

新版 ISO 17025 與營運風險管理

工研院量測中心 ISO 17025 特約講師樊國紀

一、前 言

ISO 17025 的修訂，目前已進行到 DIS 版的審查與投票，這個審查與投票自 2016 年 12 月 29 日開始，將在這個月，也就是 3 月 22 日結束，如果順利通過審查，就會發行 DIS 版並開始準備 FDIS 版。根據目前投票中之 DIS 版，我們知道除了在第四章新增公正性之風險管理，在第八章管理系統之規定中，也新增考慮風險與機會之要求，因此本文為大家簡單介紹新版 ISO/IEC 17025 DIS 中，有關風險與機會管理之要求與實驗室可以考慮之作法。

二、新版 ISO/IEC 17025 要求

根據新版 ISO 17025 DIS，在風險管理方面，新增下列要求：

- 4.1.4 實驗室需鑑別與公正性有關之風險
- 8.1 新版第 8 章對於管理系統之規定，改為實驗室有 A 與 B 兩個選擇，實驗室可以選擇 A 方案，依照 8.1.2 節之規定，在文件管制等 8 個方面建立基本管理系統，或者選擇 B 方案，建立符合 ISO 9001:2015 之要求的管理系統。如果實驗室選擇 A 方案，則實驗室要依照 8.5 節考慮風險與機會。
- 8.5 要求實驗室要考慮風險與機會，並針對風險與機會，規劃對應措施。
- 8.7.1 需要時更新矯正規劃中所決定之機會與風險。
- 8.9.2 管理審查中要審查風險鑑別之結果。

4.1.4 節實驗室需鑑別與公正性有關之風險，本系列已在第一篇新版 ISO17025 與公正性風險中討論過，對於第八章管理系統，如果實驗室選擇 B 方案，則請參考本訓練網 ISO 9001:2015 解析系列中未來各篇之說明，本文主要討論如果實驗室選擇 A 方案，則 8.5 節要如何執行，8.5 節有下列三項規定：

1. 實驗室應考慮風險和機會，以便：
 - a) 確保管理系統實現期望的結果；
 - b) 加強達成實驗室宗旨 (purpose) 與目標 (objectives) 的機會
 - c) 預防或減少在實驗室活動中非預期的衝擊與潛在失效；

d) 實現改進。

2. 實驗室應規劃

a) 風險與機會的應對處理措施；

b) 如何在管理系統納入和應用這些措施與如何評價這些措施的有效性。

3. 對於風險與機會所採取的應對措施，應適合其對實驗室結果有效性的潛在衝擊。

三、風險與機會

對實驗室來說，要確保測試或校正品質，達成實驗室之宗旨與目標，需要掌握很多可能的機會，譬如說使用新技術滿足新的測試需求，建置新的資訊系統提升服務效率等可能機會。同時實驗室也需要注意很多可能的風險，譬如說儀器沒有校正與人員操作錯誤，可能有造成測試結果不正確的風險，實驗室作業中的各種物理、化學與生物性危害，如果沒有適當防護，可能有造成災害與意外事故，影響到工作人員健康與安全的風險。

所以像關聯到醫療品質的醫學實驗室，ISO 在 2008 就發行了 ISO/TS 22367 醫學實驗室－利用風險管理與持續改善來減少錯誤這份標準，同時 ISO TC 212 目前也正在研擬實驗室生物風險管理系統之標準 ISO 35001，而醫學實驗室以外，其他一般實驗室的安全衛生管理，也一直都是大家注意的風險管理課題。

但是醫學實驗室的風險管理或一般實驗室的安全衛生管理，基本上都是針對負面影響所導致的風險，而新版 ISO 17025 同時要求考慮有正面幫助之機會，因此建議實驗室在建立風險與機會管理之相關制度時，參考 ISO 31000:2009 風險管理－原則與指導綱要，或美國 COSO 委員會(The Committee of Sponsoring Organizations of the Treadway Commission) 於 2004 年 9 月所發布之「企業風險管理－整合架構」ERM (Enterprise Risk Management－Integrated Framework)，甚至可以考慮參考策略規劃的相關理論與作法。

我們在本系列第一篇新版 ISO17025 與公正性風險中，已說明過 ISO 31000:2009 或美國 COSO 的 ERM，將風險界定為不確定性對目標或達成目標的影響。影響是與預期者之偏離，可為正面或負面。產生負面影響的是風險，而產生正面影響的是機會。所以 ISO 31000:2009 或 COSO ERM 所說的風險，是包括風險與機會。

同時 ISO 31000:2009 說明如圖 2 所示之風險管理的過程，包含風險鑑別、風險分析與風險評估等 7 項工作。COSO的 ERM 也以如圖 2 所示之風險管理立方體，說明風險管理的過程包含事項鑑別與風險評估等 8 項工作。

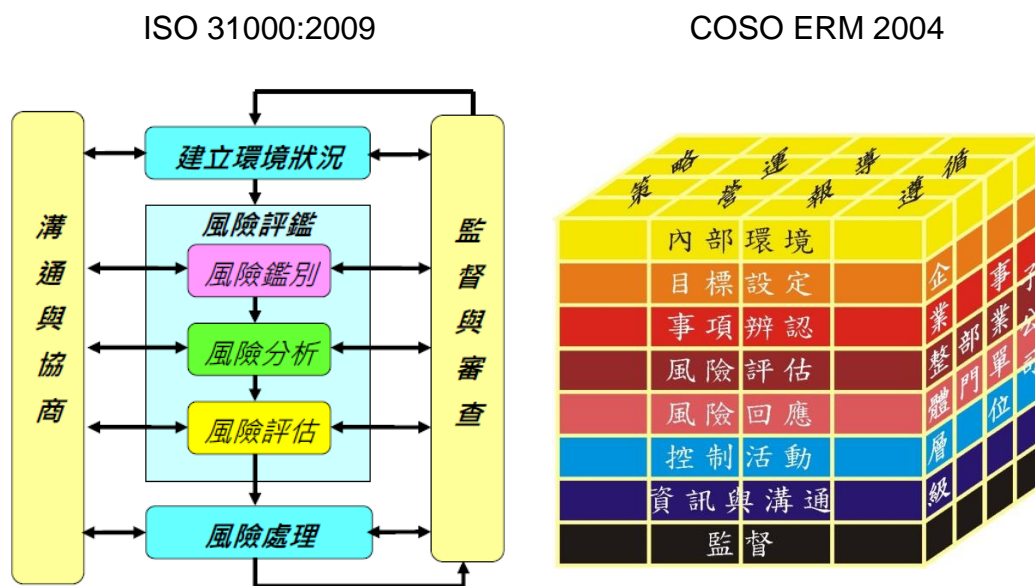


圖2 ISO 31000:2009 與 COSO ERM 的風險管理的過程

從表 1 的比較中我們可以知道 ISO 31000 與 COSO 所規劃之風險管理工作大同小異，因此將來如果實驗室對於新版 ISO 17025 第 8 章管理系統之規定，選擇 A 方案，則對於 8.5 節之要求，實驗室可以根據自己的規模與需求，參考這兩模式，規劃自己的風險與機會管理過程，或參考圖 3 所示之簡易風險與機會管理過程，推動風險管理。

表1 ISO 31000 與 COSO 的管理工作比較

ISO 31000:2009	COSO ERM:2004
溝通與協商	內部環境
確認內部及外部情境	目標設定
風險評鑑	事件辨認
— 風險鑑別	風險評估
— 風險分析	風險回應
— 風險評估	控制活動
風險處理	資訊與溝通
監督與審查	監督



圖 3 簡易風險管理過程

但無論是自己規劃風險與機會管理過程，還是參考圖 3 所示之簡易風險與機會管理過程，推動風險管理，實驗室都應將風險與機會管理，內化於決策過程、營運目標與所有業務執行流程中，讓風險與機會管理成為日常工作的一部份，才能有效經由風險與機會管理，為客戶與實驗室創造價值。

四、如何管理風險與機會

圖 3 所示之簡易風險與機會管理過程，是參考 ISO 31000 與 COSO ERA，將風險管理工作分為宗旨目標設定、衝擊事件識別、風險機會分析、風險機會評估與風險機會處理等幾個階段，同時在每一階段，都要注意溝通與協商 (Communication and Consultation) 以及監督與審查 (Monitoring and Review)，每一階段之工作，簡單說明如後：

1. 宗旨目標設定

因為新版 ISO 17025 的 8.5 節中要求實驗室要加強達成實驗室宗旨與目標的機會，並能預防或減少在實驗室活動中非預期的衝擊與潛在失效應，所以實驗室首先要確認實驗室的宗旨與目標。宗旨在新版 ISO 17025 中是用 purpose 這個字，而目標則是用 objectives，簡單的說就是實驗室想為客戶作什麼與實驗室想達成什麼？

所以實驗室可以運用使命與願景來說明宗旨與目標，使命是實驗室存在的價值以及所應從事的任務，而願景則是實驗室想要實現的夢想或心願，也就是對未來藍圖所做的宣示。也就是說實驗室要根據如總體政經環境、產業競爭、市場需求、品質文化、組織結構、服務流程等這些與測試或校正服務有關的內外部因素，來界定使命與願景，說明宗旨與目標。

使命與願景可以讓實驗室在變動的環境中，釐清我們目前在那裡？我們要往那裡去？我們要如何去？這些問題，並讓內外相關人員了解實驗室的方向，和自己要扮演的角色與要發揮的功能。

同時根據內外部因素的了解與以及使命和願景，實驗室可以了解如法規要求、產業準則，客戶期望等需求，分析實驗室的風險承受能力，而決定如風險何時需要處理、如何判定可接受或可忍受風險之決策標準等風險準則。

2. 衝擊事件鑑別

實驗室面臨的經營環境處處充滿不確定性，這些不確定因素，對實驗室實現其宗旨與目標可能會發生影響，所以實驗室要經由衝擊事件的鑑別過程，思考所有會影響目標達成的各項因素，找出實驗室營運環境與作業活動中，有那些對達成實驗室宗旨與目標的會有正負面影響的衝擊事件。

衝擊事件鑑別是風險管理的首要步驟，因為只有全盤了解會造成各種影響的衝擊事件，才能夠預測可能造成的風險，或可能帶來的機會，進而選擇處理風險與機會的有效方法。

衝擊事件鑑別是要鑑別可能發生或可能存在，且可能影響目標達成之狀況、事件或情境的原因與緣由，以及此衝擊影響之本質。這些衝擊事件可能是法規的改變，新技術的發展或是作業中的化學危害，對獨立實驗室來說，甚至可能是銀行放款利率的變動，因為會影響到營運成本。

所以在實務中我們可以從發展策略、營運作業、財務管理與災害事故等方面，來找出對實現其目標會有影響的衝擊事件。策略性風險與機會來自於總體政經環境、產業競爭與市場變動這些不確定因素。營運作業性風險與機會來自於管理制度、控制方法、人為操作及惡意破壞或積極協助等不確定因素。財務性風險與機會來自於國內外經濟因素變動、客戶之信用與現金流量等不確定因素。災害事故性風險則來自於實驗室作業中，各種對安全健康會有影響的物理、化學、生物與人因性等危害。

3. 風險與機會分析

風險與機會分析是在現有的控制方法下，估計衝擊事件的後果 (impact) 與這些結果發生的可能性 (likelihood)，確認這些影響的風險有多高或機會有多大。

風險與機會分析的基礎，其實就是我們在中學讀機率時所學過的期望值，我們知道如果 M 是當事件發生後的期望獲益情況，而 P 是事件發生機率，則期望值就等於「獲益情況」 \times 「發生機率」也就是 $M \times P$ ，因此如果 S 表示當事件發生後的可能損失情況，則風險值就等於「損失情況」 \times 「發生機率」也就是 $S \times P$ 。

分析風險與機會的方法很多，可以分為定性、半定量與定量三大類，ISO 31010:2009 風險管理－風險評鑑技術這份標準中，提供了如腦力激盪、結構化「如果-怎樣」技法、危害與操作性研究、故障樹分析、失效模式與效應分析與後果機率矩陣等 31 種風險管理方法，實驗室可以根據自己的規模與需求，來選用適當方法。

定性分析是使用文字的形式或是敘述性的分類等級，來描述可能影響的程度以及發生的可能性。譬如說在表 2 中就是以嚴重或顯著、普通、輕微表示影響的分類，以幾乎確定、可能、幾乎不可能表示發生的可能性，以高、中及低三級來界定風險或機會。

在半定量分析中，會以實際數值表示上述的定性分析等級，但是每一個敘述的數值並不直接等於實際的影響程度及機率。半定量分析的目的是決定一個比定性分析更精確的優先順序，但並不會決定風險的實際價值，我們在本系列第一篇－新版 ISO 17025 與公正性風險管理中所介紹的，在實務中最常被大家用來分析風險的 ISO 31010:2009 第 29 種方法後果/機率矩陣法，就是一種半定量方法。

有別於定性分析及半定量分析所使用的敘述性分類，定量分析則是使用來自如過去的紀錄、國外相關的經驗、產業的應用及經驗、相關文獻、行銷測試及市場研究等不同來源的實際數據，來說明影響及機率。

表 2 風險或機會定性分析

影響	輕微	普通	嚴重/顯著
可能性 幾乎確定	中	高	高
可能	低	中	高
幾乎不可能	低	低	中

本系列第一篇新版 ISO 17025 與公正性風險管理中，已簡單說明 ISO 31010:2009 第 29 種方法後果/機率矩陣法，本文再為大家介紹第 9 種方法，也是實務中常被大家用來分析風險的結構化「如果-怎樣」分析。「如果-怎樣」分析的原文是 What-If Analysis，所以也常被稱為 What-If 分析，這個方法就是

如表 3 與表 4 所示，就是以「如果事件發生，會有什麼影響？」這樣的問題，來分析衝擊事件的影響，與所可能產生的風險或所帶來的機會。對實驗室來說，後果/機率矩陣法與「如果-怎樣」分析，都是比較簡單而容易上手的方法。

表 3 以 What-If 分析法分析風險

如果	會造成	現有管控措施	風險分析			優先順序
			負面後果	可能性	風險	
沒有校正	不確定度偏高	每月催校	輕微	可能	低	
操作技術不良	化學溶液噴濺	防護衣與手套	普通	可能	中	優先

表 4 以 What-If 分析法分析機會

如果	會造成	現有管控措施	機會分析			優先順序
			正面效果	可能性	機會	
法規變嚴格	測試需求增加	經由銷售爭取客戶	顯著	可能	高	優先
購買新型設備	測試時間縮短滿意提昇	採用傳統設備	顯著	幾乎不可能	中	

What-If 分析除了可以像表 3 與表 4，根據表 2 之定性風險分級進行分析，也可以根據本系列第一篇新版 ISO 17025 與公正性風險管理中，所說明的後果/機率矩陣法之半定量風險分級進行分析，實驗室可以根據自己的需要，決定要採用那一種分析方法。

4. 風險與機會評估

風險與機會評估之目的就是要根據風險與機會分析之結果，決定那些機會需要注意？那些風險需要預防？那些風險與機會需要處理？也就是要如表 3 與表 4 中最右欄所示，決定處理實施的優先順序。

5. 風險與機會處理

新版 ISO 17025 8.5 節中要求實驗室應規劃風險與機會的應對處理措施，而且對於風險與機會所採取的應對措施，應適合其對實驗室結果有效性的潛在衝擊。所以風險與機會處理就是指綜合考慮實驗室的目標、管理能力、核心競爭力與風險承受能力和等因素，對需要處理的風險與機會，根據這些風險與機會對實驗室

結果有效性的潛在衝擊，來決定如何回應、掌握或抓住機會？如何控制、預防或降低風險？如何在管理系統過程中納入和應用這些措施？如何評價這些措施的有效性？

對於風險，實驗室可以參考新版 ISO 17025 8.5 節註 1，考慮識別與避免威脅、承擔風險以追求機會、消除風險來源、改變風險可能性或後果、分擔風險或經由掌握資訊的明智決策保留風險等各種方法。而對於機會，實驗室則可以參考新版 ISO 17025 8.5 節註 2，考慮擴大實驗室的活動範圍、對應新客戶、使用新技術與其他對應客戶需求之可能性等各種方法。

6. 溝通協商與監督審查

新版 ISO 17025 8.5 節中要求實驗室應規劃如何在管理系統中納入和應用風險與機會的應對處理措施，以及如何評價這些措施的有效性，同時在 8.9.2 節中規定管理審查中要審查風險鑑別之結果。

所以在風險與機會管理過程中，實驗室應持續與內外利害相關者保持良好的雙向溝通與協商管道，在管理系統中納入和應用風險與機會的應對處理措施，同時並對風險與機會的管理狀況與管理系統，進行持續之監督與審查，以掌握風險與機會的變化與趨勢，並確保風險與機會之處理措施的適宜性與有效性。

五、結 語

新版 ISO/IEC 17025 DIS 在管理系統之規定中，改為實驗室有 A 與 B 兩個選擇，實驗室可以選擇 A 方案，依照 8.1.2 節之規定，在文件管制等 8 個方面建立基本管理系統，或者選擇 B 方案，建立符合 ISO 9001:2015 之要求的管理系統。如果實驗室選擇 A 方案，則實驗室要依照 8.5 節考慮風險與機會。

如果實驗室選擇 A 方案，則實驗室可以引用 ISO 31000:2009 或美國 COSO 於 2004 年 9 月所發布之「企業風險管理－整合架構」中對於風險之定義，並根據自己的規模與需求，參考這兩模式，規劃自己的風險與機會管理過程，或參考圖 3 所示之簡易風險與機會管理過程，推動風險管理。

新版標準雖然還需要一段時間才會公佈，但我們如果能夠先作準備，將來將會比較能夠事半功倍，因此有興趣的實驗室可以參考本文所討論之方法，推動風險與機會管理，以便為將來推動管理革新，精益求精預先作好準備。

參 考 資 料

1. 行政院研究發展考核委員會(98年), 風險管理及危機處理作業手冊, 台北: 行政院研究發展考核委員會。
2. 廖志恆(100年), ISO/TS 22367 醫學實驗室-利用風險管理與持續改善來減少錯誤介紹, 認證報導第3期, 台北: 全國認證基金會 Retrieved from <http://www.taftw.org.tw>。
3. 廖志恆(105年), 實驗室生物風險管理系統標準之發展現況, 認證報導第21期, 台北: 全國認證基金會 Retrieved from <http://www.taftw.org.tw>。
4. 樊國紀(106年), 新版 ISO 17025 與公正性風險管理, 量測中心教育訓練網, 新竹: 工研院量測技術發展中心 Retrieved from <http://cmsschool.itri.org.tw/index.aspx>
5. COSO (2004), Enterprise Risk Management---Integrated Framework, U.S.A.:COSO.
6. ISO (2008), ISO/TS 22367, Medical laboratories — Reduction of error through risk management and continual improvement, Switzerland:ISO.
7. ISO (2009), ISO 31000:2009, Risk management — Principles and guidelines, Switzerland:ISO.
8. ISO (2009), ISO 31010:2009, Risk management – Risk assessment techniques, Switzerland:ISO.
9. ISO (2016), ISO/IEC DIS 17025, General requirements for the competence of testing and calibration laboratories, Switzerland:ISO.

作者簡介：

工研院量測中心 ISO 9001 與 ISO 17025 特約講師樊國紀

樊國紀為成大土木工程碩士，IRCA 與 TRCert 認可 ISO 9001 主導稽核員，曾任 TUV Rheinland 台灣分公司 ISO 9001 主稽核員、ABB 台灣分公司品質經理、大陸工程公司品質部經理、工研院量測中心機械認證部經理，有 30 年實務經驗，熟悉 ISO 9001 與 ISO 17025 之理論與實務。