



# 元智大學

## 內部控制及內部稽核教育訓練

### - 風險管理與內部控制

安侯建業聯合會計師事務所

107年11月23日



# 講師：黃宇歆 協理

## ■ 現職

- KPMG台灣所顧問部協理

## ■ 經歷

- KPMG台灣所顧問部經理
- KPMG台灣所講師
- 公司治理協會講師
- 上市櫃公司內部稽核

## ■ 學歷

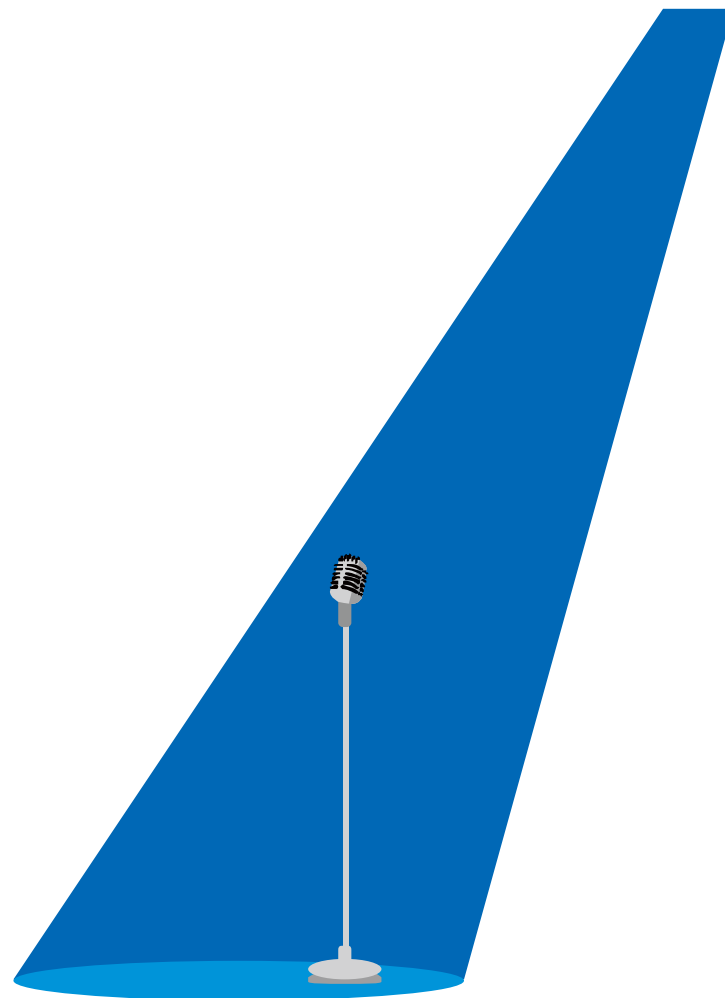
- 國立台灣大學學士

## ■ 專業資格

- 國際內部稽核師

## ■ 專業服務

- 公司治理服務
- 企業風險管理服務
- 內部控制及內部稽核服務
- 法規遵循服務





# Content

- 從案例看風險管理與內部控制
- 組織如何管理風險
  - 風險辨識、評估及回應
- 什麼是有用的內部控制
  - 評估內控有效性
  - 設計無效之改善
- 循環內控制度建置
- 問題討論與交流



# 從案例看風 險管理與內 部控制



# 案例1：普悠瑪出軌?!



照片來源：money.udn.com

## 問題探討

- ✓機械故障?
- ✓防護設備問題?
- ✓人員訓練?
- ✓運轉決策?
- ✓其他?

## 案例2：SOP是否有效？

高雄氣爆／最新死傷人數：28死 286傷

2014-08-01 聯合新聞網

作者：聯合晚報／記者楊



做對的事，而不是  
只把事情做對

資料來源：聯合新聞網、路透電

## 問題探討

- ✓ 政府與企業是否均有辨識出此重大風險？
- ✓ 若有辨識出此重大風險，是否就本身職責，建置有效的監督及管理控制程序？
- ✓ 相關單位職責是否清楚？是否有落實監管的責任？SOP之設計是否能有效管理可能發生的風險？是否均確實依循有效的SOP處理？
- ✓ 是否有定期自行檢查控制機制？對於外部環境的改變(例如:管路區變住區、到處工程都在施工等等)，是否有更新機制？是否委託獨立單位檢查落實情形？
- ✓ 災害應變計畫是否建置？是否定期演練及適當調整？

# 案例3：手術開錯刀，病患失去兩條腿

▲巴西醫師錯把該截肢的右腿搞成左腿。(示意圖 / 取自Gawker)

國際中心 / 綜合報導

手術大烏龍？巴西里約熱內盧一名醫院醫師，在為一名因糖尿病導致腎衰竭，必須切除右腿的病患進行截肢手術時，卻錯把左腿截肢，導致這名病患被迫要失去雙腿。

根據《Courier mail》報導，這名醫師不僅切除錯了腿，事後還遲遲未察覺，是因病患的女兒事後向醫院反映後，醫師才再將右腿切除想補救。院方目前正在釐清醫生是否犯下醫療失誤，還是評估後認為病人的左腿也該截肢。

- ✓ 控制設計出了什麼問題？電腦輸入資料與病歷紀錄為何無雙重檢核確認？
- ✓ 麻醉後有無再次確認？只能檢核電腦輸入資料與手術區位標記二者不符情況，無法核對病歷紀錄與手術區位二者不同之錯誤？
- ✓ 內控概念模糊，各關節均無重複檢核：  
病歷→電腦排程輸入→標記→醫師動刀。

# 什麼是內部控制？





# 關於 COSO

## ■ COSO是“不實財務報導全國委員會”下附設委員會

- The National Commission on Fraudulent Financial Reporting、又稱 Treadway Commission
- 1985年由五個單位組成，包括美國會計師公會、美國會計學會、財務主管協會、內部稽核協會與管理會計人協會。
- 目的在於辨識造成不實財務報告之因素，並提出降低不實財務報告機率之建議。

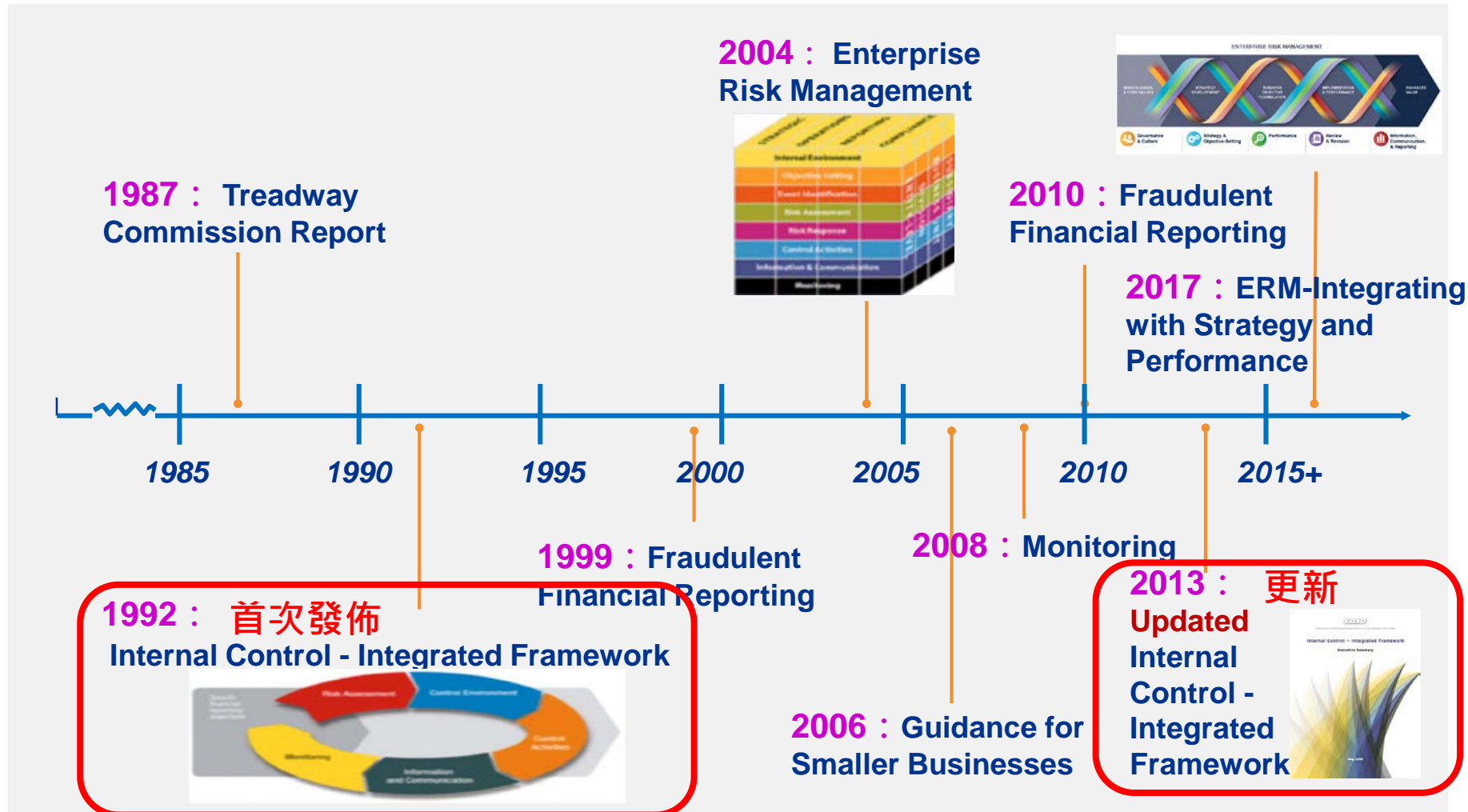


資料來源：引用自COSO網站

## ■ COSO委員會 (Committee of Sponsoring Organizations of the Treadway Commission)

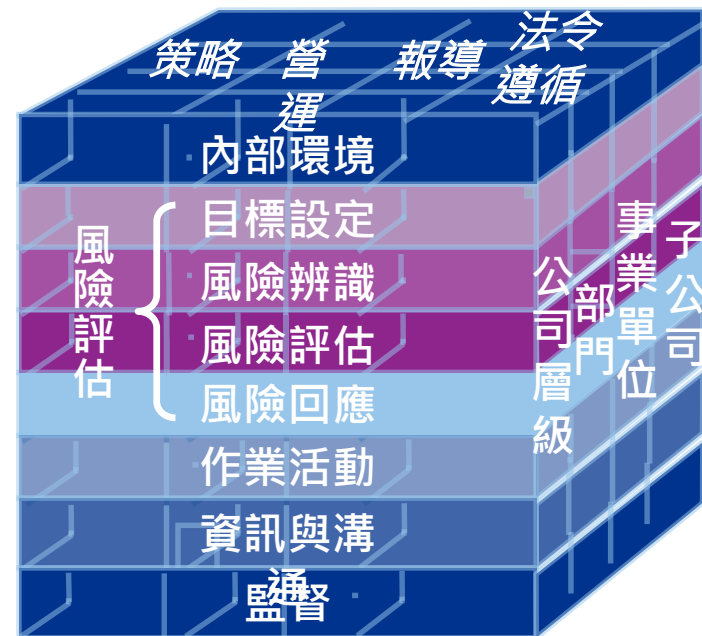
- 委員會成立於1987年；1992年發佈「內部控制—整體架構」(Internal Control-Integrated Framework)框架

# COSO 內部控制整合架構發展

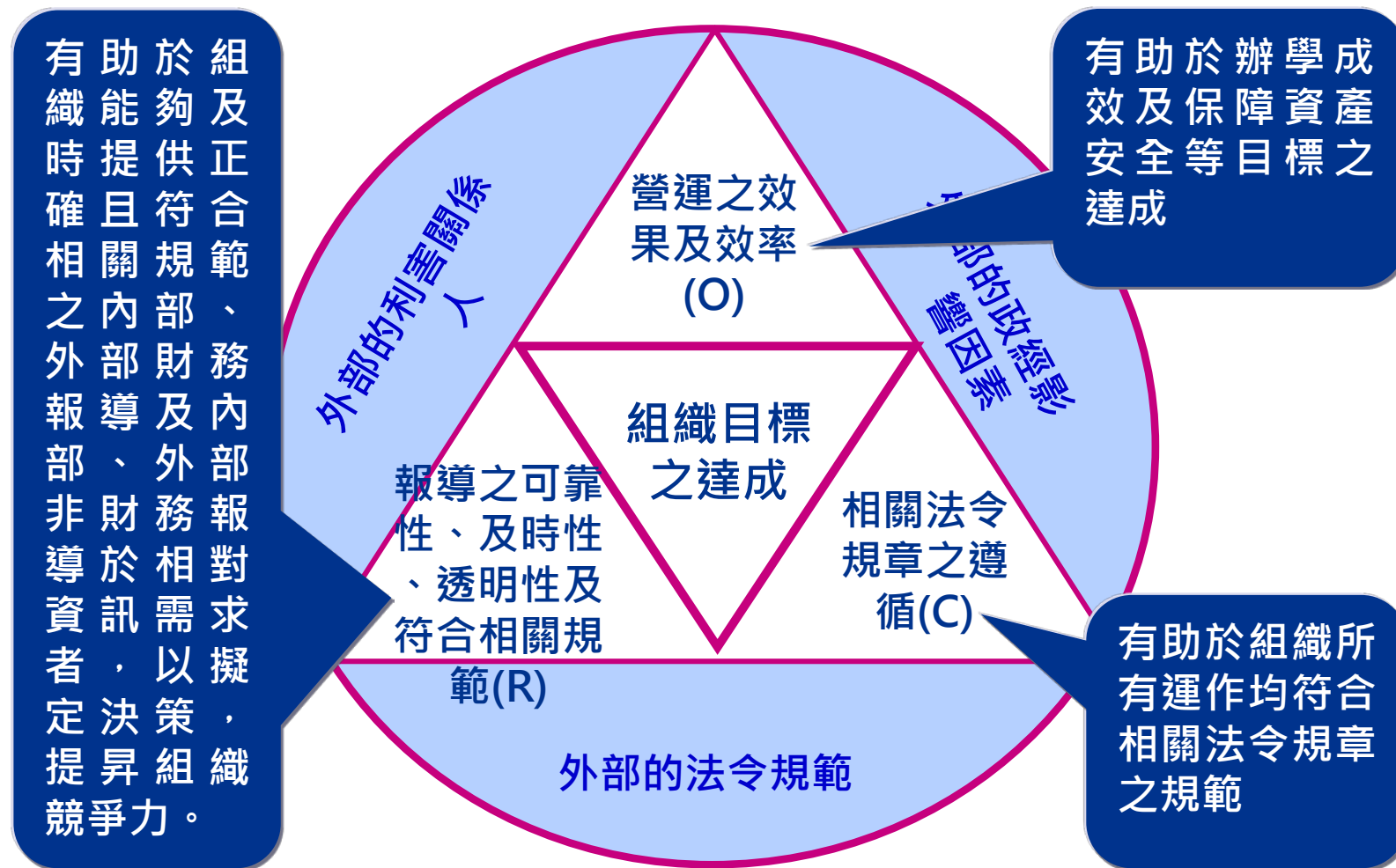


# 什麼是內部控制？

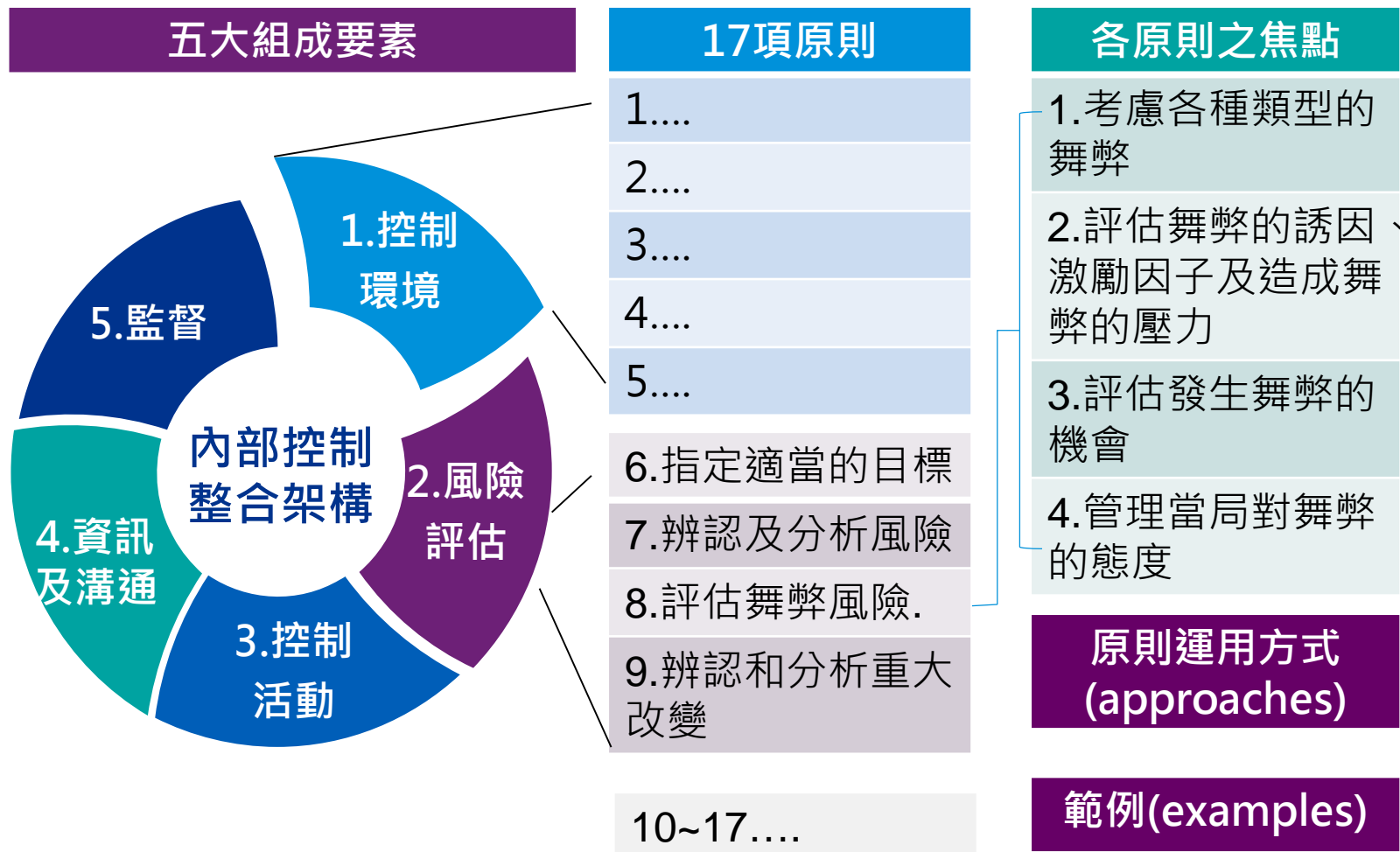
- COSO內部控制之定義：  
內部控制是一種管理的過程，受到組織董事會、管理階層及其他人員影響，被設計來提供合理的確保以達成營運、報導及遵循等相關目標。



# 內部控制制度之目的與效益



# 2013 COSO內部控制整合架構



# 17項原則支持五大組成要素基本觀念

## 組成要素

## 須符合之原則

控制環境	<ol style="list-style-type: none"><li>1. 展現誠信和道德價值的承諾</li><li>2. 董事會行使監督責任</li><li>3. 經營管理階層建立組織架構、權力及責任之劃分</li><li>4. 展現吸引、發展、並留住有能力員工的承諾</li><li>5. 強化人員對內控的之責任</li></ol>
風險評估	<ol style="list-style-type: none"><li>6. 指定適當的目標</li><li>7. 辨認及分析風險</li><li>8. 評估舞弊風險</li><li>9. 辨認和分析重大改變</li></ol>
控制活動	<ol style="list-style-type: none"><li>10. 挑選及發展控制活動以使目標達成之風險降低</li><li>11. 挑選及發展資訊科技之一般控制</li><li>12. 透過政策及程序展開控制活動</li></ol>
資訊與溝通	<ol style="list-style-type: none"><li>13. 取得、產生、使用有效資訊以支持內控運作</li><li>14. 運用資訊進行外部溝通</li><li>15. 運用資訊進行內部溝通</li></ol>
監督	<ol style="list-style-type: none"><li>16. 進行定期或不定期評估</li><li>17. 評估與溝通缺失</li></ol>

# 學校內控制度應包含五大組成要素

控制環境	學校法人及學校設計及執行本制度之基礎，包括組織文化、誠信與道德價值、組織結構、權責分派、人力資源政策、績效衡量及獎懲等。
風險評估	學校法人及學校主管階層應先確立各項目標，並與不同層級單位相連結，同時需考慮目標之適合性，並考量內外環境改變之影響及可能發生之舞弊情事，透過適當風險管理政策及程序，進行風險辨識、分析及評估。其評估結果可協助學校法人及學校及時設計、修正及執行必要之控制作業。
控制活動	學校法人及學校依風險評估結果，採用適當政策及程序之行動，將風險控制在可承受範圍內。控制作業之執行，包括學校法人及學校所有層級、業務流程內各個階段、所有科技環境等範圍之監督及管理。

資料來源：學校財團法人及所設私立學校內部控制制度實施辦法

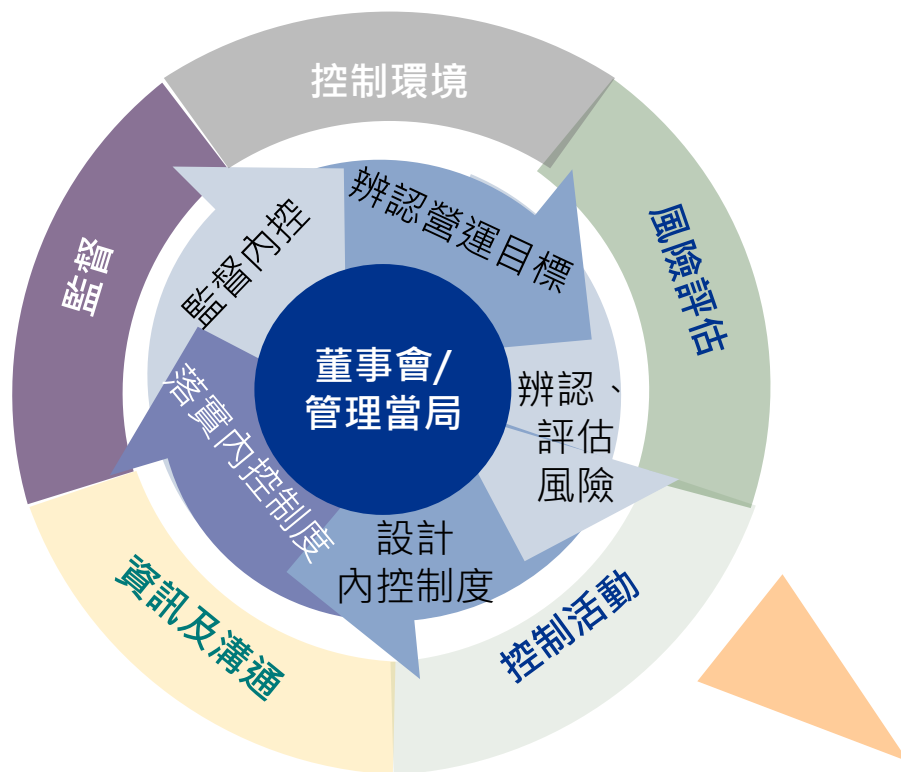
# 學校內控制度應包含五大組成要素(續)

<b>資訊與溝通</b>	學校法人及學校蒐集、產生及使用與校務規劃、執行及監督有關之內外部資訊，以支持內部控制其他組成要素之持續運作，確保資訊之有效溝通，並提供資訊需求者適時取得資訊之機制。
<b>監督</b>	學校法人及學校進行下列監督作業，以確定本制度之有效性、及時性及確實性：（一）例行監督：主管階層本於職責，就分層負責授權業務執行持續性常態督導。 （二）自行評估：由相關單位依職責分工，評估各組成要素運作之有效程度。（三）稽核評估：由內部稽核人員以客觀公正之立場，協助檢核內部控制實施狀況，並適時提供改善建議；發現內部控制制度缺失時，應向適當層級之主管階層、董事會及監察人報告。



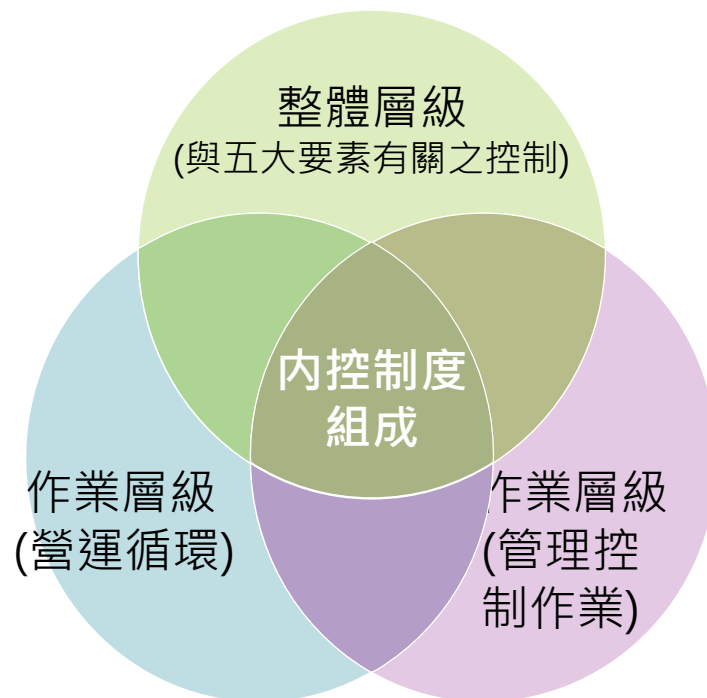
# 內部控制之基本架構與呈現

## 內部控制五大要素



- 內部制度的設計須包括控制環境、風險評估、控制活動、監督、資訊及溝通五大要素

## 於內控制度之呈現



- ✓ 內控之設計與執行是否能管理影響組織目標達成之風險，是其有效性判斷之基礎。



# 組織如何管理風險



# 什麼是風險？

## 定 義

於COSO內部控制整合架構中，風險被定義為：一個事件的發生將不利影響目標達成的可能性

風險管理之始，在於指定適當的目標

但不論組織個體有無明確陳述其目標，目標的達成都有其內部或外部之風險

風險具有不確定性：發生機率、發生所造成的衝擊程度，或發生的時間點等。

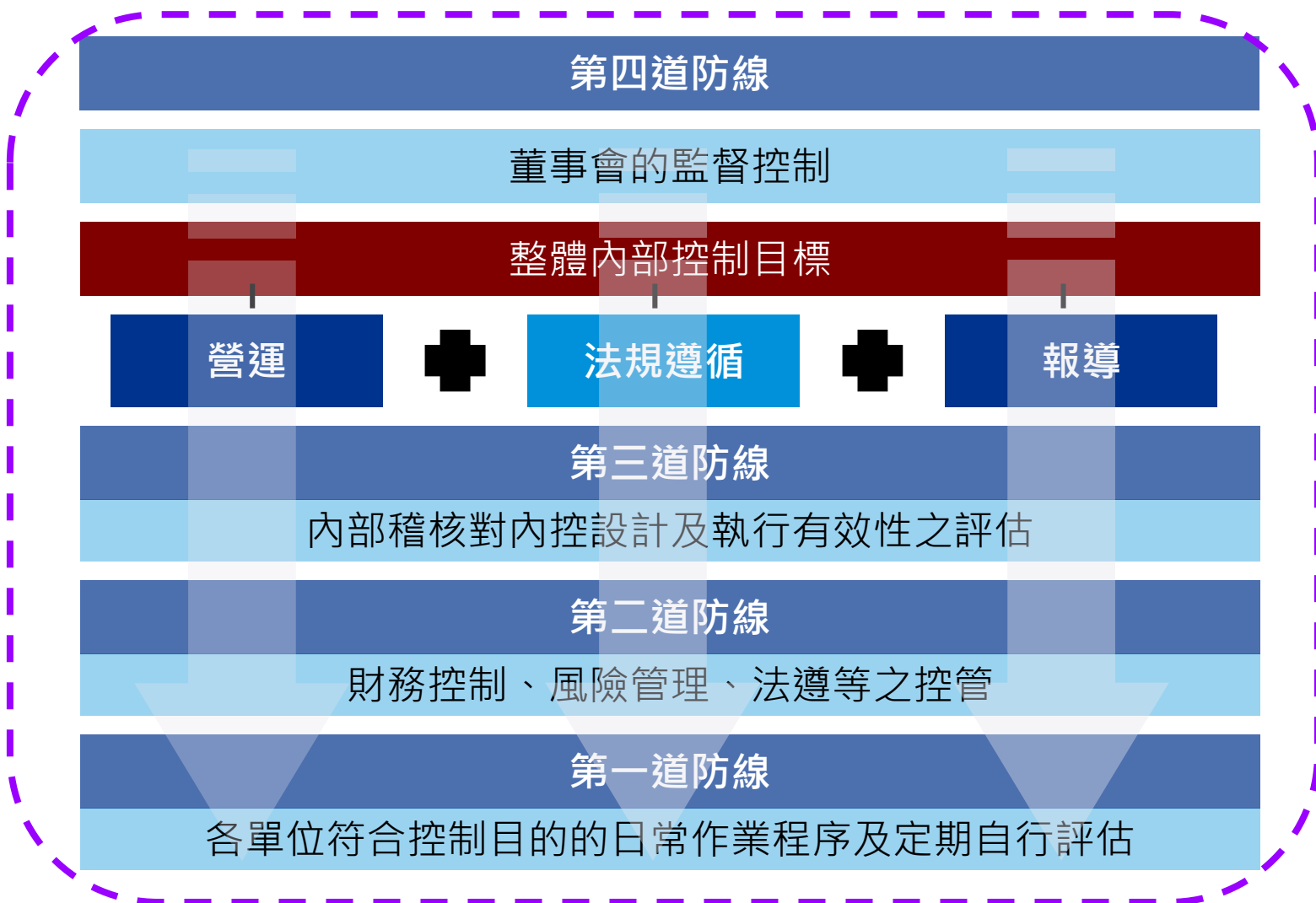


# 動動腦：以下對學校是否為風險？

- 少子化
- 運動場、游泳池設備老舊、故障
- 老師、學生可隨意取得實驗用之化學材料或藥劑
- 未設置與利害關係人溝通的管道及方法
- 學校儀器設備可以自由帶回家使用  
後再歸還



# 風險管理四道防線

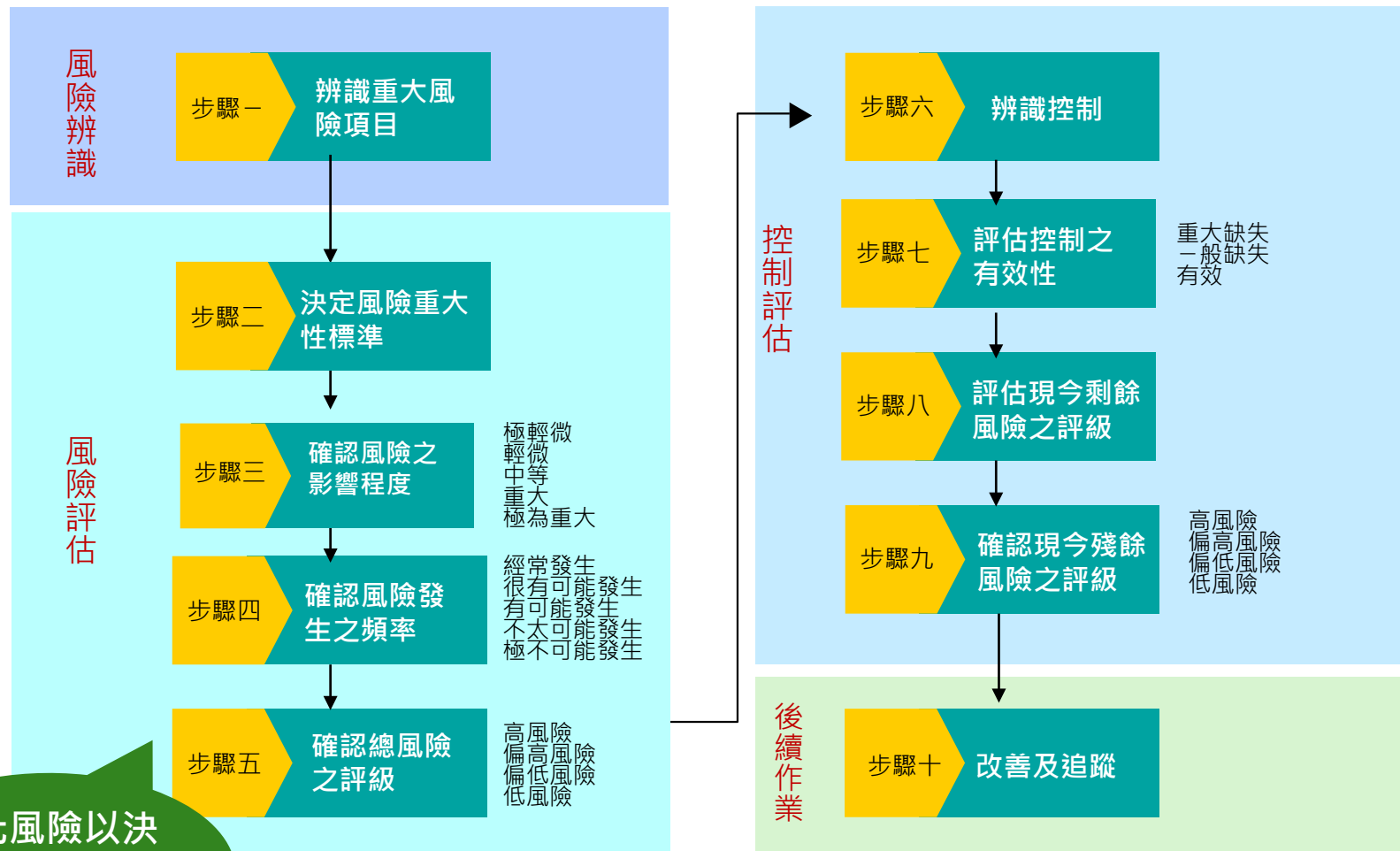


強化組織治理

# 自學校的策略目標及相關營運流程做為辨識風險的起點



# 風險管理流程



量化風險以決定優先順序及加速決策

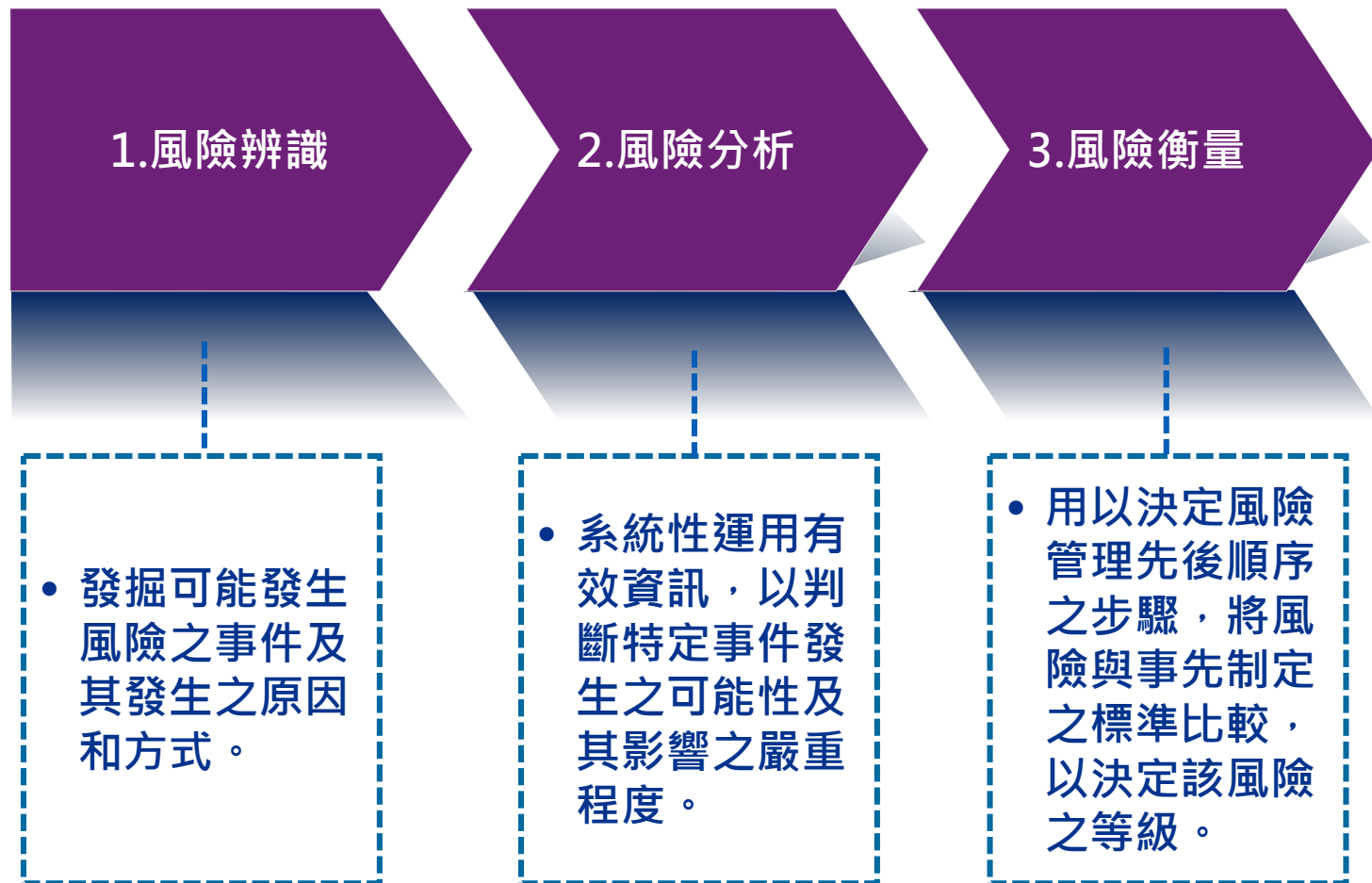


# 風險辨識、評估及回應





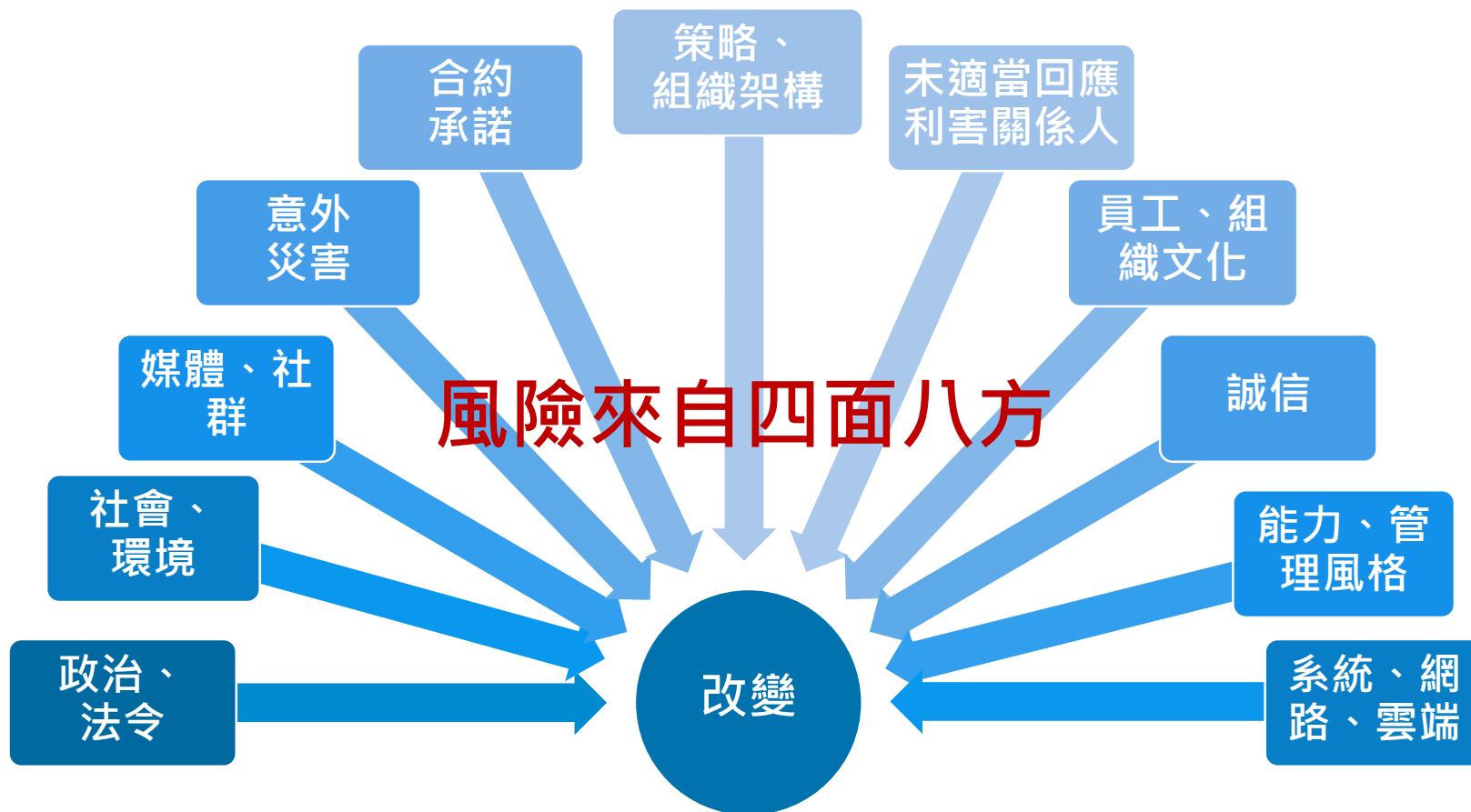
# 風險評估步驟



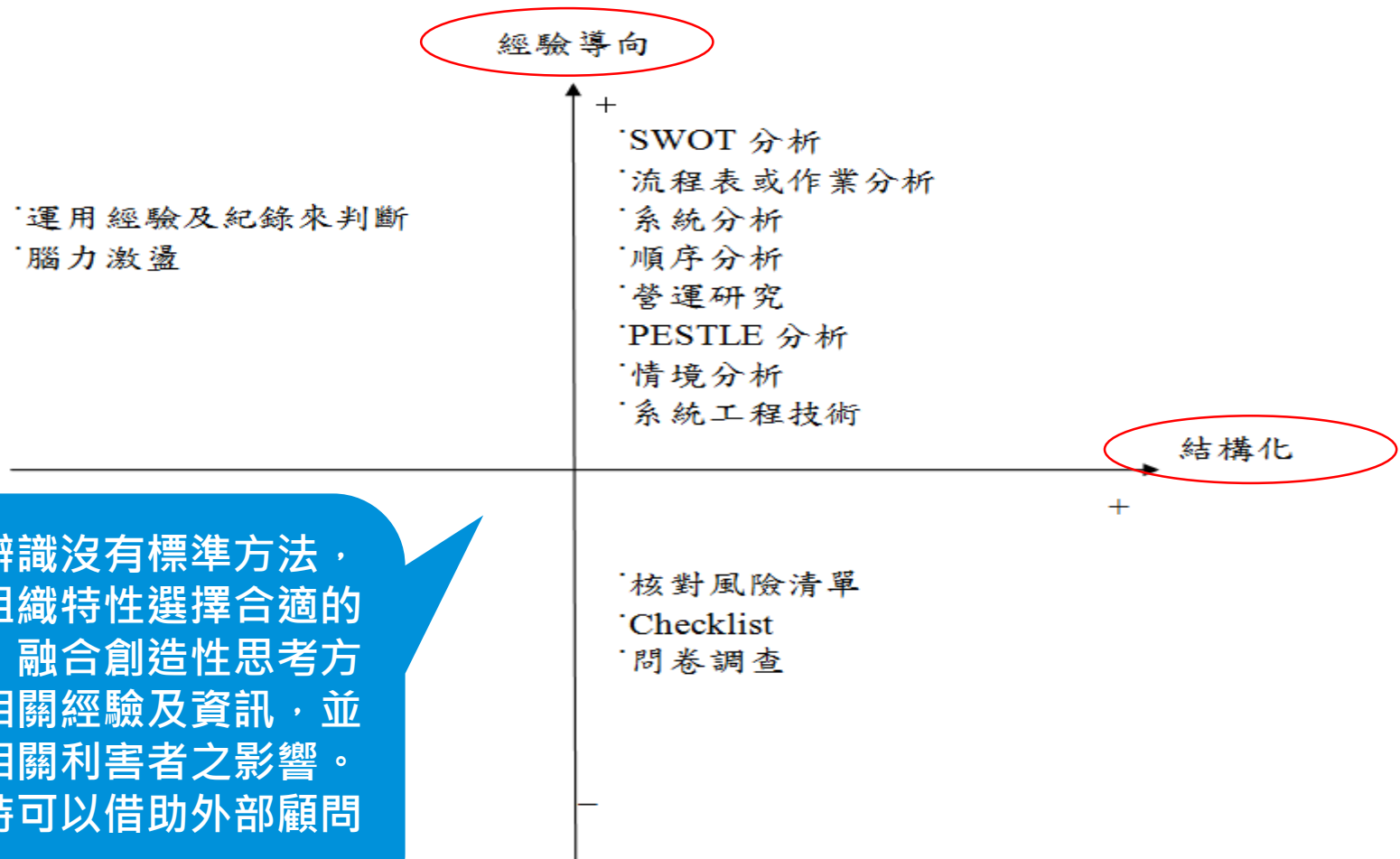
資料來源：[行政院所屬各機關風險管理及危機處理作業基準](#)

# 1. 風險辨識

- 風險辨識：發掘可能發生風險之事件及其發生之原因和方式。



# 風險辨識之方法



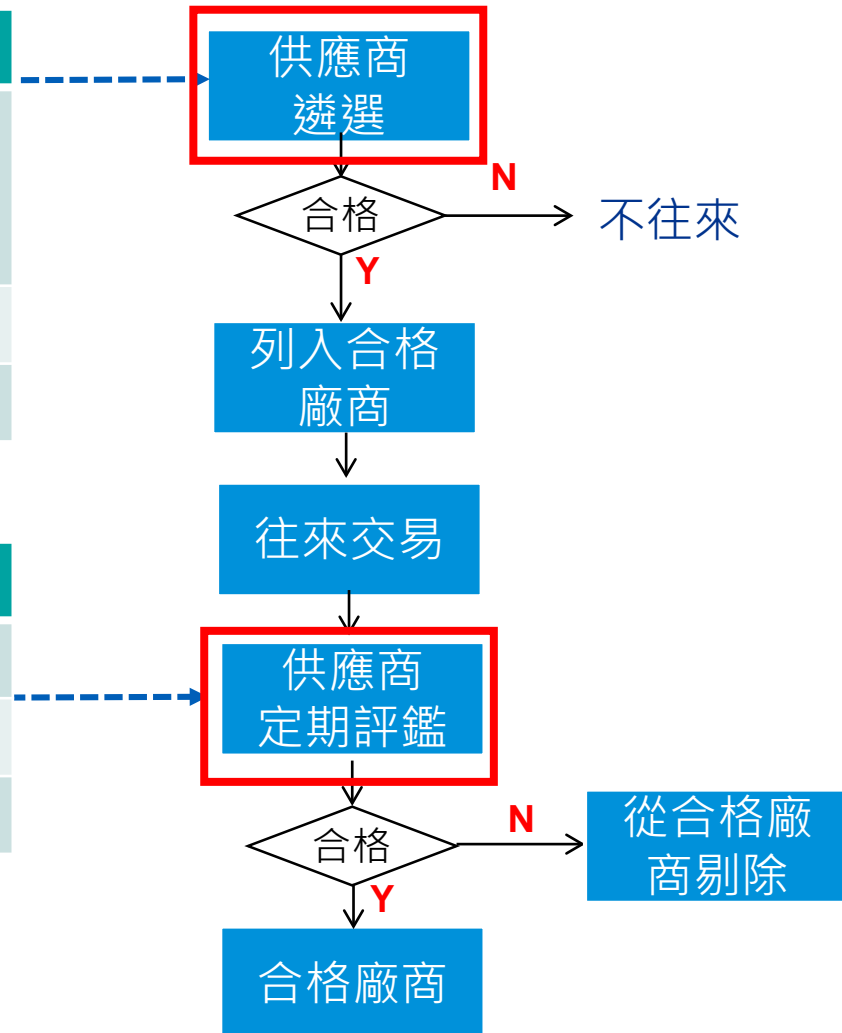
風險辨識沒有標準方法，需依組織特性選擇合適的方式。融合創造性思考方式、相關經驗及資訊，並考量相關利害者之影響。必要時可以借助外部顧問協助

圖 4.1、風險辨識的方法

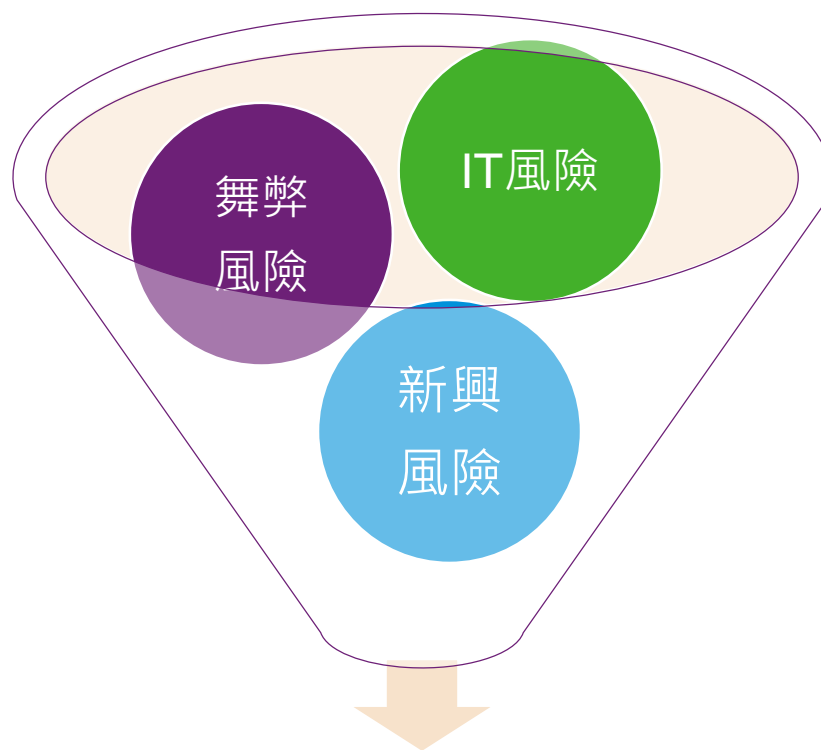
# 釋例：流程分析法\_供應商管理流程

風險事件	原因	後果
• 無法履約	• 未合法登記 • 能力條件不足	• 影響營運
• 大眾輿論	• 血汗工廠	• 聲譽受損
• ?	• ?	• ?

事件	原因	後果
?	?	?
?	?	?
?	?	?



# 舞弊、IT及新興風險應納入辨識與管理



**應納入風險辨識及評估範圍**

## 2.風險評估(衡量)

- 風險評估：系統性運用有效資訊，以判斷特定事件發生之可能性及其影響之嚴重程度。風險(值)=影響 x 機率，將風險與事先制定之標準比較，以決定該風險之等級。並用以決定風險管理先後順序之步驟

- ✓ 總風險值 vs 剩餘風險值?
- ✓ 可接受之風險值?



# 固有風險 v.s. 剩餘風險



## 固有風險

固有風險：於無執行適當控制或任何其他緩解因子的情況下，活動行為所產生之風險。

V.S.



## 剩餘風險

剩餘風險：於已執行適當控制和 / 或其他已考慮到之緩解因子的情況下，仍可能發生之風險。

# 風險評估工具：半定量影響敘述分類表

表 4.5、半定量影響的敘述分類表

等級	衝擊或後果	形象	人員	民眾抗爭	財物損失	目標達成
3	非常嚴重	國際新聞 媒體報導 負面新聞	人員死亡 (如 1 名以上)	大規模遊行抗爭	大於一億元(含)	經費/時間 大量增加
2	嚴重	台灣新聞 媒體報導 負面新聞	人員重傷 (如 1 名以上)	至中央機關抗爭	一千萬(含)以上 一億元以下	經費/時間 中度增加
1	輕微	區域新聞 媒體報導 負面新聞	人員輕傷 (如 1 名以上)	多位民眾 電話抱怨	一千萬以下	經費/時間 輕微增加

備註：所使用的測量基準必須符合機關的需求和本質



# 【範例】某研究院之影響程度敘述分類表

等級	衝擊或後果	形象	人員傷亡	法規/上級機關處分方式	財物損失	影響層面	申訴抱怨	目標達成
3	非常嚴重	國際新聞媒體報導負面新聞	人員死亡	依法懲處	超過100萬元	擴大至院外	團體(11名以上)	經費/時間大量增加
2	嚴重	台灣新聞媒體報導負面新聞	人員重傷(如1名以上)	限期改善	超過10萬元, 100萬元以下	全院性	多數人(3-10人)	經費/時間中度增加
1	輕微	區域新聞媒體報導負面新聞	人員輕傷(如1名以上)	書面說明或回應	10萬元以下	院內某些單位或區域	少數人(2名以下)	經費/時間輕微增加

# 風險評估工具：發生可能性

## ■ 質化(定性)發生可能性的衡量

層級	發生可能性	描述	範例
1	極低	風險事件幾乎不會發生。	
2	低度	風險事件可能會發生，但機率不高。	
3	中度	風險事件會發生，為一般的發生機率。	
4	高度	風險事件會發生，且發生機率高。	
5	極高	風險事件幾乎確定會發生。	

## ■ 半定量發生可能性的衡量

層級	發生可能性	發生機率百分比	描述	範例
1	極低	0-20%	風險事件幾乎不會發生。	
2	低度	21-40%	風險事件可能會發生，但機率不高。	
3	中度	41-60%	風險事件會發生，為一般的發生機率	
4	高度	61-80%	風險事件會發生，且發生機率高。	
5	極高	81-100%	風險事件幾乎確定會發生。	

# 【範例】某研究院之機率敘述分類表

定義	事件描述
經常發生	事件經常發生，例如：在未來一年內發生之機率高於95%
很有可能發生	事件在大多數情況下會發生，例如：在未來一年內有50%~95%之機率會發生
有可能發生	事件一般於疏忽時會發生，例如：在未來一年內有25%~50%之機率會發生
不太可能發生	事件發生的機會很少，例如：在未來一年內有5%~25%之機率會發生
極不可能發生	事件發生之機會極不可能，例如：在未來一年內發生之機率低於5%

# 風險評估工具：風險判斷基準

範例

影響 (衝擊或後果)	風險分布		
非常嚴重(3)	3 (high risk) 高度危險的風險，管理階層需督導所屬研擬計畫並提供資源	6 (high risk) 高度危險的風險，管理階層需督導所屬研擬計畫並提供資源	9 (extreme risk) 極度危險的風險，需立即採取行動
嚴重(2)	2 (moderate risk) 中度危險的風險，必須明定管理階層的責任範圍	4 (high risk) 高度危險的風險，管理階層需督導所屬研擬計畫並提供資源	6 (high risk) 高度危險的風險，管理階層需督導所屬研擬計畫並提供資源
輕微(1)	1 (low risk) 低度危險的風險，以一般步驟處理	2 (moderate risk) 中度危險的風險，必須明定管理階層的責任範圍	3 (high risk) 高度危險的風險，管理階層需督導所屬研擬計畫並提供資源
	幾乎不可能(1)	可能(2) 機率	幾乎確定(3)

備註：必須調整內容以符合各部會的需求

# 風險評估工具：風險圖像(風險矩陣)

影響程度

風險分布

非常  
嚴重(3)

A1、A2

B1

範例

嚴重(2)

E1

D1

E2

輕微(1)

C1

風險圖像於評估總風險與剩餘風險時都會用到。

幾乎不可能(1)

可能(2)

幾乎確定(3)

發生機率

# 風險圖像-總風險及剩餘風險

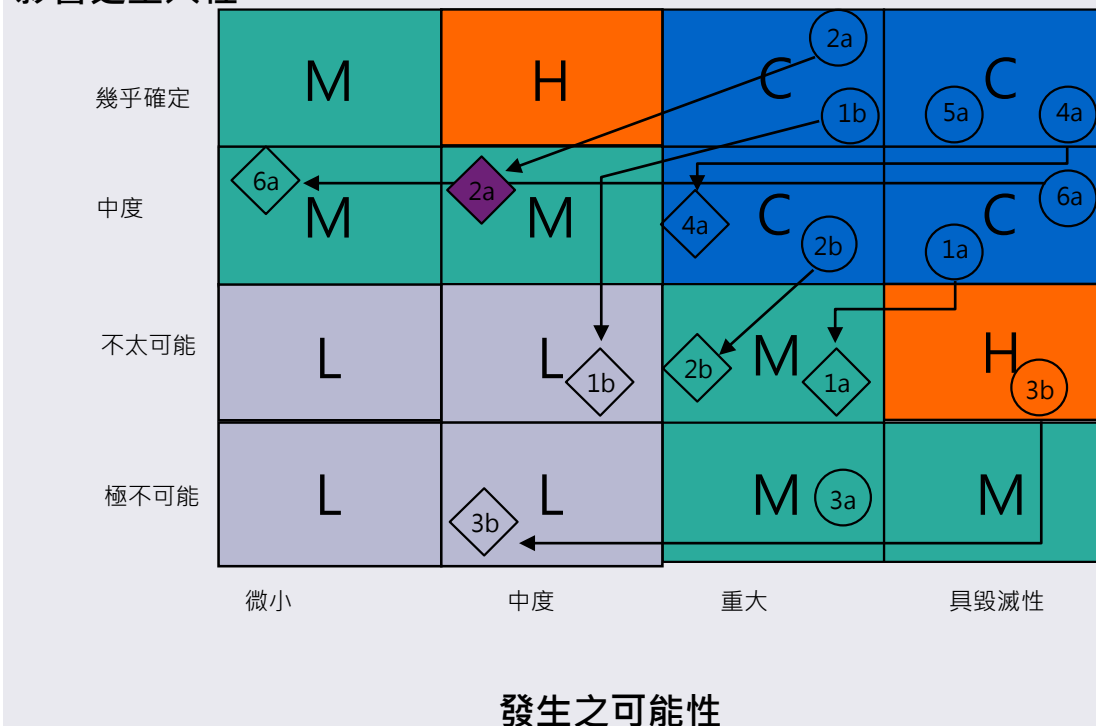
## 總風險水準

可能讓企業整體目標及流程目標無法達成之因素

## 剩餘風險水準

在考慮適當且有效之控制後，剩餘之風險水準

## 影響之重大性



○ = 總風險

◇ = 剩餘風險

低

中

高

重大的

# 風險回應(處理)

- 風險回應：對於風險評估後不可容忍之風險，列出可將風險降低至可容忍程度之對策，進而執行相關對策，以降低事件發生之可能性或其影響之嚴重程度。

✓ 決定不涉入或退出風險處境。

風險規避

✓ 選擇使用適當技巧及管理原則、以降低風險或其發生機率。

風險降低

✓ 透過立法、合約、保險或其他方式將損失之責任及其成本轉移至其他團體。

風險轉移

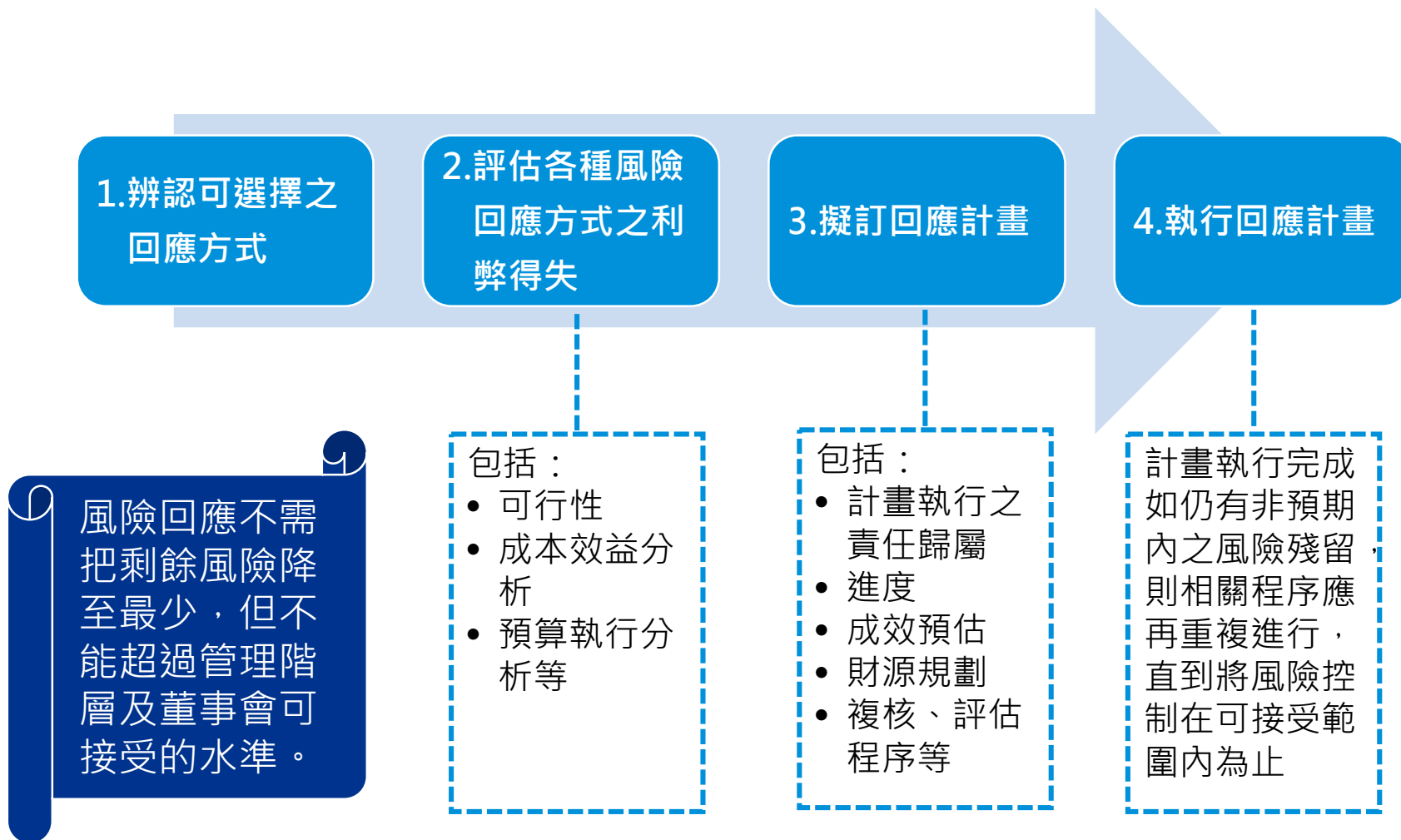
✓ 特意或非特意承擔風險所造成之損失，或為組織之財物損失負責。

風險保有

風險處理對策

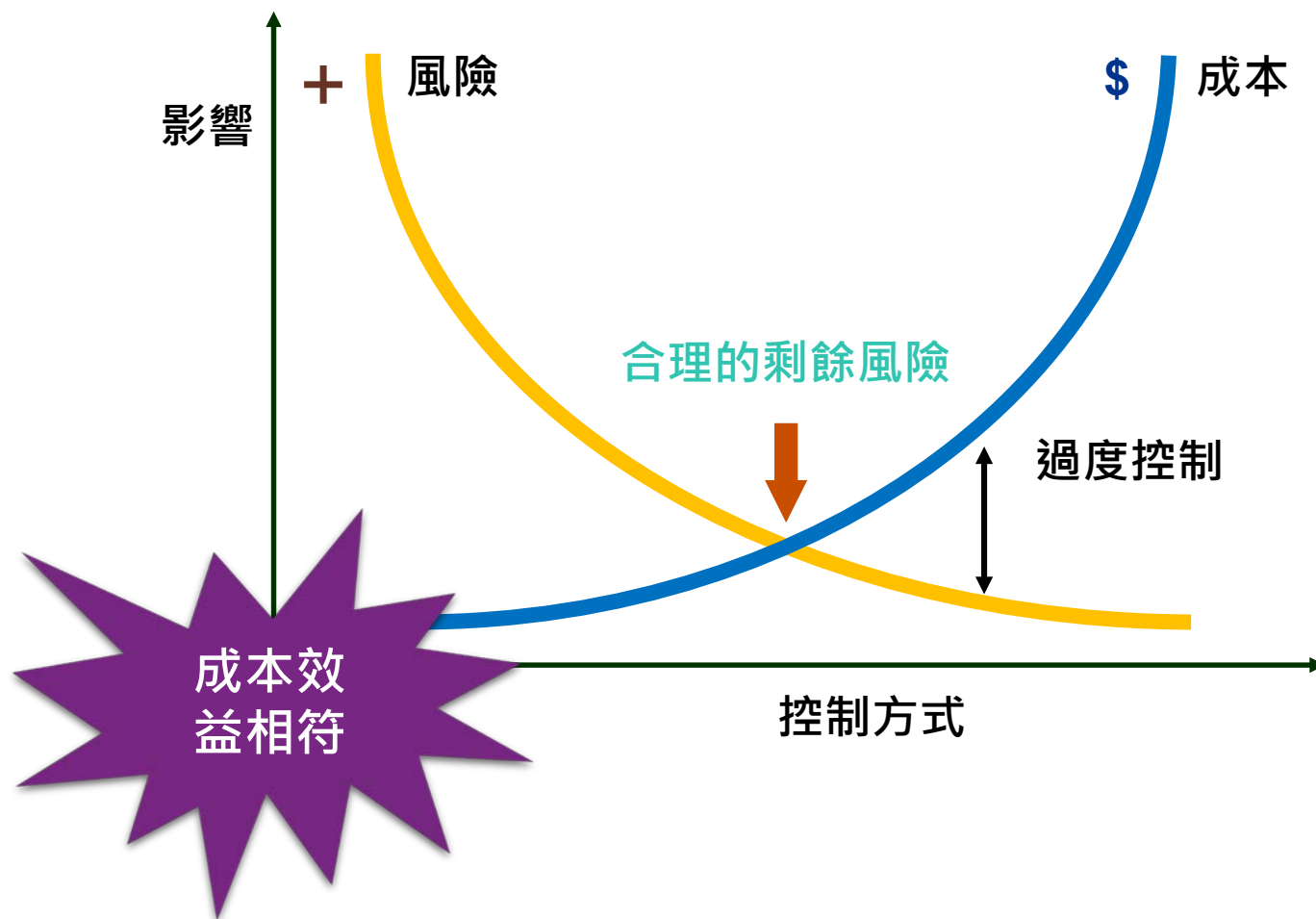
需考量成本效益、政策可行性及處理之優先順序

# 風險回應步驟



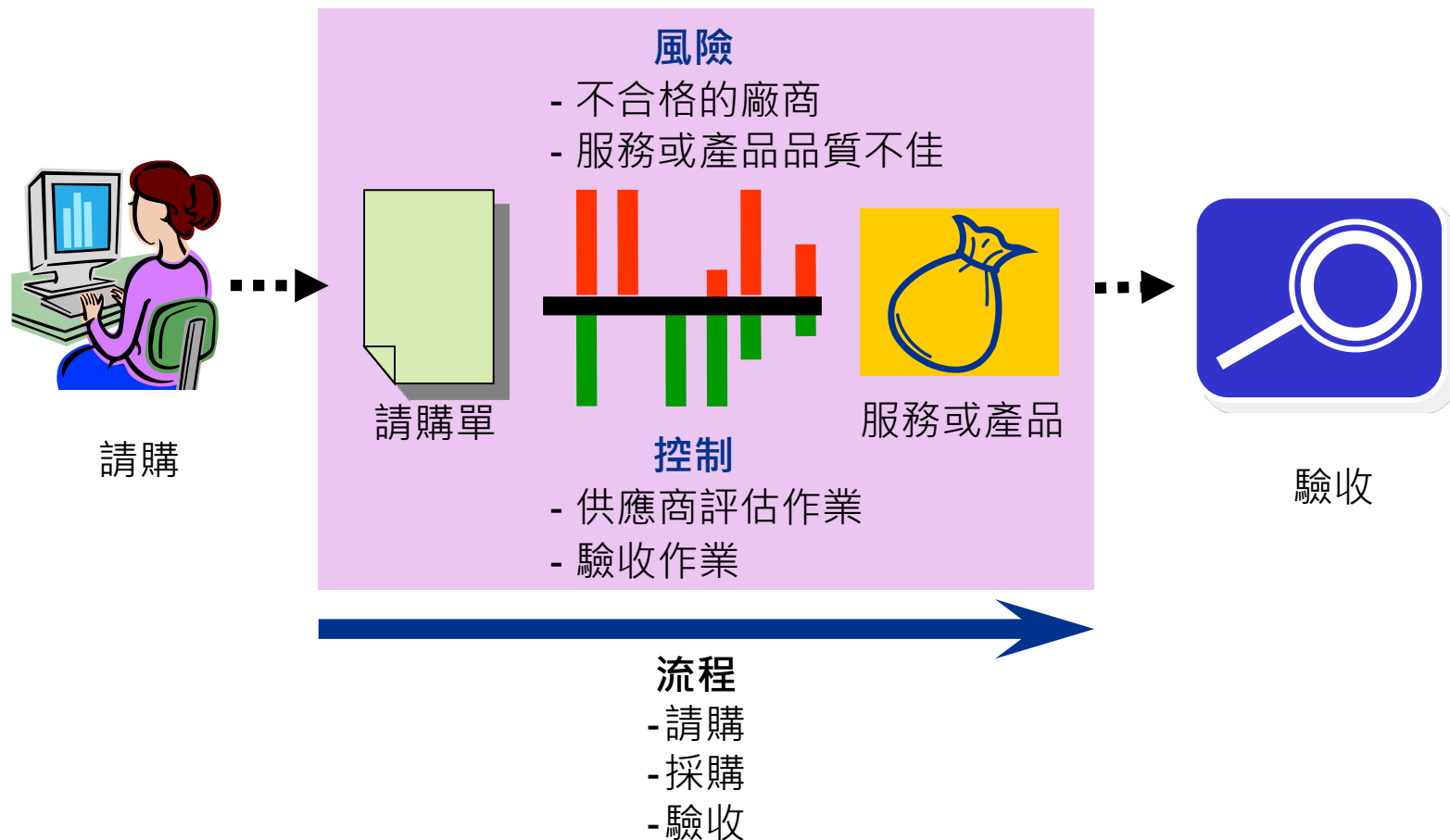


# 以風險為導向選擇合適有效的控制方式



# 控制的目的是降低流程風險

## 範例：採購流程



# 控制的分類

## 預防性(P) vs. 偵測性(D)

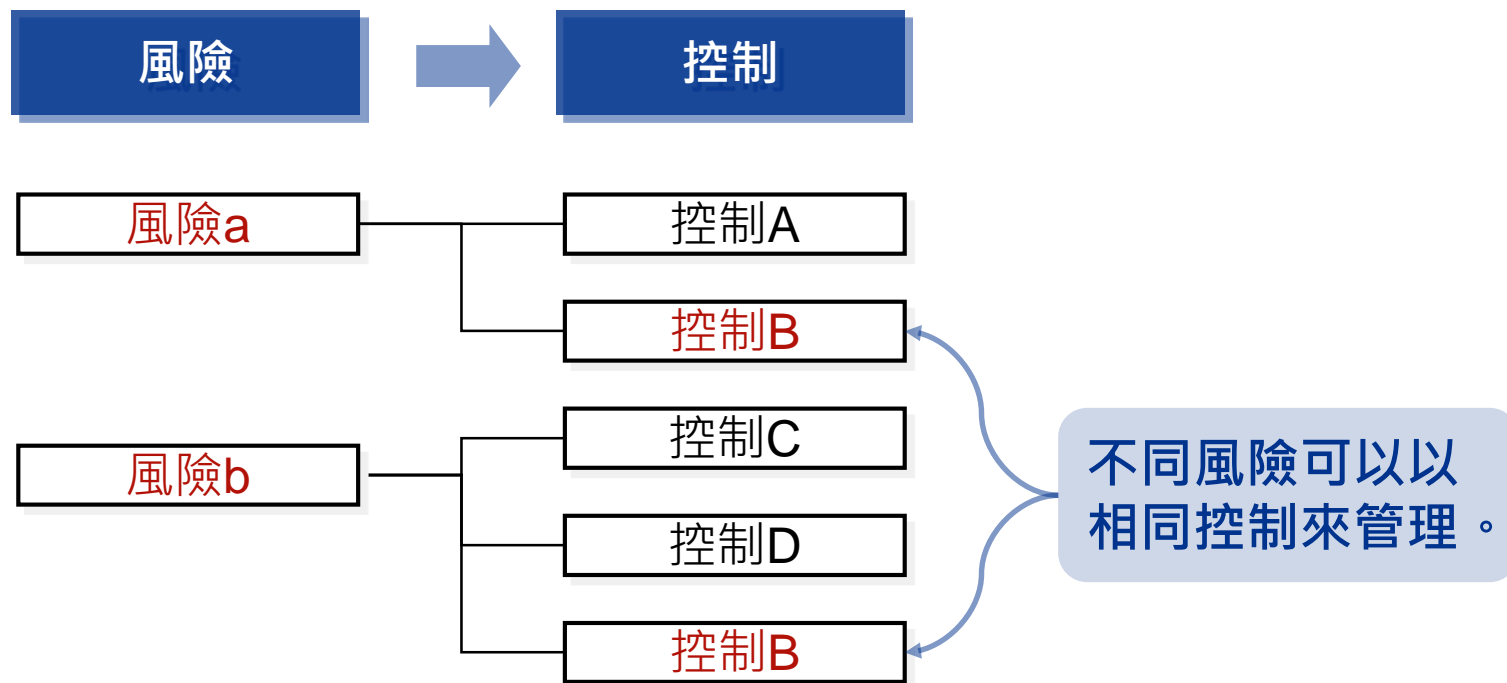
- **預防性(Preventive)**
  - 預防性控制係用以消除錯誤的引發，以及問題的發生
  - 運用密碼限制某特定帳戶之存取，即為一種預防性控制
  - 通常仍藉由偵測性控制，確認預防性控制是否有效地運作
- **偵測性(Detective)**
  - 偵測性控制係用以揭發錯誤與問題
  - 舉例：在一個組織中，內部稽核職能即為一種偵測性控制
  - 舉例：以非法入侵而言，當某人使用他人的密碼時，可被系統自動偵測出

## 自動控制(A) vs. 人工控制(M)

- **自動控制(Automatic)**
  - 自動控制係藉由電腦程式預防、偵測或改正異常
  - 自動控制在財務套裝軟體中是很常見的
- **人工控制(Manual)**
  - 人工控制係由個人來執行
  - 適當的職能分工於人工作業中，是相當必要的
  - 管理階層的覆核即為一種人為控制

# 風險和控制的關係

- 風險控制模式中的風險、控制各自的對應中存在以下關係：

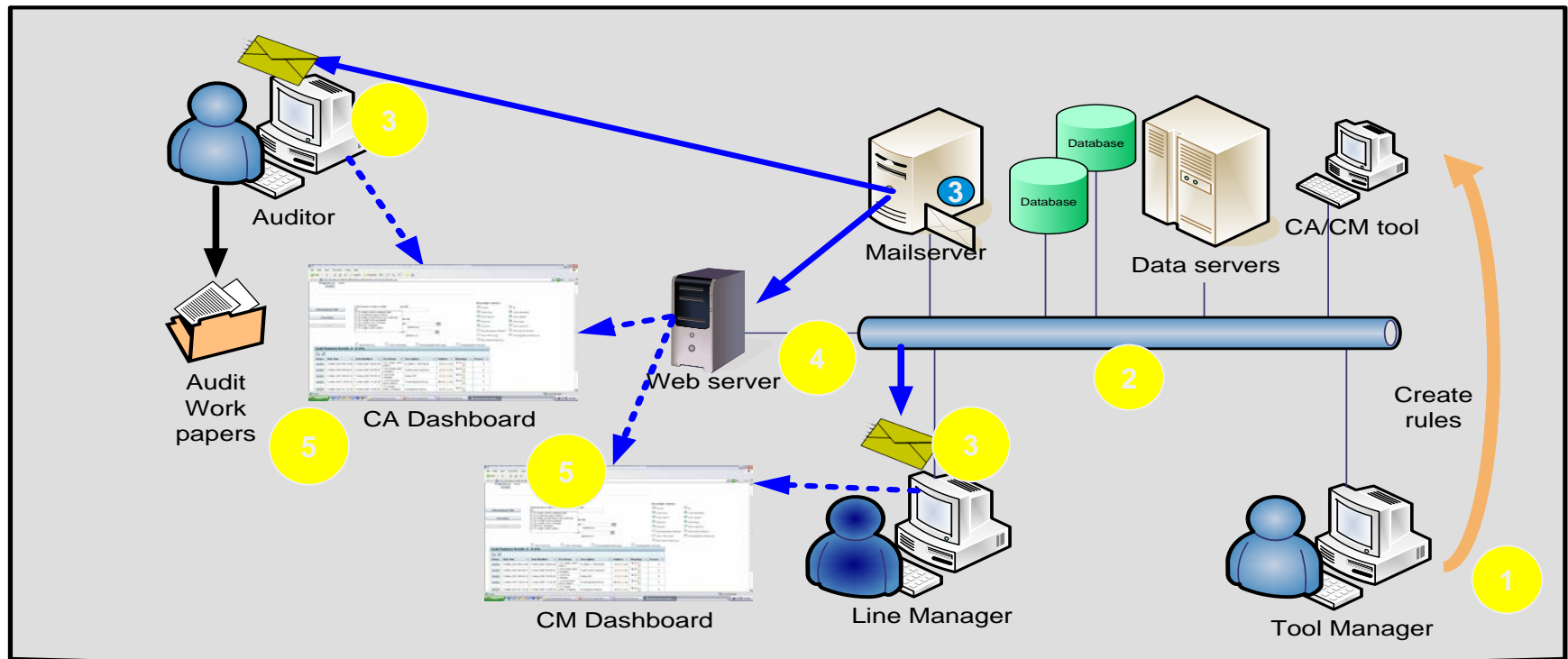


# 控制的類型(範例)

- 覆核(Management Review)
- 授權(Authorization)
- 調節(Reconciliation)
- 職能分工(Segregation of Duties)
- 重要績效指標(KPIs)
- 例外/編輯報表(Exception / Edit Report)
- 界面/轉換控制( Interface / Conversion controls)
- 系統使用權限(System Access)
- 系統配置/科目對應控制(System Configuration / Account Mapping)
- 其他(視風險性質彈性調整)

不同組織、不同行業、不同流程或不同環境等應視實際情況與資源選擇不同之控制類型，且控制類型不以此處所列為限。

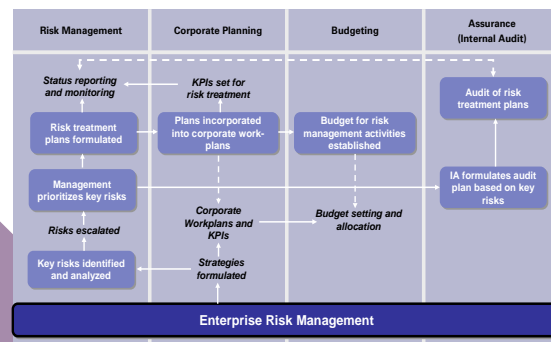
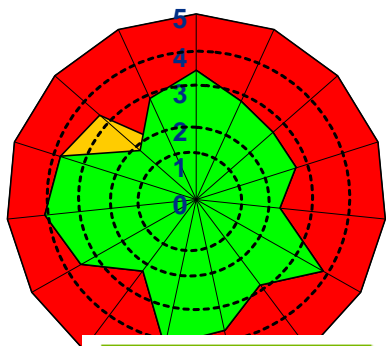
# 運用持續性稽核/監督機制管理風險



1. Rules created in CA/CM tool
2. Rules run against databases
3. E-mail alerts to auditors/management
4. CA/CM tool populates web server
5. Dashboard provides summary and drill down capability for auditors/management

高度使用資訊系統組織應考量使用CACM。

# 舞弊風險管理與內部控制應整合



## Process risk

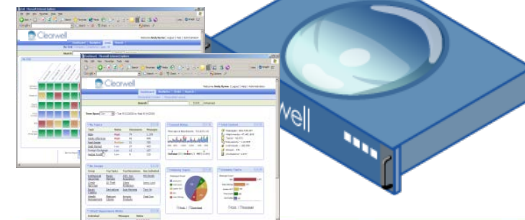
- a) Inadequate customer research to objectively develop and assess brand position/identity
- b) Insufficient competitor monitoring
- c) Divergence between strategic and brand plans
- d) Poor advertising and promotion agency selection
- e) Ineffective advertising campaign
- f) Inconsistent delivery and interpretation of advertising and promotion message by staff

## Process

- Brand management
- Advertising and promotion (A&P)
- Budgeting
- Product development
- Supplier selection and sourcing

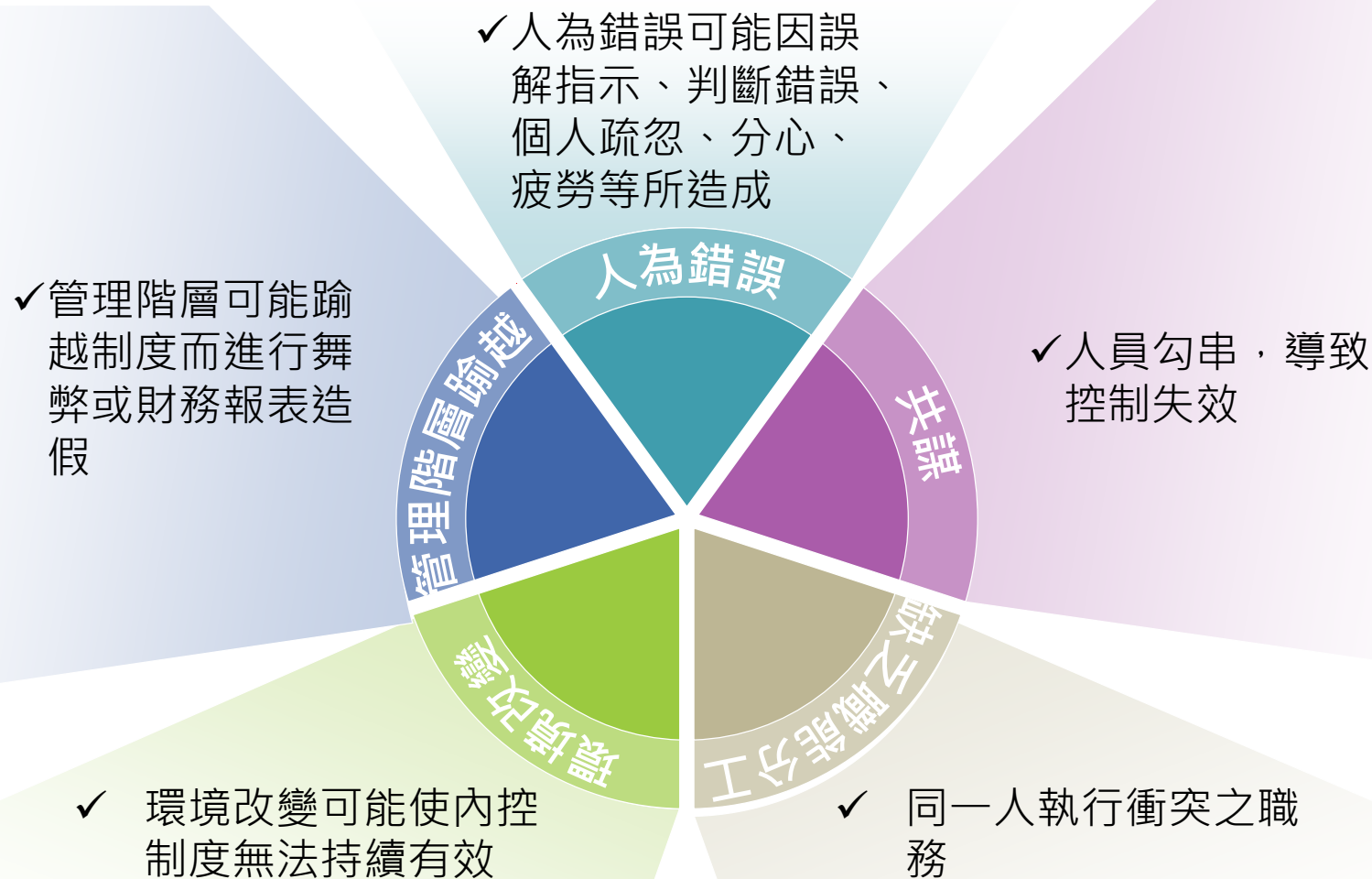
## Function

- Marketing + Sales
- Marketing + Sales+ Procurement
- Marketing + Sales+ Finance
- Marketing + Sales+ R&D
- Marketing + Sales+ Procurement



	內容	頁次		內容	頁次
第一章	總則		(續)		
第一節	目的		第三節	總風險分析	
第二節	風險的定義...		第四節	控制分析	
第三節	風險管理的定義		第五節	利益風險分析	
第四節	風險管理的內容與相關權責人員		第四章	風險的溝通	
第二章	風險管理架構		第一節	風險溝通的概述	
第一節	風險管理架構的概述		第二節	風險事件的權限與出清時點	
第二節	風險管理架構成員之角色與權責		第五節	風險的監控	
第三節	風險管理的責任		第一節	風險的監控責任	
第四節	內部稽核的角色與權責		第二節	風險監控相關表單	
第三章	風險評估流程		第六章	總則	
第一節	風險評估流程的概述		第七章	附則	
第二節	前置作業				

# 內部控制先天上之限制



**有效的內部控制提供合理之確信，而非絕對的保證**



# 風險 v.s. 肇因 v.s. 影響??

風險事件	可能導致發生風險之原因	可能影響(衝擊)
<ul style="list-style-type: none"><li>設備損壞</li></ul>	<ul style="list-style-type: none"><li>未定期維修</li><li>天災、事故</li><li>人為蓄意</li><li>其他</li></ul>	<ul style="list-style-type: none"><li>財物損失</li><li>人員傷亡</li><li>影響營運</li></ul>
<ul style="list-style-type: none"><li>採購金額過高</li></ul>	<ul style="list-style-type: none"><li>未詢比議價</li><li>採購規格高於需求規格</li><li>虛假報價單</li><li>其他</li></ul>	<ul style="list-style-type: none"><li>財物損失</li><li>其他?</li></ul>



# 什麼是有效的 的內部控制



# 內控有效性之定義

## ■ 定義

- 可合理確保達成組織目標
- 將無法達成組織目標的風險，降低至可接受水準

## ■ 標準

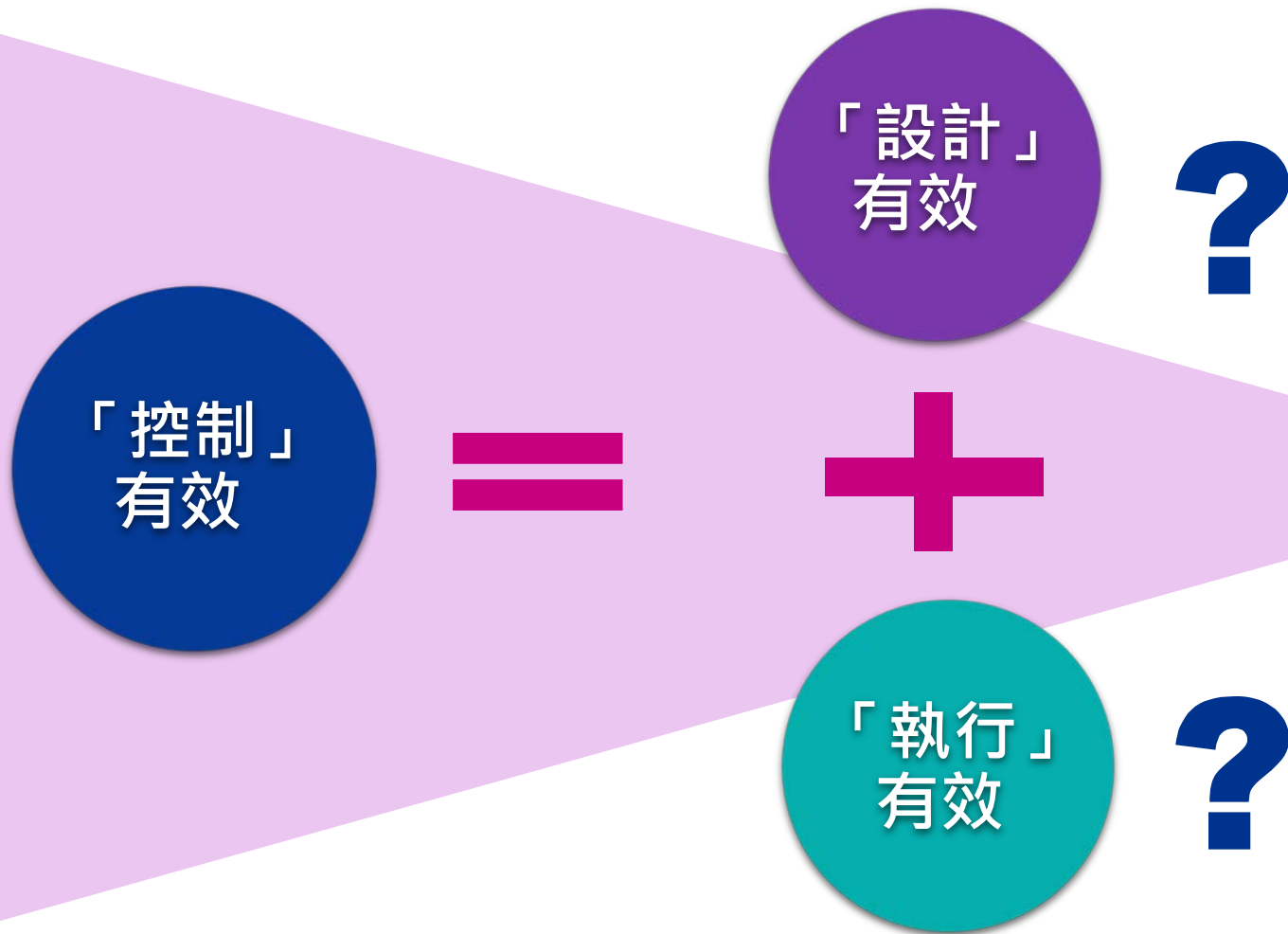
- 五個組成要素以及其相關之原則
  - Present and Functioning
    - Present (設計與實施)
    - Functioning (組成要素與原則未來仍會持續存在並實施)
  - Operate together in an integrated manner (共同降低風險)



# 評估內控 有效性



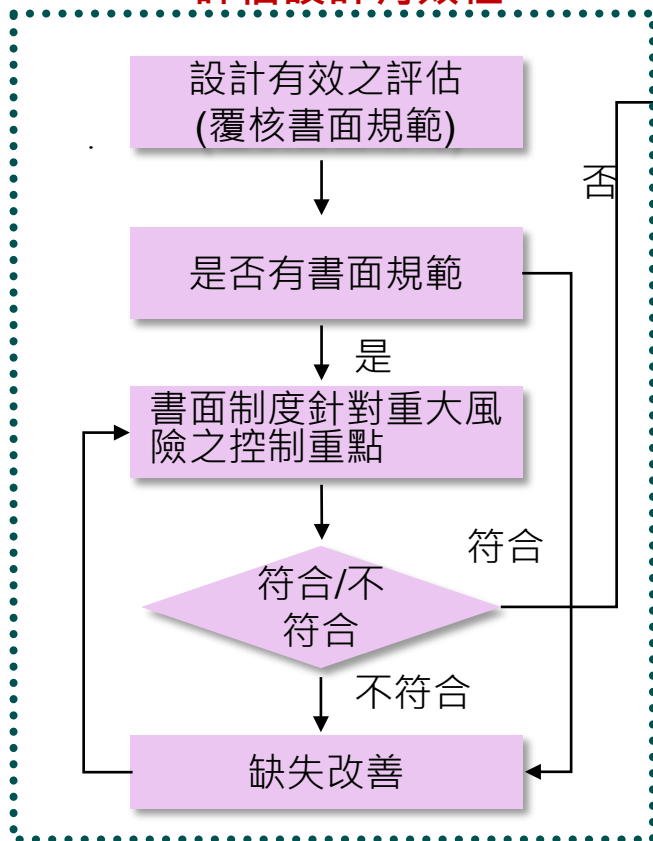
# 何謂「控制有效」？



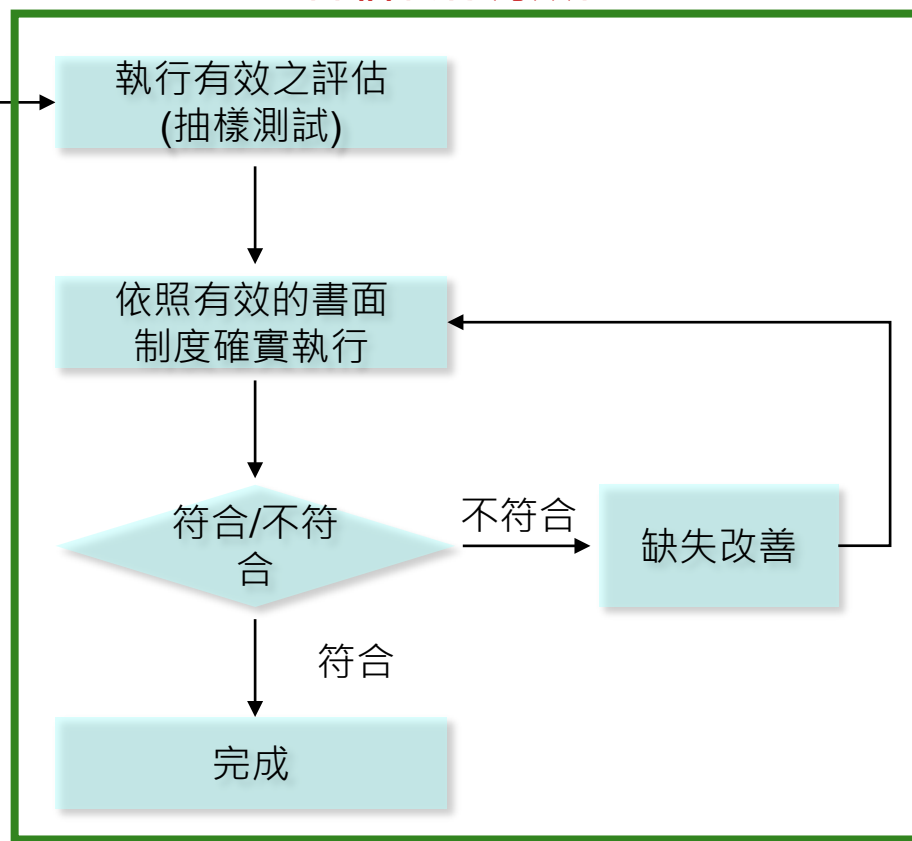
# 內控有效性評估目的及方式

目的：落實組織自我監督的機制、及時因應環境的改變，以調整內部控制制度之設計及執行

## 評估設計有效性



## 評估執行有效性



# 評估內控有效性之方法

## 方法一、內部控制自行評估

由相關單位依職責分工評估控制環境、風險評估、控制作業、資訊與溝通及監督作業等內部控制五項組成要素運作之有效程度

## 方法二、內部稽核

由內部稽核專責單位或任務編組（以下簡稱內部稽核單位）以客觀公正之立場，協助機關檢查內部控制實施狀況，並適時提供改善建議。

## 方法三、外部獨立第三方稽核





# 內部控制 制度自行 評估

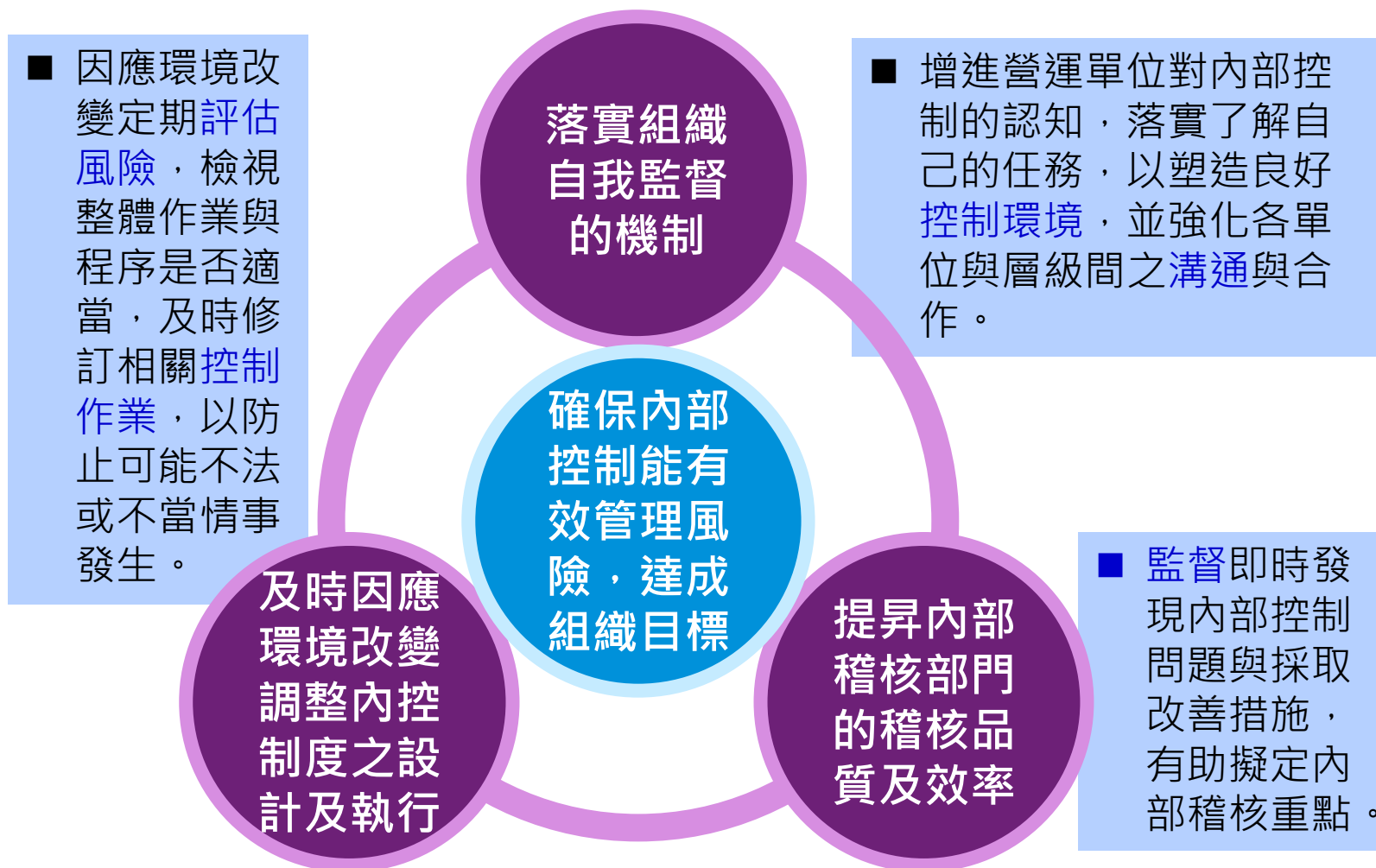


# 什麼是內部控制制度自行評估？

內部控制制度自行評估，簡單來說就是一種營運單位定期評估風險、內部控制制度設計有效性、與執行有效性的一種過程。

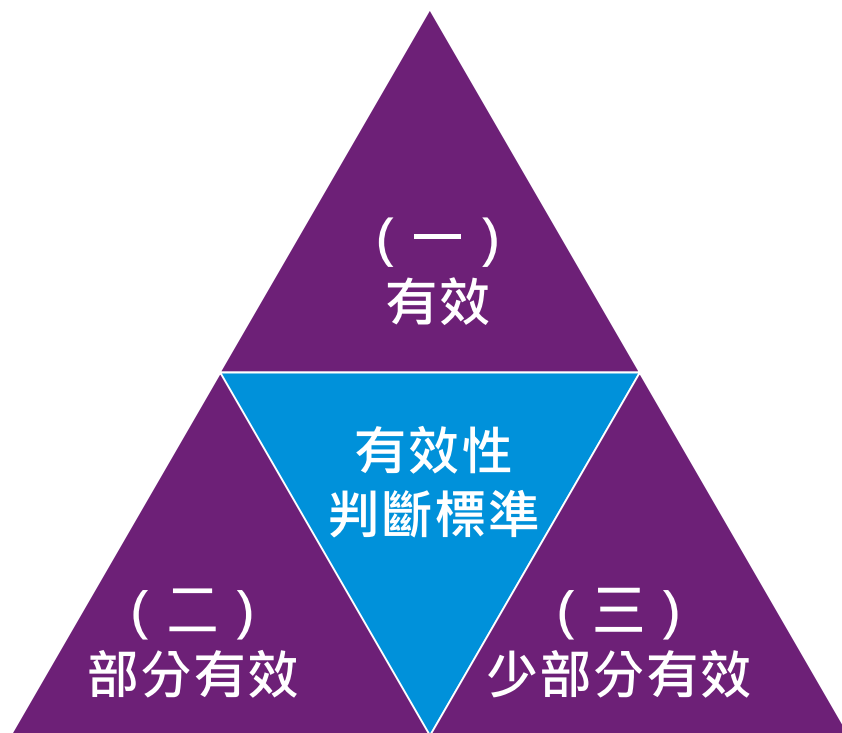


# 內部控制制度自行評估之目的及效益



資料來源：以上係彙整及引用公開發行公司建立內部控制制度處理準則及政府內控制度自行評估相關宣導資料內容

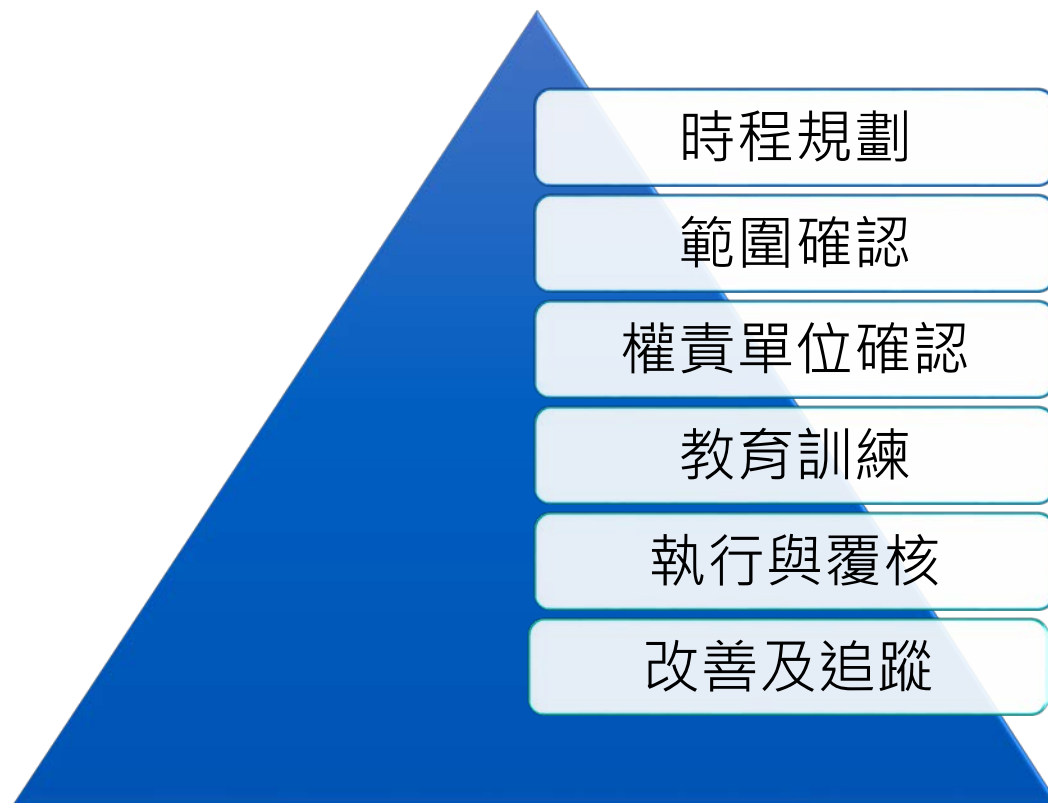
# 內部控制自行評估有效性判斷標準



評估結果	判斷標準
(一) 有效	判斷項目評估結果全數或大部分為「落實」，且無內部控制缺失或有內部控制缺失惟不影響內部控制目標之達成。
(二) 部分有效	判斷項目評估結果全數或大部分為「部分落實」，且有內部控制缺失並影響部分內部控制目標之達成。
(三) 少部分有效	判斷項目評估結果大部分為「未落實」，且有內部控制重大缺失並影響大部分內部控制目標之達成。

# 內部控制自行評估之運作釋例

內控自行評估的最重要意涵是檢視  
環境變化下現有內控是否需要調整



# 【範例】整體層級自行評估總表

## ○○學校整體層級自行評估總表

○○年度

評估期間：○○年○○月○○日至○○年○○月○○日

組成要素	評估結果
一、控制環境	<b>【範例】</b> <input checked="" type="checkbox"/> 有效 <input type="checkbox"/> 部分有效 <input type="checkbox"/> 少部分有效
二、風險評估	<input type="checkbox"/> 有效 <input type="checkbox"/> 部分有效 <input type="checkbox"/> 少部分有效
三、控制作業	<input type="checkbox"/> 有效 <input type="checkbox"/> 部分有效 <input type="checkbox"/> 少部分有效
四、資訊與溝通	<input type="checkbox"/> 有效 <input type="checkbox"/> 部分有效 <input type="checkbox"/> 少部分有效
五、監督作業	<input type="checkbox"/> 有效 <input type="checkbox"/> 部分有效 <input type="checkbox"/> 少部分有效
備 註	<b>【範例】</b> 1. 本學校內部控制制度（第○次修正），係配合學校目標（組織規程調整或法令變革等）於○年○月○日修訂。 2. ....

# 【範例】整體層級自行評估明細表

○○學校整體層級自行評估明細表【控制環境】

○○年度

評估期間：○○年○○月○○日至○○年○○月○○日

判斷項目	評估單位	評估結果	佐證資料清單	評估情形說明	改善措施/ 具體興革建議
1.1誠信與道德價值					

※ 僅供參考用，貴校應依實際情況調整。

# 【範例】作業層級自行評估表

## ○○學校作業層級自行評估表 ○○年度

評估單位：○○

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期： 年 月 日

本單位職掌業務例行監督及控制作業(包括○○○等○項控制作業)，其自行評估結果如下表：

評估重點	評估情形					部分落實/未落實/ 不適用情形說明	改善措施
	落實	部分落實	未落實	不適用	其他		
填表人：                  複核：                  單位主管：							

# 【範例】控制作業自行評估表

## ○○學校內部控制制度控制作業自行評估表 ○○年度

評估單位：○○

作業類別(項目)：○○作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期： 年 月 日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	

填表人： 複核：

註：

- 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
- 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。



# 【範例】作業層級自行評估統計表

## ○○學校作業層級自行評估統計表【範例】 ○○年度

評估期間：○○年○○月○○日至○○年○○月○○日

評估單位	各項評估重點之評估情形				
	落實	部分落實	未落實	不適用	其他
秘書室	10				
人事處	7				
⋮	⋮	⋮	⋮	⋮	⋮
總計	130(96%)	5(4%)	0(0%)	0(0%)	0(0%)

# 【範例】作業層級自行評估部分落實/未落實項目一覽表

## ○○學校作業層級自行評估部分落實/未落實項目一覽表【範例】 ○○年度

評估期間：○○年○○月○○日至○○年○○月○○日

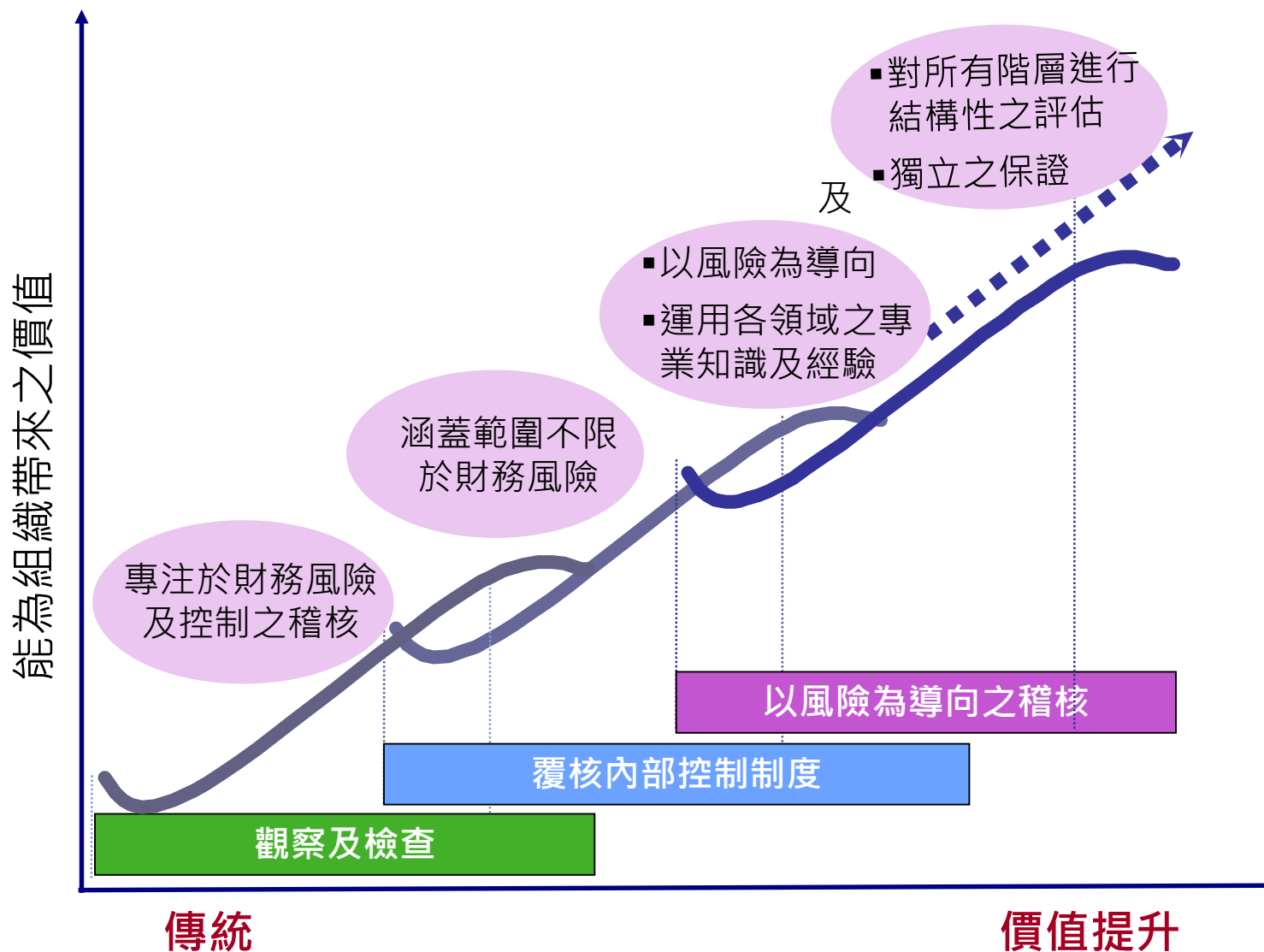
評估單位	評估重點	部分落實/未落實 情形說明	改善措施
資訊處	執行內部控制制度之各項控制作業。	應用系統上線及變更管理作業於評估期間共發生810筆系統維護申請作業，大多為常態性變更或維護，部分僅由單人維護的小型系統較難滿足資訊安全內部控制職能分工之規範。	請各科協調人力相互支援，以落實執行系統維護人員及系統管理人員由不同人員擔任之規範。
：	：	：	：

註：本表由內部控制小組幕僚單位彙整後交由內部稽核單位追蹤後續改善情形。

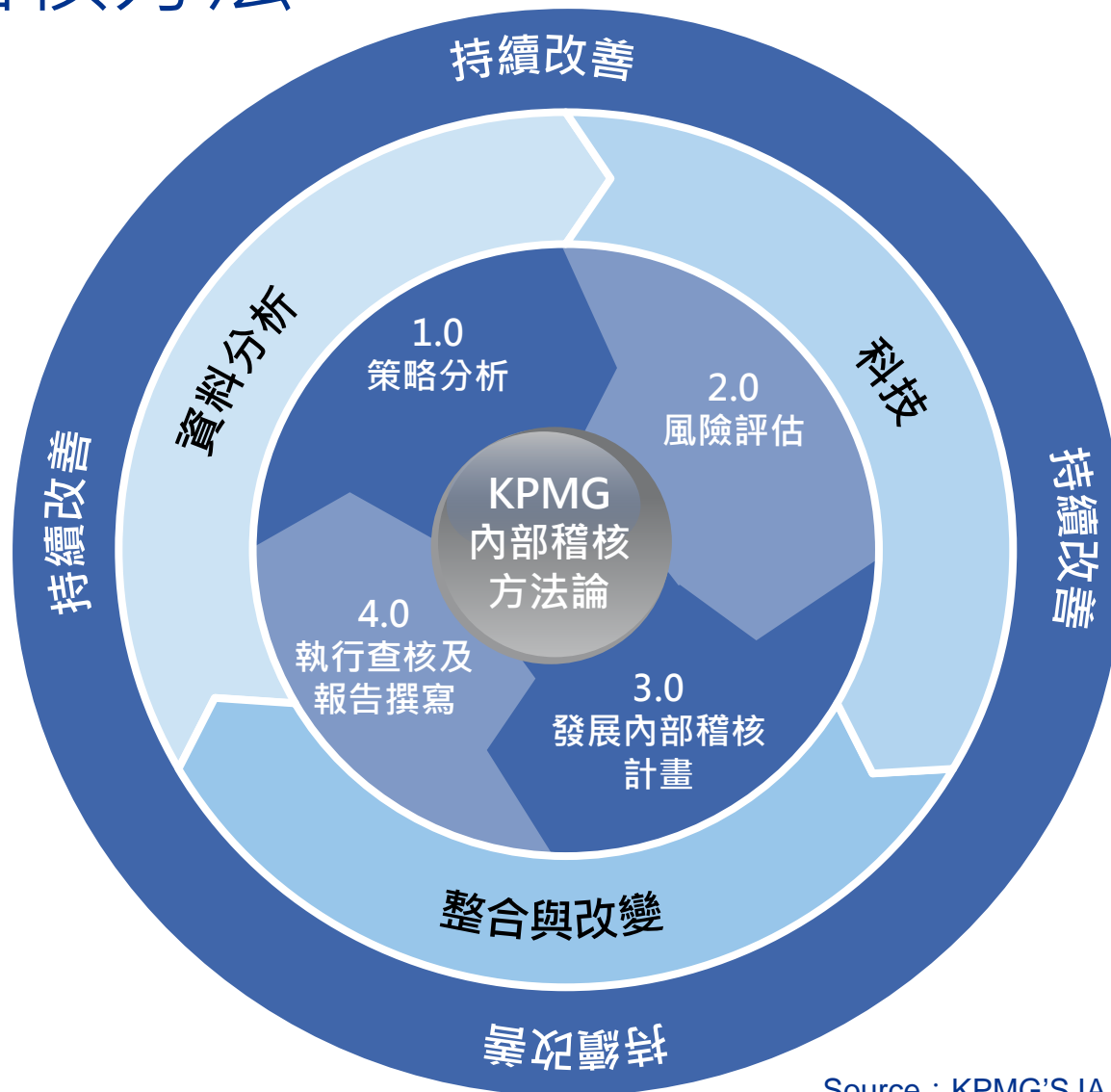


# 內部稽核

# 內部稽核角色的演變

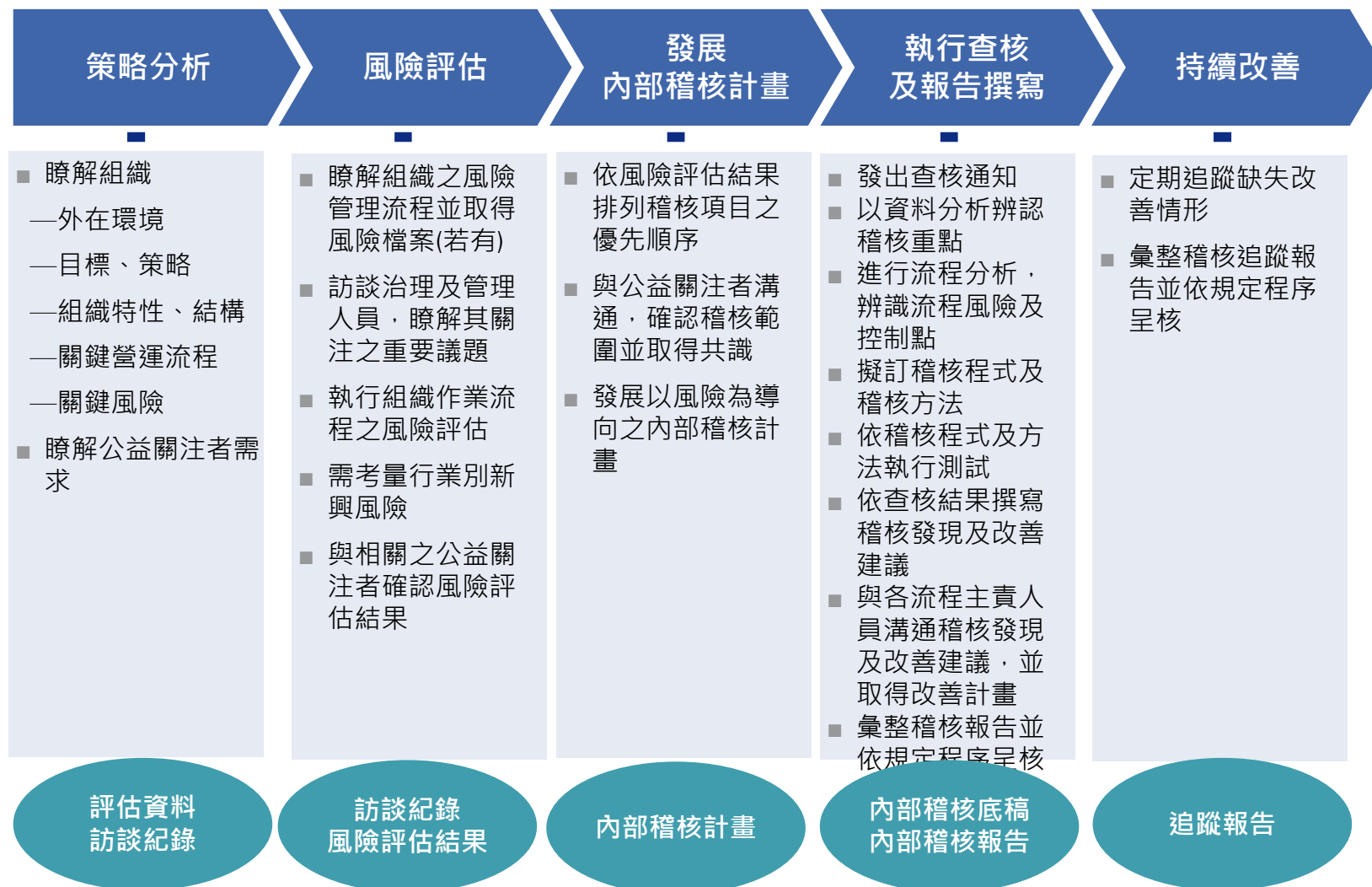


# 內部稽核方法



Source : KPMG'S IA Methodology

# 內部稽核方法(續)



# 運用資料分析優化內部稽核運作與風險監督



## 資料分析於內部稽核之運用

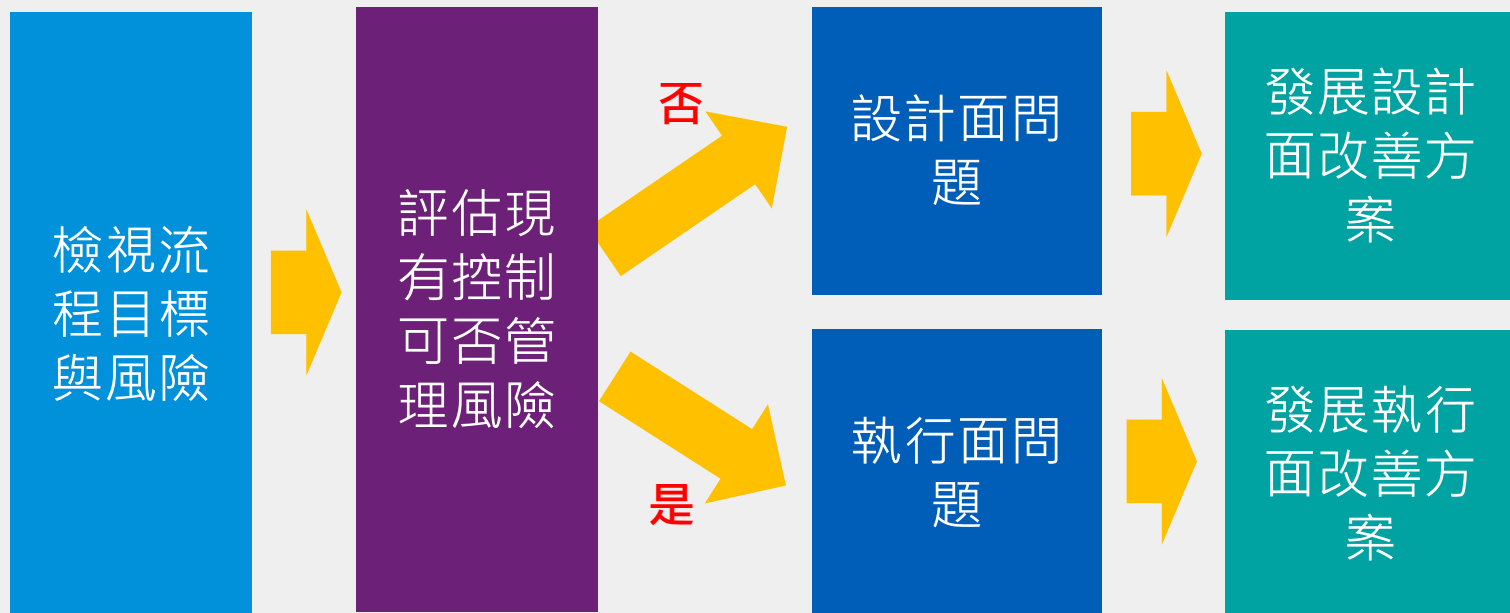


# 設計無效 之改善





# 分析控制無效之原因



# 分析設計無效之根本原因

設計無效之原因時，通常考量下列 **5W**以及**1H**：

Who

- 誰造成的？

Why

- 為什麼會發生？

What

- 詳細內容為何？

When

- 何時會發生？

How

- 如何發生？

Where

- 風險係存在於哪一個專案或部門之中？

# 釋例：分析設計無效之根本原因與改善方案

發生情況：員工的系統使用權限應與職責相配合，但於清查權限時發現某員工仍有他在舊部門時的權限，可以輕易查詢及處理與目前職務無關的作業

原因		改善方案
Who	各部門權責人員	將原職務之系統權限之撤銷列入調職程序辦理。人資部人員於處理轉調職作業時，自動知會資訊部撤銷相關人員之系統權限
Why	未於部門人員轉調職時，即時向資訊單位申請撤銷其職務之系統使用權限	
What	調職人員仍有原職務之系統使用權限	
When	員工轉調職務時	
How	轉調職人員其原職務之系統使用權限，需由所屬部門向資訊單位申請撤銷	
Where	各部門	

# 實作練習：分析設計無效之根本原因 與改善方案

發生情況：

- 1.畢業班停課期間，教師未有授課事實仍核發鐘點費。
- 2.開口合約之執行，未隨時注意核銷金額是否已超過契約金額。

	原因	改善方案
Who		
Why		
What		
When		
How		
Where		



# 循環內控制 度建置



# 學校循環別內部控制制度

營運循環	內控應含括項目
招生循環	包括招生策略、策略聯盟、入學管道分析、試務與宣導等之政策及程序。
入學至畢業循環	包括註冊、學籍及成績管理、獎懲、獎助學金、休退學、畢業等之政策及程序。
教學作業循環	包括修業規定、排課、開課、選課、實習、學分抵免等之政策及程序。
學生輔導循環	包括學生之課外活動、社團、賃居、生活、課業、升學、就業、三級輔導與申訴處理等之政策及程序。
人事管理循環	包括教職員工之招聘僱、報到、敘薪、待遇、福利、保險、退休、資遣及撫卹、職務輪調、出勤、差假、訓練、進修、考核、獎懲薪資計算、支付與調薪等之政策及程序。
採購及付款循環	包括供應商管理、請購、招標、比議價、訂購、預支、交貨、驗收、付款與財產保管等之政策及程序。

資料來源：學校財團法人及所設私立學校內部控制制度實施辦法

# 學校循環別內部控制制度(續)

營運循環	內控應含括項目
不動產、建築物及設備循環	包括不動產、建築物及設備之發包、營建管理、取得、財產登錄、盤點、使用維護與報廢處分等之政策及程序。
融資循環	包括借款、還款、租賃等資金融通事項之授權、執行與記錄等之政策及程序。
投資循環	包括投資有價證券（股票、基金、債券等金融商品）、附屬機構、衍生企業及其他投資決策之授權、執行與記錄等之政策及程序。
資訊管理循環	包括資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序。

# 如何撰寫循環內部控制文件？






# 循環內部控制文件之主要組成



與現有架構  
並無太大差異

# 建立文件格式範例及統一方式表達項目

	文件類別	作業程序	文件編號	GA-CP-07	頁次	3
	文件名稱	採購流程管理	制修日期	2016-04-15	版次	1.4

壹、目的：  
確保本校為提供教學行政服務之物品（含設備）及服務取得時，能滿足本校需求及品質要求，並符合政府相關法令之規定。

貳、範圍：  
用於提供教學行政服務之財物買受、定製、承租及勞務委任或僱傭等。

參、權責：  
1.總務處事務管理組（簡稱事務組）主辦本校財物與勞務採購作業辦法第二條作業範圍之採購（不包括授權單位自辦新台幣貳萬元內之採購案及單位以簽呈簽請核准自辦方式之採購案），各請購單位及相關單位協辦之。  
2.二萬元以下之物品採購由各請購單位自行辦理。  
3.總務處財務管理組（簡稱財管組）主辦本校採購之設備會驗、登錄財產與盤點和付款，各請購單位及相關單位協辦之。  
4.總務處工程組（簡稱工程組）負責審核「元智大學採購儀器設備水電需求表」是否為特殊水電需求設備。

肆、定義：  
無。

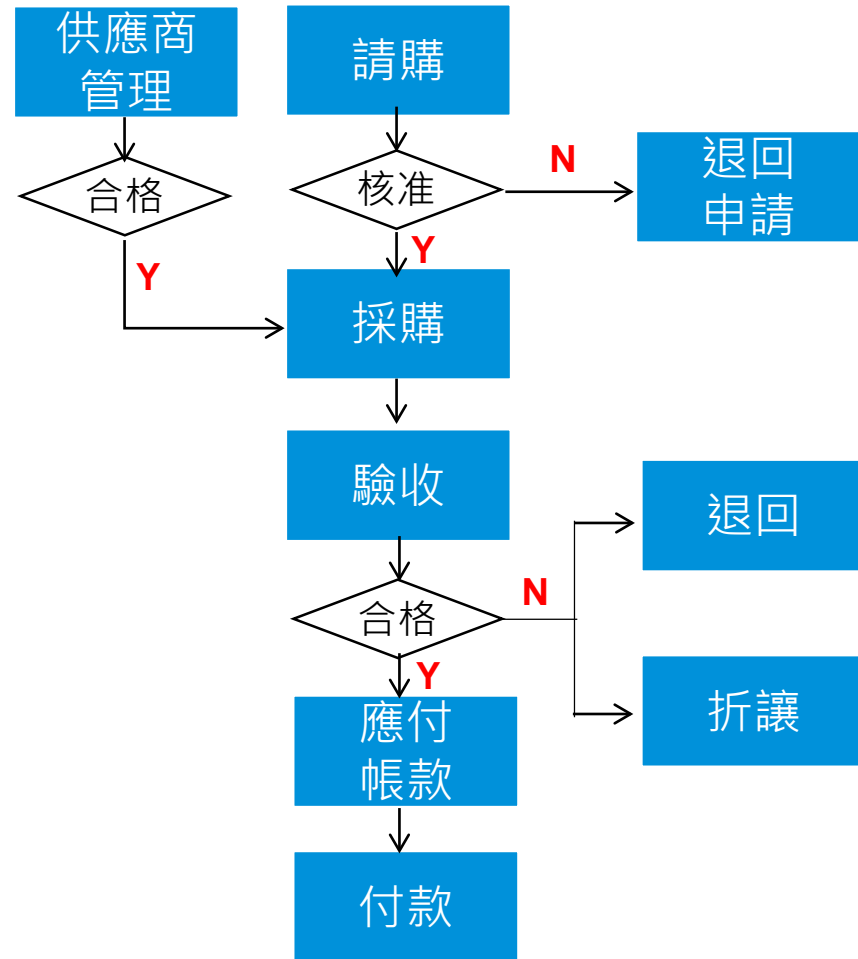
伍、依據及相關文件：  
1.校內及校外相關法規  
(1)元智大學財產管理辦法。  
(2)元智大學財物及勞務採購作業辦法。  
(3)元智大學科學技術研究發展採購作業要點。  
(4)政府採購法  
(5)科學技術研究發展採購監督管理辦法  
2.相關作業說明書與作業標準書  
無。

## 統一方式表達項目釋例：

- 權責單位：「教務單位」 v.s. 「教務處」
- 執行人員：「會計擔當」 v.s. 「會計人員」
- 管理階層：「採購權責主管」 v.s. 「總務處主任」
- 資訊系統：「ERP系統」 v.s. 「Oracle/SAP/..系統」
- 其他視需求需統一之項目

# 一、流程圖：以採購覆款循環為例

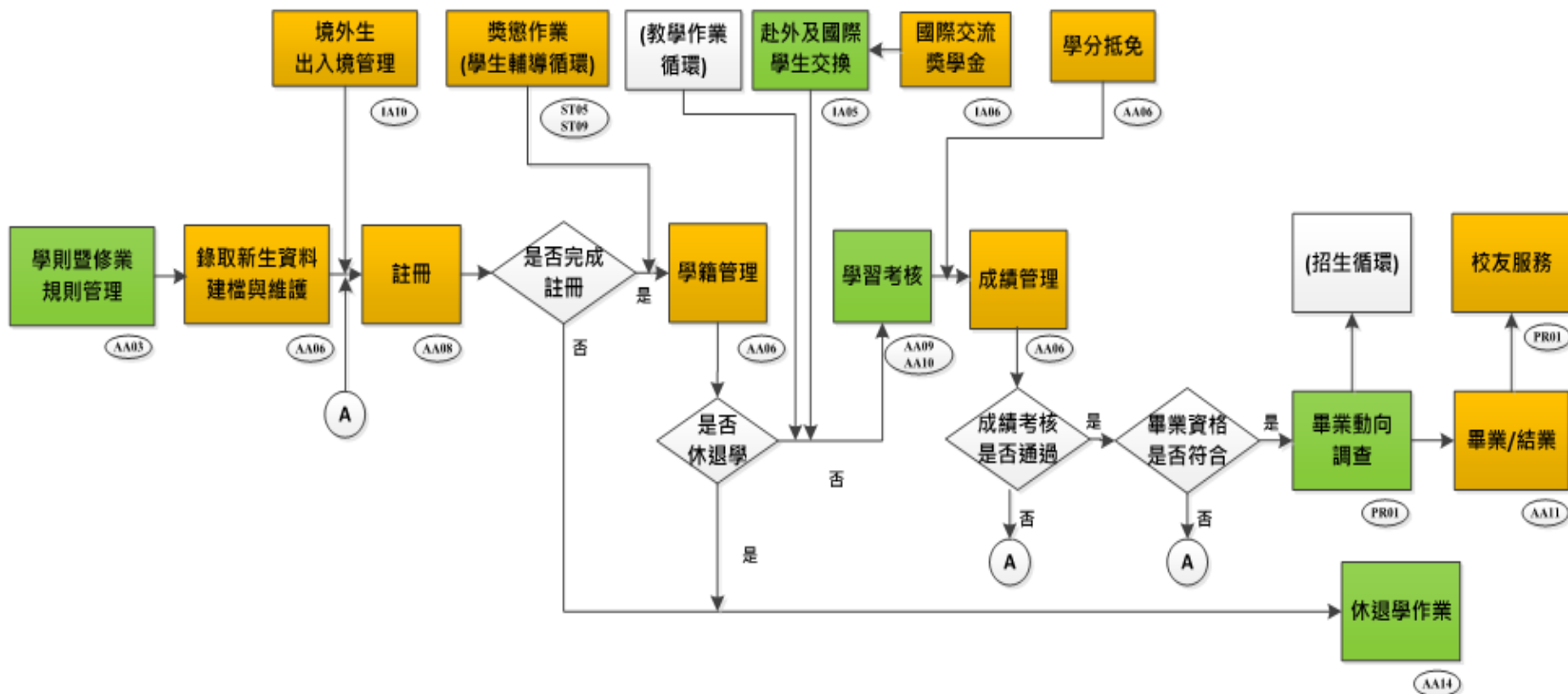
- 流程圖主要用來說明某一過程。這種過程既可以是企業進行採購的流程，也可以是完成一項任務必需的管理過程。
- 每個循環應至少繪製一份流程圖，它必須包含所有作業項目。
- 子作業可視需求繪製詳細作業流程圖



# 釋例：貴校入學至畢業循環流程圖

## 02 入學至畢業循環

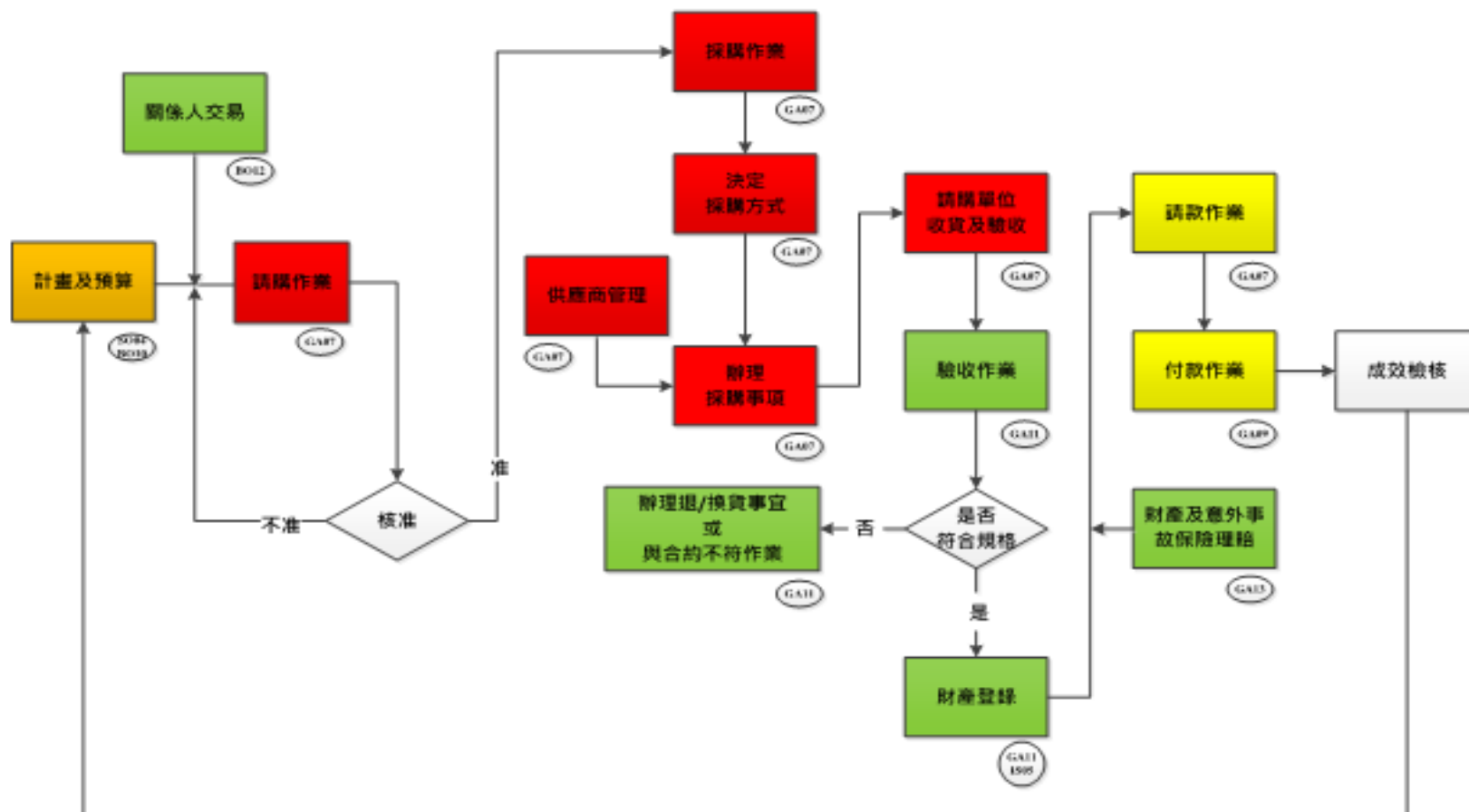
元智大學



# 釋例：貴校採購及付款循環流程圖

## 07 採購及付款循環 (財物及勞務)


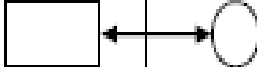

元智大學



# 釋例：貴校供應商評核作業管理流程圖

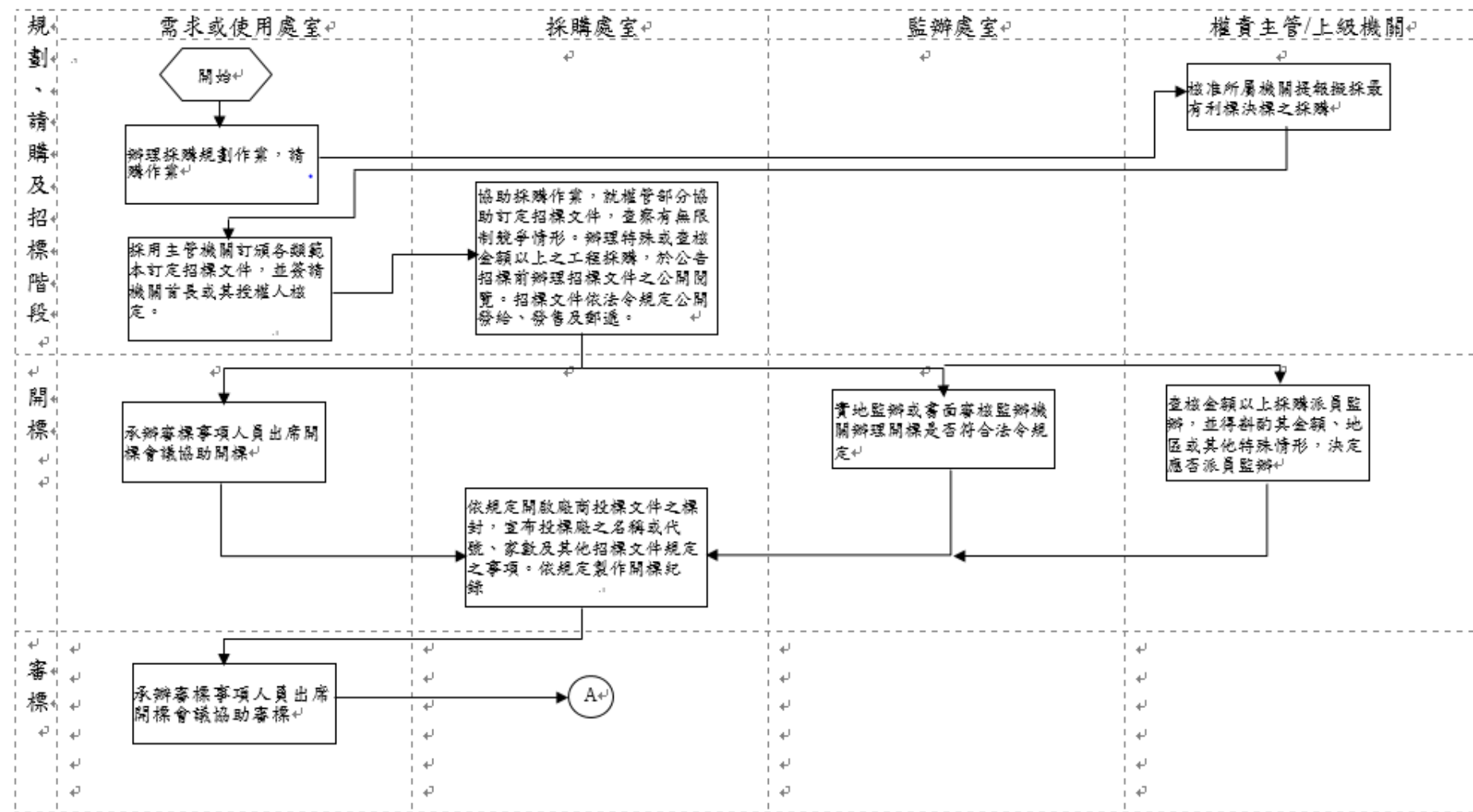
## 4. 供應商評核管理

### 4-1 作業流程圖

項次	作業項目	總務處 事務組	相關單位			
1	經常往來優良廠商名冊之建立(新增)					
2	經常往來優良廠商之監控					
3	經常往來優良廠商之評估					

□：主辦單位      ○：協辦單位

# 釋例：參考流程圖-公開招標作業



## 二、作業程序

- 作業程序應包括該作業之主要流程，包括資訊蒐集與彙整、提出申請、通知聯絡、文件覆核或憑證檢核、審查、授權、系統輸入控制、及文件保存(歸檔)等，但不以此為限。
- 作業程序如已經有其他更詳盡的“作業辦法”或“SOP”等進行規範，可以以“連結”的方式進行整合，但需指出該作業程序另需依據什麼規範/辦法/SOP辦理。整合後，等於標準只有一套，沒有重覆作業的困擾。
  - 例如：員工請假已訂有詳細之「請假管理辦法」，並依「核決權限表」簽准，則內控制度中相關的作業程序可寫成：員工請假應依「請假管理辦法」規定檢附憑證於請假系統提出申請，並依「核決權限表」經權責主管核准後辦理。
- 作業程序必須涵蓋所有控制重點所列事項。
- 管理辦法/SOP等內容不得違反內部控制之控制重點。





# 如何撰寫作業程序 - 4W1H原則

Who

- **誰**執行該項作業？

When

- 該項作業**何時**被執行？或**多久**執行一次？

Where

- 該項作業於哪一個**單位/處室**執行？

What

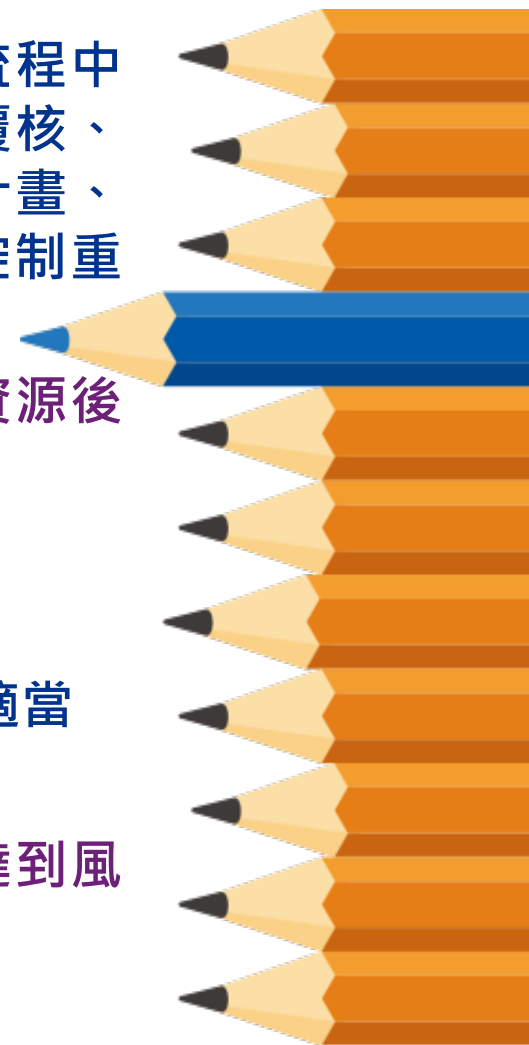
- 該項作業之執行須使用**什麼**資訊/文件？

How

- 該項作業**如何**被執行？

# 三、控制重點

- 為降低風險發生的機率或影響的程度，於作業流程中須設置相關控制活動例如核准、驗證、調節、覆核、定期盤點、記錄核對、職能分工、實體控制及計畫、預算或前期績效之分析...等以進行管理，此即控制重點。(不以前述釋例為限)
- 控制重點的調整應基於風險評估的結果與考量資源後進行。
- 如需增加控制重點，可採以下方式：
  - 1.評估流程風險的發生機率及影響
  - 2.分析流程風險相關的控制程序是否存在及是否適當
  - 3.視實際情況及資源，採取合適的控制方式
- 控制方式須確認實務上可行，否則無法落實及達到風險管理的效果
- 控制活動的導入，應經過相關單位充分溝通



# 四、依據資料

- 依據資料包括兩部份：

1. 依據資料：(包括但不限於下列各項)

- 法令、規則、辦法、作業手冊、SOP、說明書
- 企劃案、評估報告、設計圖、合約
- 其他

2. 使用表單：(包括但不限於下列各項)

- 各類申請單及報表，例如調節表、明細表、分析表、彙總表
- 傳票、發票、INVOICE、折讓證明單
- 處理報告
- 其他



# 釋例：內控文件(非 貴校版本)

- 控制重點應能降低風險發生機率或影響程度
- 作業程序應包含控制重點所要求之控制程序。

目標	風險因素	作業程序	控制重點	資料文件及表單
確保工程、財物、勞務各項採購依照政府採購法規定辦理。	RPP0X 開標過程未能有獨立監督處室監督開標作業，可能導致未依循程序之情事違反法令(如政府採購法)之規範。	採購處室檢附核准之招標文件依「 <b>採購監辦作業標準</b> 」規定通知監辦處室(即XX處及OO處)派員監辦，監辦處室於開標、比價、議價、決標作業可採派員實地監辦或書面審核監辦，並於紀錄上簽章，採書面審核監辦則另須於紀錄上載明「書面審核監辦」。	開標、議(比)價、決標應依規定派員監辦，會同於各紀錄簽章。	<b>採購監辦作業標準</b>

# 釋例：元智大學循環控制作業風險評估及內部控制點

NO	活動	可能發生的錯誤及舞弊	風險本質評估				內部控制點	作業程序	殘餘風險評估				負責單位
			可能性	影響程度	風險值	風險等級			可能性	影響程度	風險值	風險等級	
7-4	採購	1. 採購人員與供應商勾結。 2. 未經核准即予採購 3. 本校自有經費招標資訊不夠公開。	4	4	16	A	1. 校內預算案，是否依照元智大學財物及勞務採購作業辦法規定辦理。 2. 政府機關補助預算案，是否依照政府採購法及元智大學財物及勞務採購作業辦法規定辦理。 3. 科學技術研究發展計畫案，是否依照科學技術研究發展採購監督管理辦法及元智大學科學技術研究發展採購作業要點規定辦理。 4. 是否依已核准之採購單進行採購採購作業是否於完成簽核後始予訂購。 5. 採購案是否依規定辦理公告招標公告招標作業是否符合規定。 6. 學校應落實綠色採購（即採購時優先購買政府認可之環境保護標章產品、再生資源或以其一定比例以上為原料製成之再生產品）（私校行政運作考核項目）	G A- C P- 0 7 採 購 流 程 管 理 作 業 程 序	2	4	8	C	總務處

# 總結

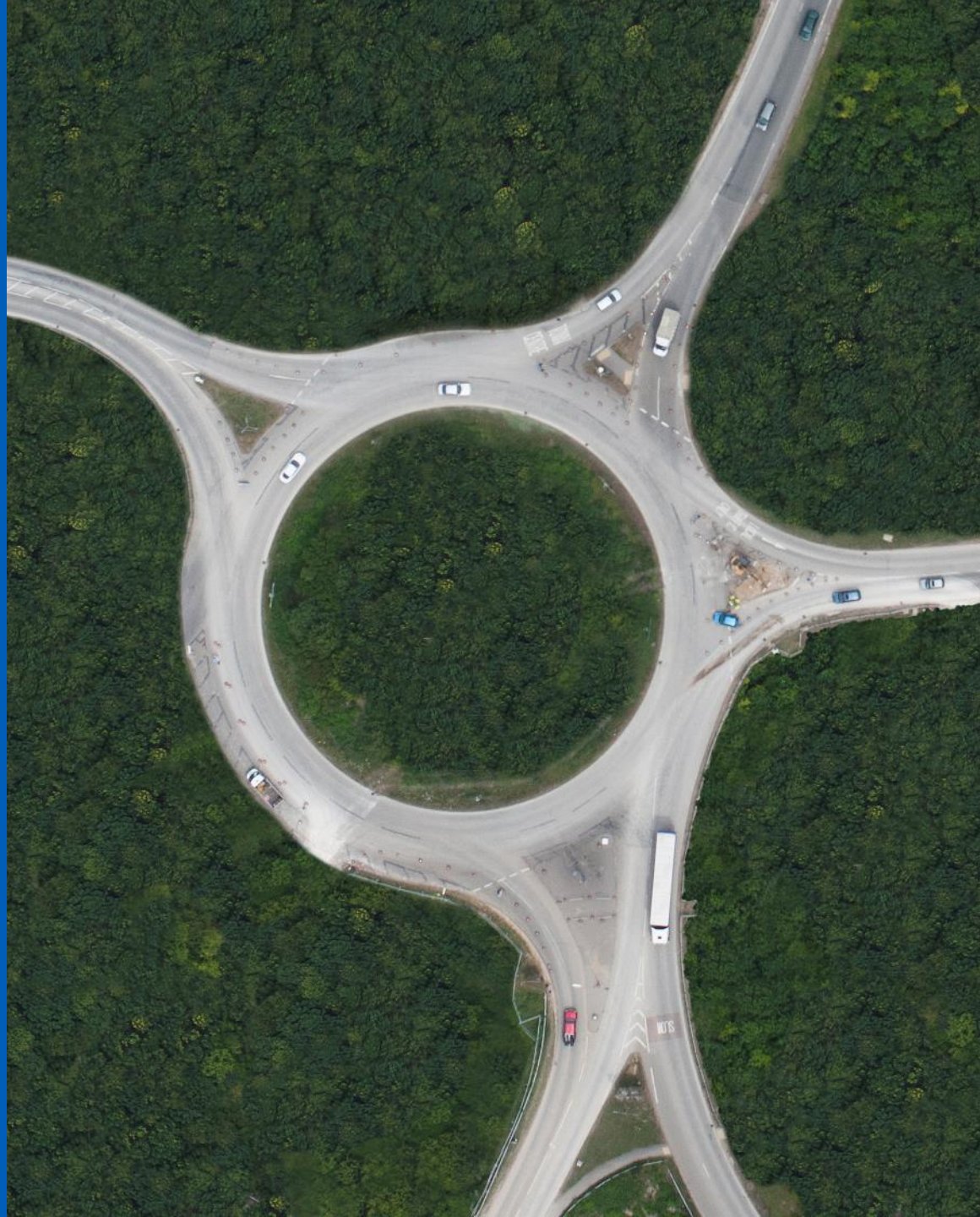


- 作業程序須承先啓後。
- 建置過程擬定之改善計畫事項須納入內控檔案。
- 每一項控制重點應有相對應之作業程序。
- 依據資料的名稱須與文件或表單實際名稱一致。
- 已有相關規範者，例如：SOP、各類作業流程及管理辦法等，於內控文件建議以索引之方式連結，勿將相關規範內容直接複製拷貝到內控檔案。





# 問題與交流





# Thank you

**[kpmg.com/tw](https://kpmg.com/tw)**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG , a Taiwan partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in Taiwan.

The KPMG name, logo are registered trademarks or trademarks of KPMG International.





# Contact

KPMG 台灣所 風險顧問 協理

黃宇歆 Michela Huang

T : +886 2 8101 6666 ext.13352

E : [michela.huang@kpmg.com.tw](mailto:michela.huang@kpmg.com.tw)

KPMG

68F, Taipei 101 Tower, No. 7, Sec. 5, Xinyi Road,  
Taipei, 11049, Taiwan, R.O.C.