IATF 16949:2016 之風險分析

撰文： BSI 英國標準協會
IATF 16949 產品經理
劉昱廷（Benson Liu）

風險思維是 ISO 9001:2015 改版所引入之重要概念，是規劃與實施品質系統都要考量的重點，控制風險，使品質系統能發揮其功能，以達成組織之目標。但條文對此風險分析只給出基本框架之要求，各業界也發展出許多不同之方法，優劣各表，總是令大家覺得迷惑，不知如何上手。故我們參酌 ISO 31000 風險管理指導，依照 ISO 9001:2015 條文之要求，發展出各行業皆可適用之風險分析方法，以令組織人員能輕易理解上手，容易鑑別出品質系統之顯著風險。之後能建立風險管理平台，整合決策所有流程活動，持續降低風險，達成組織目的與目標。

此風險分析方法以表單格式，展現其風險分析之架構與邏輯展開，以能夠收斂之方式鑑別出組織的顯著風險，再進一步管理這些顯著風險，亦即將這些管控措施內化於程序書或系統文件中，形成制度，形成 PDCA 循環，方能真正落實風險管理於品質系統中。

基於風險之思維（Risk Based Thinking），ISO 9001:2015 揭櫫一個主要概念：風險與機會之分析與處理。在建置規劃品質系統時（系統即是由流程所構成），每個流程在訂定時，皆須考量風險與機會，設置相關管控以確保達成流程之目標。當每個流程都分析過風險並採取對應措施策略時，整個品質管理系統的風險就控制了。以下就以標準在組織流程中使用風險導向方法（Risk Driven Approach）進行說明：

ISO 9001:2015 所提之風險

ISO 9001:2015 4.4 條文：

4.4.1 組織應依照本國際標準之要求建立、實施、維持和持續改善品質管理系統，包括所需的流程和流程的相互關係。

組織應決定品質管理系統所需的流程和其於組織中的應用，並應：

a) 決定這些流程所需要的輸入與預期的輸出；

b) 決定這些流程的前後順序和相互關係；

c) 決定和應用所需的準則與方法(包括監督、量測和相關的績效指標)，以確保有效運作以及控制這些流程；

d) 決定這些流程的所需的資源，並確保可取得；

ISO 9001:2015 6.1 條文：

6.1.1 規劃品質管理系統時，組織應考慮條款 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，以：

a) 給予品質管理系統能達成其預期結果的保證；

b) 提高所期望的效果；

c) 預防或降低不期望的影響；

d) 達成持續改善。

6.1.2 組織應規劃：

a) 處理風險和機會的行動；

b) 該如何：

1) 在品質管理系統流程中，整合和實施這些行動（見第 4.4）；

2) 評估這些行動的有效性。

處理風險和機會的行動，應與其對產品和服務符合性的潛在衝擊相對稱。

風險之定義（ISO 9000）

Risk is the "effect of uncertainty on an expected result" and an effect is a positive or negative deviation from what is expected.

達成預期結果的不確定性

風險之定義（ISO 31000）

Risk - the effect of uncertainty on realization of objectives

不確定性對目標的影響

Deviation from the expected

Can be negative or positive

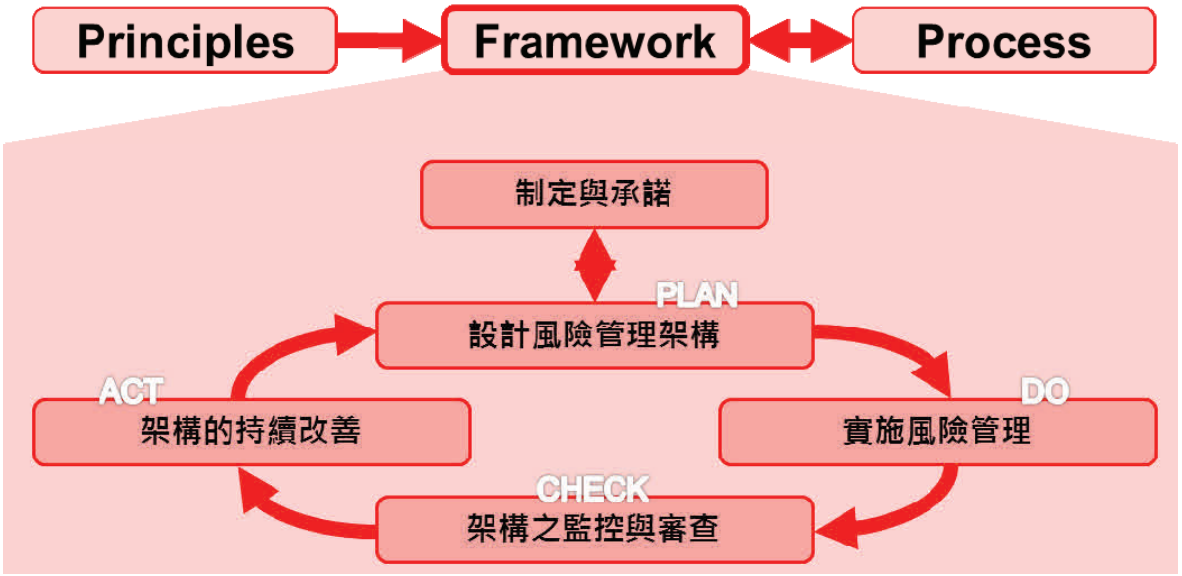
Can have multiple aspects (financial, environmental, health and safety…)

Can exist at different levels (strategic, organizational, site-specific, product, process…)

風險管理原則（ISO 31000）

1. Creates and protects value 風險管理創造並保護價值
2. Is an integral part of all organizational processes 風險管理嵌入組織的管理過程
3. Is part of decision making 風險管理支持決策過程
4. Explicitly addresses uncertainty 明確風險管理涉及的不確定性
5. Is systematic, structured and timely 風險管理是系統化的，結構化與及時的
6. Is based on the best available information 風險管理是基於最可信的訊息
7. Is tailored 風險管理是定製的
8. Takes human and cultural factors into account 風險管理考慮文化因素
9. Is transparent and inclusive 風險管理是透明與包容的
10. Is dynamic, iterative and responsive to change 風險管理是動態的，迭代的和適應變化的
11. Facilitates continual improvement of the organization 風險管理有利持續改善

風險管理架構（ISO 31000）

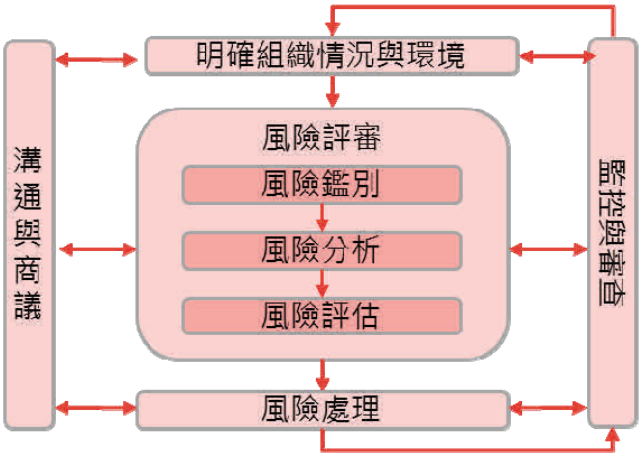


風險管理流程（ISO 31000）

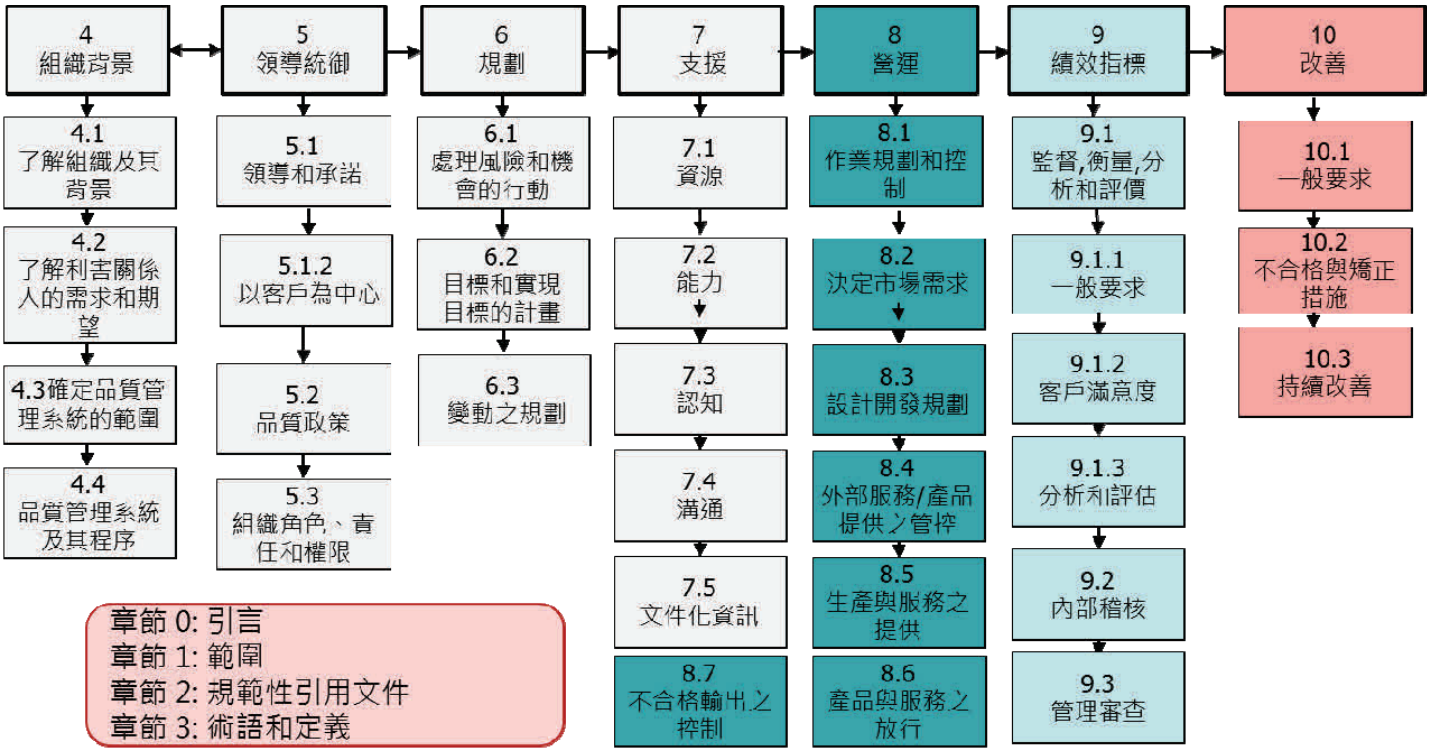
風險鑑別: 鑑別罩門與威脅，碰撞則形成風險，其隱含衝擊與機率。

風險分析: 對嚴重度與機率轉換成可量度的數字，以利科學化管理。

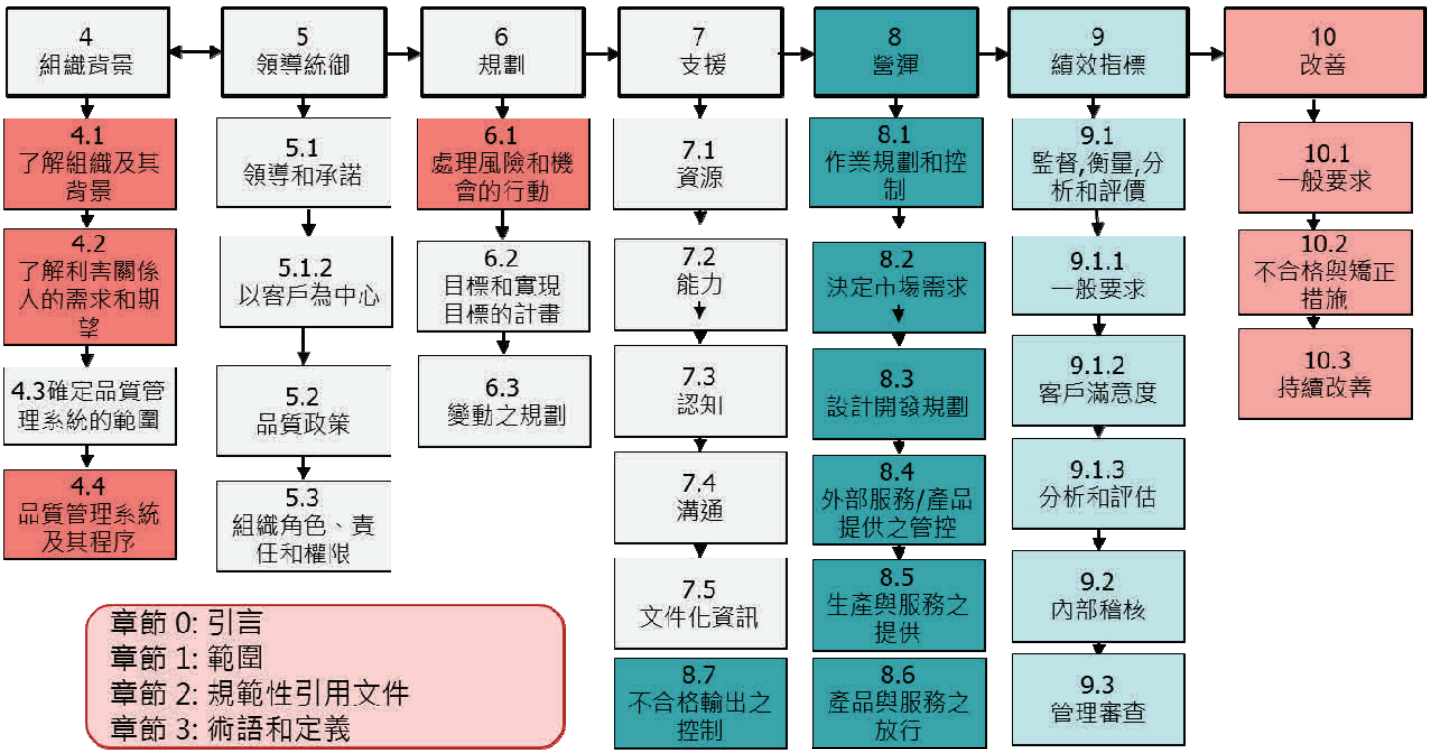
風險評估: 將各種風險相關評分和風險可接受水準做比對，超過者考慮進行風險處理。



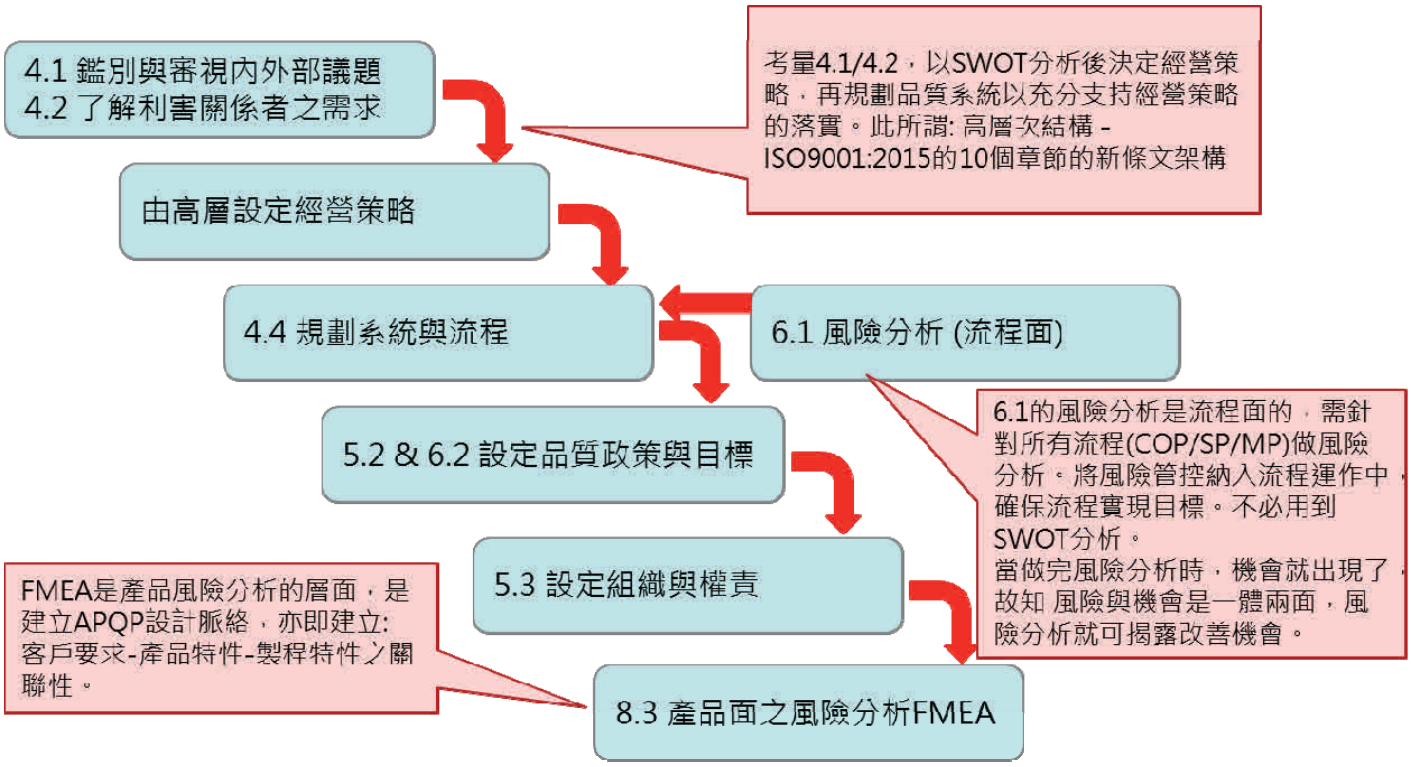
ISO 9001:2015 高階結構和「品質管理系統」結構

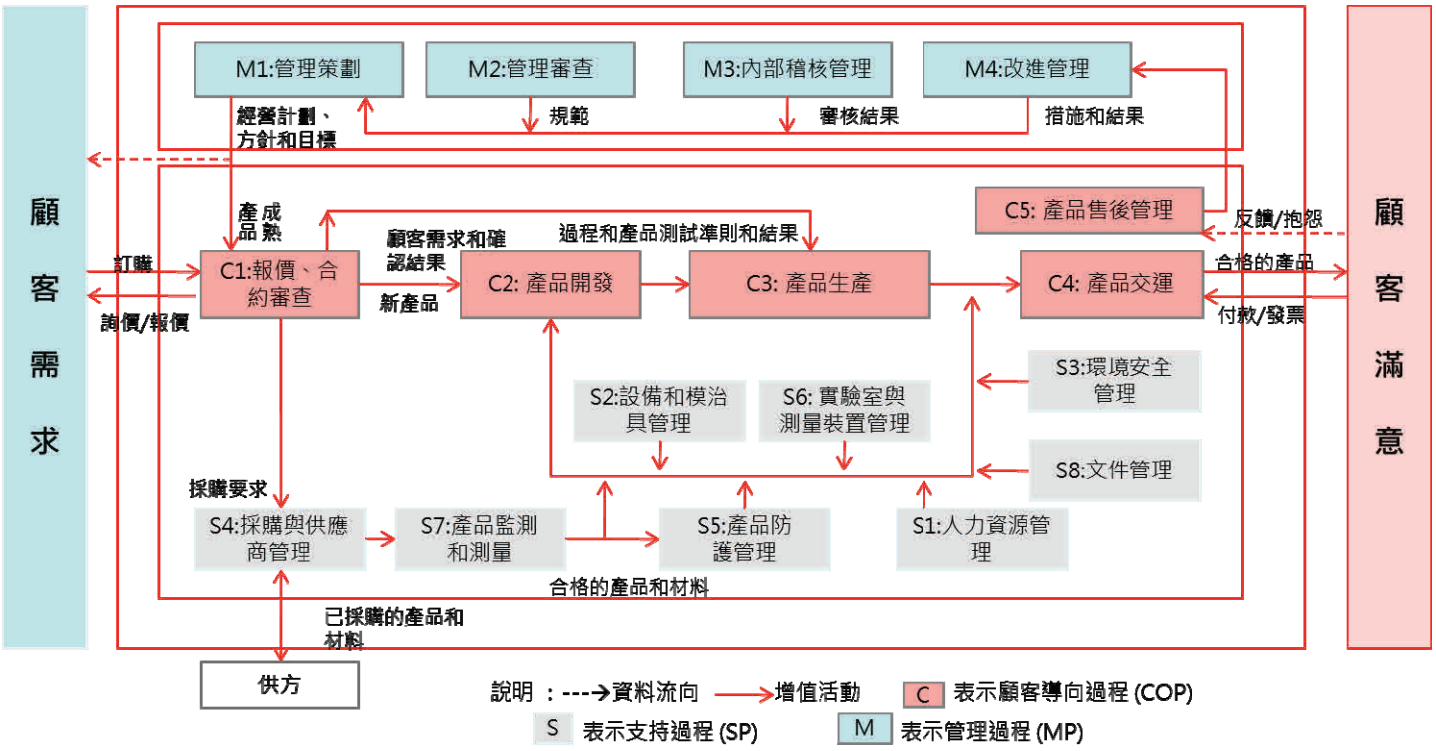


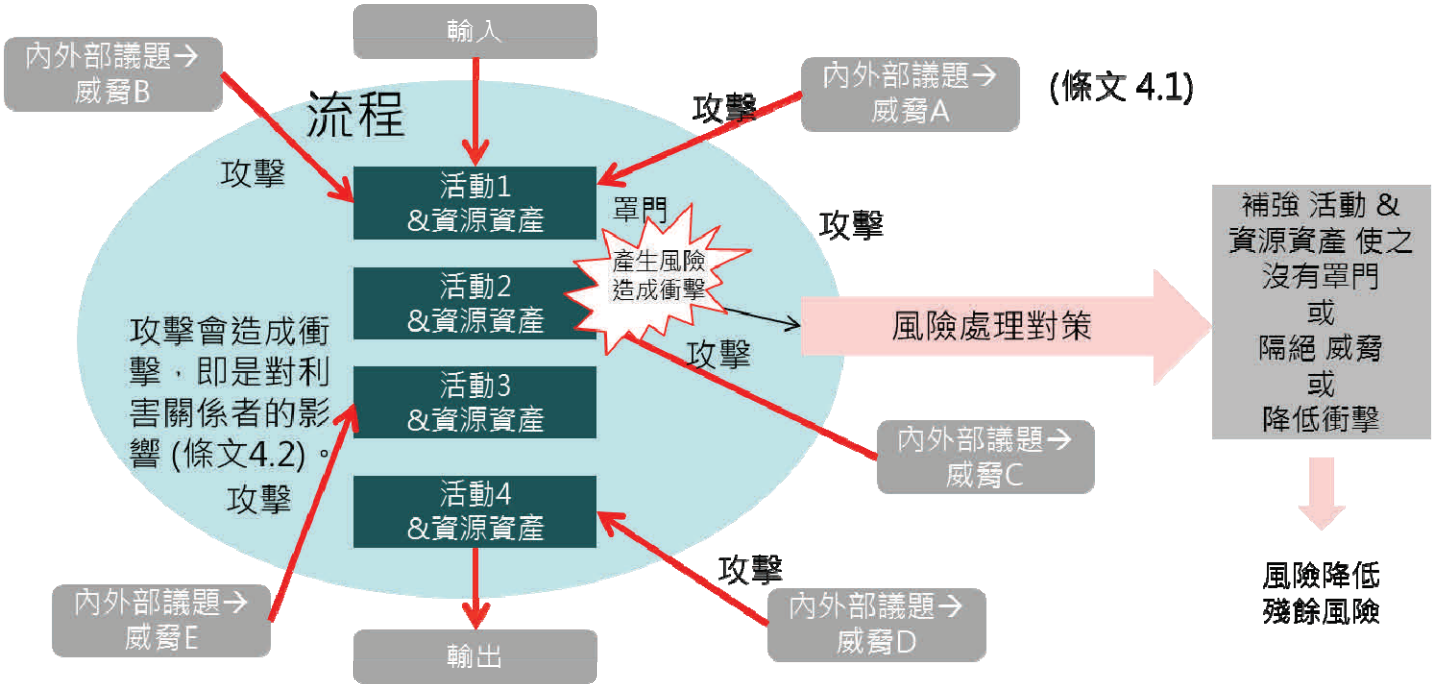
ISO9001:2015 高階結構「流程與風險」之主要相關條款



風險分析的層次


4.1 鑑別與審視內外部議題
4.2 了解利害關係者之需求
考量4.1/4.2，以SWOT分析後決定經營策略，再規劃品質系統以充分支持經營策略的落實。此所謂: 高層次結構 - ISO9001:2015的10個章節的新條文架構
由高層設定經營策略
4.4 規劃系統與流程
6.1 風險分析 (流程面)
6.1的風險分析是流程面的，需針對所有流程(COP/SP/MP)做風險分析。將風險管控納入流程運作中，確保流程實現目標。不必用到SWOT分析。
當做完風險分析時，機會就出現了，故知 風險與機會是一體兩面，風險分析就可揭露改善機會。
5.2 & 6.2 設定品質政策與目標
5.3 設定組織與權責
FMEA是產品風險分析的層面，是建立APQP設計脈絡，亦即建立: 客戶要求-產品特性-製程特性之關聯性。
8.3 產品面之風險分析FMEA


顧客需求
顧客滿意
M1:管理策劃
M2:管理審查
M3:內部稽核管理
M4:改進管理
經營計劃、方針和目標
規範
審核結果
措施和結果
產品成熟
訂購
詢價/報價
C1:報價、合約審查
顧客需求和確認結果
新產品
C2: 產品開發
過程和產品測試準則和結果
C3: 產品生產
C4: 產品交運
C5: 產品售後管理
反饋/抱怨
合格的產品
付款/發票
S3:環境安全管理
S2:設備和模治具管理
S6: 實驗室與測量裝置管理
S8:文件管理
採購要求
S4:採購與供應商管理
S7:產品監測和測量
S5:產品防護管理
S1:人力資源管理
合格的產品和材料
已採購的產品和材料
供方
說明 ：---→資料流向
增值活動
C 表示顧客導向過程 (COP)
S 表示支持過程 (SP)
M 表示管理過程 (MP)

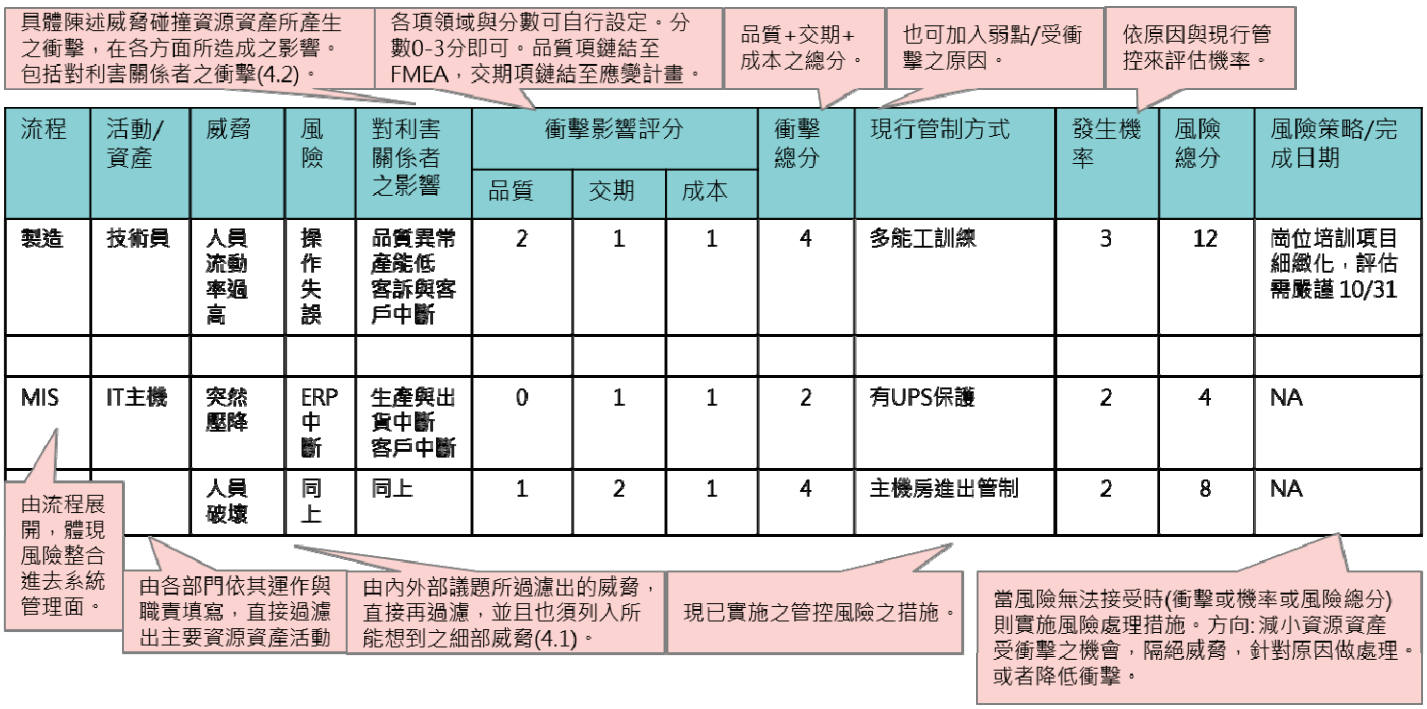


6.1 風險分析

風險之產生有兩個主要構成因素：罩門（流程裡面的重要活動或者重要活動裡面的重要資源資產）與 威脅(由內外部議題而來)。兩者缺一不可。互相碰撞產生風險，風險造成對利害關係者之影響以及發生之可能性。例如: 身體的免疫系統弱，碰巧遇上較強之病毒 就造成感冒。
風險分析在鑑別風險時，則同時也鑑別出了機會，因每一條都有可能變成改善之機會。是故風險與機會並提，風險與機會是一體兩面。

依此風險所構成之兩要素，改善機會出現時，改善方法有三個方面，一者強化罩門，如加強免疫系統，即使強大病毒來襲也不會受害；二者隔絕威脅，例如環境消毒或不到公共場所，則不會遇到病毒，就不會感冒；三者降低衝擊，例如儘速吃藥有效治療。

風險分析方法



流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
製造	**技術員**	**人員流動率過高**	**操作失誤**	**品質異常產能低客訴與客戶中斷**	2	1	1	4	**多能工訓練**	3	12	**崗位培訓項目細緻化，評估需嚴謹 10/31**
MIS	IT主機	**突然壓降**	ERP中斷	**生產與出貨中斷客戶中斷**	0	1	1	2	**有UPS保護**	2	4	NA
		人員破壞	同上	同上	1	2	1	4	**主機房進出管制**	2	8	NA

風險分析方法（表格範例展開）

- **流程**

依條文 4.4 與 6.1 之要求，風險分析需由流程來展開，故第一欄需先鑑別所需風險分析之流程，風險分析方能聚焦。且應該是由流程負責人去主導做此流程之風險分析。也需注意管理者與使用者的區別。如製造流程可以不用分析物料短缺與設備風險，因物料屬採購流程為管理者，由採購流程去展開物料短缺之風險分析。設備則是廠務單位為管理者，由廠務單位展開設備管理流程之風險分析。製程是使用者，採購與廠務應詢問製程二者風險發生時對製程的影響程度以執行風險分析。不可由部門來展開，條文強調流程方法。

- **活動/資產**

風險分析由流程來展開，但流程很大，需予以切割出重要活動，重要資源資產（包括設備、基礎設施、ERP、database、技術、專利...），才能和威脅碰撞，得出確切之風險。不重要之活動/資源/資產可以不列出，因為既然不重要，則必定是低風險，直接可忽略不列出。風險分析的原則是「收斂」，此是第一個收斂。舉例：冰水主機是空調的製冷機構，是否為重要資產則看生產線是否需依賴它維持作業環境，以確保品質，或者 IT 主機房需依賴它降溫，否則當機，會造成生產中斷或出貨停止，則知冰水主機是重要資產，應列入並和威脅碰撞，以分析其風險。當填入的項目過大，則無法分析時，則需再切割，如：若填入「設備」，則太廣，無法得到確切風險，則須分裂為： CNC 機床、研磨機...方能展開其風險分析。

重要活動如：訂單審查，客訴的原因與問題解析，調機首件確認...等等。若能解析則予以風險分析，不行就再切割成：人員、設施、設備...等等，再做風險分析。

- **威脅**

威脅即是由內外部議題過濾而來的。活動/資產必須遇到威脅才會產生風險。兩者缺一不可。故風險分析需考慮 4.1 之要求。而威脅需由流程負責人參考內外部議題，自行找出對其流程有影響者，碰撞以產生風險。此為第二個收斂。

製造流程風險分析很多時候做起來會跟 P-FMEA 一樣。其實兩者有很大不同。流程面風險分析主要對應到議題與風險。而 P-FMEA 則是建立產品特性與製程特性之設計脈絡。

一般常見之威脅：人員流動、技能/知識不足、供應商支持、客戶要求提高、市場競爭、匯率/原物料變動....。

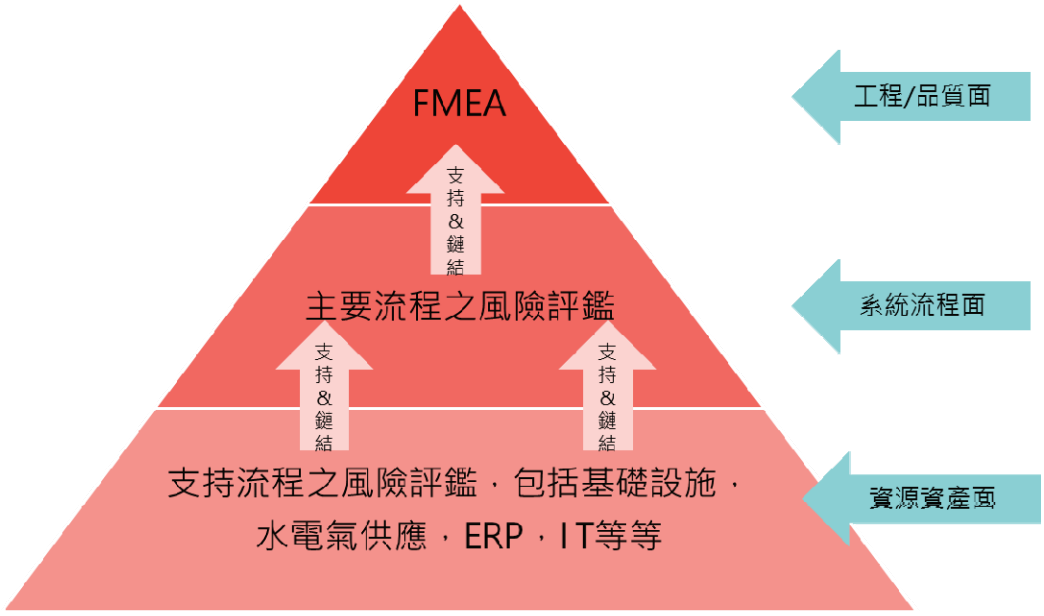
風險分析方法『錯誤』示範

第一行與第二行之威脅內容偏向製程條件異常，屬於P-FMEA範疇。應考慮大方向，如內外部議題: 停電，壓降，人員技術能力不足 等等來展開風險。

流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
製造	**首件調機活動**	**溫度異常**	**品質跳動**	**品質異常客訴與客戶中斷**	2	1	1	4	**首件確認**	3	12	NA
	生產中	**刀具磨耗**	**同上**	**同上**	2	1	1	4	**自主檢&巡檢**	3	12	NA
	CNC車床	**突然壓降**	**機台內傷**	**品質異常造成客訴**	2	1	1	4	**有UPS保護**	1	4	NA

第三行之資產屬於廠務部範疇。應由管理者”廠務”來展開風險，衝擊影響再詢問使用者: 製造與品保部。

風險評鑑分析之層次



● 風險

活動/資產碰到威脅才能產生風險，風險即是組織可觀察到的危害情況，一般比較少列出正面情況。如：產生大量報廢、設備故障停機、設備精度劣化、生產效益降低、生產中斷、產品損壞....等等。（此即所謂「風險鑑別 Risk identification」）。
許多組織會不顧活動與威脅，直接列出風險，假設一個流程有七個活動，就直接列出七個「某某活動沒有做好」。如此則形成發散分析，沒有聚焦。所提風險改善行動也會粗糙並且漏掉隔絕威脅的方案。

● 對利害關係者之影響

風險所造成對於利害關係者之衝擊與影響需明確指出於此欄位（汽車業還是最關注對汽車客戶之衝擊）。活動資產與威脅是因緣，造成果的風險。而風險又成為因，造成利害關係者之衝擊為果。此即所謂二重因果。此欄位亦即呈現條文：風險分析需考慮 4.2 之要求。
風險包含衝擊影響與機率，需予以數據化（即 ISO 31000 所謂風險分析 risk analysis）方能做科學化管理。而數據化之前須明確其影響程度。其後就能接者做出衝擊影響評分。

● 衝擊影響評分

依據前面具體的衝擊，我們可以建立一個評分表，來衡量此衝擊在各個面向的分數，即代表程度。此表各面向評分為 0-3 分，0 分是沒影響，3 分則影響程度高。此範例揭露三個面向：品質、交期、成本，一般是利害關係者最關注的期望。若覺得需要可以再加上「法令」，亦是一般利害關係者的期望。此即 ISO 31000 所謂的風險分析（Risk analysis）。

● 衝擊總分

衝擊總分為所有面向之衝擊分數加總。此範例之方法論係用加總。衝擊總分愈高，代表衝擊影響程度愈高。

● 現行管制方式

風險包括衝擊與機率。例如：人們走路喜歡走在騎樓內或人行道上，因為車輛會撞到的機率低，可能會跟腳踏車或他人相撞，但衝擊程度就較低。總的來說，衝擊與機率都低，故說風險低。而發生機率端視流程內的管控程度。有風險管控手段，發生機率就低。故此範例表格加入「現行管制方式」欄位，需實際反映現行流程針對風險管控之方式具體說明，方能於隨後之機率做正確之評分。另一方面是在風險發生後降低衝擊。衝擊與機率是互相獨立的。

● 發生機率

可以建立風險發生機率之評分表。此範例分數為 1,2,3,4 三個等級。4 的發生機率是最高的。此發生機率是和現行管控關聯。若無管控手段，則機率評分為 4。管控手段稍差，則機率評分為 3。以此類推。

- **風險總分**

風險總分則是衝擊總分乘以發生機率。此範例之方法論係用乘的。此風險總分呈現風險之程度，分數愈多代表風險愈高。

- **風險策略/完成日期**

應依據品質衝擊、交期衝擊、成本衝擊、衝擊總分、發生機率與風險總分，判斷其是否可接受（此即 ISO 31000 所謂的風險評估 Risk Evaluation），來決定風險處理策略（任何一項分數過高都可以考慮啟動風險處理策略）。

採取風險處理策略後（完成日期之後，應由流程負責人主導跟進），應評估其有效性，再決定其殘餘風險（即降低後的衝擊分數、機率分數與風險總分），若殘餘風險可接受，則納入流程管控中，修訂相關系統文件。並於此風險分析表另寫一行，呈現其現行管制方法與殘餘風險分數。

風險評估紅黃綠表

衝擊 機率	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16
5	5	10	15	20
6	6	12	18	24
7	7	14	21	28
8	8	16	24	32
9	9	18	27	36

風險評估可以參考左表。紅色代表需要採取風險處理行動，黃色代表可以考慮採取風險處理行動，綠色代表暫可接受此風險。但此表僅供參考，仍需依照各組織之合理適當之認定來決定是否採取行動以及何種程度之行動。

決定風險處理選項

可以從下列方向考慮：

■避免風險：當該風險影響極大時，便應設法極力阻隔風險

■降低風險：採取適當控制措施，當風險發生時可因適當控制而將損失減少。例如：建立災難應變的聯繫機制。

■轉移風險：考慮購買適當的保險，作為持續營運過程的一部分。許多遭逢災變的災民，均因缺乏保險，而沒有任何理賠補償，加重了災後復原的負擔與痛苦！

■接受風險：對於可接受之風險便可採取接受因應。

風險分析方法涵蓋其他條文 6.1.2.3

流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
MIS	IT 主機	突然壓降	ERP 中斷	生產與出貨中斷 客戶中斷	0	2	1	3	有 UPS 保護	1	3	BCP02
		人員破壞	同上	同上	1	2	1	4	主機房進出管制	1	4	BCP02

依條文 6.1.2.3 之要求，應變計畫擬定前須做風險分析，故可使用同一張風險分析表，來解析各流程可能會發生生產中斷或交貨中斷的風險，以決定在那些罩門須做應變計畫。

如上表所示 IT 主機掛掉，雖然機率不高，但因交期衝擊較大，仍需考慮應變計畫，故擬定應變計畫 BCP02，充作其風險對應策略。

有些時候，以適當之現行管制方式，也可不需制定應變計畫。例如設備故障，但有同型號機台備用，則直接於管制方式填入「使用同型號機台」，則可不須制定應變計畫。例如也可推高成品庫存，等設備修理好後再生產，則可不須制定應變計畫。當然其最長修理時間須估算，不能超過庫存用完之時間。

總之風險分析完才知需要那些應變計畫，再去擬定具體的應變計畫。

風險分析方法涵蓋其他條文 7.1.6

流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
製造	技術員	人員流動率過高	操作失誤	品質異常 產能低 客訴與客戶中斷	2	1	1	4	多能工訓練	2	8	崗位培訓項目細緻化，評估需嚴謹 10/31
開發	模具技術	依賴供應商	開發延誤	樣品延誤 客戶中斷	2	3	2	7	維持兩家供應商	2	14	徵入模具技術人才 12/31

依條文 7.1.6 組織知識之要求，風險分析表可於各流程鑑別維持流程運作之關鍵技術或知識，分析其缺漏風險，以決定其風險對應行動。

風險分析方法涵蓋其他條文 8.5.1.4

流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
廠務設施設備	CNC 五軸加工機	人員技能不足	撞機	品質異常 客訴與客戶中斷	2	2	2	6	多能工訓練	2	12	修復與額外驗證
	CNC 五軸加工機	瞬間斷電	內傷	品質異常 客訴與客戶中斷	2	2	2	6	NA	2	12	修復與額外驗證

依條文 8.5.1.4 之要求，風險分析表可鑑別精密設備，分析其風險，以決定其量產前的額外驗證。

風險分析方法涵蓋其他條文 6.3

流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
製造	技術員	人員流動率過高	操作失誤	品質異常 產能低 客訴與客戶中斷	2	1	1	4	多能工訓練	2	8	崗位培訓項目細緻化，評估需嚴謹 10/31
開發	模具技術	依賴供應商	ERP 中斷	生產與出貨中斷 客戶中斷	0	1	1	2	有 UPS 保護	1	2	NA

依條文 6.3 之要求，風險分析由流程來展開，故當有變更時，應需回到各流程之風險分析表，審視其風險是否可接受，是否延伸有其他副作用風險。

風險分析方法『錯誤』示範

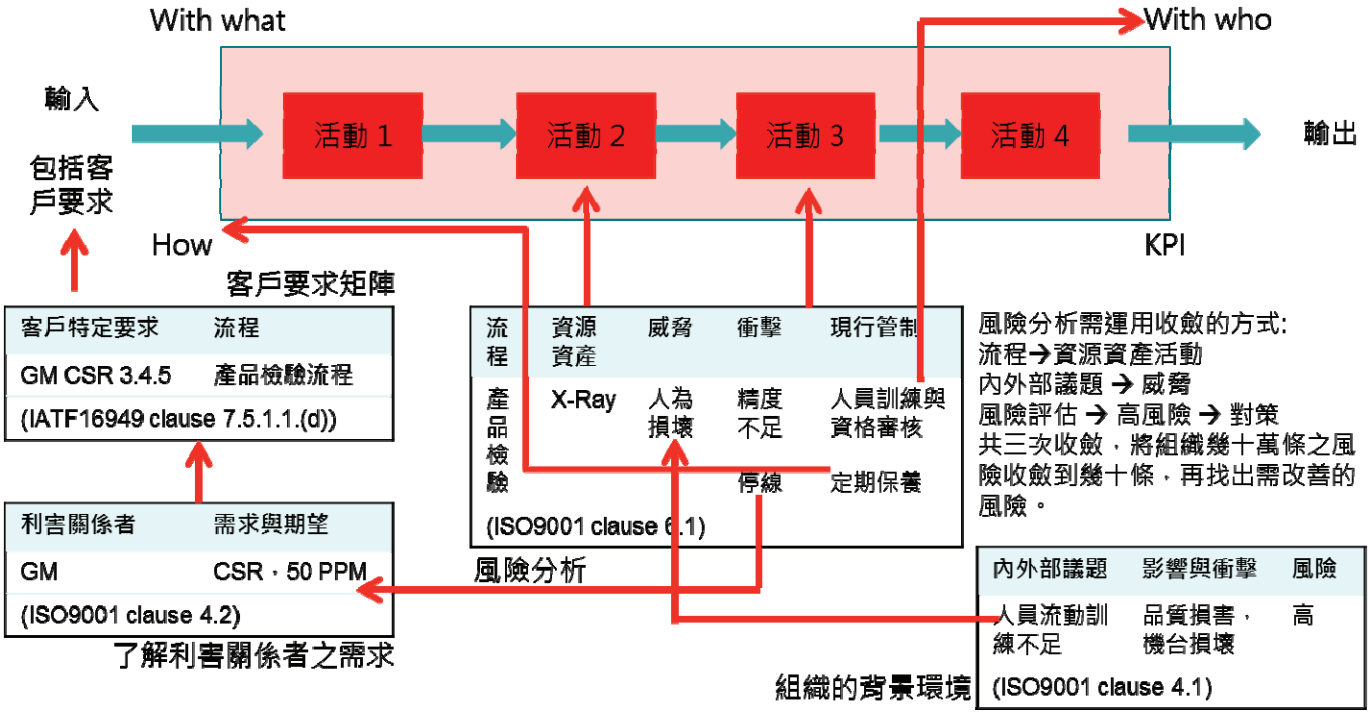
不能由"部門"展開風險分析。違反流程方法。

部門	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
			品質	交期	成本					
業務	訂單審查錯誤	品質不良	3	1	1	5	加強訂單審查	1	5	NA
	報價單出錯	虧錢	1	2	3	6	加強報價審查	1	6	NA
	回覆客戶錯誤	客訴	2	2	2	6	注意客戶回覆	1	6	NA
	給生管之內部訂單出錯	交期延誤	1	2	1	4	加強管控	1	4	NA
	客訴回覆錯誤	客訴	2	1	1	4	注意客戶回覆	1	4	NA

風險分析沒有包括主要活動與內外部議題(威脅)。風險直接列出。以各步驟沒做好直接列出風險。風險分析破碎沒有聚焦。

風險分析破碎沒有聚焦。導致其管控方式過於空泛。無法針對提升活動/資產強度與隔絕威脅之方式提出具體解決方案。

流程方法融入風險思維



風險評鑑 : ISO 9001:2008 → ISO 9001:2015（範例僅供參考）

具體陳述威脅碰撞資源資產所產生之衝擊，在各方面所造成之影響。包括對利害關係者之衝擊(4.2)。

各項領域與分數可自行設定。分數0-3分即可。品質項鏈結至FMEA，交期項鏈結至應變計畫。

品質，交期，成本之總分。

也可加入弱點/受衝擊之原因。

依原因與現行管控來評估機率。

流程	活動/資產	威脅	風險	對利害關係者之影響	衝擊影響評分			衝擊總分	現行管制方式	發生機率	風險總分	風險策略/完成日期
					品質	交期	成本					
製造	技術員	人員流動率過高	操作失誤	品質異常產能低客訴與客戶中斷	2	1	1	4	多能工訓練	2	8	崗位培訓項目細緻化，評估需嚴謹 10/31
MIS	IT 主機	突然壓降	ERP 中斷	生產與出貨中斷	0	1	1	2	有 UPS 保護	1	2	NA
		人員破壞	同上	同上	1	2	1	4	主機房進出管制	1	4	NA

由流程展開，體現風險整合進去系統管理面。

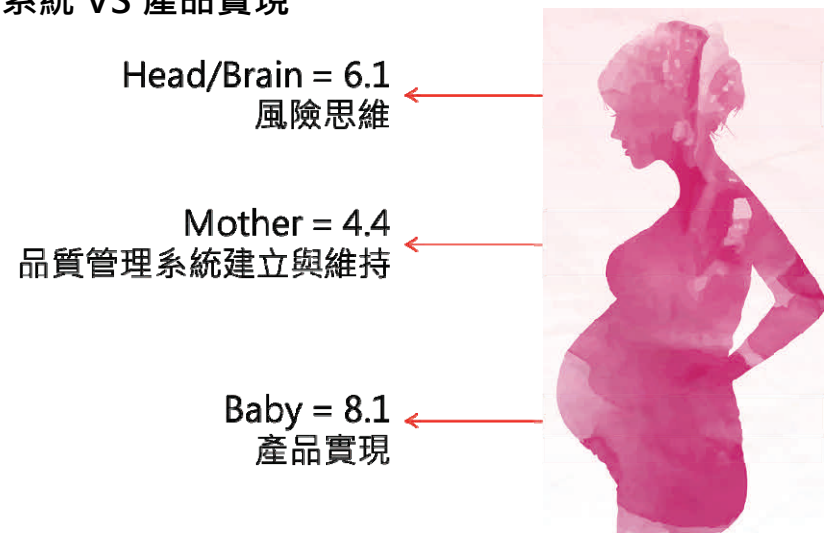
由各部門依其運作與職責填寫，直接過濾出主要資源資產活動

由內外部議題所過濾出的威脅，直接再過濾，並且也須列入所能想到之細部威脅(4.1)。

現已實施之管控風險之措施。

當風險無法接受時(衝擊或機率或風險總分)則實施風險處理措施。方向: 減小資源資產受衝擊之機會，隔絕威脅，針對原因做處理。或者降低衝擊。

品質管理系統 VS 產品實現



風險分析稽核之注意事項

工廠於導入 IATF 16949 時，應要求各流程之負責人展開其流程風險，並於管理代表處做彙整與審查。需確認各流程之所有顯著風險已被列入，風險分數適當正確，各風險管控措施與風險處理措施已被執行，併入各程序書或 SOP/表單中形成制度。

正式稽核時，稽核員會訪談流程負責人，了解其顯著風險，再審視風險分析表，看看是否顯著風險都已羅列，說寫一致。再確認其管控措施是否已執行，其功效如何，也會從其流程之 KPI 達成狀況相互印證。

例如，客訴處理常見之顯著風險：(1) 問題根因不易找出，威脅是人員技能經驗不足或無完整之分析設備。(2) 改善無效，威脅可能是設備能力或檢驗設備能力不足或供應商不支持...各流程負責人必須將風險管理思維融入其日常運作當中，確保說寫做一致。

新版！ IATF 16949 全球汽車產業品質管理系列課程

新版全球汽車品質管理系統標準已在 2016 年 10 月發布，更名為 IATF 16949:2016，並將取代目前 ISO/TS 16949。藉由新版系列課程學員可以了解新版標準條文、新舊版差異，以及五大核心工具的運用及作法。

IATF 16949:2016 轉版訓練課程

2 天

講解新舊版的差異。適合取得舊版內稽證書的學員轉版，以及需要知道新舊版差別的種子人員。

IATF 16949:2016 建置暨內部稽核員訓練課程

4 天

講解條文和運用，以及內部稽核技巧手法等訓練。

IATF 16949:2016 五大核心工具課程

2 天

解說五大核心的每個工具運用及作法。

BSI 訓練學苑

T: +886 2 2656 0333 Ext. 139

E: training.taiwan@bsigroup.com

IATF 16949 課程訊息請按此>