淺談風險管理與稽核之運用

分享人：張志洵 Charlie
mpcc.charlie@gmail.com

分享大綱

- 風險之定義與名詞介紹
- 風險管理架構
- 風險評鑑 (風險辨識、分析與評估)
- 稽核之運用
  - 年度稽核計畫
  - 專案稽核

風險之定義與名詞介紹

風險的定義(1/2)

COSO 內部控制整合架構

一個事件將發生的可能性與對目標達成的不利影響

The possibility that an event will occur and adversely affect the achievement of objectives

ISO31000

對目標的不確定性影響

Effect of uncertainty on objectives

- **An effect is a deviation from the expected – positive and/or negative**
- **Objectives can have different aspects and can apply at different level**

風險的定義(2/2)

PMBOK Guide 第四版

不確定的事件或情況，若一旦發生則對專案目標產生正面或負面的影響

An uncertain event or condition that, if it occurs, has a positive or negative effect on the projects objectives

ISO17799 (2005)

一個事件的機率與其後果的組合

Combination of the probability of an event and its consequence

- 風險常被描繪為可能的事件與後果，或兩者的組合
- 風險常以某事件(包含狀況的改變)後果的組合結合發生的可能性之方式來表達

名詞介紹

Risk Appetite(風險胃納/偏好)：

- 追求某目標或願景的公司或個體，由較為廣闊基礎下之考慮而願意接受且承擔的風險數量（COSO ERM，馬秀如博士譯文：一家企業在追求其價值時，所願意接受風險的數量）

Risk Tolerance(風險容忍/承受度)：

- 相對於所欲達成之目標而可接受的變異程度，亦即在目標實現過程中，對差異的可接受程度

Risk Appetite屬於較上層與廣闊的概念，Risk Tolerance則屬於較為落實與具體的層次。PWC顧問Chris Matten解釋Risk Appetite 較接近對風險正面的涵意，即考慮由於願意多承擔風險而多希望獲取的報酬，而Risk Tolerance更側重風險原本負面的概念，亦即所可容忍的風險；兩者實為一體之兩面。

名詞介紹

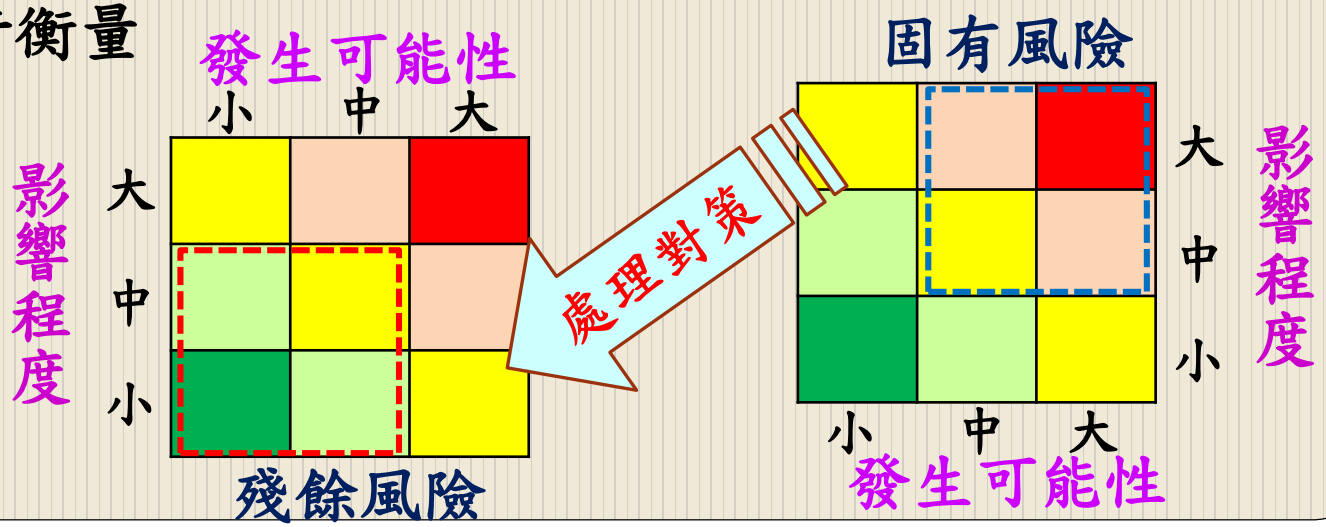
Inherent Risk (固有風險)：

- 在不考慮現有的內部控制機制下，風險發生的可能性與其對目標造成的影響

Residual Risk(殘/剩餘風險)：

- 在採取了相關內部控制後，風險仍會發生的可能性與其影響程度

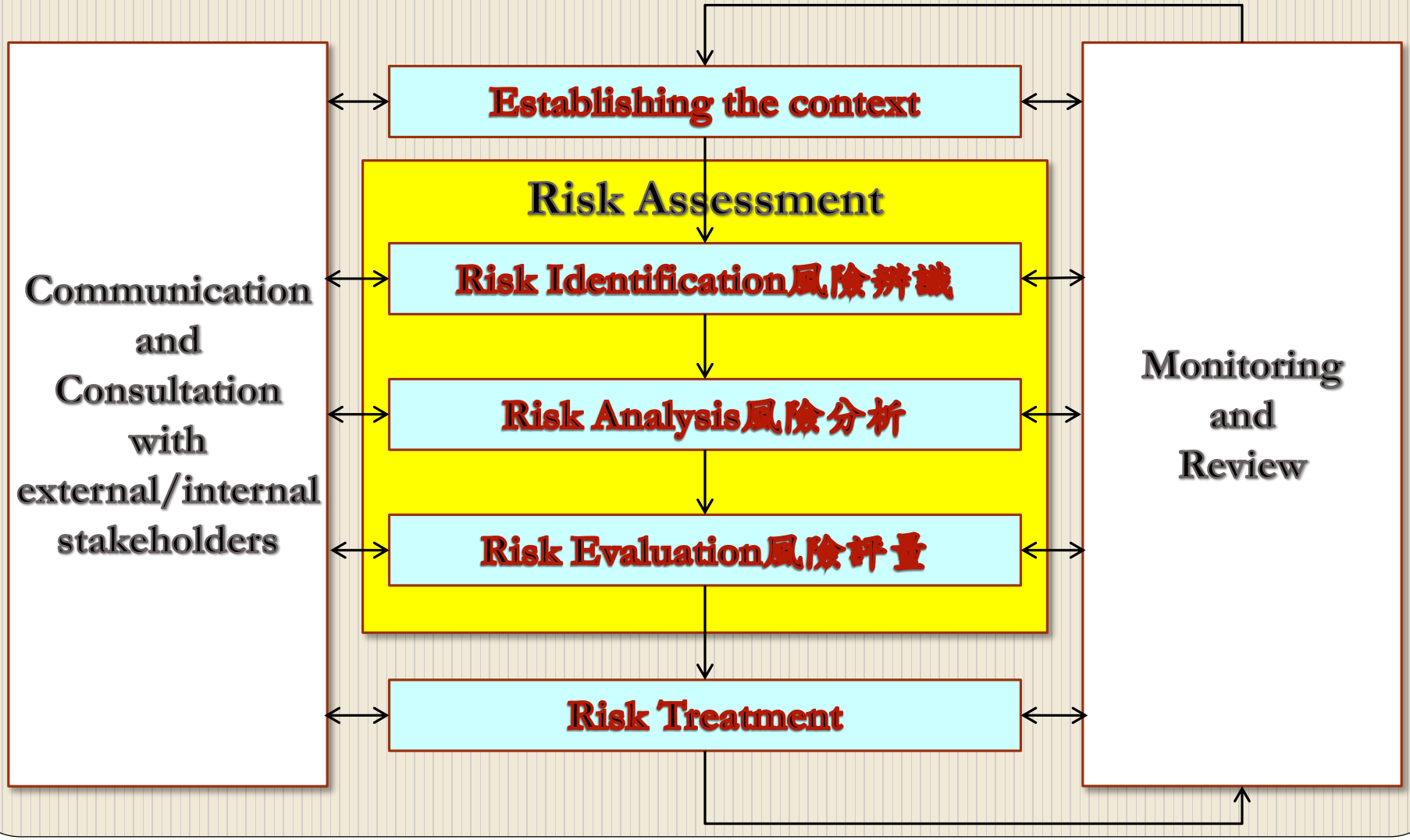
風險評鑑應先就固有風險進行分析，在完成風險處置規劃後再對殘餘風險進行衡量



風險管理架構

Risk Management Process

ISO31000



Establishing the context

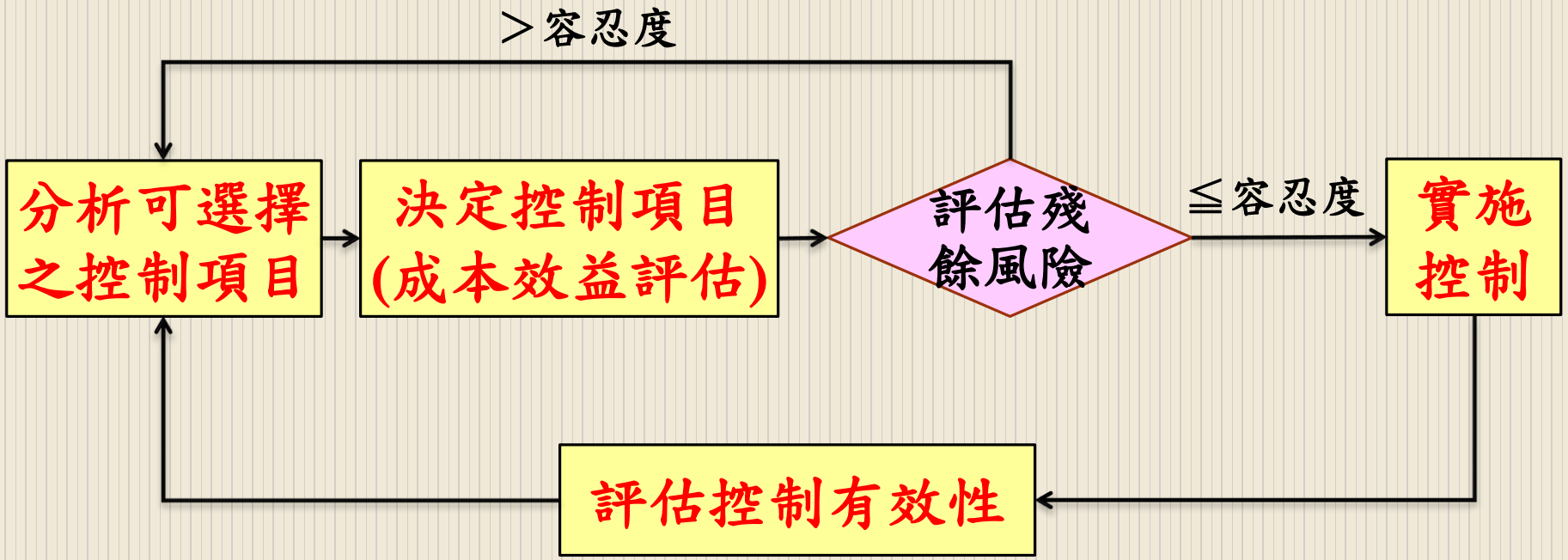
藉由建立前後關係與脈絡，組織清楚的表達其目標，並確定管理風險時所應考量的外部與內部因素，以及為過程中其餘步驟設定範圍與風險準則。

- **Establishing the external context**
- **Establishing the internal context**
- **Establishing the context of the risk management process**
- **Defining risk criteria—**

  定義估算風險重大性時所使用的準則，考量因素如下：
  - 可發生的原因與後果之性質與類別，及其如何量測
  - 可能性如何決定，以及可能性與/或後果的timeframe(s)
  - 風險層級如何決定，以及可接受或容忍的風險程度
  - 利害關係人的看法
  - 是否考量多重風險組合，以及那些應被考量與如何考量

Risk Treatment

風險處置主要在選擇並實施一或多個控制項目來減緩風險，其循環過程如下：



Risk Assessment風險評鑑

風險評鑑是風險辨識(Risk Identification)、風險分析(Risk Analysis)與風險評量 (Risk Evaluation)的整體過程：

- 風險辨識=>找出潛在的威脅/機會
  發現、辨認與記錄風險的過程
- 風險分析=>決定風險發生的可能性/影響程度
  理解風險的本質與決定風險的層級之過程
- 風險評量=>決定哪些風險應處理與其優先順序
  評定風險等級，並與風險基準比較之過程

風險評鑑--
風險辨識

風險辨識概述

風險辨識的目的在辨識可能發生什麼事或存在什麼狀況而影響系統或組織目標的達成，其過程包含辨識風險、事件、狀況或環境的原因與來源，以及其影響性質，一旦風險被辨識出來，組織應辨識任何既存的控制，諸如，設計的特性、人、流程與系統等。

風險辨識的方法可包含：

- 基於證據的方法：如檢查表與歷史資料回顧
- 系統化的團隊方式：以一組專家團隊遵循系統化的流程，藉由有組織的提示或問題的手段來辨識風險
- 歸納推理技術：如HAZOP(危害與可操作分析)、作業流程分析

基於證據的方法-風險分類檢視(1/3)

可透過對各類別的風險逐一進行檢視，並回顧與記錄以往相關或類似作業上所發生過的風險。

通常風險可歸類為以下類別：

- 環境風險：指企業外部存在的風險，包含來自於市場、產業、政府法令、政治、金融、天然災害等層面，屬不可控的風險
- 流程風險：流程愈長愈集中，風險愈增。故流程設計應以「服務客戶」、「產生效益」為原則，不能因人設事，流程風險通常再區分為營運、授權、資訊處理與科技、道德(舞弊)和財務等五類風險
- 決策風險：指決策活動中，因主、客體不確定因素的存在，導致決策不能達到預期目的之可能性及其後果

基於證據的方法-風險分類檢視(2/3)

- 流程風險的再分類：
  - 營運風險：指企業在營運過程中遭遇的各種風險。例如，遵循法令與否、營運淡旺週期、資源平均分配、績效高低落差、人力資源充裕、徵信不實等
  - 授權風險：指將財務、生產、行銷等權限透過「轉移」，暫時讓員工客戶、供應商或其他廠商，取得與公司本體一樣決定權時，所產生的風險
  - 資訊處理與科技風險：指以知識科技去進行生產、供銷與營運時，有關使用IT科技所產生的風險，包括資訊領域不同、各地資訊法令與規範差異，以及資訊遭受盜拷、仿冒、剽竊、竄改之風險

基於證據的方法-風險分類檢視(3/3)

- 道德(舞弊)風險：指內部員工以不正當的手法實施欺騙、拐誘、買空掏空、作假帳等種種管理上的舞弊牟取不法利益和侵蝕股東和廣大投資人的權益
- 財務風險：指企業在對外融資調度、平日資金流動與營運資金分配上，所產生資產、資金失衡或耗損問題風險，讓企業經營運作岌岌可危。這些風險包括「匯率」、「金融工具」、「現金流量分配」等

系統化的團隊討論(1/3)

- 重點在於如何透過有系統、有組織的方式，引導團隊透過腦力激盪的方式進行風險辨識
- 特性要因圖(魚骨圖)法簡介
  - 1953年日本石川馨教授所提出
  - 能一目瞭然的表示出結果(製品的 特性)與原因(影響特性的要因)之影響情形或二者間關係之圖形
  - 箭頭向右找原因(why)、箭頭向左找對策(how)
  - 大要因分類：

    4M-人力(Man)/機器(Machine)/原料(Material)/方法(Method)

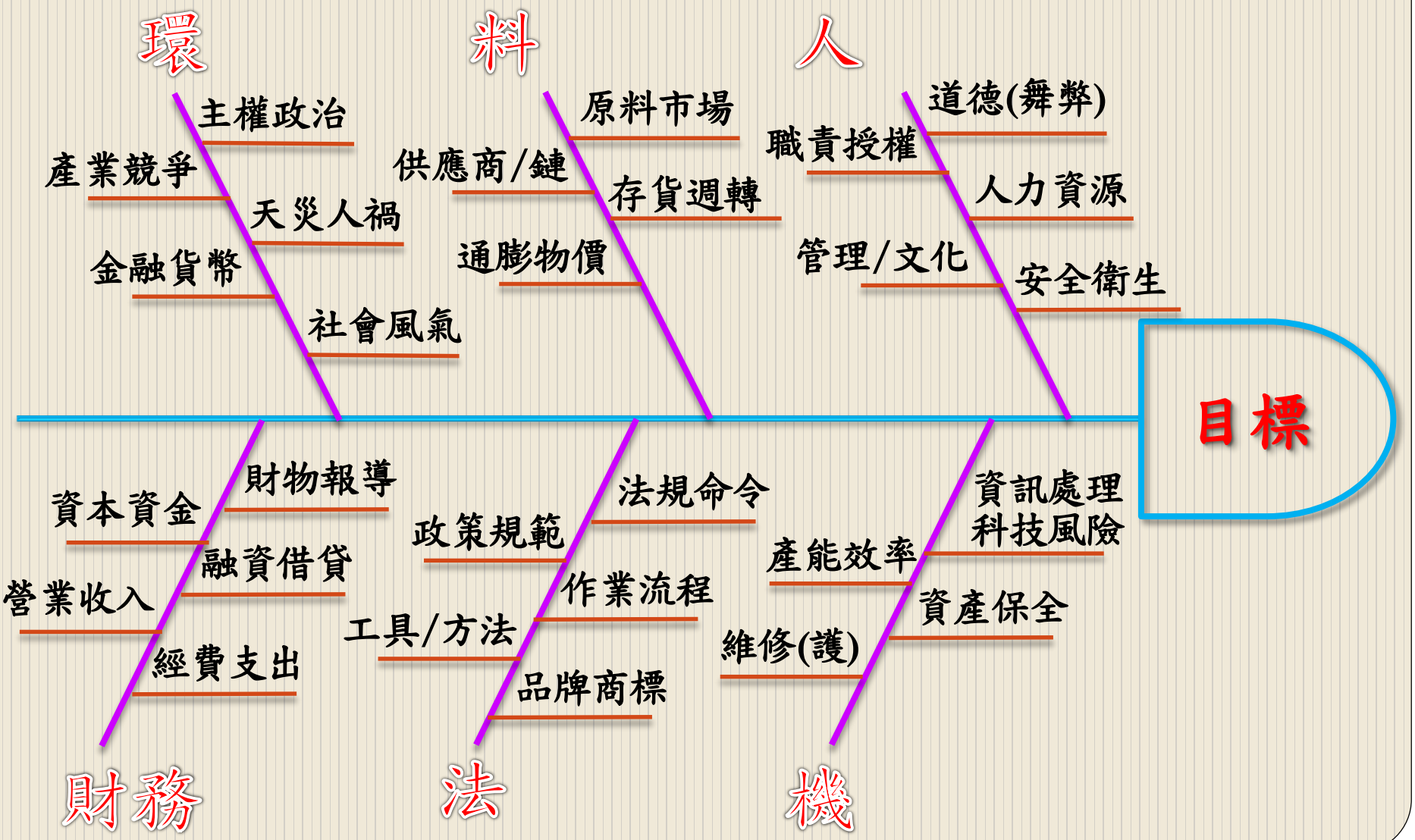
    4P-政策(Police)/程序(Procedure)/人員(People)/設備(Plant)

    4M1E-人/機/料/法/環(Environment)

系統化的團隊討論(2/3)

- 利用特性要因圖辨識風險的步驟
  - 決定作業目標(風險辨識的基礎)
  - 列出各主要風險類別(人/機/料/法/環/財務)=>大要因
  - 於各主要風險類別中進行再分類(4~6項)=>中要因
  - 於中要因中找出可能影響作業目標達成的相關事件=>小要因
  - 將小要因以若發生什麼事將造成什麼後果的方式加以描述，並列表整理

系統化的團隊討論(3/3)


環
主權政治
產業競爭
天災人禍
金融貨幣
社會風氣
料
原料市場
供應商/鏈
存貨週轉
通膨物價
人
道德(舞弊)
職責授權
人力資源
管理/文化
安全衛生
目標
財務
財物報導
資本資金
融資借貸
營業收入
經費支出
法
法規命令
政策規範
作業流程
工具/方法
品牌商標
機
資訊處理
科技風險
產能效率
資產保全
維修(護)

危害與可操作分析-HAZOP(1/6)

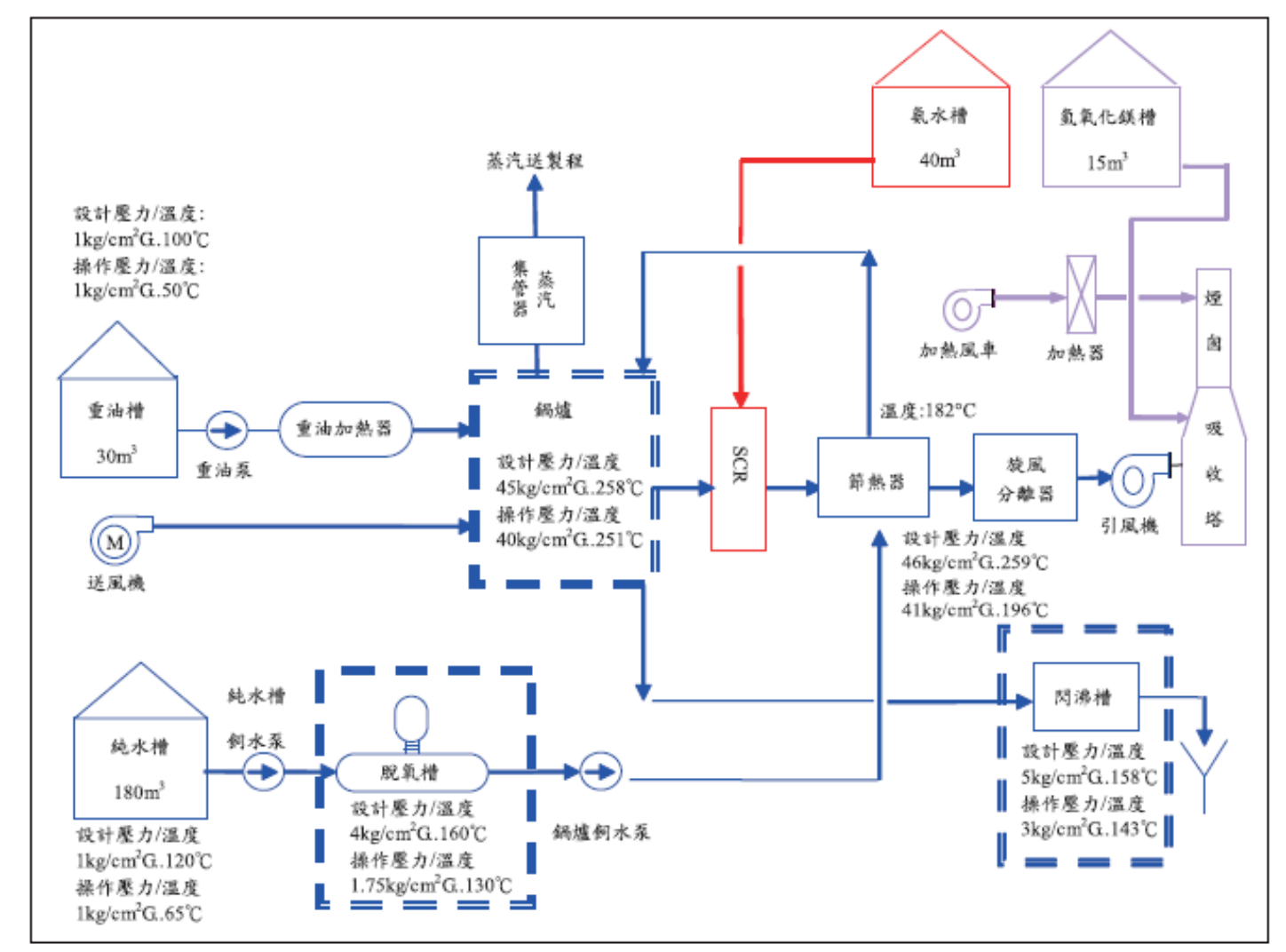
- HAZOP最初用來分析化工廠的程序控制系統，之後延伸到許多複雜的軟硬體系統。其係由幾個不同背景的專家透過引導詞(guide-word)，進行意見交換的非量化技術，一般會包括一個標示許多個別設備及連接管(線)路的製程流程圖。每個設備或管路皆列出其「設計目的」
- HAZOP將製程分割為許多節點(Node)，並藉助引導詞逐項分析製程參數(例如：溫度、壓力、流量、液位、濃度、成份等)的偏離，以尋找偏離參數的原因、可能的結果及影響，並提出建議與各種改善及措施
- 引導詞加上製程參數可以形成多種組合的製程偏離，其關係式為：製程偏離＝引導字＋製程參數。例如：引導字為「較多」，製程參數為「壓力」，則組合的製程偏離為「較多壓力」。若組合有意義，即為一個潛在的製程偏離

危害與可操作分析-HAZOP(2/6)

範例：蒸汽鍋爐廠的鍋爐用於燃燒燃料油產生熱能加熱汽水鼓之間的管群，使內部的純水變成蒸汽，其產生40kg/cm2的飽和蒸汽壓(飽和溫度為250℃)，最大蒸汽產生量為79T/H，加熱時每小時注入10L濃度70%之脫氧劑避免鍋爐爐管點蝕

引導詞	意義
無（NO）	完全不符合設計目的
較多（MORE）	定量的增加
較少（LESS）	定量的減少
不僅……又（AS WELL AS）	定性的變化/增加
只有部份（PART OF）	定性的變化/減少
相反（REVERSE）	和設計意圖的邏輯恰好相反
除……以外（OTHER THAN）	完全取代
早（EARLY）	相對於某一時間
晚（LATE）	相對於某一時間
……	……

危害與可操作分析-HAZOP(3/6)



蒸汽鍋爐方塊流程圖

危害與可操作分析-HAZOP(4/6)

引導詞及參數的組合

引導詞 參數	較多	較少	無	相反	不僅...又	只有部份	除.....以外
流量	較多流量	較少流量	無流量	倒流			
壓力	較多壓力	較少壓力	真空		delta-p		爆炸
溫度	高溫	低溫					
濃度					濃度偏高	濃度不足	劑量錯誤
時間	太長/太遲	太短/太早	跳過程序中某步驟	程序逆行	省略動作	額外的動作	時間錯誤
攪動	快速混合	慢速混合	無混合				
反應	快速反應/失控	慢速反應	無反應				不期望的反映
Start-up / Shut-down	too fast	too slow			actions missed		wrong recipe
維護			無				
振動	太小	太大	無				頻率錯誤

危害與可操作分析-HAZOP(5/6)

危害與可操作性分析表 - 爐內結垢

製程／操作程序名稱：鍋爐

研討節點描述：1002-燃燒燃料油產生熱能加熱汽水鼓之間的管群，使內部的純水變成蒸汽

管線／設備編號：

設計目的：蒸汽產生

圖號：

項目	製程偏離	可能原因	可能危害／後果	防範措施／補充說明	嚴重性	可能性	風險等級	改善建議
1002.38	雜質	鍋爐藥劑加藥量不當。	1. 加藥量過多導致汽水共騰，液位不穩。 2. 加藥量過少導致汽鼓結垢，引起局部過熱嚴重時會使汽鼓或爐管破裂。 3. 爐水水質不佳。	1. 定期檢測水質。 2. 鍋爐水質連續監測異常值警報。 3. 適當調整加藥量。	D	3	4	定期請廠商化驗水質。

危害與可操作分析-HAZOP(6/6)

危害與可操作性分析表 - 重大危害：爆炸

製程／操作程序名稱：鍋爐

研討節點描述：1002-燃燒燃料油產生熱能加熱汽水鼓之間的管群，使內部的純水變成蒸汽

管線／設備編號：

設計目的：蒸汽產生

圖號：

項目	製程偏離	可能原因	可能危害/後果	防範措施/補充說明	嚴重性	可能性	風險等級	改善建議
1002.18	高壓	汽鼓出口閥誤動作關閉。	1. 汽鼓超壓爆炸。 2. 影響製程使用蒸汽。	1. 雙安全閥高壓跳脫。 2. 現場壓力計定時巡視。 3. 自動連鎖排放蒸汽。	B	3	3	1. 安全閥定期測試。 2. 定期實施緊急應變計劃演練。
1002.19	高壓	壓力傳送器故障（偏低）。	1. 汽鼓超壓爆炸。 2. 影響製程使用蒸汽。	1. 雙安全閥高壓跳脫。 2. 現場壓力計定時巡視。 3. 自動連鎖排放蒸汽。	B	3	3	1. 定期實施緊急應變計劃演練。 2. 傳送器定期校正。
1002.20	高壓	燃料供給量過大。	1. 汽鼓超壓爆炸。 2. 影響製程使用蒸汽。	1. 雙安全閥高壓跳脫。 2. 現場壓力計定時巡視。 3. 自動連鎖排放蒸汽。	B	3	3	1. 安全閥定期測試。 2. 定期實施緊急應變計劃演練。

風險評鑑--
風險分析

風險分析概述(1/2)

- 風險分析應考量風險的肇因與其來源，以瞭解其種類與性質，並評估該風險將導致的負面或正面的後果與發生的可能性，風險分析的結果將做為風險評量的輸入，用以決定該項風險是否需被處理。
- 在進行風險分析時，應考慮各項先決條件與假設，並與各決策者與關係人有效溝通，另專家間的意見差異、不確定性、合宜性、質化、量化，抑或模擬上的相關限制應被陳述或加以強調。

風險分析概述(2/2)

- 後果與其可能性可以藉由模擬事件的結果予以確定，抑或藉由實驗研究與其它可用的資料進行推斷，後果可用有形的或無形的影響加以表述，某些情形需要一個以上的數值或描述詞，以說明在不同的時間、地點、群組或狀況時的後果與其可能性。
- 在某些情況下，一個後果可能是由一連串不同的事件或條件，或由尚未辨識的事件所引發的，在這種情形下，風險評鑑的重點則是將重點置於分析該系統中各項元件的重要性與弱點，而其處理對策則是關於對該元件保護與復原策略的程度。

風險分析技術(1/3)

定量分析與定性分析：

方法	定量分析	定性分析
說明	以模擬、試驗或藉由歷史統計資料庫等，用實際數據來描述發生可能性與影響程度	用文字敘述的分類等級來描述發生可能性與影響程度，最常用與簡單的方式為高、中、低三分法
優點	客觀且合理的將風險予以量化，並對不同因素進行靈敏度分析，能更真實反映風險實際狀況	較具有彈性，適用於數據不足、缺乏理論或欠缺足夠的資源時使用。可提供評估人員快速完成判斷，有助於決策的形成
缺點	需具備專業能力與工具，並對於風險成因及各影響因子進行詳細的分析與研究，所需花費的時間、資源亦較多	評估的結果因人而異；較易因個人偏見產生主觀的推論；難以掌握評估結果的不確定性
常用方法	失誤樹分析、事件樹分析、人為可靠度分析	初步危害分析、What-If分析、查核表

常用的風險分析方法(2/3)

半定量分析：

- 融合定性與定量分析的優缺點
- 以定性技術為基礎，差別在於給予事故後果影響程度與可能性約略的數值範圍
- 數值範圍設定應能適當的反應數值與真實情況相關性，避免分析結果錯誤或不適當
- 可能性分類等級範例：

等級	1	2	3	4	5
	極不可能	不太可能	有可能	很可能	極為可能
敘述數值範圍	數十年難得一見 $<10^{-1}$/年	十年發生一、兩次 $=10^{-1}$/年	沒一、兩年就發生 $=10^{0}$/年	一年偶而發生幾次 <10/年	每年時常發生 >10/年

常用的風險分析方法(2/3)

- 影響程度應就不同類別的後果進行分級，範例如下：

影響等級		人員傷亡	財物損失	環境/法令	商譽/形象
5	極嚴重	3人以上死亡	>NT$10,000K	1.無法恢復之環境損害 2.勒令長期歇業、停工	國際媒體關注報導
4	嚴重	1人以上死亡	NT$1,000K-NT$10,000K	1.毒化物外洩至廠外 2.暫時停工待檢 3.負擔管理刑責	全國媒體大肆報導
3	中度	3人以上住院或送醫處理	NT$100K-NT$1,000K	1.廠內毒化外洩需求援 2.遭主管機關行政裁罰	地方媒體負面評論
2	輕度	1人以上住院或送醫處理	NT$5K-NT$100K	1.立即控制之毒化外洩 2.遭主管機關告誡	少數居民關注
1	可忽略	傷者無需送醫處理	<NT$5K	1.無影響之少量溢漏 2.不違反法令之疏失	無人關切

殘餘風險分析

- 在完成風險處置規劃，以及在風險監控與覆核階段實施
- 殘餘風險分析應考量預定採取或已採取之控制措施的效果與效率
- 有效之控制應能降低風險發生之可能性或其影響程度，使其殘餘風險降低到組織可接受之程度
- 控制設計之有效性評估即在評估殘餘風險是否已降低至組織風險容忍度以下

風險評鑑--
風險評量

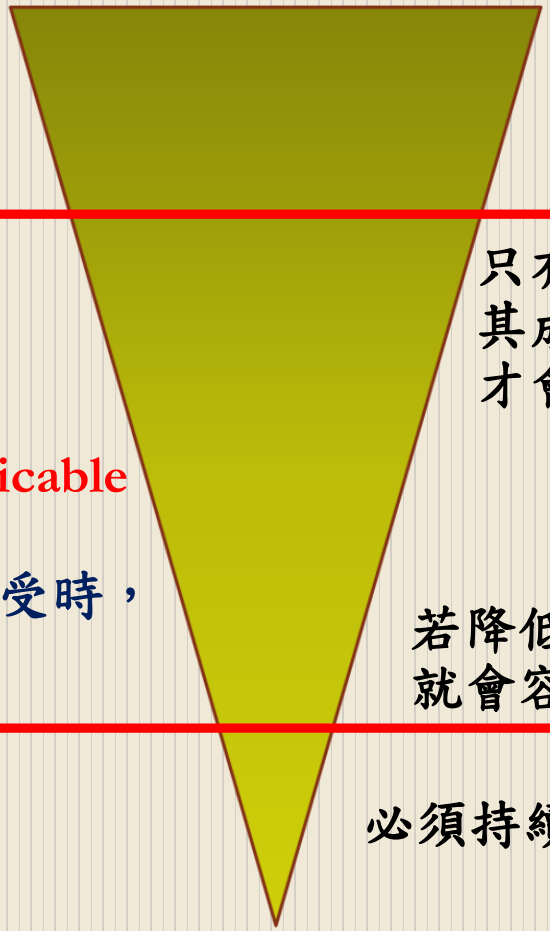
風險評量概述(1/2)

- 風險評量係將風險分析後所估算的風險級別與之前所定義好的風險基準進行比較，以決定那些風險需要處理、處理的優先順序，以及處理的應對方法
- 雖然風險基準定義與風險級別估算在之前的階段即已完成，惟本階段仍需就各項特定風險逐一進行更詳細的檢視
- 關於是否處理與如何處理風險，可以憑藉接受風險所需的成本與效益，以及降低風險所實施的改善控制成本與效益來加以決定。

風險評量概述(1/2)

- 通用的方式是將風險區分為三個區域：
  - 上層區域：這個等級中的風險被視為是無法容忍的，無論是這些活動能帶來什麼利益，且風險處理也是必要的，無論其成本是多少
  - 中層區域：應考量成本與效益，並比較機會平衡與潛在後果
  - 下層區域：這個等級中的風險被視為是微不足道的，或者是小到不需要任何風險處理措施

ALARP(最低合理可行原則)概念



不可接受的區域

在此特定區域的風險，
應不計成本的加以控制

只有在降低風險是不切實際或
其成本與改善利得極不相稱時
才會容忍

可容忍的區域 或
ALARP區域
as low as reasonably practicable

只有當改善的效益不被接受時，
才會承擔風險

若降低的成本超過改善的利得時
就會容忍

廣泛接受的區域

必須持續確認風險維持在此一級別

風險基準矩陣

影響程度						
	5	15	19	22	24	25
	4	10	14	18 控	21 制	23
	3	6	9	13	17	20
	2	3	5 監	8 控	12	16
	1	1 接	2 受	4	7	11
		1	2	3	4	5
		發生可能性				

風險處理的應對方法

規避 avoidance	亦即不實施可能帶入該風險的營運活動，但其同時意味著無法賺取該活動可能帶來的獲利與機會；此應對方法係運用在影響程度與發生可能性最高，且一旦發生將危及組織營運，或投入之控制成本遠高於可能之獲利的風險
分享 sharing	簡要地定義為“與另一方共享 風險 或 降低風險所採行之控制措施 的損失負擔或取得之利益”，常見的做法是透過保險或作業委外方式執行
降低 reduction	或稱最佳化，亦即透過最佳化的措施來降低風險發生的可能性或發生後的影響程度，所謂最佳化意味著找到風險負面影響與該作業或活動所產生之利益，以及降低的風險與所採取之工作間的平衡 (成本與效益)
保留 retention	亦即在風險發生時承受其損失或利得。風險保留對會隨著時間使確保成本逐漸大於承受總損失的小風險；此外，某些較少發生，但無法投保或投保金額不切實際的大型或災難性的風險(如戰爭等)亦可採取此應對方法

風險基準與應對矩陣

影響程度						
	5	15	19 分 享(保險)	22	24 規	25 避
	4	10	14	18	21 分 享	23
	3	6	9	13 降 低	17	20 (委外)
	2	3	5 保留	8	12	16
	1	1	2	4	7	11
		1	2	3	4	5
		發生可能性				

稽核之運用--
年度稽核計畫

依據

公發公司建立內控制度處理準則

第13條:公開發行公司內部稽核單位應依風險評估結果擬訂年度稽核計畫

國際專業實務架構 IPPF

作業準則

2010－規劃

內部稽核主管須訂定一套以風險為基礎的計畫，以決定符合機構目標之內部稽核業務優先順序

2010.A1－內部稽核單位之工作計畫須基於至少每年一次之書面風險評估，並須考量高階管理階層及董事會提供之意見

評估步驟

① 廣泛蒐集各單位主管、高階經理人、董事長、審計委員與其他關係人之concern與意見

② 參考各風險類別與關係人之意見，決定風險因子、權重與評分等級

③ 詳列除必須列為每年年度稽核計畫項目外之其他可稽核項目(auditable items/audit universe)

④ 逐一進行各可稽核項目之風險評分

⑤ 排訂評分高低順序

⑥ 依評分結果決定稽核週期，並詳列各稽核項目最近一次稽核年度

⑦ 決定次年度稽核計畫項目

決定風險因子、權重與評分等級

可稽核項目 (Auditable items)	環境風險 (10%)	營運風險 (15%)	授權風險 (10%)	資訊科技風險 (10%)	道德風險 (10%)	財務風險 (20%)	決策風險 (10%)	安全風險 (15%)	評分結果

Ranking value為1~5

詳列各項可稽核項目

可稽核項目 (Auditable items)	環境風險 (10%)	營運風險 (15%)	授權風險 (10%)	資訊科技風險 (10%)	道德風險 (10%)	財務風險 (20%)	決策風險 (10%)	安全風險 (15%)	評分結果
銷售及收款循環									
訂單處理									
授信管理									
運送物品/提供勞務									
……									
採購及付款循環									
供應商管理									
代工廠商管理									
請購									
……									
……									

事先排除法令規定應列為每年年度稽核計畫之稽核項目

逐一進行風險評分

可稽核項目 (Auditable items)	環境風險 (10%)	營運風險 (15%)	授權風險 (10%)	資訊科技風險 (10%)	道德風險 (10%)	財務風險 (20%)	決策風險 (10%)	安全風險 (15%)	評分結果
銷售及收款循環									
訂單處理	1	3	2	3	2	4	3	1	2.50
授信管理	2	2	3	1	3	3	3	1	2.25
運送物品/提供勞務	3	1	1	1	1	2	1	3	1.70
……									
採購及付款循環									
供應商管理	3	4	1	1	2	2	3	1	2.15
代工廠商管理	3	3	3	2	2	2	2	2	2.35
請購	1	3	2	2	3	2	2	1	2.00
……									

評估時應考量相關項目近期是否發生產業條件、法令、科技技術與主管/主要承辦人員等變動

排訂評分高低順序

可稽核項目 (Auditable items)	環境風險 (10%)	營運風險 (15%)	授權風險 (10%)	資訊科技風險 (10%)	道德風險 (10%)	財務風險 (20%)	決策風險 (10%)	安全風險 (15%)	評分結果
訂單處理	1	3	2	3	2	4	3	1	2.50
代工廠商管理	3	3	3	2	2	2	2	2	2.35
授信管理	2	2	3	1	3	3	3	1	2.25
供應商管理	3	4	1	1	2	2	3	1	2.15
請購	1	3	2	2	3	2	2	1	2.00
運送物品/提供勞務	3	1	1	1	1	2	1	3	1.70
……									
……									
……									
……									

決定稽核週期與詳列最近稽核年度

可稽核項目 (Auditable items)	環境風險	營運風險	授權風險	資訊科技	道德風險 (10%)	財務風險 (20%)	決策風險 (10%)	安全風險 (15%)	評分結果	稽核周期	最近稽核年度
訂單處理	1	3	2	3	2	4	3	1	2.50	2	102
代工廠商管理	3	3	3	2	2	2	2	2	2.35	3	103
授信管理	2	2	3	1	3	3	3	1	2.25	3	101
供應商管理	3	4	1	1	2	2	3	1	2.15	3	102
請購	1	3	2	2	3	2	2	1	2.00	3	101
運送物品/提供勞務	3	1	1	1	1	2	1	3	1.70	5	100
……											
……											
……											
……											

可透過將所有項目評分結果進行統計分析，換算常態分配與標準差後，決定適當之稽核周期，例如：3分以上項目每年稽核，2.5至3分每兩年稽核，2至2.5分為每三年稽核，2分以下每五年稽核

決定次年度稽核計畫項目

- 估算次年度稽核資源(稽核人力與可使用天數)
- 評估執行法定稽核項目所需人天數
- 排訂應列入本年度執行之可稽核項目與優先順序
- 評估各可稽核項目所需之稽核資源
- 邀集各業務單位就次年度稽核項目與執行時程進行研討與確認
- 完成年度稽核計畫草案之訂定後，提報審計委員會與董事會核定

稽核之運用--
專案稽核

依據

公發公司建立內控制度處理準則

第10條:公開發行公司應實施內部稽核，其目的在於協助董事會及經理人檢查及覆 核內部控制制度之缺失及衡量營運之效果及效率...

第12條(內部稽核實施細則)第二項:對內部控制制度進行評估，以衡量現行政策、程序之有效性及遵循程度與其對各項營運活動之影響

國際專業實務架構 IPPF

作業準則

2120－風險管理

內部稽核單位須評估風險管理過程之有效性，並對其改善做出貢獻

2120.A1－內部稽核單位須評估與機構之治理、營運及資訊系統有關之暴險

評估步驟

① 確認受稽核項目之作業目標

② 利用特性要因圖辨識可能影響該目標之風險

③ 繪製授稽核作業之現有作業流程，並標註流程中可能發生之風險與現有之控制措施

④ 進行所辨識之風險描述，以及既存之控制說明

⑤ 登入於風險評估表並進行風險評估

⑥ 分析可能之風險與既有風險之關聯性，並評估既有控制之適足性(控制不足 or 過度控制)

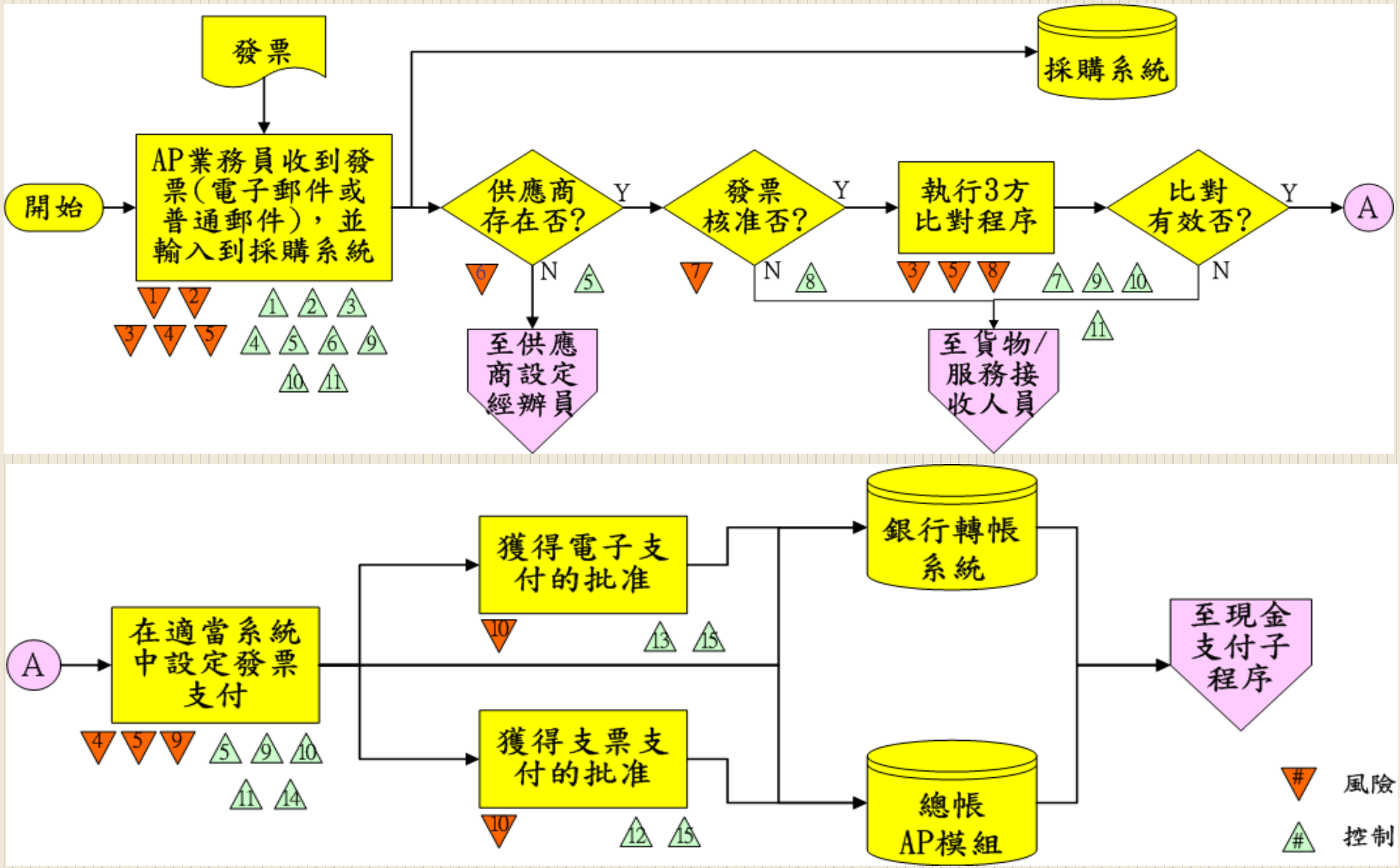
⑦ 與受稽核單位主管研討風險評估與控制適足性分析結果

⑧ 進行查核程式設計

作業流程分析法簡介

- **優點：**
  - 能結合實際作業流程，更清楚的辨識作業中各階段可能發生的風險
  - 可清楚掌握風險與目前既有的控制間之關聯，便於控制有效性評估
- **缺點：**
  - 較難辨識出環境與財務風險
  - 若流程本身不完整或有疏漏，則可能無法辨識出相應的風險

範例—發票處理流程



資料來源：Internal Auditing : Assurance & Consulting Services

風險描述

No	Description
1	Invoice is not received timely by accounts payable, resulting in liability not being properly reflected in the financial statements.
2	Invoice is not processed timely by accounts payable, resulting in lost opportunities to take discounts or incurring late-payment fees.
3	Invoice information is entered inaccurately into the purchasing system, resulting in inaccurate or inappropriate payments.
4	Duplicate invoices are entered and processed for payment, resulting in payment for the same invoice twice.
5	Accounts payable clerks have inappropriate access to the various systems, allowing them to establish ficticious vendors, purchase orders, or the other payments.
6	Payments are processed to wrong or nonexistent vendor, resulting in late payments to correct vendor, the need to collect refunds form incorrect vendor.
7	Payments are processed for invoice that have not been approved yet, resulting in payment before the good or service is received.
8	Invoices are processed that don't match purchase order, receiving report or other relevant document, resulting in establishing a liability & paying incorrect amount.
9	Payments are made before the due date, resulting in lost time value of money.
10	Payments without approval, resulting in payments being made by a costly or inefficient means, or in a manner inconsistent to meet the cash flow requirements.

資料來源：Internal Auditing : Assurance & Consulting Services

既有控制說明

No	Description
1	As part of the month end close process, the AP manager will solicit information on unprocessed invoices and will prepare an accrual accordingly.
2	Once an approved invoice is entered, the system will automatically book the credit to AP and debit to the appropriate expense or balance sheet account.
3	Open purchase orders are reviewed once per month by the Purchasing Manger to determine their status.
4	The AP clerk runs a report at the end of each week showing invoices entered but not approved. For invoices outstanding more than a week, a reminder is sent to user.
5	The purchasing system requires all invoice fields are completed before processing is allowed. An invoice cannot be entered without a match to an approved vendor.
6	The purchasing system alerts the AP clerk if the vendor number, invoice number, and invoice amount match an invoice previously entered.
7	The purchasing system confirms a match between quantity & price on an invoice, purchase order, and receiving document. If don't match, invoice is placed on hold.
8	Invoice approval limits are confirmed with department heads annually and updated if necessary.
9	Username & password is required to access all of the systems. Passwords are subject to naming parameters, and must be changed every 90 days.
…	…

資料來源：Internal Auditing : Assurance & Consulting Services

作業流程分析法簡介

作業名稱：								
作業目標：								
風險描述	影響程度				可能程度	風險級別	既有控制說明	控制適足性分析
	傷亡	財損	法令	商譽				

評估之風險等級高，但無控制措施或控制不足
評估之風險等級低，但過度控制
行有餘力：評估風險承受成本與實施控制成本

Discussion

環境風險(1/2)

風險	說明
競爭對手 *Competitor*	當有主要或新的競爭對手進入市場, 進而建立並維持優於我們的競爭力, 甚至於威脅到我們的生存時
敏感度 *Sensitivity*	當經營者提供公司資源並期望從這些資源的運用獲取現金回收時, 某種程度降低了公司對於環境因素改變的忍受程度, 而這改變可能超出公司可控制的範圍時
股東關係 *Shareholer Relations*	當投資者的信心下降, 威脅到公司有效籌資能力的情形發生時
可取得資本 *Capital Availability*	當公司沒有一個有效的方式去籌到所需的資金以配合公司的擴充、執行公司策略、創造財務盈餘的情形發生時
災難損失 *Catastrophic Loss*	當公司由於一個大災難的發生而沒有能力繼續營運、提供主要的商品與服務、或支付營運成本的情形發生時

環境風險(2/2)

風險	說明
主權/政治 *Sovereign/ Political*	當公司大量投資在一個國家並十分依賴這項投資，或者與這個國家的某一企業簽具法律效力的合約，卻因為這個國家的政治措施改變而產生對這項投資有不利影響時
法令 *Legal*	當公司的交易、契約以及特定的策略、業務活動，不是在法律許可範圍內實施時
規範 *Regulatory*	當一個國家的規範或政策改變，而導致公司的競爭壓力增加，並且劇烈地影響到公司有效營運時
行業特性 *Industry*	當下列因素改變，因此而失去產業吸引力時：1)產業競爭優勢的因子，包含機會和威脅；2)現有及潛在競爭者的能力；3)相較於現有及未來競爭者的優點與弱點
金融市場 *Financial Market*	當對收入、費用或資產負債表有影響之金融市場發生變化(例如匯率)，可能會影響公司的盈餘或經濟價值時

流程風險-營運類(1/4)

風險	說明
顧客滿意度 *Customer Satisfaction*	當公司的業務無法持續滿足或高於客戶的期望,進而導致公司業務損失、營收下降以及市場佔有率喪失時
人力資源 *Human Resources*	當負責管控組織或業務流程的人員,不具備確保達成公司重要經營目標,及降低重大風險至可接受程度所應有之知識、技能和經驗時
產品開發 *Product Development*	當公司產品開發過程發生下列情形時：1)產品不符合客戶需求；2)產品價格是客戶不願意支付的,或者；3)產品於市場上推出的時間晚於競爭者
效率 *Efficiency*	由於在滿足客戶需求的作業流程上沒有效率,而產生較競爭者高的成本,例如：將公司作業流程所需的成本與世界級之相關作業成本比較後,有很大的差異發生時
產能 *Capacity*	當有效資源沒有被充份利用,較少的產出必須分攤既有的固定成本,導致較高的單位成本與較低的單位利潤

流程風險-營運類(2/4)

風險	說明
績效落差 *Performance Gap*	由於作業設計不佳, 導致較低的品質、較高的成本或較長的生命週期, 使作業流程無法達到世界水準
循環時間 *Cycle Time*	當作業程序從開始到結束(或者一個程序中的活動)由於重複的、不需要與不相關的步驟, 而導致時間的浪費
資源限制 *Sourcing*	不論在商品和原料方面, 當公司欠缺替代來源, 而影響到提供具價格競爭力的產品和客戶當時所需之服務時
作廢/耗損 *Obsolescence /Shrinkage*	存貨及作業上所需使用、消耗的資產, 由於過多、過時或遺失(盜竊行為、減少或破壞)導致公司有巨大損失時
遵循 *Compliance*	不論是在設計或運作上的瑕疵或人為錯誤、忽視、漠不關心, 而導致公司運作無法在第一時間滿足客戶的需求或不符合公司既定程序或政策時

流程風險-營運類(3/4)

風險	說明
營運干擾 *Business Interruption*	當主要作業或生產無法適時取得高度倚賴之固定原料、資訊技術、有技能的勞工和其他資源時
產品服務失敗 *Product/Service Failure*	當提供給客戶的產品或服務有瑕疵或不完整, 導致客戶抱怨、擔保賠償、維修、退貨、換貨、特別折扣(由於產品/服務瑕疵)、產品缺失賠償以及訴訟的情形發生時
環境保護 *Environmental*	當公司發生下列潛在巨大不利情況時：1)污染導致對第三人有身體上的傷害或財務損失；2)對政府或第三人有處理污染源所需的成本再加上嚴重罰金的損失
健康與安全 *Health & Safety*	當員工或委外勞工在工作場所發生重大健康與安全事故時，公司可能會面臨重大的勞工賠償與罰金，以及可能面臨勒令停工

流程風險-營運類(4/4)

風險	說明
商標品牌受損 *Trademark/Bran-dname Erosion*	當商標在產生、維繫對產品和服務的需求上,無法滿足顧客的期望時，會隨時間流逝而降低它的價值
商務開發 *Business Development*	當無法確認及轉化潛在商機（新的與現存的客戶）成為訂單,導致公司生存面臨威脅時
維修 *Maintenance*	當設備/機器維修不適當，導致無法有效發揮應有的產能時
供應鏈 *Supply Chain*	若與供應商之間的互動沒有計劃且不協調,導致存貨囤積、供應不及或品質不佳，而無法滿足客戶要求時
專案管理 *Project Management*	當對專案的評估、執行規劃、以及相關資訊的監控,都缺乏適當的考慮,可能導致不恰當的決策、計劃延誤與成本損失

流程風險-授權類(1/2)

風險	說明
領導風格 *Leadership*	對成功的業務風險管理、變動管理、業務流程再造，以及持續性改善而言,領導風格絕對重要；例如領導風格屬開放式或高壓式、過度信賴或過於猜疑等，都可能造成相關的風險
權限/限制 *Authority/ Limit*	無效的授權機制導致管理階層或員工做不該做的事或沒有做他們應該做的事。沒有建立個人行為的底限,因而導致管理階層或員工承諾了沒有被授權或不符合道德規範的行為、或承擔沒有被授權或不被接受的業務風險時
委外 *Outsourcing*	當外在服務的提供者並沒有在授權的規範內運作,其執行也與公司的價值、政策及目標不一致，以及將策略性的業務流程 外包而給組織帶來競爭時

流程風險-授權類(2/2)

風險	說明
績效誘因 *Performance Incentives*	當以績效評估來衡量管理階層和員工,但此衡量指標的誘因卻使他們的行為與公司經營目標、策略、道德規範與經營理念不一致時
變革準備 *Change Readiness*	當組織的成員在流程的執行和產品/服務的改善上,無法趕上市場的變化時
溝通 *Communication*	當組織中垂直或平行的溝通無效，導致接收到的訊息與權責或既有的慣例不一致時

流程風險- 資訊處理與科技類

風險	說明
攸關性 *Relevancy*	當產生的資訊無法支援決策、營運或生產所需，或者是未經適當的篩選、過濾與整理，以致無法獲難以參考時
完整性 *Integrity*	各種應用系統的載入、運作、彙整以及報導的功能中，均存在交易完整性及正確性等相關的風險
存取 *Access*	當可以經由不適當的方式取得資訊、或不恰當的人員可以獲得機密資料時
可用性 *Availability*	當連線中斷(如電纜斷裂、通話系統損壞、衛星損壞)、作業能力受損(如：火災、水災、電力損壞)以及操作問題(如：磁碟機當機、操作員疏失)，導致所需要的資料無法獲得時
基礎建設 *Infrastructure*	當缺乏有效的資訊基礎設施(如：硬體, 網路, 軟體, 人才與流程), 以最經濟, 符合成本效益與良好控制的方式, 來因應現在和未來的業務需要時

流程風險- 道德(舞弊)類

風險	說明
管理舞弊 *Management Fraud*	當管理階層意圖以錯誤的財務報表, 誤導投資大眾和外部稽核人員或從事賄賂、收回扣、影響付款以圖謀公司的利益時
員工舞弊 *Employee Fraud*	當員工, 客戶或供應廠商個別或聯手一起詐騙公司, 而導致財務的損失或未經授權使用公司實體, 財務或資訊資產時
非法行為 *Illegal Acts*	當管理者和員工，個別或聯手從事非法行為, 導致公司, 負責人和主管因為這項非法行為而受影響時(如：坐牢、罰款、制裁、歇業、利潤受損、客戶流失以及商譽毀損)
未授權使用 *Unauthorized Use*	員工或其他的人未經授權即使用公司實體、財務或資訊資產, 而導致組織發生不必要的資源浪費與財務損失時

流程風險-財物類(1/2)

風險	說明
利率 *Interest Rate*	當預期所得因為利率變動而有變化，導致投資報酬低於預期，或者超出預期的借款成本或生產成本時
匯率 *Currency*	匯率的波動而導致公司在經濟或會計上有損失時
權益 *Equity*	資金來源會隨著股東成員而有所波動，主要股東變動或其財務發生問題時，對公司會是一種風險
商品 *Commodity*	當提供商品生產的大宗原料或產品(如, 金, 能源, 銅, 咖啡)發生波動，導致公司因為低於預期的售價或高於預期的購入成本，而發生預算或預期營收短缺時
金融工具 *Financial Instrument*	組織在金融市場運作的結果並不如預期或操作工具組合不恰當，而導致公司有具大損失的情形時
現金流量 *Cash Flow*	當現金收支、移轉等控管不良時，所導致之資金調度、跳票、信用額度降低、銀行緊縮等風險

流程風險-財物類(2/2)

風險	說明
機會成本 *Opportunity Cost*	當組織現金流量及投資收益無法即時與有效率的運作與管理，導致透過財務機制運作的資金發生價值損失時
財務流通侷限 *Concentration*	組織財務流通性侷限在一個狹隘的市場，進而造成公司的損失時
違約 *Default*	當公司無法履行財務交易上的義務，導致財務損失時
信用集中 *Concentration*	銷售量及收入過度集中於單一、少數客戶，產業或其它經濟來源，導致組織超額損失時
短期信用 *Settlement*	當財務往來者由於時間或地點不同而影響到款項支付，導致組織短期信用風險發生時
擔保品 *Collateral*	當提供給組織做為擔保品之價值，部份或全部喪失，致組織有財務上損失時

決策風險(1/4)

風險	說明
訂價 *Pricing*	當缺乏相關或可靠的資訊，導致決定的價格客戶不願意支付、或無法吸收研發及其它成本，或組織風險費用時
合約承諾 *Contract Commitment*	當公司無法有效、即時的追蹤未到期的契約承諾，導致決策者在將財務相關的事項列入新增加的承諾時，無法予以適當考慮時
績效衡量 *Performance Measurement*	當不存在、不相關或不可靠的非財務性衡量，導致營運成果有錯誤的評估與結論時
校準 *Alignment*	當一個公司的作業目標、績效衡量,與公司整體目標和政策不一致時
預算與計畫 *Budget & Planning*	當不存在、不確實、不相關或不可靠的預算及計劃資訊而導致不適當的財務判定與決策時

決策風險(2/4)

風險	說明
法規回報 *Regulatory Reporting*	當提供主管機關所要求的營運資訊報告不完整、不正確或不即時，而導致公司遭受罰金、刑罰與制裁時
完整與正確 *Completeness & Accuracy*	當編輯與分析的營運記錄不適當，可能會提供不正確/不精準的營運成果, 導致欠缺/延遲採取改善行動時
會計資訊 *Accounting Info.*	當提供給現有與潛在的投資者以及債權人的財務報告中存在重要事項的錯誤敘述或漏列，因此誤導他們時
財報評鑑 *Financial Reporting Evaluation*	當提供給現有與潛在的投資者以及債權人的財務報告中存在重要事項的錯誤敘述或漏列，因此誤導他們時
稅賦 *Taxation*	無法累積及考慮與稅法相關資訊，導致與稅法規範不符或不利的稅務後果時

決策風險(3/4)

風險	說明
退休金 *Pension Fund*	退休基金並沒有被正確地提列,不足以滿足計劃中所定義的支付義務（風險影響包含商譽的毀損、士氣的低落工作的停滯、訴訟、以及公司額外的基金需求）
投資評估 *Investment Evaluation*	管理階層沒有足夠的財務資訊來作為決定短期與長期投資及將資金運用與可接受之風險程度相連結的依據
環境審視 *Environmental Scan*	當公司沒有有效的程序以獲得外部環境的相關資訊，或對外部環境所做的主要假設與實際狀況不符，或是公司沒有監控的機制，而使公司無法監督與因應快速的環境變化，因而導致公司政策過時
評價 *Valuation*	當因缺乏相關及可靠的評價資訊，因而阻礙了主事者或是未來的主事者，對組織價值或與策略相關的任何部份進行評估時

決策風險(4/4)

風險	說明
組織結構 *Organization Structure*	當管理階層缺乏所需要的資訊去評估公司組織結構的有效性，進而威脅到公司在因應改變，或達成長期策略的能力時
資源分配 *Resource Allocation*	當公司沒有建立一個資源分配，以及維持競爭優勢或將股東盈餘最大化之機制時
計劃 *Planning*	一個無法想像又冗贅的策略規劃流程，產生一些不相關的資訊，而威脅到組織在制定可行的業務策略的能力時
生命週期 *Life Cycle*	當組織對管理生產線，以及隨生命週期調整產業(也就是開始、發展、成熟與衰退)的方式，對業務策略最終的成功或失敗有重大的影響時