利用情境分析來管理技術風險
Using Scenario Analysis for Managing Technology Risk

作者：Mukul Pareek, CISA, ACA ,AICWA, PRM,
is a risk professional based in New York, USA. He has more than 20 years of audit and risk experience in industry and financial services. He is copublisher of the Index of Cyber Security, *www.CyberSecurityIndex.org*. He can be reached at *mp@pareek.org*.

譯者：徐立群, 國立成功大學會計學系,教授、電腦稽核協會編譯出版委員會委員

在這充滿各種市場與信用風險的世界裡，情境分析被應用於壓力測試。國家立法者與央行會執行壓力測試，並要求金融機構必須考慮到資金與償付能力出現負面情況時產生的影響。情境模擬包括歷史事件比方說市場崩盤與負債違約，以及其他假設下的情境，如利率水準、房價與外匯超乎預期的變動。

至於作業風險，在巴賽爾架構下情境分析則會拿來結合損失分配法來估計作業風險的資金。

針對技術風險管理人，情境分析有助於辨識、了解與詮釋組織面對的技術風險。更進一步的說，它能被用來量化與表達技術價值風險值，並以損失分配的形式呈現。

本質上，情境分析包括辨別出未來可能出錯的狀況，這樣的狀況很可能造成企業的損失。而這也正是技術風險管理人每天的例行任務—向經理人解釋各種控制的情況。(舉例來說，解釋風險或查核事件或對安全增加新的投資)。情境分析讓我們意識到那些負面情況可能發生，如何預防不利的結果並解釋在合理範圍內整體狀況可能惡化的程度。

情境分析與技術風險管理人

以下有幾個理由解釋為何風險管理人需要把情境分析納入他們的風險管理中：

- **風險與控制可了解性**—情境分析把控制放進日常作業中，讓利損經理人可以理解。情境分析把這些對話轉成平易近人的商業語言，而不是難以理解的控制架構。情境分析幫助討論間的轉換，比方說從身份管理系統上的控制效益討論到競爭者竊取商業資料的討論。
- **範圍完整性**—如果情境分析是完整的，並且涵蓋了技術風險下的保護，它對於企業來說是個拿來解釋技術風險功能價值的好用工具。它還能在各種功能運作與保護的限度上設下界限並幫助高階管理人設立預期值。
- **反應預備**—情境分析幫助企業去應對它們所找出來的事件。
- **辨認風險產生原因**—在系統化的建造下，情境分析可以幫助獨立出風險產生的原因，並且專注其行動。
- **控制有效性**—辨識出情境必須要考慮到控制讓這些情境不發生，藉此產生對控制有效性的質化分析。情境分析幫助我們理解控制間如何互動與加強。

從本質上來看，情境分析與風險分析並非那麼不一樣，其明顯不同之處在於大多數的個體風險必須結合創造出完整與合理的情境。單一情境會依

照以往的說故事的傳統，然而細尺度的列舉風險對於風控經理來說就是一大挑戰了。

歷史與假設情境

廣泛來說，有兩種方式可以辨別情境：

第一，透過分析歷史事件。 第二， 創造假想的情境模擬出可能發生的負面情況。 把兩者放一起看，情境分析應該是完整且隨著時間更新的。

情境分析應該是完整且隨著時間更新的。

基於歷史事件的情境分析可能包括實際發生在組織身上或是同行間的事件（比方說帳務系統洩漏大量敏感個資）創造假想情境需要主觀判斷，技巧與對企業的全盤理解。假想情境分析十分重要，因為它彌補了過去事件遺留的漏洞。

根據歷史事件的情境分析基於可信度高不需做解釋。而假想情境則可透過企業經理人的積極參與以建立可信度。

創造假想情境需要主觀判斷，技巧與對企業的全盤理解。假想情境分析十分重要，因為它彌補了過去事件遺留的漏洞。

根據歷史事件的情境分析基於可信度高不需做解釋。而假想情境則可透過企業經理人的積極參與以建立可信度。

情境分析應包含那些元素?

情境分析在最低限度下應包含以下：

- **各種狀況**—針對一系列事件造成的負面結果的解釋。這些情況可能與特定產業或組織有關，但必須包括：
  - BCP事件
  - 來自駭客、競爭者或國家單位的外部攻擊
  - 內部人員惡意竊取資料
  - 意外散布機密資訊
  - 供應商或第三方對資料處理不當
- **結果**—清楚的分辨出對組織不利的結果。單一事件可能會造成數種結果，比方說相同的情境分析可能會出現不同的利益外損失，法律成本與罰款等不同的結果。每種結果都必須明確的列出，以及評估它們的影響。
- **適當的控制**—控制乃是扮演不同的防衛線，大多時候是連續的，其他時間則是彼此相互呼應—幫助防止負面情況的發生。通常正確的運作下一項控制即可提供適當的保護或抑制。如果各種控制間為獨立運作，如同他們通常的作法，那這些控制同時無法運作的機率自然比個別無法運作的可能性低上不少。以一個打算駭進互聯網的外部攻擊者為例，他一開始可能會先對付入侵偵測與防禦系統（IDS/IPS），系統失敗的機率約為10%。但即使駭客成功闖入且試圖植入惡意程式，還是得面對反惡意程式的保護機制，系統失敗的機率同為10%。以上兩種保護控制同時失效的機率僅1%，表示多個控制同時運作可提供十倍的安全保護，即使這些控制就個別來看並不是非常有效。

  第三種控制，像是限制使用者的管理權限，可進一步減低甚至完全排除有效的攻擊。
- **發生的頻率**—情境發生的頻率，或者說發生的可能性應是情境分析的一部份，而最好的評估方式就是與企業主管的討論。

  風險管理者在意的莫過於事件發生的機率，但更重要的問題在於情境發生在多久期間內如何去判定（比方說十年）。這個問題最好由企業主管與技術風險管理人一同回答。如果答案是某個情境每隔十年會重現一次，那每年發生的機率即是10%。
- **後果的嚴重性**—與發生頻率有許多相同之處，每種結果帶來的負面效應都必須個別評估。嚴重性是什麼意思? 是表示最糟糕情況下的損失?還是最有可能或者中間值的損失?在某些案例來說，最糟的結果無法被得知，或者表示該企業悲慘結束營業的結局。某些可能發生在長遠未來的情境應與其他情境分開來看。

就其它例子來看，估計最糟的結果可能是無意義的舉動，因為技術風險小組缺乏足夠的授權來處理這樣的後果。雖然有點令人意外，但我們一般不會預期技術風險管理會考量核子攻擊或隕石撞擊

技術風險分析針對嚴重性至少要達成兩項資料特性。其一為 50 個百分位，以及更高的 90 個百分位。關於 50 百分位可以簡單地指出:預期損失的中間值為多少?至於 90 百分位，更適當的問題為：在所有可能的損失範圍內，前 10%的損失為多少?這裡我們不要求完全正確的預測，因為他們可能無法達成或是無意義。

校正偏差

人們通常對於自我的能力或運氣有著樂觀的偏差。這樣的偏差很有可能反應在任何情境分析中，像是技術風險管理人低估了事件的頻率或發生或嚴重性。

其中一種解決方式為風險分析人員修正其情境分析，把焦點從自己公司轉移到其他類似公司或競爭者（比方說這樣類似的情境發生在前四或前五強的競爭者時可能性有多高，假設真的發生，他們又必須負擔多高的損失?）。所有內部受損情況資料或是真實發生情況都可能幫助我們修正臆測到更進一步的事實。

情境完整性—繪製出完整的風險範疇

情境分析必須包括企業可能會面對的已知技術風險，已記錄的控制必須能處理一個或更多的情境，如果風險管理者發現控制無法處理某個情境，就表示情境有不完整或是該控制缺乏作用。在下列各種範疇下，比如程序與工作流程錯誤、資料洩漏事件、企業連續性事件與外部攻擊（這些可能因組織而異），它們都會產生許多情境。

編輯一份可接受的風險的情境清單， 包括所有前面描述過的屬性不是一件簡單工作，這需要 P&L 經理的幫助以及技術風險管理人對企業的了解。情境創造可以由技術風險管理人或分析人員在會議室進行。

在許多例子中，情境分析的演練是有價值的。而在某些例子中，風險經理可能選擇執行額外的量化分析，透過計算技術價值風險的數值，這也是下一章節的討論細節。

計算技術價值風險

一旦情境被辨識出來，包含在前面章節討論過的預期發生頻率與嚴重性，而這些評估可被轉為評估不同信賴區間下的損失，與價值風險類似。我們稱為「技術價值風險」，是為了把它與一般在衡量的財務風險做區隔。下列步驟決定技術價值風險：

1. 頻率與嚴重性評估的分佈之假設

一般來說，頻率的波松分佈與嚴重性的對數正　態分佈都是合理的選擇。

使用分佈法是因為頻率或嚴重性皆非單點評估，而是能涵蓋許多的數值。這使計算的過程在管理會議中更能被接受，因為技術風險的分析師並不宣稱任何計算的絕對性。

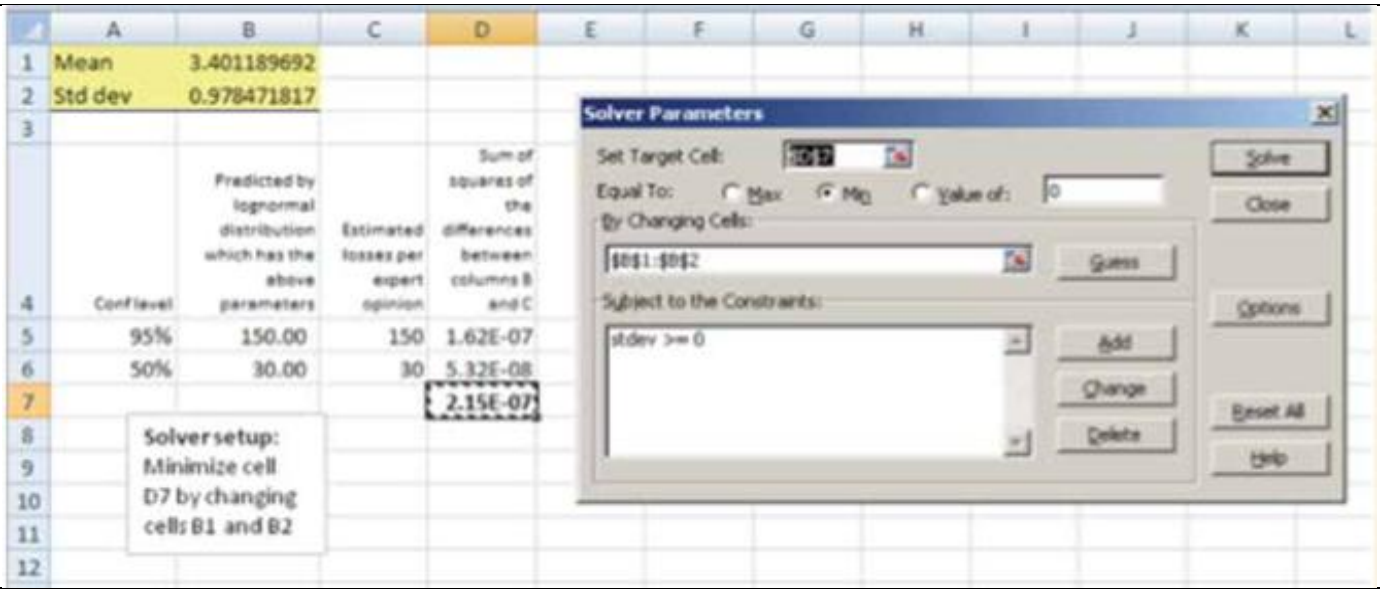
這篇文章接下來將會進入分佈選擇（比如波松分配或對數正態）即便其他的分佈被挑選，整個過程依然會非常相似。

在波松分佈下的頻率分佈，只需有一種參數—平均值，來建立分佈。平均值的評估包含在整個情境分析中。在對數正態分佈下的嚴重性分佈中，需要兩個參數來描述整個分佈的型態—平均值與標準差。估計這些參數會需要取得經由情境分析下評估得到的兩點（或更多）損失資料—也就是最有可能的損失與 90 百分位數的損失額度。使用最小平方法，兩點分析可被用來估計嚴重性分配的最適平均值與標準差。我們可利用 EXCEL 裡的 Solver(見圖 1)或是數據包比方說 R^3(見圖 2)。

圖 1 — 使用 EXCEL 來實際建模

步驟一: 使用最小平方法決定出對數正態分佈下的分佈參數。

在 EXCEL 中，對數正態分配的平均值與標準差可以利用 Solver add-in 獲得，所有的例子都在下列呈現。



步驟二: 在分配參數估計出來後利用蒙地卡羅法模擬

在波松與對數分配下我們可以利用 EXCEL 的分析工具箱選取隨機值模擬頻率與嚴重性，它是 EXCEL 裡的標準附加功能。將嚴重性與頻率交乘可獲得損失分配的資料點。之後技術價值風險便可計算在想要的信賴區間下，比方說 99 百分位數下的損失會是=PERCENTILE（data_range_loss_column,0.99）。

2.建立損失分佈圖

損失分佈是頻率分佈與嚴重性分佈下的產物，正如損失額會等於頻率乘上嚴重性。然而在波松分佈（頻率）與對數正態（嚴重性）分佈下是不能透過公式相乘的，只能使用蒙地卡羅法來求得損失分佈。此法乃分別由頻率與嚴重性分配中挑出隨機值再另兩者相乘獲得一個單點資料表示損失額。此過程將會重複上千次以取得足夠的資料，方可繪製損失分佈圖。

3.在情境分析下計算技術價值風險數值

一旦經過大量資料點運算後得出損失分佈後，特定情境的技術價值風險可以藉由計算有興趣的數量來獲得。舉例來說，如果想知道在 99 百分位數時的損失額度，只要對照在分配圖表上 99 百分比為下的損失水準。

4. 加總技術價值風險

還有額外的一個步驟，我們對於技術價值風險總合包含了所有經由蒙地卡羅法同時計算出來的情境進行加總。這是在所有的損失事件都是獨立不相關的前提下所計算出。

這些步驟同樣可以在 EXCEL 下進行, 或是數據包 R。雖然 EXCEL 針對做雛型與解決較單純問題來說是個不錯的選擇，但若是高負荷的任務，那 R 即是更適合的選擇。要選擇哪種方法取決於風管經理使用的風險模型有多廣泛與重複程度，以及可掌握的技能。

圖 2—使用 R 來實作建模

當我們在使用 R 的時候，上述步驟可用下列指令來執行。在跑這些指令前，起始變數必須由風險分析師來設置。

```
#Initial variables
simulations <- 1000000
lambda <- 0.1
exp_est1 <- 10
exp_est2 <- 80
conf1 <- 0.5
conf2 <- 0.95
#Two estimates for Scenario 1 placed in dataframe s1
s1 <- data.frame(conf=c(conf1,conf2),
expert_est=c(exp_est1,exp_est2))
#Setting a function up to calculate the sum of squares
ss <- function(x) {
x1 <- x[1]
x2 <- x[2]
sum((qlnorm(s1$conf,x1,x2) - s1$expert_est)^2)
}
#Minimizing the sum of squares function a
pp <- optim(c(0,1),ss)
s1mean <- pp[[1]][1]
s1stdev <- pp[[1]][2]
#Calculating the loss distribution function
ld <-
rlnorm(simulations,s1mean,s1stdev)*rpois(simulations,lambda)
qt <- quantile(ld, probs=c(0.95, 0.99, 0.995, 0.999))
#Publish everything we calculated thus far
s1
s1mean
s1stdev
ss(c(s1mean,s1stdev))

qt
```

總結來說， 技術價值風險計算包括以下步驟，如圖 3 所示：

1. 辨別情境。

2. 針對個別情境：

- 決定頻率時採用單點分析，將所得的值用在波松分佈下估計事件發生可能性的平均值。
- 決定嚴重性時採用兩點或多點資料分析。使用這些資料，計算在對數正態分佈下最接近的平均值與標準差。對數正態分佈在這裡可說是定義了嚴重性分佈。
- 模擬損失分佈，同時選取頻率分配與嚴重性分配的單一值。

3. 針對每個情境， 計算適當的百分位數（通常是 95 或 99）來作為技術價值風險。

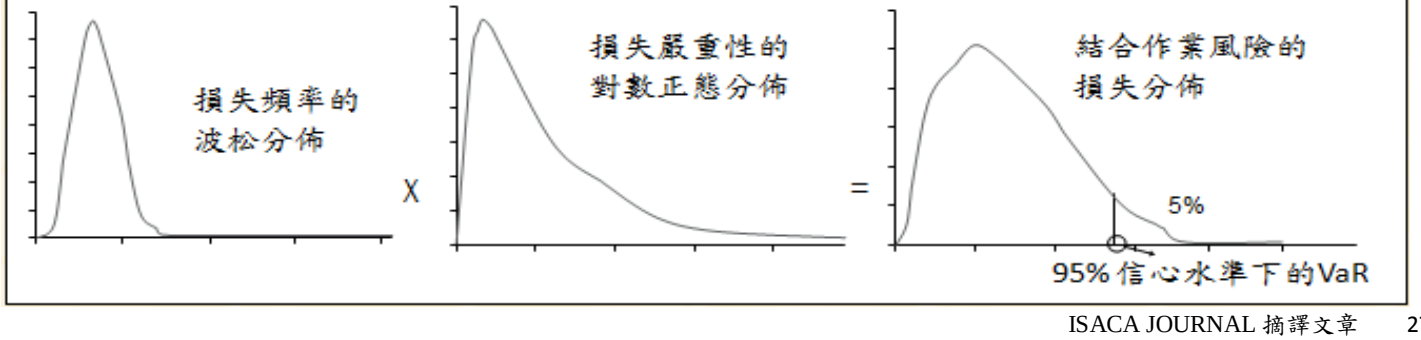
4. 計算出所有情境下技術價值風險的加總，同時模擬所有情境下可能的損失。

結論

情境分析，即便計算出來的結果不做額外的量化，依然可以把技術風險管理者與他們服務的企業做一個有效的連結。它可以使員工之間有適當交流與參與並使管理層把注意力集中在攸關組織的重大事務上。同樣的它也能幫助企業評估各種實際商業運作下的控制活動，並辨別出在風險不會極度增長的情況下能夠安全中斷的控制。如果情境轉換成技術價值風險的數值，那企業就能評估出增加或移除控制活動所帶來的經濟影響。

然而此法並非沒有限制。現實世界十分複雜，負面的結果可能會不可避免地加重惡化。此外，情境的影響時常超出技術的範疇。要成功將伴隨技術風險事件的策略、法律與聲譽風險加以模型化是困難的。模型建立者在任何情境分析中都必須考量到這些限制。

圖 3—作業風險損失模型化



ENDNOTES

1. Basel Committee on Banking Supervision, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version*, *www.bcbs.org*
2. Solver is a native Microsoft Excel add-in that allows complex problems to be solved using optimization routines. It may be enabled under the Add-Ins menu in Excel.
3. R is a popular open-source software used for mathematical and statistical analysis. It can be downloaded from *cran.r-project.org*.
4. Monte Carlo simulations are a statistical method where data points are obtained by repeated random sampling. This allows for simulating complex systems and interactions that may be difficult to express analytically (e.g., as a clean formula).

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 6, 2012 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：
ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2012,Volume 6中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。