

ISO 9001:2015 之風險管理稽核實務

如何滿足新版 QMS 標準的風險管理要求？

撰文：BSI 英國標準協會台灣分公司

品質管理系統產品經理

蘇宗明 (Jeffrey Su)



ISO 9001:2015 標準自 2015 年 11 月 15 日發佈後，許多企業感覺到新版對風險管理 (Risk-based thinking) 的新要求，很不好展現如何滿足條款此一要求。首先我們須了解的是，ISO 9001:2015 條款並沒有要求組織一定要採用何種風險管理標準。不過，目前有幾個風險管理國際標準可供企業界參考或使用，簡介如下：

ISO 31000:		
(a)	Risk Management– Principles and Guidelines	風險管理—原則及指引
ISO 31004:		
(b)	Risk Management– Guidance for the implementation of ISO 31000	風險管理—執行 ISO 31000 之指導綱要
ISO 31010:		
(c)	Risk Management– Risk Assessment Techniques	風險管理—風險評估技術
ISO 14971:		
(d)	Risk Management for Medical Device	醫療器材之風險管理

在 ISO 9001:2015 標準中許多地方提及風險管理要求，要求組織應以風險為基礎的思考模式 (Risk-based thinking)，例如：條款 6.1.1 及 6.1.2 (處理風險和機會的行動；Actions to address risks and opportunities)、0.1(總則)、0.3.1 (流程方法—總則)、0.3.3 (流程方法—風險導向的思維)、4.4.1 (f) (品質管理系統及其流程；QMS and its Processes)、5.1.1 (d) (領導統御與承諾—一般要求；Leadership and commitment)、5.1.2(客戶導向；Customer focus)、

9.3.2 (e) (管理審查的輸入；Management Review input)，附錄 A4、A5 及 A8.....等。

風險是不確定性的影響，可以是正面或負面的

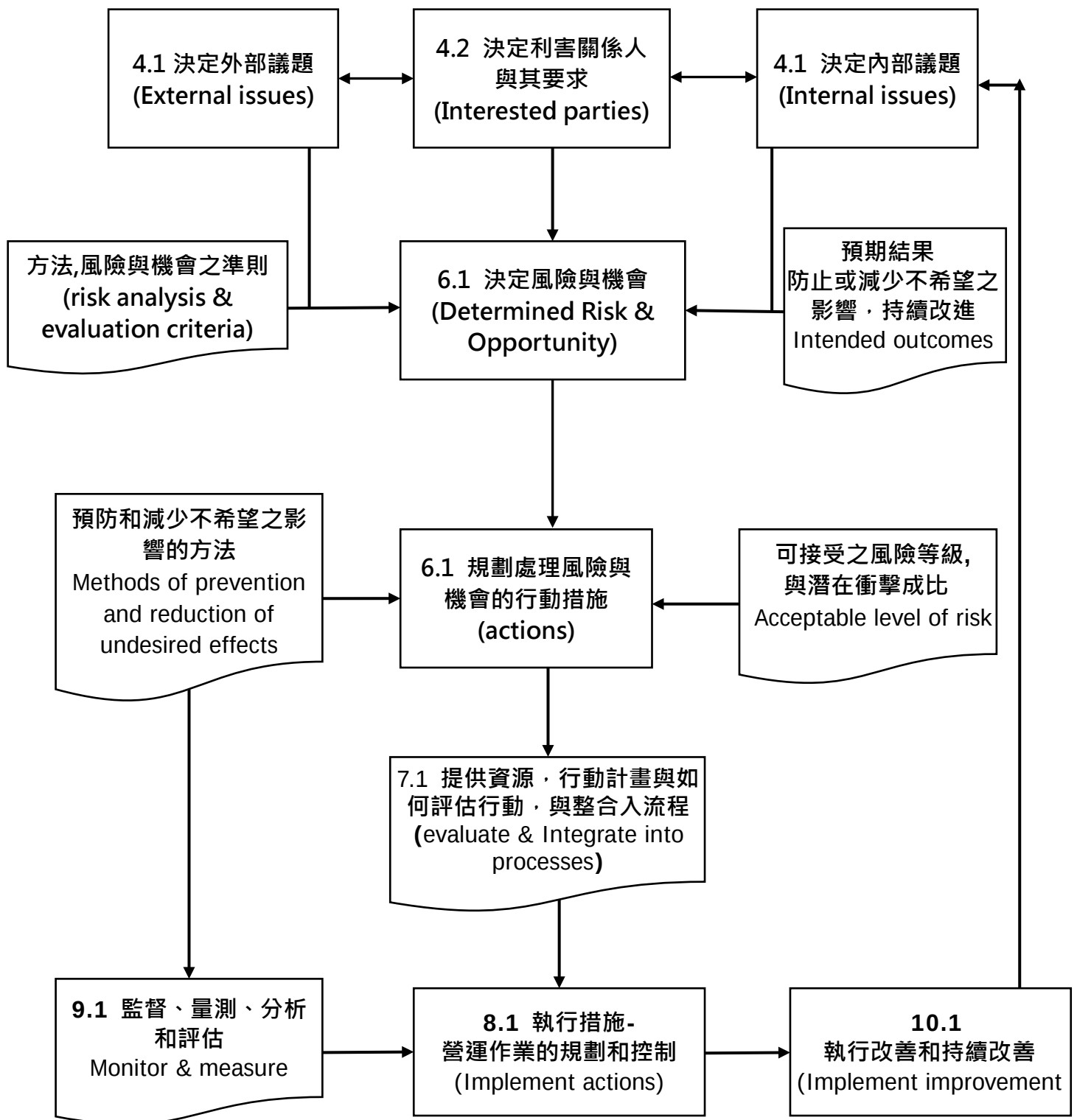
依據 ISO 9000:2015 標準之定義，風險是「不確定性之影響」(effect of uncertainty)。此影響乃是指對預期結果之偏離。按 ISO 31000:2009 標準之定義，風險是「對目標之不確定性的效應」。兩者的定義不但相同，而且同時說明風險可以是正面的，也可以是負面的。此點與一般世俗的認知不同，一般人大都認為風險是負面的。在 ISO 9001:2015 標準中，正面的風險可以形成機會 (Opportunity)，此機會 (Opportunity) 組織應考慮加以善用，以形成組織的競爭優勢。另外，ISO 14971:2012 標準定義風險是「傷害發生的機率與該傷害的嚴重度之結合」(Risk: combination of the probability of occurrence of harm and the severity of that harm)。雖然說法不同，但是其精義是一樣的。

按 ISO 31000:2009 標準之定義，風險管理是「指導及管制組織有關風險的協調活動」(risk management: coordinated activities to direct and control an organization with regard to risk)。因此組織可以考量從條款 4.1 了解組織及其背景，條款 4.2 了解利害關係人的需求和期望，及組織的產品和服務出發，外加考慮其他的輸入，以規劃組織所需要的品質管理系統。同時應考慮條款 4.1 所提及的議題，和條款 4.2 所提及的要求，並決定所需要處理的風險和機會，進而規劃處理風險與機會的行動措施，將行動計畫與如何評估行動整合入組織商業

流程，執行措施-營運作業的規劃和控制，進行監督、量測、分析和評估，及執行改善和持續改善。以流程方法呈現，形成 PDCA 循環，及展現持續改善之精神。此風險管理運作流程如下頁圖一所示。



圖一：風險管理流程



考量組織背景的內外部議題

當組織考量條款 4.1 了解組織及其背景時，可從下列方面考量組織的內部議題及外部議題，進而決定出所需處理的風險及機會。例子可能包括，但是不局限於：

1. 外部議題有關於

(a) 社會因素 (social factors)	例如：本地失業率、治安知覺、教育水準、例假日和工作日
(b) 政治因素 (political factors)	例如：政治穩定、公共投資、本地基礎設施、國際貿易協定
(c) 技術因素 (technological factors)	例如：新技術、材料和設備、專利終止、專業道德規範
(d) 經濟因素 (economic factors)	例如：經濟狀況、匯率變動、通貨膨脹、銀行放款
(e) 競爭的市場因素 (market factors)	例如：組織的市場配額、類似產品或者服務、市場領導者趨勢及行動、客戶發展趨勢、市場穩定、供應鏈關係
(f) 影響工作環境的法律和規章因素	例如：有關該產業的工會規章和規章

2. 內部議題有關於

(a) 組織的績效 (overall performance)	
(b) 資源因素 (resource factors)	例如：基礎設施、內部經營環境、組織所擁有的知識及技術
(c) 人力因素 (human aspects)	例如：人員能力、組織行為、組織文化、與工會的關係
(d) 操作因素 (operational factors)	例如：流程或者生產和服務供應能力、品質管理系統的績效、客戶滿意度
(e) 管理因素 (factors in the governance)	例如：組織結構及領導統御和決策的原則及程序

從策略觀點，也可利用 SWOT 及 PESTLE 工具。所謂 SWOT 分析是指：強項、弱點、機會和威脅分析；所謂 PESTLE 分析是指：政治、經濟、社會、技術、法律和環境分析。此外，一些簡單方法，例如腦力激盪法 (brainstorming) 及「如果，怎麼辦」問題法 (what if questions) 則對於一些小型企業或組織，也是可以考慮的方法。

考量利害關係人的需求和期望

當組織考量條款 4.2 了解利害關係人的需求和期望時，可從下列方面考量組織的內部關係人及外部關係人的需求和期望，進而決定出所需處理的風險及機會。每個組織之利害關係人都是獨特的。組織可以透過考慮下列要素，發展出決定利害關係人之準則：

考 量 要 素	(a) 可能影響或者衝擊組織的績效或者決策
	(b) 產生風險和機會的能力
	(c) 可能影響或者衝擊市場
	(d) 透過他們的決定或者活動影響組織之能力

而內部關係人及外部利害關係人的例子可能包括下列各項，但是不局限於：

內 、 外 部 利 害 關 係 人	(a) 客戶 (customers)
	(b) 最終使用者 (end users)
	(c) 經銷商 (franchisors)
	(d) 智慧產權的擁有人 (owners of intellectual property)
	(e) 總公司和附屬機構 (parent and subsidiary organization)
	(f) 擁有人，股東 (shareholders)
	(g) 銀行家 (bankers)
	(h) 工會 (unions)
	(i) 外部提供者 (external providers)
	(j) 員工和其他人代表組織工作 (employees)
	(k) 法律和規章當局 (statutory and regulatory authorities)
	(l) 貿易和專業組織 (trade and professional associations)
	(m) 地方社團 (local community groups)
	(n) 非政府組織 (non-government organizations)
	(o) 相鄰組織 (neighboring organizations)
	(p) 競爭者 (competitors)

為了理解利害關係人的需求和期望，下列幾項活動和方法可以進行。方法包括，但是不局限於：

方 法	(a) 審查訂單
	(b) 審查法律和規章要求
	(c) 游說和聯絡網
	(d) 參加相關協會
	(e) 標竿企業
	(f) 市場監視
	(g) 審查供應鏈的關係
	(h) 執行客戶或者客戶調查
	(i) 監督客戶需求、期望和滿意程度

因此，可能的利害關係人之要求包括，但是不局限於下列各項：

利 害 關 係 人 要 求	(a) 對於產品一致性，價格，供應性，或者準時交貨的要求
	(b) 與客戶或者外部提供者的合約
	(c) 工業規則和標準
	(d) 與社團或者非政府組織的協議
	(e) 提供的產品或者服務的法定和規章要求，以及影響組織的提供那種產品或者服務的能力的那些
	(f) 與他機構的備忘錄
	(g) 授權的許可證或者其他形式
	(h) 主管機構發布的命令
	(i) 條約，議定書，和協議
	(j) 與政府機構和客戶的協議
	(k) 自願的工業規則或者業務守則
	(l) 自願實施或者環境承諾
	(m) 在合約下的組織義務
	(n) 對員工的政策

在規劃品質管理系統時，應考慮此些活動產生的訊息。組織應該意識到利害關係人和他們的相關要求，此些要求會因不同產品或提供不同服務而不同，並且會因不可預期的事故或者市場的回應而有所改變。

選擇適當方式評估風險，以完成風險管理流程

風險評估(Risk assessment) 基本上包括風險鑑別(Risk identification)、風險分析 (Risk analysis) 及風險評價 (Risk evaluation) 的整個流程。

風 險 評 估		
風險鑑別	風險分析	風險評價
風險鑑別是指發現，認知及描述風險的流程。	風險分析是理解風險的本質，並決定風險等級的流程。	風險評價是將風險分析之結果與風險準則相比較，以決定風險及/或其規模是否可接受或可容忍之流程。

至於風險分析的方法亦有許多方式可供組織使用，例如：

- 失效模式與效應分析 (Failure Mode and Effects Analysis, FMEA)
- 多因子打分評價法 (Multiple Factors Scoring Analysis, MFSA)
- 初步危害分析 (Preliminary Hazard Analysis, PHA)
- 故障樹分析 (Fault Tree Analysis, FTA)
- 危害與可操作性研究 (Hazard and Operability Study, HAZOP)
- 危害分析與關鍵控制點 (Hazard Analysis and Critical Control Point, HACCP) ...等

組織可以依自我情境選擇適合自己的風險分析方法，以執行風險導向的思考模式，完成風險管理流程，以滿足 ISO 9001:2015 標準的要求。●



bsi. 訓練學苑
Training Academy



取得 ISO 9001:2015 標準

- [BSI 商店](#)
- [BSOL 線上標準資料庫](#)

[ISO 9001:2015 轉版課程](#)

- 轉版建置課程
- 稽核員轉版 (IRCA) 課程

[ISO 9001:2015 稽核驗證](#)

- 轉版稽核

BSI英國標準協會

T: +886 2 2656 0333 | E: infotaiwan@bsigroup.com | www.bsigroup.tw