1 之新增脆弱性 1，如下圖:



4. 餘類推。

八.若資產類別的威脅項目不敷使用時，可以自行擴充。步驟如下：

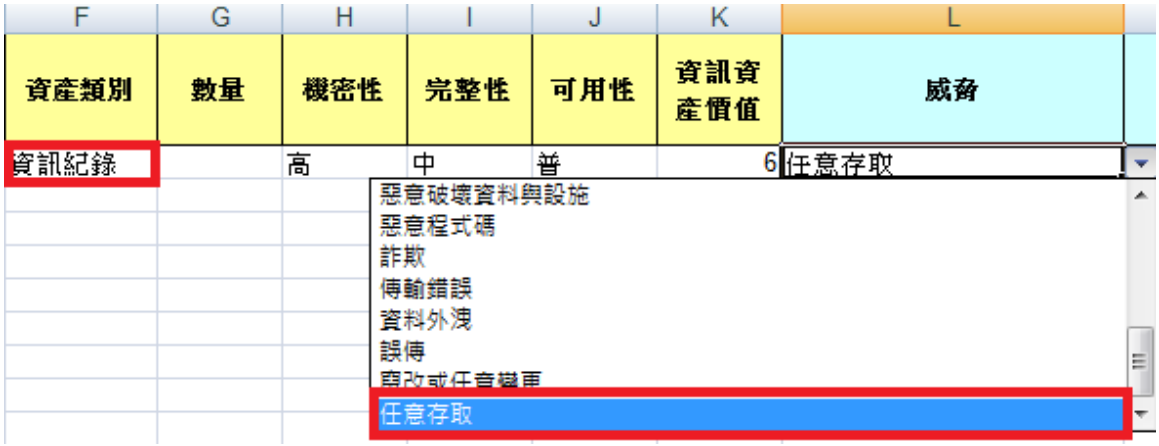
1. 在欲新增威脅之資產類別下方新增所需之威脅，如在資訊記錄的下方增加任意存取，即在資產威脅對照表中的 A21 欄位輸入任意存取，如下圖：



	A	B
1	資訊紀錄	電腦系統
2	火災	入侵
3	未授權存取資料	阻斷服務攻擊
4	作業人員或使用者錯誤	未授權軟體變更
5	作業失能	未授權撥接存取
6	委外作業失能	作業人員或使用者錯誤
7	社交工程	技術失能
8	冒充	使用盜版軟體
9	破壞	委外作業失能
10	竊聽	社交工程
11	偷竊	破壞
12	軟體程式錯誤	軟體程式錯誤
13	通訊失能	惡意程式碼
14	惡意破壞資料與設施	
15	惡意程式碼	
16	詐欺	
17	傳輸錯誤	
18	資料外洩	
19	誤傳	
20	竄改或任意變更	
21	任意存取	
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		

風險評鑑結算表 | 資產威脅對照表 | 資產威脅與弱點對照表

2. 在資產威脅對照表的資訊記錄威脅下拉式選單中，即出現資訊記錄新增的威脅-任意存取，如下圖:



F	G	H	I	J	K	L
資產類別	數量	機密性	完整性	可用性	資訊資產價值	威脅
資訊紀錄		高	中	普	6	任意存取

惡意破壞資料與設施
惡意程式碼
詐欺
傳輸錯誤
資料外洩
誤傳
竄改或任意變更
任意存取

3. 再依照新增脆弱性方式於資產威脅脆弱性對照表中增列相對應之脆弱性。

九. 若威脅的脆弱性項目不敷使用時，可以自行擴充。步驟如下：

1. 在欲新增脆弱性之威脅下方新增所需之脆弱性，如在資產威脅脆弱性對照表擴充「資訊記錄」中「火災」的「延長線過載」脆弱性項目，即資產威脅脆弱性對照表中的 A3 欄位輸入延長線過載，如下圖：

2. 在風險評鑑試算表的資訊記錄中火災威脅的脆弱性下拉式選單中，即出現火災威脅新增的脆弱性，延長線過載，如下圖：

一〇. 資訊及資通系統資產類別、威脅及脆弱性最多可支援 255 個項目。