本局資訊安全風險評鑑作業經驗分享

林昆平／台南分局技正

前言

期望成為政府行政機關導入資訊安全管理系統(簡稱 ISMS)示範願景下，經濟部標準檢驗局於 95 年開始全面導入 ISO27001 資訊安全管理系統，範圍涵蓋總局、六個分局及 15 個辦事處。ISO 27001 可說是所有管理系統中章節最多內容也最繁鎖的，除主文八個章節，還有附錄 39 個目標與 133 個控制措施需遵守，主要以「風險評鑑作業」為起點，識別出各資訊資產潛在風險並納入系統管理，過程包括資訊資產盤查清冊建立、CIAL 面向指標評估資訊資產體質健康度、選擇有效風險類型衝擊、選擇風險評鑑方法論、計算風險值、判定風險等級等，最後對高風險等級採取風險處理，並透過組織年度管審會議定期追蹤，期望降低潛在風險所導致的資安事件(故)發生。標檢局採用的風險評鑑方法論並不簡單，為讓相關作業人員與讀者能更深入了解風險評鑑內涵，筆者分別以人類社會及資訊資產世界運行作對比，解釋 CIAL 間的關係及實際意義；說明什麼是風險類型，如何選擇有效風險類型去衝擊資訊資產，尤其選錯風險類型將導致風險發生率與脆弱度變成 1，失去挖掘潛在風險的機會；也特別解釋「脆弱點」與「威脅」兩個名詞的關係，尤其前因後果常讓人搞不清楚；最後再以常見硬體資產、隨身碟、機敏紙本、電子檔、應用程式(分資料庫及軟體)進行演練，希望對相關作業人員有所幫助。

一、資訊資產的健康檢查 CIAL

(一)資訊資產定義

資訊世界的資訊並非只有電腦相關檔案；資產也不僅限於電腦與週邊設備，依 ISO27002 第 7.1.1 節對資訊資產的定義：「資訊」是資料庫、資料檔案、契約、協議、系統文件、研究資訊、手冊、訓練教材、程序、營運計劃、稽核記

錄、歸檔等；「資產」分成軟體資產(應用軟體、系統軟體、開發工具、公用程式)、實體資產(電腦設備、通信設備、可移除式媒體、其它設備)、無形資產(公信力、商譽、企業形象)、服務(公用設施如暖氣、照明設備、電源、空調、消防、通信)、人員(內部及外部)等五項。因此組織內部的資訊資產是龐大的，並非大家認知中的電腦相關設施與其產出資訊而已，這一點讀者務必釐清。

(二)人體身心健康指標 BCSS

人類社會運行與否與個人身心健康狀況有關，一個失能的人無法貢獻社會，還會拖累社會，如能先識別出那些人有失能的潛在風險，就可預防以避免事件發生。人體失能原因很多例如血壓(Blood pressure)太高中風癱瘓，血脂肪(Cholesterol)過高心血管堵塞，血糖(Sugar)過高引發慢性病，血清素(Serotonin)過低導致憂鬱症，前述因素 B、C、S、S 似乎已可作為人體失能評估指標，而且指標種類尚有擴展空間。各指標值可透過儀器量測與標準值作比對，並依定義評估其健康度例如 1：低於標準值過多 2:接近標準值 3:超過標準 4:高於標準值過多。

(三)資訊資產健康指標 CIAL

跟人類社會運行是一樣的，資訊世界運行的個體就是資訊資產，資訊資產夠健康資訊世界運作才順暢，公司因此獲利，但如資訊資產出了問題，例如公司機密性資料(Confidentiality)被競爭者盜取，離職員工挾怨報復竄改與破壞生產機台參數的完整性或正確性(Integrity)，駭客癱瘓公司網路的可用性(Availability)，員工違反業務安全規範觸法(Liability)等，都可能造成公司業務中斷而損失，因此 CIAL 四個面向指標就可用來評估資訊資產健康度。CIAL 指標值需透過附件一定義來架構，越重要資訊資產其健康度越差，理由就在公司不希望其發生問題，舉個例子「客戶個資」CIAL 各指標值都是偏高的，C：洩密造成競爭對手搶走客戶，L：洩密行為也抵觸個資法或公司業務執行安全規範(如表 1 舉例)，A：個資遺失導致取用中斷，I：個資資訊不正確影響公司營運。再如業務用「數位相機」的 CIAL 指標值卻是偏低的因其，C:無洩密問題，I:無資訊正確問題，A：遺

失可立即購得，L：無觸法問題，說穿了其對公司營運並無太重要影響。以上，藉由 CIAL 指標值判定，可評估出資訊資產未遭受風險衝擊前的健康情況。

表 1 台南分局業務執行安全的適法性規範

(1)CNS17025(ISO17025)　(測試與校正實驗室能力一般要求)

本標準為台南分局實驗室使用標準方法/非標準方法/自行開發方法去對產品執行試驗或對儀器校正的規定.其中與ISMS有關為第4.13節紀錄管制，規定本局實驗室產出之試驗及校正報告記錄文件或電子檔，應被保護及保密，防止資訊洩密，盜取，遺失，竄改，未授權存取及環境因素損毀。

(2)CNS13250(GUIDE65)　(執行產品驗證系統機構之一般要求)

本標準為台南分局對執行產品驗證登錄，自願性產品驗證，型式認可案件，各商品檢驗，工廠檢查，市場檢查，涉違規調查等工作之規定.其中與ISMS有關為第4.10節保密，規定執行上列工作時，規定執行人員必需對其執行業務之資訊加以保密，產品及廠商資訊，未經業主同意，不得洩密.要求員工填寫「資訊安全責任及工作分配表(保密具結書)」。

(3)CNS14725(ISO17020)(不同型式的執行檢驗機構運作的一般準則)

本標準為台南分局對執行工廠檢查工作規定之依據，其中與ISMS有關為第5節保密性，規定執行工廠檢查工作時，規定執行人員必需對執行工廠檢查過程所獲得資訊加以保密。

二、風險類型介紹

2.1 人體失能的風險類型(威脅型態+脆弱點)

「風險類型」由外在威脅型態與個體脆弱點組成，脆弱點是物體特質衍生出來的，例如人體皮膚特質會被燙傷，但鋼鐵結構卻不會，兩者在面對外來威脅型態-高溫水，人體會燙傷鋼鐵卻不會。「脆弱點」就是物體吸引威脅型態侵犯的原因，它是物質衍生出來的特質，只是「威脅型態」來自外界，物體不一定有相對應的脆弱點可供侵犯，底下舉例人體健康指標 BCSS 的風險類型，其有助於對資訊資產 CIAL 指標面向的風險類型了解。

2.1.1 血壓(B 值)的風險類型

(1)風險類型 1

外界威脅型態：吃鹹食。

誘使威脅侵犯的原因(脆弱點)：高鹽使血液內水份量降低。

風險類型：因為脆弱點，吃鹹食會引發腦中風失能。

(2)風險類型 2

外界威脅型態：長期過食。

誘使威脅侵犯的原因(脆弱點)：肥胖使心臟加倍跳動傳送血液。

風險類型：因為脆弱點，長期過食會引發腦中風失能。

(3)風險類型 3

外界威脅型態：藥物。

誘使威脅侵犯的原因(脆弱點)：藥物成份加速心臟跳動(如發炎藥)。

風險類型：因脆弱點，藥物會引發腦中風失能。

2.1.2 血脂肪(C 值)的風險類型

血脂肪包括膽固醇、三酸甘油酯及磷脂等，下列是它的風險類型：

(1)風險類型 1

外界威脅型態：攝取過多高膽固醇食物(如肥肉、腦、肝、魷魚、蛋黃、動物油脂等)。

誘因(脆弱點)：膽固醇會堵塞血管。

風險類型：因脆弱點，攝取過多高膽固醇食物會引發心血管堵塞。

(2)風險類型 2

外界威脅型態：長期過食。

誘因(脆弱點)：肥胖使三酸甘油酯上升。

風險類型：因脆弱點，長期過食會引發心血管堵塞。

(3)風險類型 3

外界威脅型態：抽煙喝酒。

誘因(脆弱點)：煙酒造成血液磷脂成份上升。

風險類型：因脆弱點，抽煙喝酒會引發心血管堵塞。

2.1.3 血糖(S 值)的風險類型

血糖長期偏高導致胰導素分泌失常糖尿病。

(1)風險類型 1

外界威脅型態：攝取甜食。

脆弱點：長期糖份使血糖上升。

風險類型：因脆弱點，攝取甜食會引發糖尿病。

(2)風險類型 2

外界威脅型態：長期過食。

脆弱點：肥胖使血糖上升。

風險類型：因脆弱點，長期過食會引發糖尿病。

(3)風險類型 3

外界威脅型態：情緒壓力。

脆弱點：長期壓力傷害胰島素分泌細胞。

風險類型：因脆弱點，情緒壓力會引發糖尿病。

2.1.4 血清素(S 值)的風險類型

血清素由色氨酸轉換，色氨酸需大量蛋白質，血清素分泌不足引發憂鬱症。

(1)風險類型 1

外界威脅型態：情緒壓力。

脆弱點：長期壓力使腦神經元分泌血清素不足。

風險類型：因脆弱點，情緒壓力會引發憂鬱症。

(2)風險類型 2

外界威脅型態：低蛋白飲食。

脆弱點：低蛋白食物無法提供足夠色氨酸濃度。

風險類型：因脆弱點，低蛋白飲食會引發憂鬱症。

(3)風險類型 3

外界威脅型態：營養素不均。

脆弱點：缺乏 B6 使血清素合成變少。

風險類型：因脆弱點，營養素不均會引發憂鬱症。

2.1.5 同時衝擊 BCSS 多個指標的威脅型態

觀察 2.1.1~2.1.4 節，可發現 BCSS 各指標間的外界威脅型態，有些是具有同時衝擊各指標的能力，這是因 BCSS 指標間尚存在某種關聯，例如「長期過食」就可同時衝擊 BCS 指標，它可使心臟加倍跳動傳送血液、三酸甘油酯上升、胰島素分泌失調，而造成這種現象是因人體生理結構是彼此相聯通的，所以會發生同一個風險威脅型態卻可以衝擊多面向指標情形，這一觀念非常重要，資訊世界的 CIAL 面向指標也會發生同樣情形。

2.2 資訊資產失能的風險類型(威脅型態+脆弱點)

資訊資產的風險類型也是由「外在威脅型態」與本體「脆弱點」組成，資訊資產種類繁多產出風險類型更多，而風險類型也會同時衝擊 CIAL 多個面向指標。

2.2.1 外界威脅型態

資訊資產所面臨外界威脅型態可就下列因素考量來選擇：

(1)環境天災：水災、火災、地震、風災、爆炸。

(2)人為非故意：軟體 bug、系統故障、過載、硬體失效錯誤、事故。

(3)人為故意：內部人員(組織人員、契約人員、僱員) 及 外部人員(駭客、病毒、競爭敵對公司)。

(4)技術問題：系統參數誤值、硬體維修失當、操作意外。

(5)管理問題：保存方式強弱、使用程序有無、監控設施有無。

2.2.2 脆弱點

資訊資產脆弱點可就下列因素考量：

(1)所在地理位置

(2)適用材質

(3)使用方式

(4)設計方式

(5)管理方式

2.2.3 資訊資產風險類型舉例

(1)伺服器的風險類型

■外界威脅型態：地震(選擇環境因素)

■脆弱點分析

1.所在地理位置：位於 1F 水泥隔間，對地震結構可承受 9 級。

2.適用材質：金屬殼，對地震並不堅固。

3.使用方式：網路連線，對地震易斷線。

4.設計方式：主機板及硬碟所構成之電腦，對地震無防震能力。

5.管理方式：資料備份，對地震採異地備份。

所以面對地震，伺服器產出多個脆弱點 2、3、4。

■產出的風險類型

風險類型 1：因金屬殼對地震並不堅固，地震會引發損毀。

風險類型 2：因網路連線對地震易斷線，地震會引發斷線。

風險類型 3：因主機板及硬碟無防震能力，地震會引發磁軌損壞。

■風險類型衝擊 CIAL 面向

風險類型 1：A。

風險類型 2：A。

風險類型 3：A。

因風險類型不會造成洩密、正確性、觸法等問題，故無法衝擊到 CIL 指標面向。

(2)機敏性紙本的風險類型

■外界威脅型態：複製揭露(選擇人為故意因素)

■脆弱點分析

1.所在地理位置：辦公室，對複製揭露上班較可能，下班則上鎖。

2.適用材質：紙本，對複製揭露可以引影印、照相、偷走。

3.使用方式：承辦人自行管理，對複製揭露可能因疏於注意放於桌面。

4.設計方式：應用程式登打產出後列印，對複製揭露可能發生在列印後未拿取。

5.管理方式：承辦人上鎖抽屜，對複製揭露可能忘了上鎖。

所以面對人為故意複製揭露，機敏性報告產出多個脆弱點 1、2、3、4、5。

■產出的風險類型

風險類型 1：因上班期間辦公室較鬆散，複製揭露引發洩密觸法。

風險類型 2：因紙本易影印、照相、偷走，複製揭露引發內部人員洩密觸法。

風險類型 3：因承辦人疏乎放桌面，複製揭露引發內部人員洩密觸法。

風險類型 4：因印出報表後未立刻拿取，複製揭露引發內部人洩密觸法。

風險類型 5：因承辦人忘了上鎖，複製揭露引發內部人員洩密觸法。

■風險類型衝擊 CIAL 面向

風險類型 1：C、L。

風險類型 2：C、L。

風險類型 3：C、L。

風險類型 4：C、L。

風險類型 5：C、L。

因威脅型態複製揭露並未拿走紙本也不無竄改，故無衝擊 A、I 面向。

(3)機敏性電子檔的風險類型

■外界威脅型態：複製揭露(選擇人為故意因素)

■脆弱點分析

1.所在地理位置：位於辦公室內，對複製揭露上下班空間會發生。

2.適用材質：硬碟，對複製揭露可拔出複製。

3.使用方式：承辦人以 WIN 帳號密碼登入電腦使用，對複製揭露因未登出電腦被竊取

4.設計方式：採用電腦螢幕 MICROSOFT WORD 畫面登打，對複製揭露觀看不可能發生。

5.管理方式：存於電腦未設密碼，對複製揭露可能發生。

所以面對人為故意複製揭露，機敏性電子檔產出多個脆弱點 1、2、3、5。

■產出的風險類型

風險類型 1：因上下班期間電腦未作好防護措施，複製揭露引發洩密觸法。

風險類型 2：因硬碟可被拔走，複製揭露引發洩密觸法且拔走有可用性問題。

風險類型 3：因離座未登出，複製揭露引發洩密觸法。

風險類型 4：因電子檔未設密碼，複製後輕易揭露引發洩密觸法。

■風險類型衝擊 CIAL 面向

風險類型 1：C、L。

風險類型 2：C、A、L。

風險類型 3：C、L。

風險類型 4：C、L。

(4)開放民眾使用網頁程式之風險類型

■外界威脅型態：網路駭客入侵

■脆弱點分析

1.所在地理位置：位於機房伺服器，此與網路駭客入侵無關。

2.適用材質：伺服器硬碟，此與網路駭客入侵無關。

3.使用方式：資訊室人員定期維護更新，可能誤操作使網路駭客入侵。

4.設計方式：委外部網頁公司開發設計，程式可能有漏洞使網路駭客入侵。

5.管理方式：具備使用者權限、帳號、密碼等設定功能，網路駭客也可能攻破入侵。

所以面對被駭客入侵，網頁程式產出的脆弱點是 3、4、5。

■產出的風險類型

風險類型 1：因資訊室人員維護更新誤操作，駭客入侵引發洩密、竄改、破壞。

風險類型 2：因程式有漏洞，駭客入侵引發洩密、竄改、破壞。。

風險類型 3：因帳號密碼設定系統被破解，駭客入侵偷取機敏資料。

■風險類型衝擊 CIAL 面向

風險類型 1：C、I、A、L。

風險類型 2：C、I、A。

風險類型 3：C。

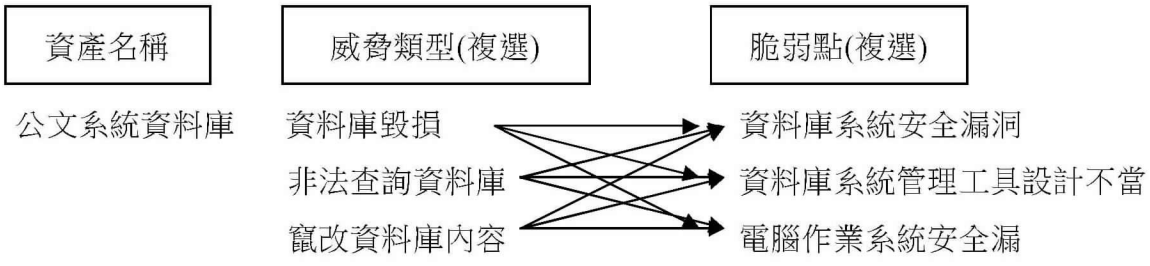
(5)資料庫的風險類型

多個風險類型組合舉例，說明：

1.資訊資產相同的脆弱點可能面對不同威脅型態侵犯。

2.相同的威脅型態也可能侵犯到資訊資產不同脆弱點。

3.風險類型對 CIAL 衝擊面向有其專屬性。



三、本局風險評鑑方法論

「風險評鑑方法論」在 ISO31010 多所著墨，是統計機率學的一種，本局採用的是矩陣法。

一般完成資訊資產風險評鑑作業要經過四道程序：第一道選擇有效的風險類型進行衝擊；第二道計算資訊資產面對衝擊產出的風險值；第三道是考慮衝擊破壞或然率問題調整資訊資產健康度；最後根據風險值與調整健康度來計算風險等級，整個過程是在 CIAL 四個面向指標均考慮下進行個別計算。

3.1 選擇有效的風險類型

在 2.2 節資訊資產失能的風險類型中，已發現各種風險類型有其專屬的衝擊面向，因此「有效風險類型」指的就是能衝擊到資訊資產 CIAL 面向指標中健康

度最差的指標類型，例如某資訊資產 CIAL=(1,2,4,1)，那麼風險類型應選擇可以衝擊 I(竄改、變更、誤打)與 A(可用性、損毀、破壞、遺失)面向的類型才有意義，若選擇衝擊面向 C(複製揭露洩密)與 L(違法)的風險類型，由於該資訊資產在 CL 健康度極佳(值偏低)，此類型就屬無效，作了等於白作，產出結果永遠是低風險。

3.2 計算風險可能值

3.2.1 決定資訊資產脆弱度值

資訊資產的有效風險類型一旦選擇後，威脅型態與脆弱點都可獲知，脆弱點的強度值(脆弱度)是由針對此類型威脅的安全措施控制程度來決定，越強固得防衛措施可使脆弱度值下降，脆弱度依本局定義如下：

3：該脆弱點曾遭威脅利用

2：考慮目前對威脅型態的安控程度，該脆弱點是否仍容易遭威脅利用

1：考慮目前對威脅型態的安控程度，該脆弱點是否不易遭威脅利用

3.2.2 決定威脅型態的發生率

威脅型態發生機率稱為發生率，其值應由歷年發生次數統計出，依本局定義如下：

3：1 年內可能發生 1 次以上

2：1 年以上，3 年以下可能發生 1 次

1：3 年以上才可能發生 1 次

3.2.3 依脆弱度與發生率計算出風險值

考慮圖 1(a)矩陣法，脆弱度與發生率都偏高才可能產出高風險值(3 或 4)；脆弱度與發生率偏低僅能產出低風險值(1 或 2)，然脆弱度比發生率有較佳防衛面，因此(脆弱度,發生率)=(3,2)產出風險值 4，但(脆弱度,發生率)=(2,3)卻產出風險值 3，不管如何還是偏高。計算的風險值雖只有一個，但由於風險類型衝擊到多個指標，此風險值為衝擊到之指標所共享。

3.3 考慮風險衝擊或然率調整資訊資產健康度

3.3.1 風險衝擊廣度(衝擊或然率)

風險評鑑通常會將相同特質的資訊資產歸成一組，以免重復個別相同作業，由於多個數量的存在，風險衝擊失能程度不會是全面的，有部份正常運作有部份失能；這和個別資訊資產被風險衝擊後也可能出現損毀程度不是 100%狀況是一樣的，半殘不代表沒有營運能力。為貼切實際狀況，風險衝擊必需納入或然率稱之為「衝擊廣度」，依本局對衝擊廣度定義：

4：對資訊資產(群組)造成 80%-100%的損失

3：對資訊資產(群組)造成 50%-80%的損失

2：對資訊資產(群組)造成 20%-50%的損失

1：對資訊資產(群組)造成 0%以上-20%的損失

■例如 某單位傳真機共 3 部，若風險為

(1)設備保養不當無法使用：此時可能僅 1 部失效，不是全部失效，因此衝擊廣度約 33%，衝擊廣度=2。

(2)設備安置處不牢地震摔壞：此時 3 部設備皆有此風險，則衝擊廣度為 100%，衝擊廣度=4。

■例如 某同仁將業務個資 100 筆存放於電腦，其中 10 筆複製至 usb 隨身碟，後因攜出遺失，則個資的 CIAL 可能面對風險為

(1) I 、A：因遺失隨身碟不涉正確性，姬盎資料備份於電腦，故 AI 無需探討衝擊廣度。

(2) C ：遺失一定會洩密，10%的洩還有 90%未揭露，故衝擊廣度依定義可取 1。

(3) L ：個資洩漏就屬違法，沒有數量考慮問題，故衝擊廣度依定義可取 4。

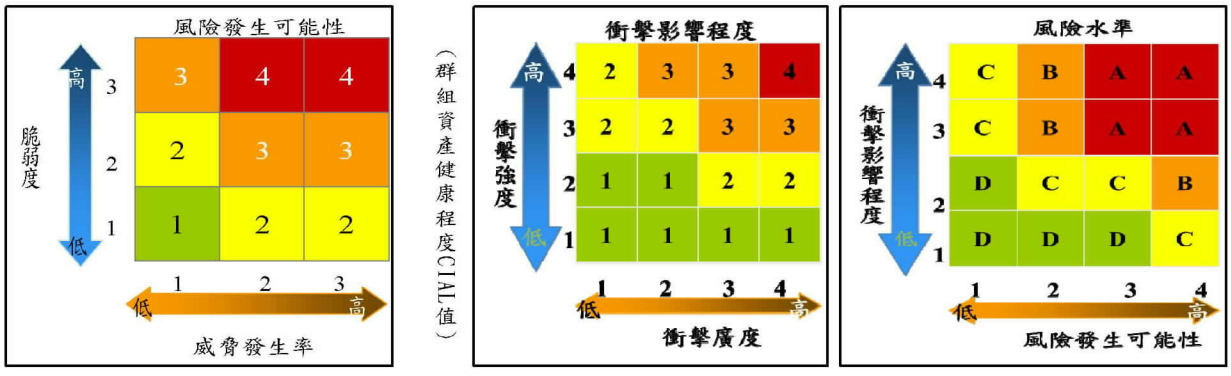
3.3.2 因應衝擊廣度調整資訊資產健康度

考慮風險衝擊廣度的成效應由調整資訊資產健康度來呈現。調整後的健康度又稱「衝擊影響度」，圖 1(b)顯示 Y 軸為原資訊資產衝擊前 CIAL 各指標面向健康度；X 軸為衝擊廣度，對應結果即為調整後的健康度。例如 X=4 代表資訊資產有 4/4(100%)被衝擊到，則 Y 軸原健康指標值(4321)調整後仍

是(4321)；X=3 代表資訊資產 3/4(75%)被衝擊到，則原健康指標值(4321)調整後為(3321)；X=2 代表資訊資產 2/4(50%)被衝擊到，則原健康指標值(4321)調整後為(3211)；X=1 代表資訊資產 1/4(25%)被衝擊到，則原健康指標值(4321)調整後為(2211)。

3.4 計算風險等級

取得反應實際風險衝擊的健康度與風險值後就可評估風險等級。圖 1(c)顯示風險值偏高且健康強度不佳(值偏高)兩個條件同時成立下才會產出 AB 級高風險，而一高一低如(4，1)或(1，4)僅會產出 CD 級低風險，說明了：面對風險類型產出高風險值者，不代表資訊資產會產出高風險等級，理由就在資訊資產還有健康強度問題，很健康的面向指標值碰上高風險值，結果可能扯平，並不會發生高風險等級，只有指標面向不健康(值偏高者)碰上高風險值才有機會產出高風險等級。



(a)風險可能值計算　　(b)衝擊廣度計算　　(c)風險等級計算

圖 1 本局風險評鑑方法論

3.5 風險可接受等級

AB 級高風險最後需由資訊安全管審會議決定，是否採取風險處理以降低風險等級成 CD，CD 級風險就是可接受風險。而風險處理會加強資訊資產在此風險類型衝擊下的安全控制措施，措失執行後鞏固脆弱點，脆弱度因而降低使風險值