資訊資產 D009 威脅及弱點風險發生可能性及衝擊值評估說明

一、 威脅暨弱點評估

參考教育體系資通安全管理規範將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。

二、 事件發生機率與影響程度評估

(一) 依風險發生可能性評估表（表 1）評估各事件之可能性：

表 1 風險發生可能性評估表

評估標準	評估值
每年發生次數小於等於 1 次	1
每年發生次數為 2 至 3 次	2
每年發生次數大於等於 4 次	3

(二) 依衝擊值評估表（表 2）評估各事件之衝擊：

表 2 衝擊值評估表

評估標準	評估值
無傷害 1、 對組織無任何影響。 2、 資料無損毀，組織資料可正常提供。 3、 組織可容許該風險造成服務失效 3 工作天以上。	1
低度傷害 1、 該風險對組織造成的衝擊(含組織聲譽及財務影響)為可接受範圍。 2、 資料損毀或遭竄改，組織資料可供回復。 3、 組織可容許該風險造成服務失效 8 工作小時以上，3 工作天以下。	2
中度傷害 1、 該風險對組織造成一定程度的衝擊（含組織聲譽及財務影響）。 2、 資料損毀或遭竄改，組織有備份資料可供回復。 3、 組織可容許該風險造成服務失效 4 工作小時以上，8 工作小時以下。	3
重大傷害 1、 該風險對組織造成重大的衝擊（含組織聲譽及財務影響）。 2、 資料損毀或遭竄改且組織無任何備份資料可供復原。 3、 組織可容許該風險造成服務失效 4 工作小時。	4

三、 風險值的計算

評估事件發生機率及影響程度後，計算出風險值。

風險值=（資訊資產價值 × 可能性評估值 × 衝擊值）