明新科技大學
內控作業
(風險評鑑)

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association

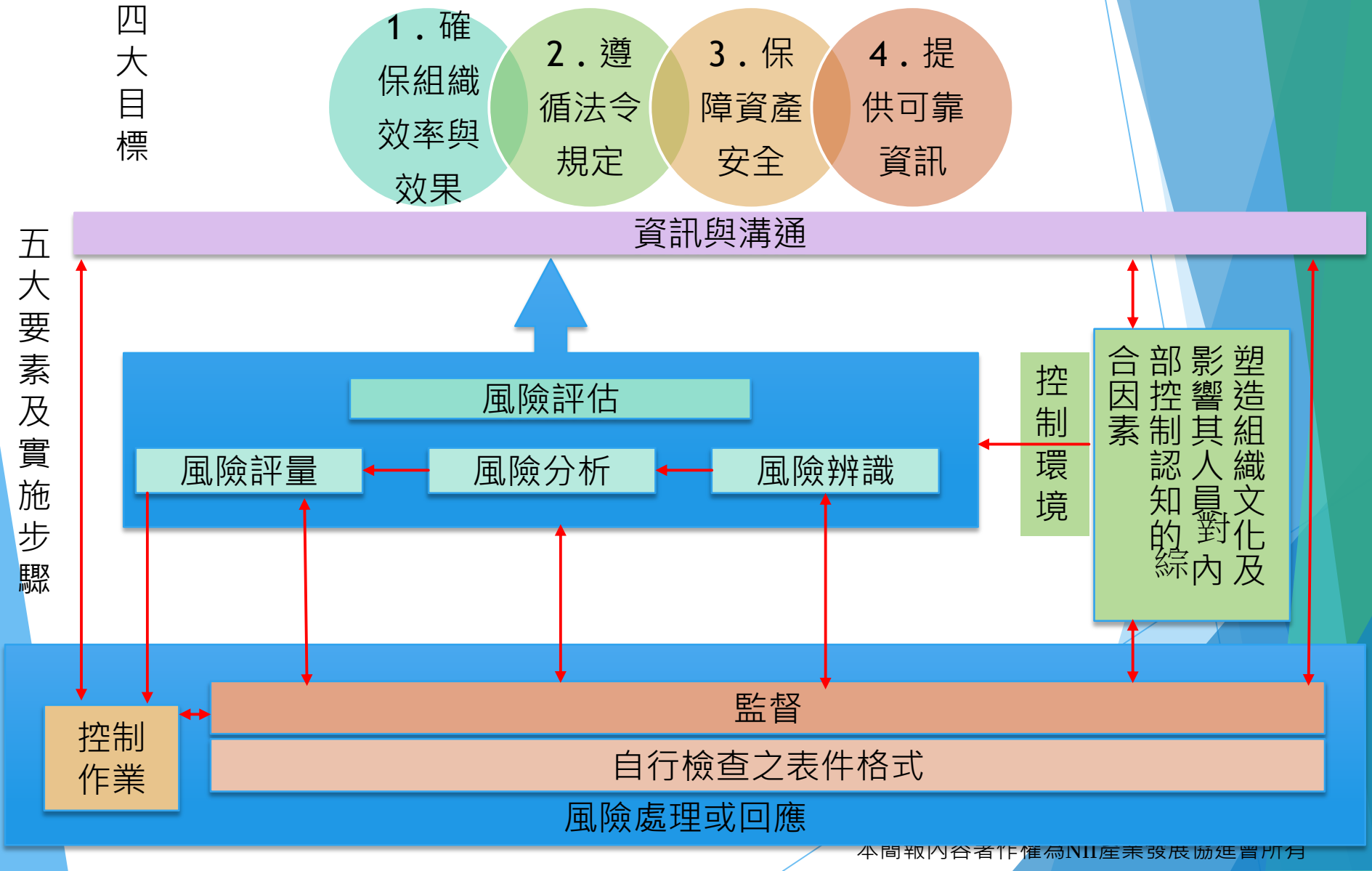
NII 產業發展協進會
☏ (02) 2508-2353
✉台北市松江路 317 號 7 樓

簡報大綱

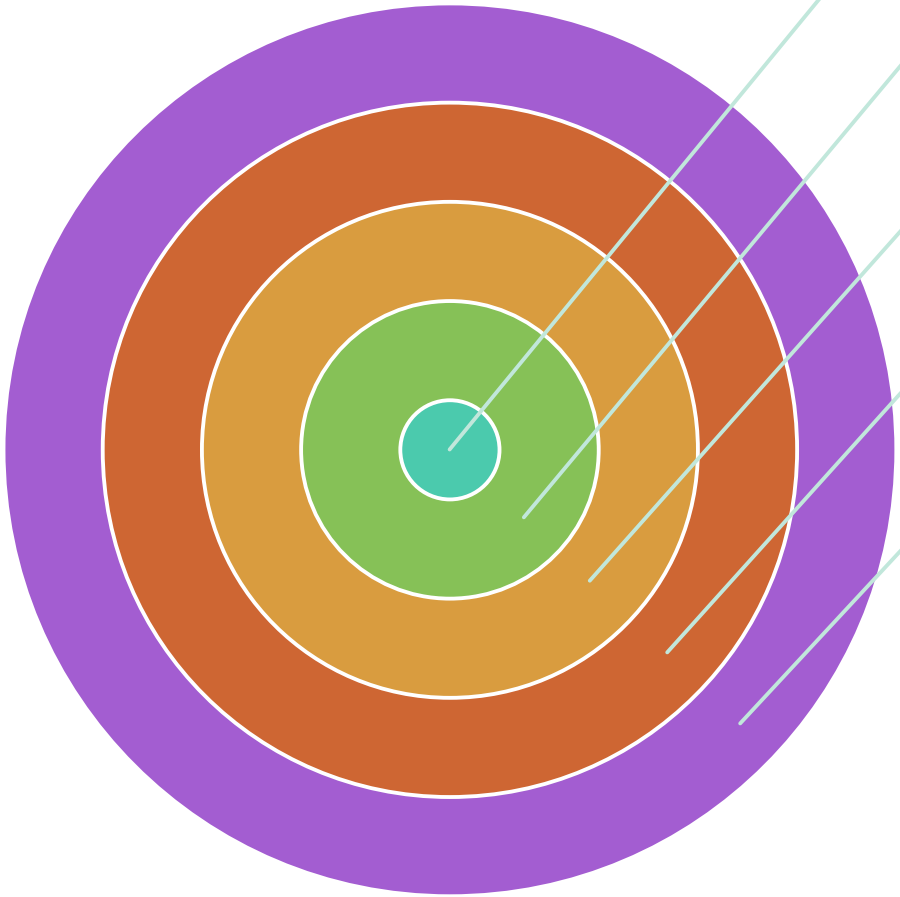
1. 內部控制基本概念
2. 內部控制之規劃
3. 內部控制之風險評鑑
4. 內部控制之問題與討論

內部控制基本概念

內部控制的觀念架構



內部控制的定義



整合組織內部各種控管及評核措施之管理過程

由組織內全體成員共同參與

避免錯誤或非常態性事件

辨認問題所在

確保改善活動的落實執行。

內部控制之目標： CARES

Compliance-對政策、計畫、程序、法令、規章及契約約 定事項之遵循(遵循法令規定)

Safeguard-資產(包括人力資產)的保障(保障資產安全)

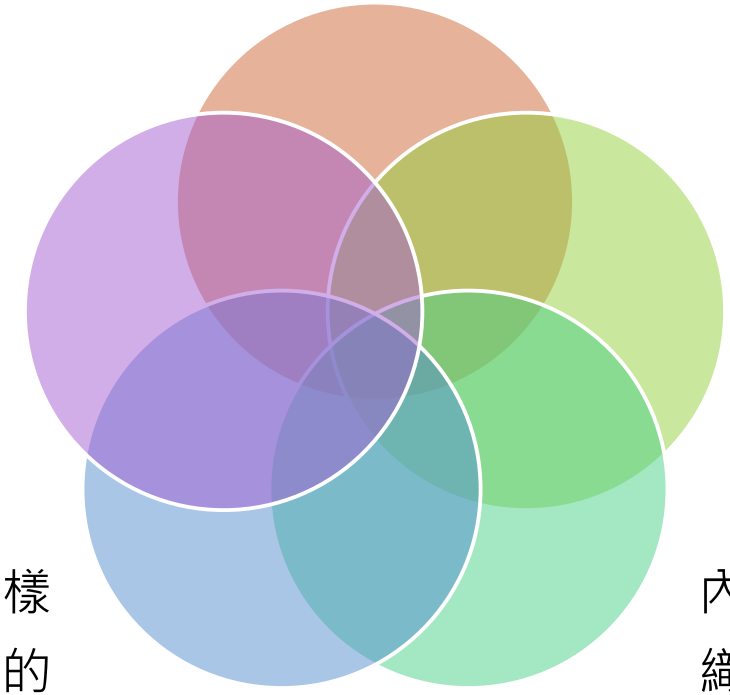
Accomplishment-成功達致整體目標(達成組織目標)

Efficiency and **E**ffectiveness-最經濟且有效率的資源使用 (確保效率及效果)

Relevance & **R**eliability-資訊的可靠性、正確性與及時性 (提供可靠資訊)

內部控制之基本精神

管理階層必須建構及
維持組織的控制環境



沒有任何系統是完
全有效的

內控架構應能提供
財務報導正確性的
合理保證

內控不單單是官樣
文章或繁瑣程序的
制定

內控應該內化於組
織運作、文件紀錄
及管理系統中

內部控制之組成要素

控制環境	風險評估	控制作業	資訊與溝通	監督
• 為內部控制所有組成要素的基礎	• 辨識、分析顯著相關的風險，以順利達成目標	• 合理確保組織目標得以達成，所需採取的機制	• 協助所有人員清楚瞭解相關資訊，以完成工作任務並達成組織目標	• 評估內控品質並促進持續改善

有效內部控制17項原則

要素	原則
控制環境 (Control Environment)	1.對誠正與道德價值表明承諾
	2.執行監督之責
	3.建立結構、職權及責任
	4.展現留住適任人才之承諾
	5.實施課責
風險評估 (Risk Assessment)	6.具體指明適合攸關目標
	7.辨識及分析風險
	8.評估舞弊風險
	9.辨識及分析重大改變
控制作業 (Control Activies)	10.選擇及建立控制活動
	11.選擇並發展科技之一般控制
	12.制定相關政策及程序
資訊與溝通 (Information &. Communication)	13.使用攸關資訊
	14.內部溝通
	15.外部溝通
監督活動 (Monitoring Activities)	16.進行持續性及/或個別評估
	17.評估及溝通缺失

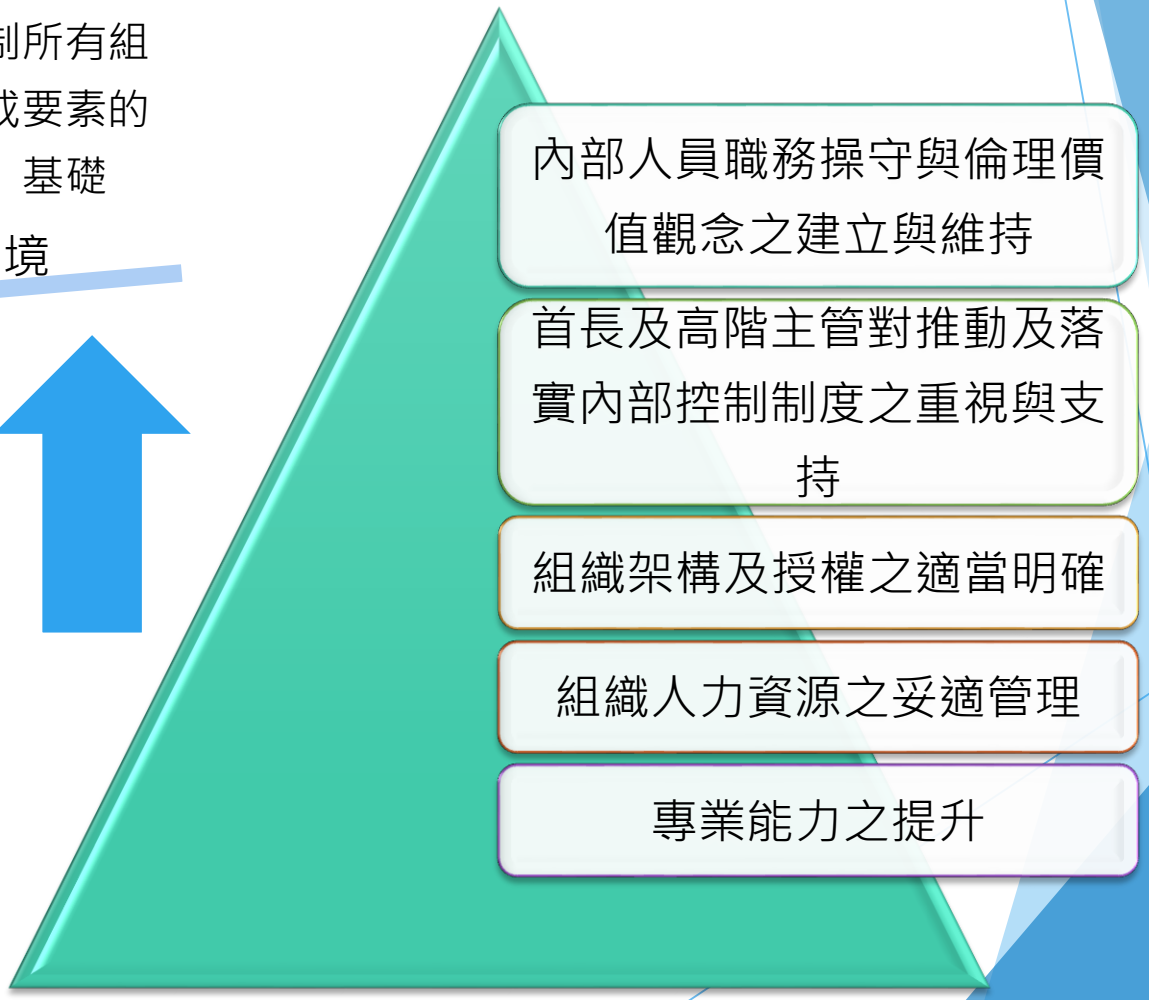
資料來源： http://www.wrasb.gov.tw/%E8%A1%8C%E6%94%BF%E9%80%8F%E6%98%8E/2-6-2-1-2.html

內部控制之組成要素(控制環境內涵)

為內部控制所有組成要素的基礎

控制環境

塑造組織文化及影響其人員對內部控制認知的綜合因素



控制環境

任何企業的核心，包括人及其所處的環境。
人的營運是在某一個環境中，人的屬性(操守、價值觀、能力)是推動企業的引擎，也是其他一切之所繫。
控制環境塑造企業文化，影響企業員工的控制意識，提供紀律與架構，是其他組成要素的基礎，包括企業人員的操守、價值觀及能力，管理階層的管理哲學與經營風格，管理階層指派權責、組織及培養員工的方式及董事會所提供的關注及指引。
控制環境是塑造組織文化、影響員工執行控制制度成效的綜合因素。員工的操守、價值觀及能力、經營者的經營風格及管理哲學、董事會及監察人的關注及指導都是影響控制環境的因素，這些因素共同作用而形成了公司內部的控制環境。控制環境的良窳會影響企業經營者的其他內部控制活動，所以也是其他四大要素的基礎。

原則	範例
對誠正與道德價值表明承諾	所有員工之操守(含價值觀)及能力
執行監督之責	董事會、行政主管之管理哲學與經營風格
建立結構、職權及責任	組織部門劃分與分工
展現留住適任人才之承諾	聘僱與訓練員工
實施課責	指派權責之方式

內部控制之組成要素(風險評估內涵)

- 辨認攸關之策略風險，分析該風險之 影響程度與發生可能性，評量對風險容忍度之過程。
- 可協助及時修正及執行必要之控制作業

風險辨識

- 辨識影響目標達成之風險因素，考量可能引 發組織整體層級目標、作業層級目標無法達 成之風險因素，必要配套措施及可辨認之替代方案。

風險分析

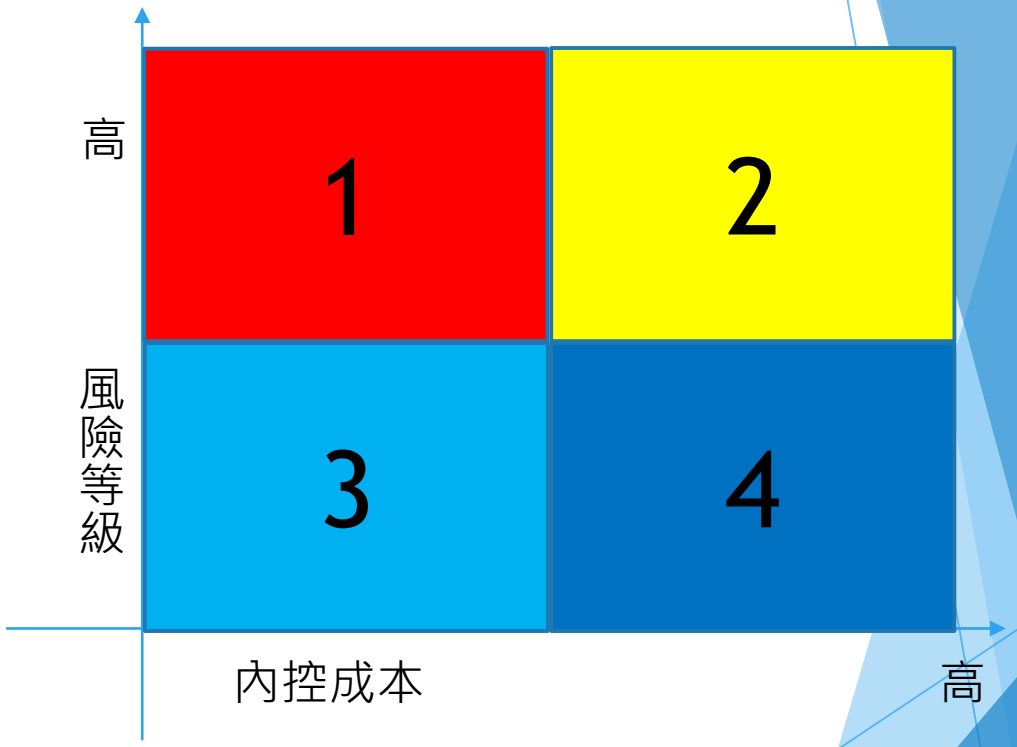
- 分析風險因素發生之機率，及其對組織之影 響程度，綜合兩者據以評估風險等級。

風險評量

- 風險之可容忍度，考量風險等級及內控成本 以決定優先處理之風險因素或加強控制之程 序。

內部控制之組成要素(風險評估內涵)

1. 高風險、低內控成本
2. 高風險、高內控成本
3. 低風險、低內控成本
4. 低風險、高內控成本



風險評估

企業須了解所面臨的風險並加以處理。
企業必須訂定與銷售、生產、行銷、財務等作業相結合的目標，才能堅實運作；且須設立可辨認、分析和管理相關風險的機制。任何組織須留意並處理它所面臨的風險，以作為該風險應如何管理之依據。
所謂風險係指讓目標無法達成之原因，目標因承接業務而達成，每個企業均會面對來自企業內外部的多種風險，管理階層應先決定企業願意承擔風險之水準，再進行風險管理，將風險控制在水準之內。

原則	作法
具體指明適合攸關目標	風險評估，係指公司辨認影響其目標達不成之因素(即風險因子)、評估風險因子之嚴重程度(magnitude)及發生可能性(likelihood)之過程(項目、金額、機率)。
辨識及分析風險	EX：招生缺額、人才流失，這些因素的嚴重程度及發生機率。
評估舞弊風險	
辨識及分析重大改變	

內部控制之組成要素(控制作業內涵)

- 為確保達成組織目標、降低風險、落 實策略方案，所設立之完善控制架構及各層級之作業程序。
- 控制作業內化於所有作業之SOP 。

整體層級控制

- 對各單位多項業務有較廣泛影響之控管措施或控制規範。

作業層級控制

- 各單位依個別業務職掌所確立之作業層級目標，選定業務項目，設計控制重點；並配合業務調整及作業變動，適時檢討修訂。

控制作業

企業必須訂定控制之政策及程序並予執行，以幫助管理階層為保證能達成企業目標，以落實辨認風險及處理風險所必須採取之行動。
針對評估出來的風險，訂定必要指令要求員工執行，例如以營業活動循環，幫助管理階層確保員工有效執行營運活動的政策及程序。
控制活動出現在組織中的各個層級，會以不同的面貌呈現，諸如上級的批准、認可、授權、調節、覆核、營運表現的事後檢討、資產資訊的保護以及責任區隔等。這些方法或是企業內部的各種營運流程的建立都是控制活動的一環

原則	作法
選擇及建立控制活動	幫助主管確保其政策規章制度已被執行的行動。
選擇並發展科技之一般控制	作業控制本身不是營運活動，而是確保營運活動會被落實執行的活動。 包含：事前的核准或授權、事後的驗證或覆核、調節、在定期盤點後再與記錄相核對、職能分工、接觸控制(亦稱存取控制)、拿實際的結果與計畫、預算或前期績效相比較等。
制定相關政策及程序	

內部控制之組成要素(資訊與溝通內涵)

- 適時搜集並傳遞資訊給相關人員，使其履行其職責或瞭解責任履行情況。
- 可以紙本、電子或其他方式對內部控制制度進行有效管理與傳達，以支援其他構成要素 。

資訊

- 與組織有關之財務或非財務資訊，以供決策及監督之用，可由內部產生或自外部取得。

溝通

- 內部溝通-告知組織全體人員在內部控制所扮演之角色與責任，並建立資訊交流之管道，以使組織內部資訊能充分傳達。
- 外部溝通-依法對外部機關(主管機關及社會大眾)公開提供資訊，並於外界提出意見時及時處理與追蹤。

資訊與溝通

圍繞在控制活動周邊的資訊與溝通系統，使相關人士能取得在執行、管理和控制企業營運時所需的資訊並交換資訊。
所謂相關人士包括員工、也包括外界個體如供應商、消費者，員工能向上溝通也能和外界溝通。
資訊與溝通則是貫穿整個內部控制制度的骨幹，可以說是五個要素裡面最重要的一個。
資訊與溝通必須充份且適當，內部控制才有良好的成效，如果資訊與溝通不充足，不適當，那麼就會產生決策錯誤、弊案防不勝防的危機。

原則	作法
使用攸關資訊	資訊指資訊的產生，溝通指資訊的傳遞。資訊因企業統辨認、衡量、處理及報導而產生；惟與學校攸關，作決策時須用之資訊，亦包括與(如競爭對手)有關之他校資訊。這些資訊，可與學校的營運、財務報導或遵循法令等目標有關，可為財務資訊或非財務資訊，可供規劃、監督等所需。
內部溝通	溝通，則指把前者資訊適時告知資訊需求者，或讓其適時取得資訊。至於資訊需求者，包括學校內部的教職員工，以及外部的各種利害關係人(stakeholder)。
外部溝通	

內部控制之組成要素(監督內涵)

- 評估內控制度品質及執行成效之過程，藉以瞭解控制環境是否良好，風險評估是否及時，控制作業是否適當，資訊及溝通是否確實。
- 可適時修正、改善內部控制制度。

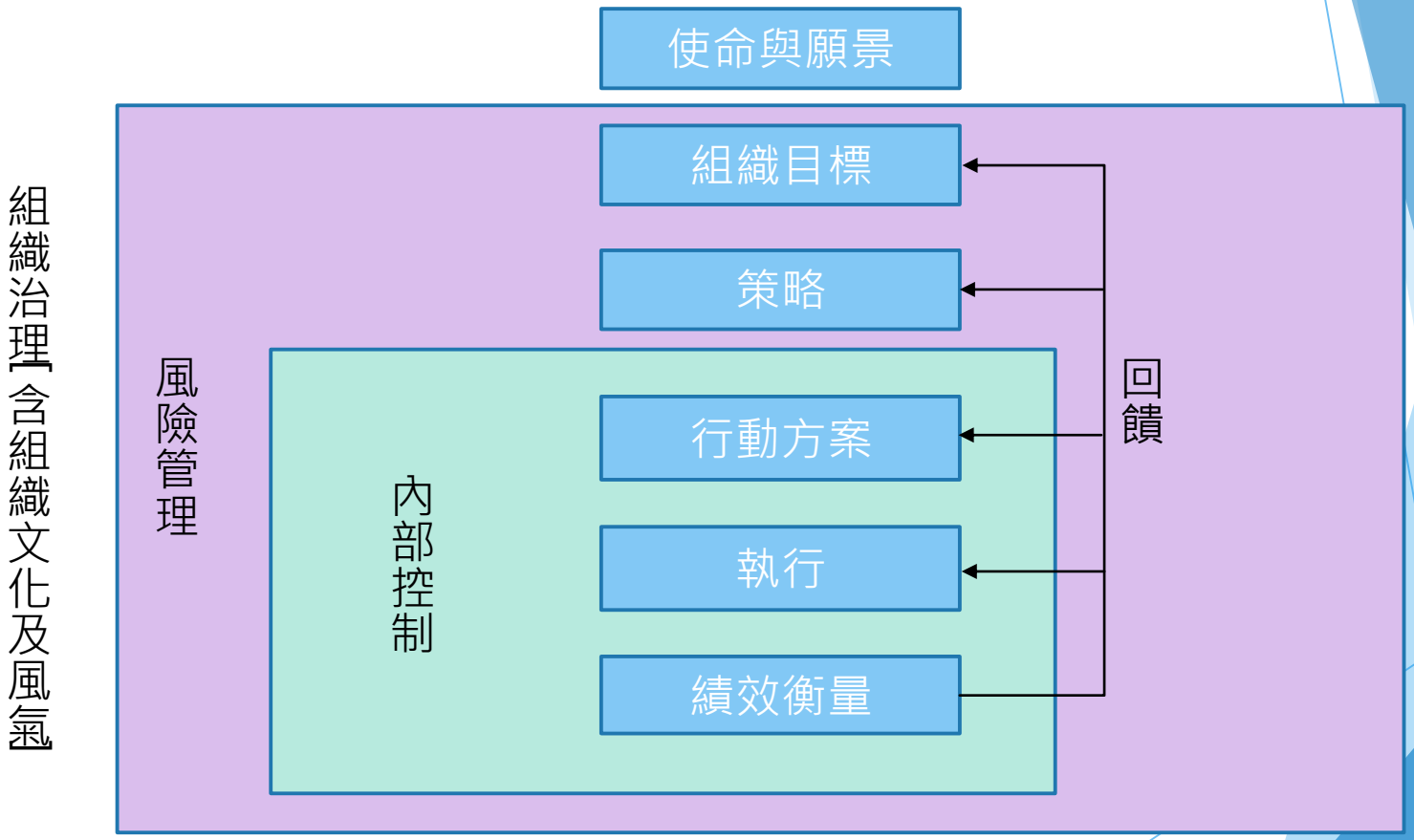
例行監督	自我評估	稽核評估
• 由各項業務承辦單位主管人員執行督導作業。	• 由內部各單位自行檢視，就其內部控制制度之設計與執行之有效性加以評估，並作成紀錄。	• 由稽核人員提出有效性及健全性之評估。

監督活動

整個內部控制的過程須被監督，必要時加以修正，如此才能隨情況之改變而做出動態反應。
隨時間經過而評估營運及控制活動品質的過程，目的在確保營運及內部控制能持續有效運作。
持續監督的程序應溶入企業日常的作業活動中；
個別評估由內部稽核人員進行，檢視內部控制制度是否有效。

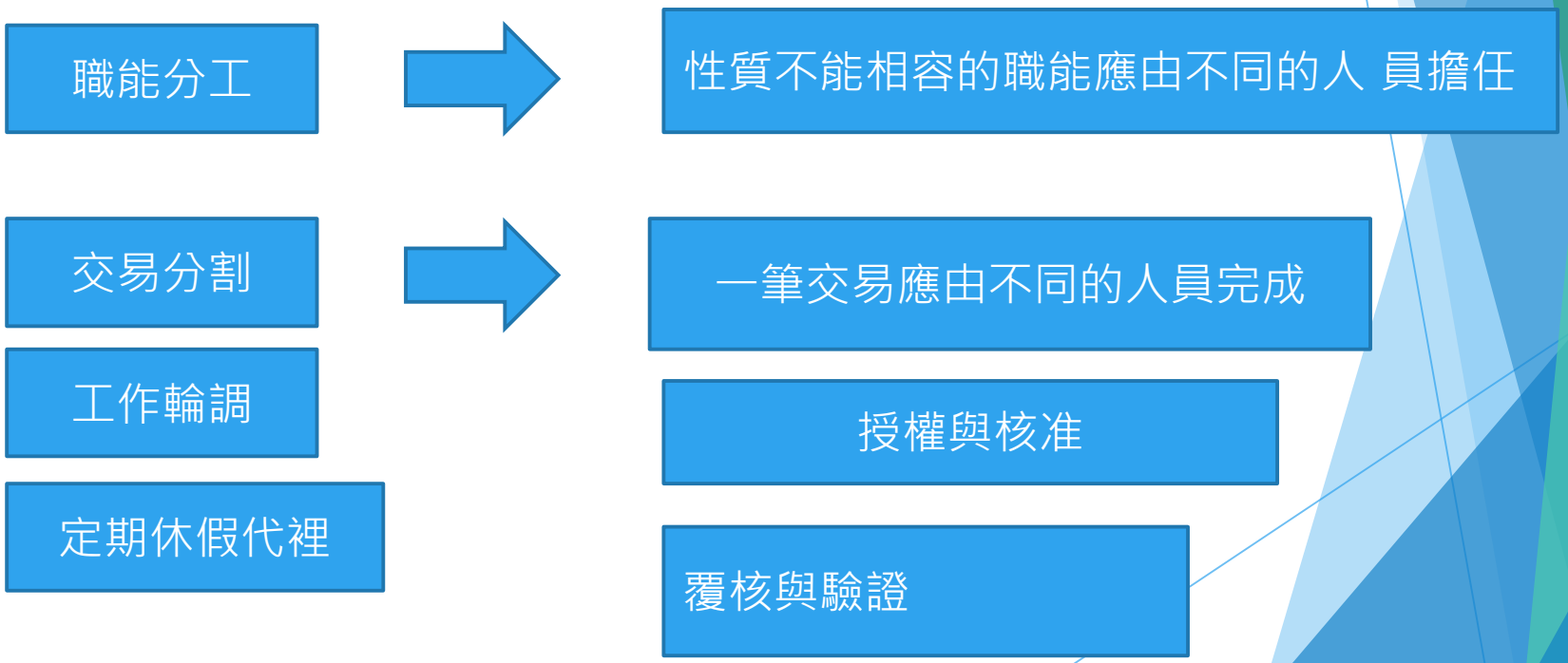
原則	作法
進行持續性及／或個別評估	持續性監督：係指營運過程中之例行監督，非由負責營運活動的人自己進行不可(承辦人 、主管)，因此強調其持續不斷監督 。
評估及溝通缺失	個別評估：後者的評估係由內部稽核人員、監察人等人士進行，由於這些人不是被評估業務的主要負責人，他(她)們評估完即離開，不可能持續不斷，故強調其中斷而稱為個別或間斷評估。

內部控制之運作機制



內部控制制度之內涵

- 1. 內部控制存在於各項作業之SOP中，並非獨立存在於 作業之外的機制。
  2. 常用的內部控制設計:



內部稽核的功能

1. 檢查及覆核內部控制制度之缺失及衡量績效， 俾適時提供改進建議。
2. 檢查財務活動的正確性及忠實性，包括舞弊及 不法行為的揭發。
3. 透過系統化的方法，對風險管理、控制及治理 加以評估並建議改善，以增加價值並改善經營 。

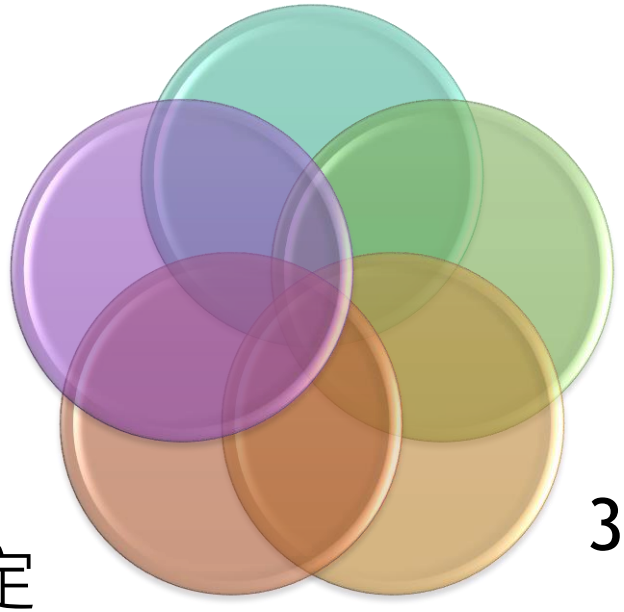
內部控制缺失檢討及改進

1. 國際最高審計組織(INTOSAI)發布之政府審計 準則ISSAI 1265號:「向治理單位及管理階層 溝通內部控制缺失」列舉重大缺失指標為:
   1) 無效的控制環境;
   2) 機關未進行風險評估;
   3) 機關風險評估過程是無效的;
   4) 對已辨識之重大風險所採取的風險回應是無效的;
   5) 重大缺失無法由機關透過內部控制加以預防、偵測及改正。
2. 內控重大缺失之認定
   1) 以內控組成要素為基礎
   2) 以結果論為基礎:
      a. 有礙組織目標達成;
      b. 營運效能不彰;
      c. 損害組織聲譽及形象;
      d. 損及公眾(病患)權益;
      e. 明顯違反法律規定;
      f. 貪瀆公款及侵占財物;
      g. 濫用職權等。

內部控制之規劃

（一）建立健全的組織結構與職掌劃分

1.組織系統圖



2.職掌劃分表

3.工作說明書

4.授權規定

5.獨立責任

（二）設計合理與適切的標準

（三）建立健全的會計制度

1.適當的文件

2.會計科目表

3.會計政策及程序手冊

4.財務預測

5.成本會計制度

（四）重視人事管理制度

面談

休假等

調查

工作輪調

訓練

保證

考核

（五）設計有效的制度及管理辦法，並隨時注意或定期檢討修正

（六）其他

1. 加強資產安全及保險措施
2. 建立內部稽核制度
3. 利用電腦協助處理資料，防止人為錯誤與弊端
4. 聘請外界會計師及專家檢討改進各種管理辦法
5. 獲取高階主管之重視與支持

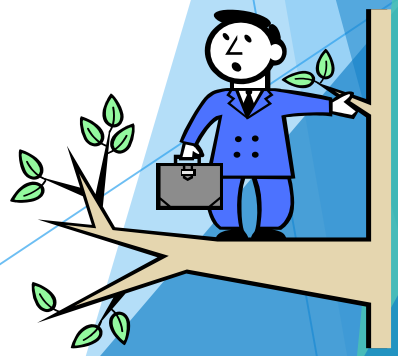
內部控制之風險評鑑

何謂風險

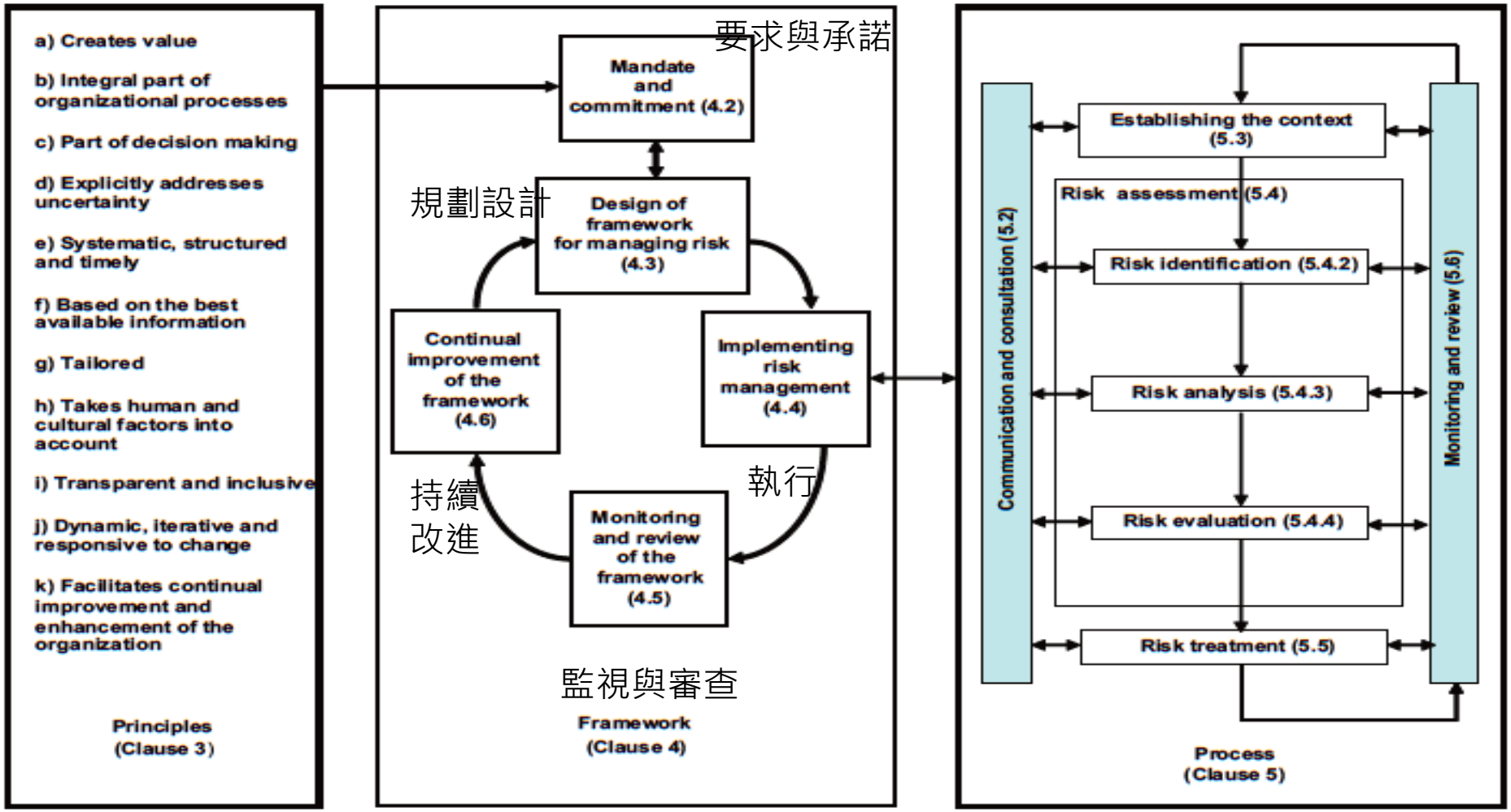
- 風險是具有破壞某種事物發生的**可能性**
- 風險評鑑程序是

識別風險 → 分析風險 → 評估風險

- 風險管理則是藉由風險評鑑過程中找出風險，並採用風險處理的方法將風險減小到一個**可以接受的程度**



風險管理原則、架構與過程關係圖



參考：ISO31000:2009

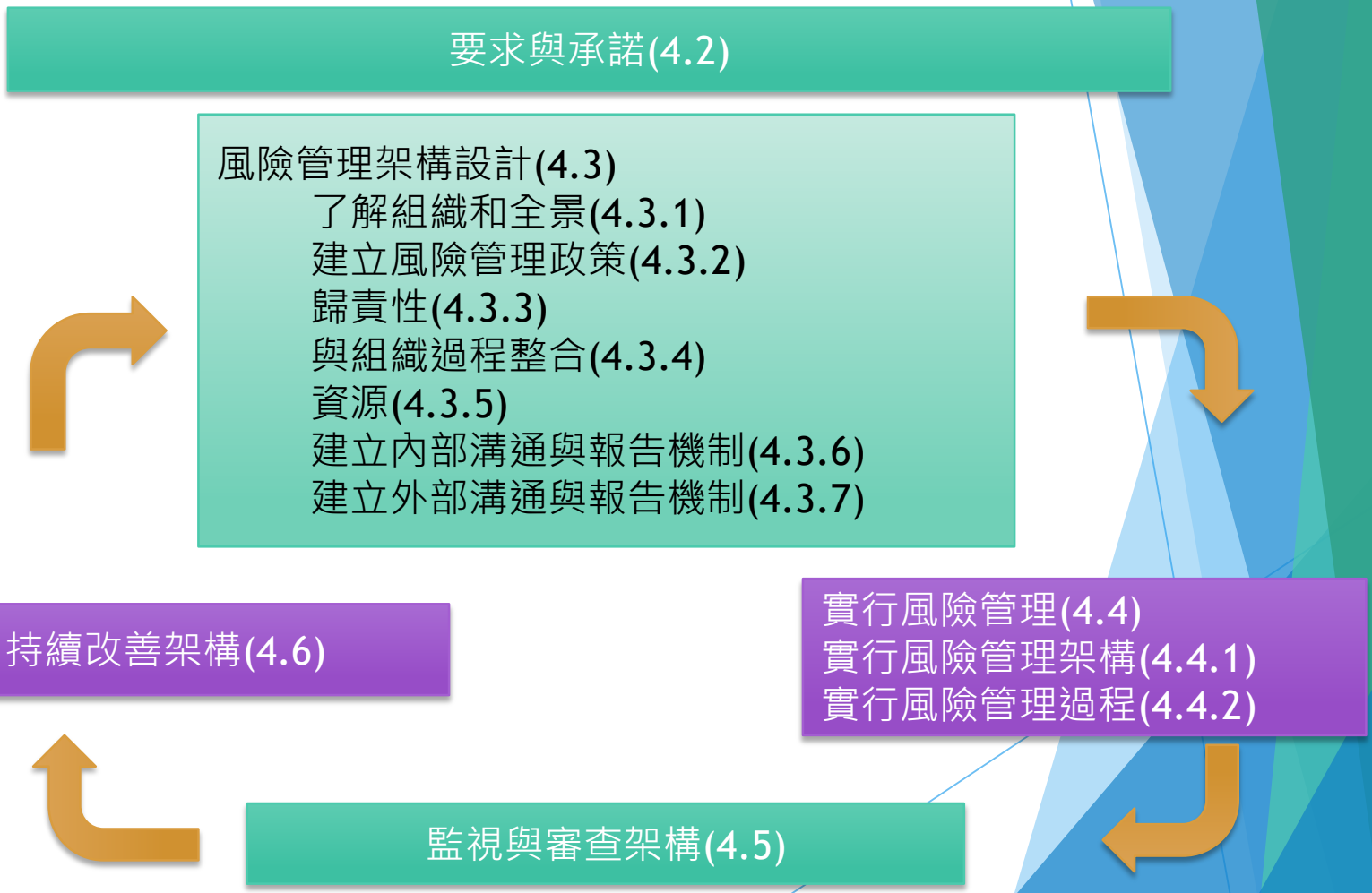
風險管理原則

為使風險管理有效，組織應該在所有層次上遵循如下原則。

a) 風險管理創造及保護價值。
b) 風險管理是組織所有過程整體性的一部分。
c) 風險管理是決策的一部分。
d) 風險管理清晰的闡明不確定性。
e) 風險管理是系統化的、結構化的及適時的。
f) 風險管理基於最可利用的資訊。
g) 風險管理是訂製的。
h) 風險管理考慮人員及文化因素。
i) 風險管理是透明的、包容的。
j) 風險管理是動態的、互動的及易感應的對變動。
k) 風險管理促進組織的持續改進。

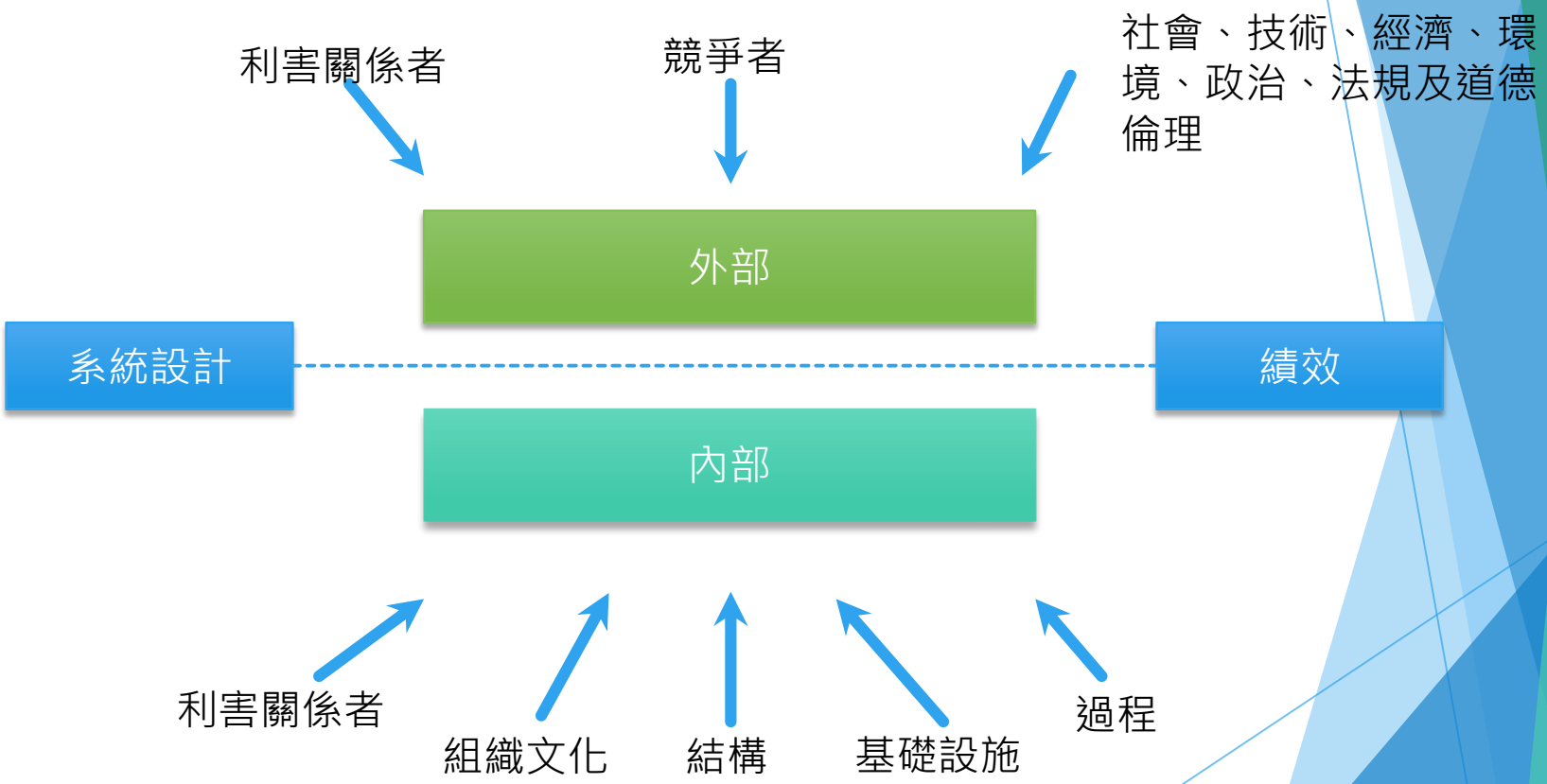
參考：ISO31000:2009

風險管理架構



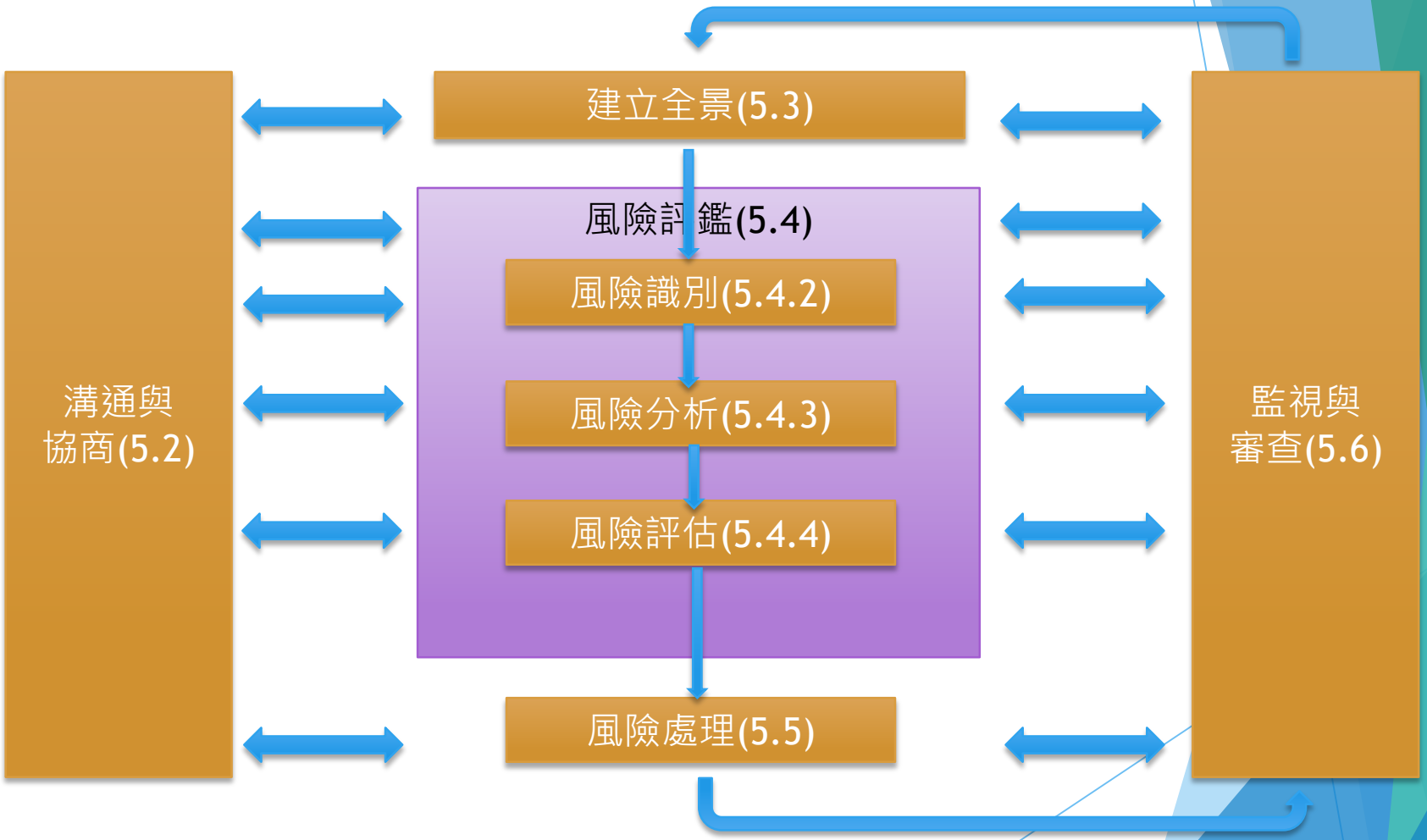
參考：ISO31000:2009

組織內外部情境



參考：ISO31000:2009

風險管理過程



參考：ISO31000:2009

風險識別

- 目的
  - 為依據可能產生、增強、防止、降低、加速或延遲目標達成的事件，產生一包羅廣泛的風險清單。
  - 鑑別出不利用某一機會的相關風險有其重要性，包羅廣泛的鑑別係重要的。
  - 因未在此階段鑑別出的風險將不涵蓋在進一步的分析內。

風險識別

- 識別須包括不論其緣由是否在組織控管下的風險，縱使其緣由或結果(後果)可能不顯著。
- 風險識別須包括
  - 特定的結果(後果)推擠效應，包含串聯與累積效應之檢查。
  - 亦須考量廣範圍的結果(後果)，縱使風險緣由或結果(後果)可能不顯著。
  - 以及鑑別可能發生的前後環節，必須考慮到可能的緣由與顯示可能產生何種結果(後果)的情境，
  - 所有重要的緣由與結果(後果)均須予以考量。
- 組織須應用適合其目標與能力及所面臨的風險之風險鑑別工具與技術。相關與更新的資訊在識別風險時係重要的，此須在可能時包括適當的背景資訊。須有具備適宜知識的人員參與風險識別。

風險分析

- 風險分析涉及對瞭解風險之發展。風險分析提供風險評估之輸入並決定風險是否需予以處理，以及決定最適宜的風險處理策略與方法。
- 風險分析亦可提供形成決策之輸入，該決策必須作出選擇而選項包含不同類型與等級的風險。
- 風險分析涉及考量風險之原因與緣由、其正面與負面結果(後果)，及該等結果確實發生的可能性。
- 會影響結果的因素及可能性須予以識別。
- 風險係藉由決定結果(後果)與其可能性，以及此風險之其他屬性分析之。
- 一事件可具有多重結果(後果)且可影響多個目標，現有控管與其有效性及效率亦須予以考量。

風險分析

- 結果(後果)與可能性的表達方式，與兩者綜合以決定風險等級之方式，須反映風險之類型、備妥的資訊以及風險評鑑之輸出的使用目的，此須與風險準則一致。考量不同風險與其緣由之相互依賴性亦是重要的。
- 決定風險等級的可信性及其對於先決條件與假設事項的敏感性須在分析中予以考量，同時須與決策者及在適當時與其他事件相關者進行有效的溝通。各項因素諸如專家間的意見分岐、不確定性、可取用性、品質、數量及資訊之進行中的關聯性或模式化之限制等，須予以說明且可予以強調。

風險分析

- 風險分析可依不同的詳細程度予以進行，端視此風險、分析之目的以及可取得的資訊、資料及資源而定。分析可為定性、半定量或定量方式，或為此等之組合，視狀況而定。
- 結果(後果)與其可能性可透過模式化一事件或一組事件之結果，或由實驗研究或可取得數據外插以決定之。結果(後果)可以有形或無形的影響之方式表示。在某些案例中，需有一個以上的數值或解說符號來詳述不同時間、地點、群體或情況的結果(後果)與其可能性。

風險評估

- 風險評估之目的係依據風險分析之結果，協助形成有關何項風險需處理，以及處理實施的優先順序之決策。
- 風險評估涉及將分析過程中所發現的風險等級與考量前後環節時所建立的風險準則相比較。可依據此項比較，考慮風險處理之需求。
- 決策須考量風險更廣的前後環節，並包括考量由此風險受益的組織除外之團體所承受的風險裕度。須依據法令規章及其他要求作決策。
- 在某些狀況下，風險評估可導致進行進一步分析之決策。風險評估亦可導致除了維持現有的控管外，不對風險作任何處理之決策。此決策會受到組織面對風險的態度與已制定的風險準則之影響。

風險評估程序

- 應根據所界定之個人資料，及其相關業務流程，分析可能產生之風險。並根據風險之高低，訂定不同層級之管控措施，且確認受管控之風險在可接受範圍內。

定義風險準則

- 組織應定義要用於評估風險的重要性的準則。該準則應該反映組織的價值、目標和資源。風險準則應與組織的風險管理政策相一致（見4.3.2），在任何風險管理程序的開端定義，並不斷檢討。
- 當定義風險準則，需要考慮的因素應包括以下內容：
  - 原因的本質和類型和可能發生的結果以及將如何進行測量
  - 可能性如何定義
  - 可能性和/或結果的時間表
  - 風險水準如何決定
  - 利害相關者的意見
  - 風險可接受或可容忍的水準
  - 應考慮到是否為多風險的組合，如果是，哪些組合應予以考慮

參考：ISO31000:2009

風險處理過程

- 風險處理涉及一個循環的過程：
  - 評估風險處理
  - 決定剩餘風險水準是否是可以容忍
  - 如果無法容忍，產生新的風險處理
  - 評估處理的成效。
- 風險處理方案並不一定是相互排斥的，或適用於所有情況。該選項可以包括以下內容：
  - a) 避免風險，不繼續執行或從事相關風險活動
  - b) 尋求新機會
  - c) 去除的危險來源
  - d) 變更可能性
  - e) 變更情況
  - f) 與另一方或多方 (包括合約和風險融資) 分擔風險
  - g) 藉由選擇或放棄讓風險自留

參考：ISO31000:2009

準備和實施風險處理計劃

- 風險處理計劃的目的是記錄如何選擇處理方案將得到執行。
- 在處理計劃中提供的資訊應包括：
  - 選擇處理方案原因，包括可以得到的預期收益
  - 誰負責批准計劃和負責實施計劃
  - 提議的行動
  - 資源需求，包括突發事件
  - 執行措施和限制
  - 報告和監測要求
  - 時機和進度。

參考：ISO31000:2009

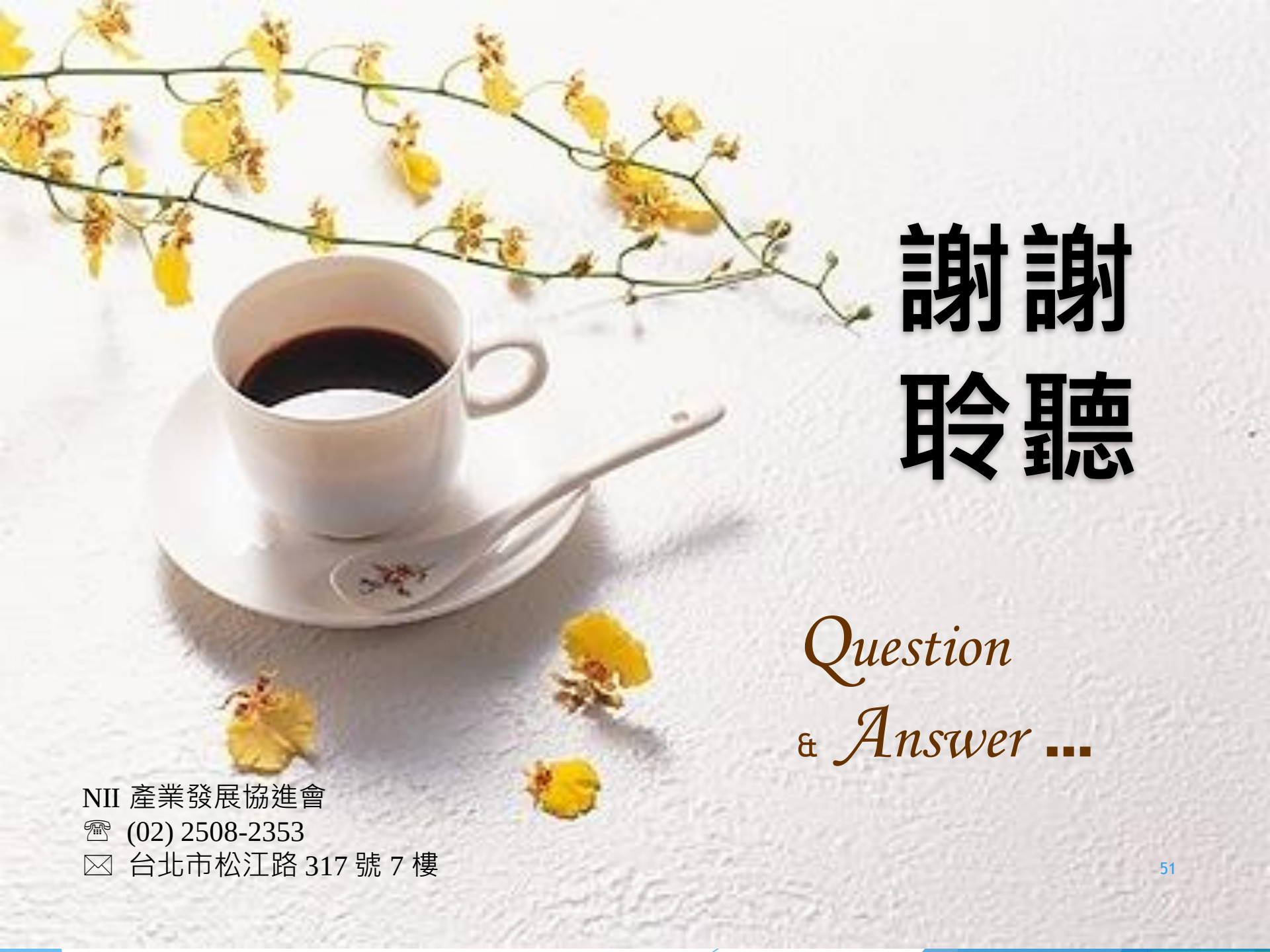
人事事項內部控制整體層級風險評估表

項次	作業項目名稱	風險發生原因(來源)	影響程度(A)	機率(B)	風險係數(A×B)	風險等級	過去三年是否發生弊端或違失	
							否	是(詳述)
1	聘僱							
2	敘薪與待遇							
3	保險							
4	福利							
5	退休、撫卹及資遣							
6	出勤							
7	差假							
8	訓練							
9	研究進修							
10	休假研究							
11	考核評鑑及獎懲							

明新學校財團法人明新科技大學人事事項內部控制整體層級風險評估

- 對學校營運之影響程度
- (A)分為：輕微(1)、嚴重(2)、非常嚴重(3)。
- 風險發生機率
- (B)分為：幾乎不可能(1)、可能(2)、幾乎確定(3)。
- 風險係數A×B，即是「對學校營運之影響程度(代號A)」乘以「風險發生機率(代號 B)」所得之數據。
- 風險等級分成低度、中度、高度及極度共四級。

內部控制之問題與討論



謝謝
聆聽

Question
& *Answer* ...

NII 產業發展協進會
☎ (02) 2508-2353
✉ 台北市松江路 317 號 7 樓