



不可不知 內部控制概念 與管理原則

KPMG

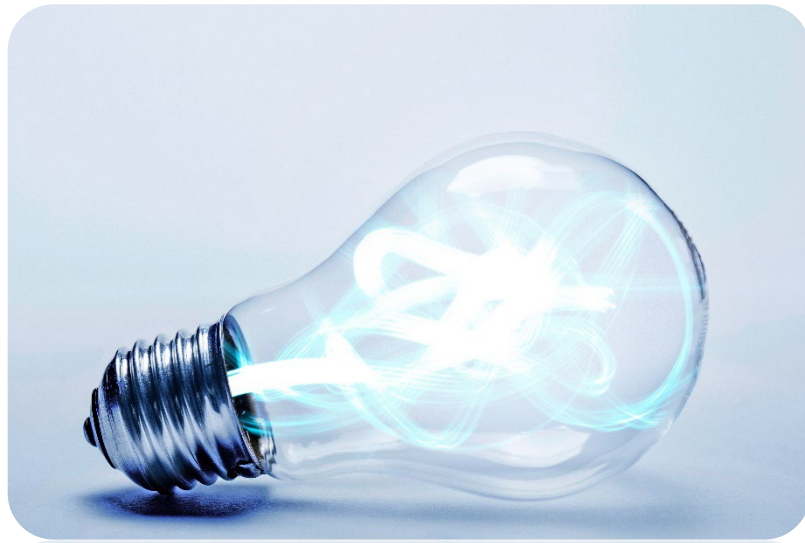
—
2024/03/05



Content

- 01 內部控制概念
- 02 五大要素與管理原則
- 03 內部控制效益及限制

課程目標



01

了解內部控制定義

02

了解內部控制框架

03

了解內部控制所需之內容

01

內部控制概念

違反誠信經營案例



LTN 自由財經

造假醜聞狂燒！豐田大發賠5000家廠商、損失恐達220億

陳麗珠 / 核稿編輯〔財經頻道 / 綜合報導〕日本豐田 (Toyota) 旗下子公司大發汽車 (DAIHATSU) 日前爆出安全測試造假醜聞，大發28日宣布，補償對象包括...

2023年12月29日



上報Up Media

瑞幸咖啡高層造假銷售額案1.8億美元與美國政府和解--上報

《路透》 (Reuters) 報導，具有超高人氣的中國連鎖咖啡品牌「瑞幸咖啡」 (Luckin Coffee) ，4月爆出前高層造假銷售額與財務數字風波，成為輿論抨擊和...

2020年12月17日



ESG永續台灣

「環境金害獎」糾污染慣犯！中油連五年蟬聯榜首，這九家公司也上榜

綠色公民行動聯盟每年依污染裁罰金額、次數，頒發「環境金害獎」給污染最重的事業單位，中油連續五年獲得榜首，空污違規次數、裁罰金額都是領先。

2023年6月14日

註：上課案例如未經判決確定，依無罪推定原則，僅供教學參考。

內部控制重要性

衝擊：

- 聲譽面
- 遵循面
- 財務面



何謂內部控制？



管理過程



由組織之董事會、管理階層及其他成員負責執行

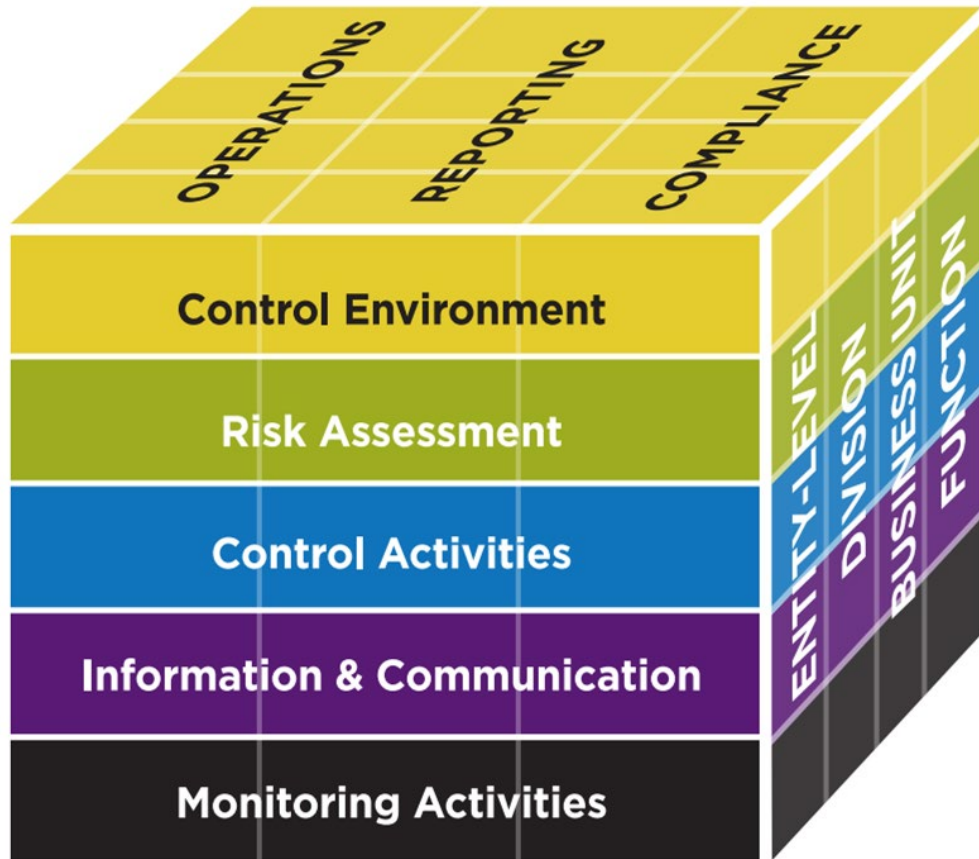


合理確保達成營運、報導及遵循等目標

資料來源：COSO 2013

內部控制整體架構

COSO 2013 Framework



三大目標

- 營運
- 報導
- 遵循

五大要素

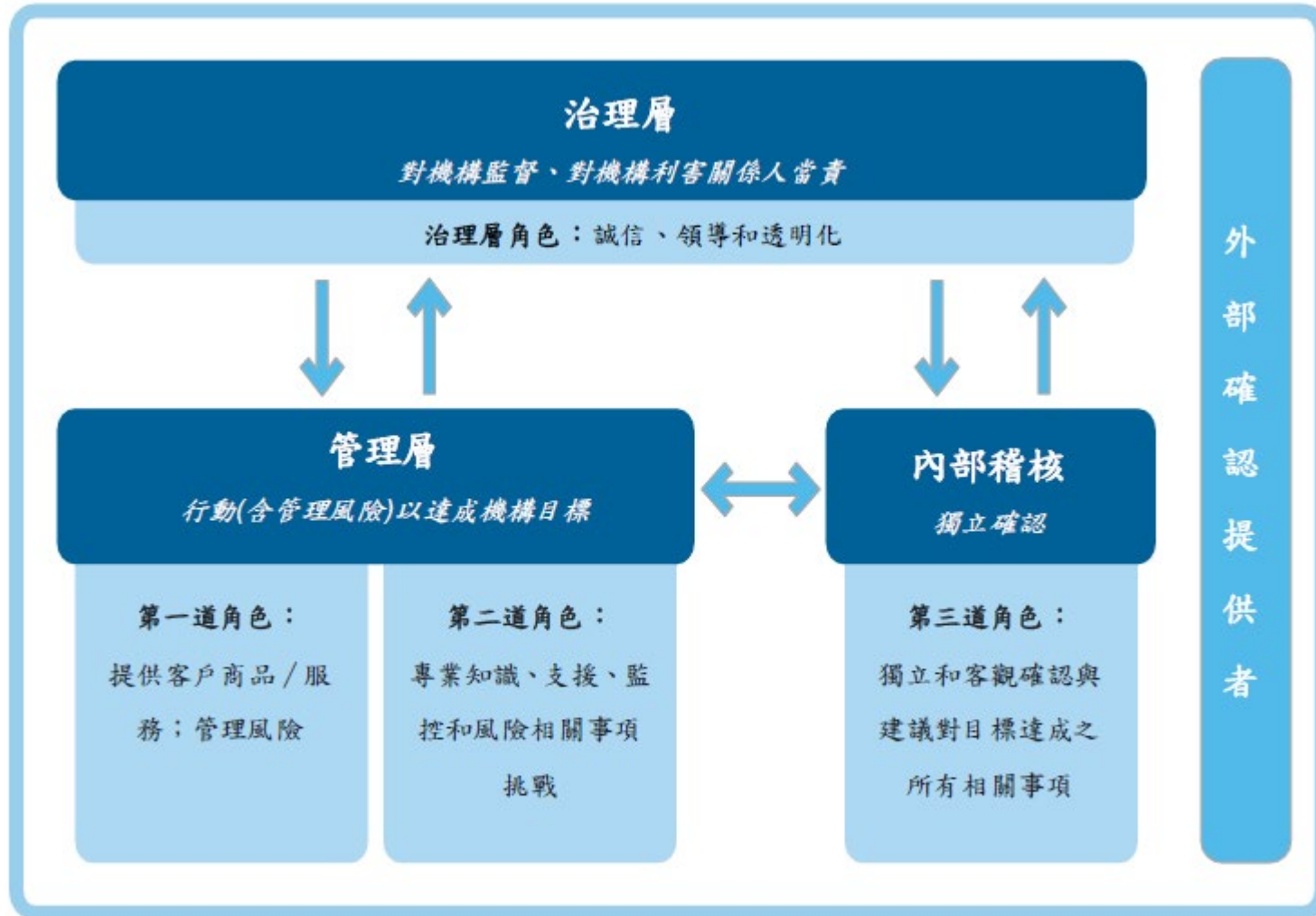
- 控制環境
- 風險評估
- 控制作業
- 資訊與溝通
- 監督作業

組織結構

- 組織層級
- 部門
- 營運單位
- 職能

內部控制三道防線

國際內部稽核協會三道模型



關鍵： ↑ 當責、報告 ↓ 委任、指導、資源、監督 ↔ 一致性、溝通、協調、協同

02

五大要素與管理原則

內部控制17項原則



1. 展現誠信與道德價值之承諾
2. 行使獨立之監督權
3. 建立結構、呈報體系及適當權限與責任
4. 延攬、培養及留用有能力之人才
5. 要求個人對內部控制負責以達成目標

6. 明確界定目標
7. 辨識並分析各項風險
8. 考量可能發生之舞弊
9. 辨識及評估對內控產生重大影響之各項改變

10. 選擇及建立控制作業
11. 運用科技選擇及建立科技之一般控制
12. 透過所建立之政策及程序，建置其控制作業

13. 蒐集、產生及使用攸關且具品質之資訊
14. 內部溝通
15. 與外部人士溝通

16. 選擇、建立及執行持續性或個別評估
17. 及時評估內控缺失，並與負責採取改善行動者溝通

控制環境

- ✓ 誠正及職業道德價值觀
- ✓ 管理階層的管理哲學與經營風格
- ✓ 組織結構
- ✓ 權利及責任分派
- ✓ 董事會之監督
- ✓ 人力資源運用及發展

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
其他內部控制組
成要素的基礎。



軟控制 vs. 硬控制



軟控制

- 不成文的非正式規定
- 例如公司文化、管理者經營風格、等對企業內部成員所造成的影響

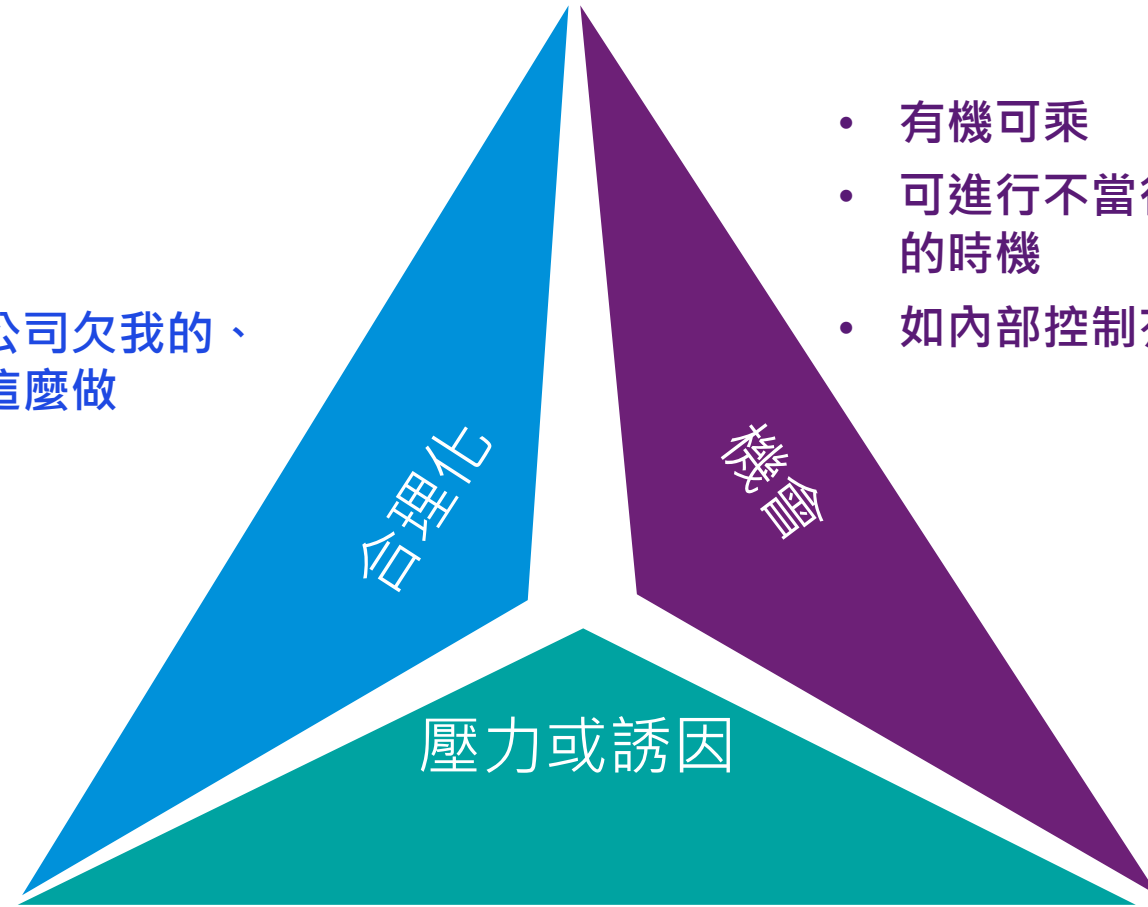


硬控制

- 書面的成文規定
- 例如明確組織、權利及責任、處罰及獎勵、監督

舞弊三角理論

- 睡得著
- 常見合理化藉口：公司欠我的、借了會還、大家都這麼做



- 有機可乘
- 可進行不當行為且又能掩蓋不被發現的時機
- 如內部控制有疏失、監督機制不完善

- 不當行為動機
- 財務穩定性或獲利能力受影響

控制環境實施指引



西門子賄賂案



事件

- 期間：2001年~2007年
- 目的：達成銷售目標
- 賄賂金額：約14億美金
- 涉及國家：阿根廷、孟加拉、中國、伊拉克、以色列等
- 關係人：政府官員、顧問/中介機構

衝擊

- 為了不失去美國政府標案資格，於2008年向美國DOJ及德國政府和解，支付13億美金罰款

根因

- 歷史背景：1999年以前賄賂款合法
- 企業文化：賄賂積習難改、績效壓力

改善

- 更換管理階層、設立法遵長
- 遵循績效與年終獎金連結
- 增加遵循部門人力 (170人->620人)
- 多重檢舉管道
- 強化中間人管理

風險評估

- ✓ 確認整體目標及作業層級目標
- ✓ 辨識關鍵性之經營風險
- ✓ 評估風險發生之衝擊及可能性
- ✓ 對經營風險採取對策
- ✓ 監督內外環境變化及制度遵循

辨認及分析可能面臨之風險、不可能達成組織目標之可能性及內部因素與外部因素發生原因。



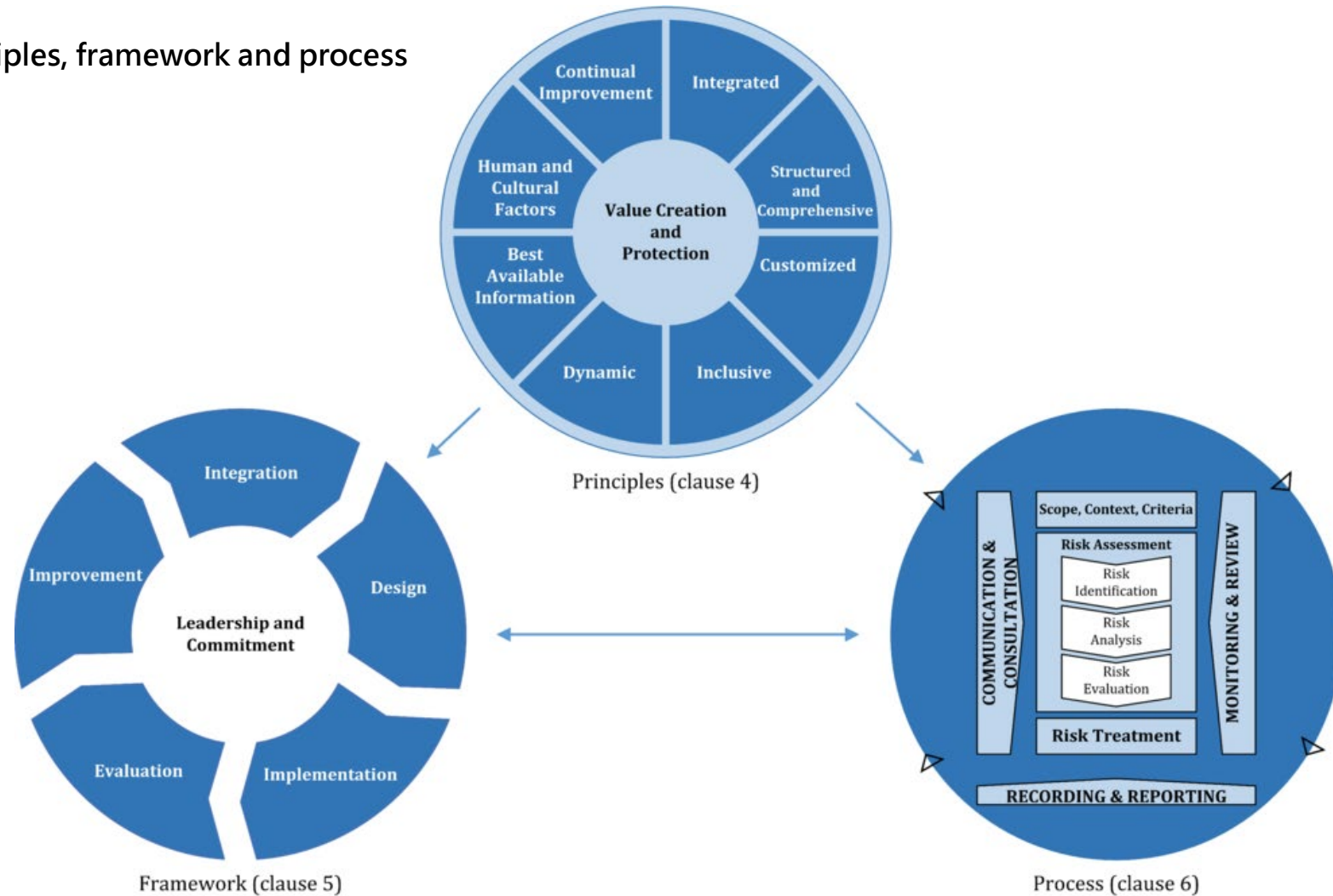
全球風險



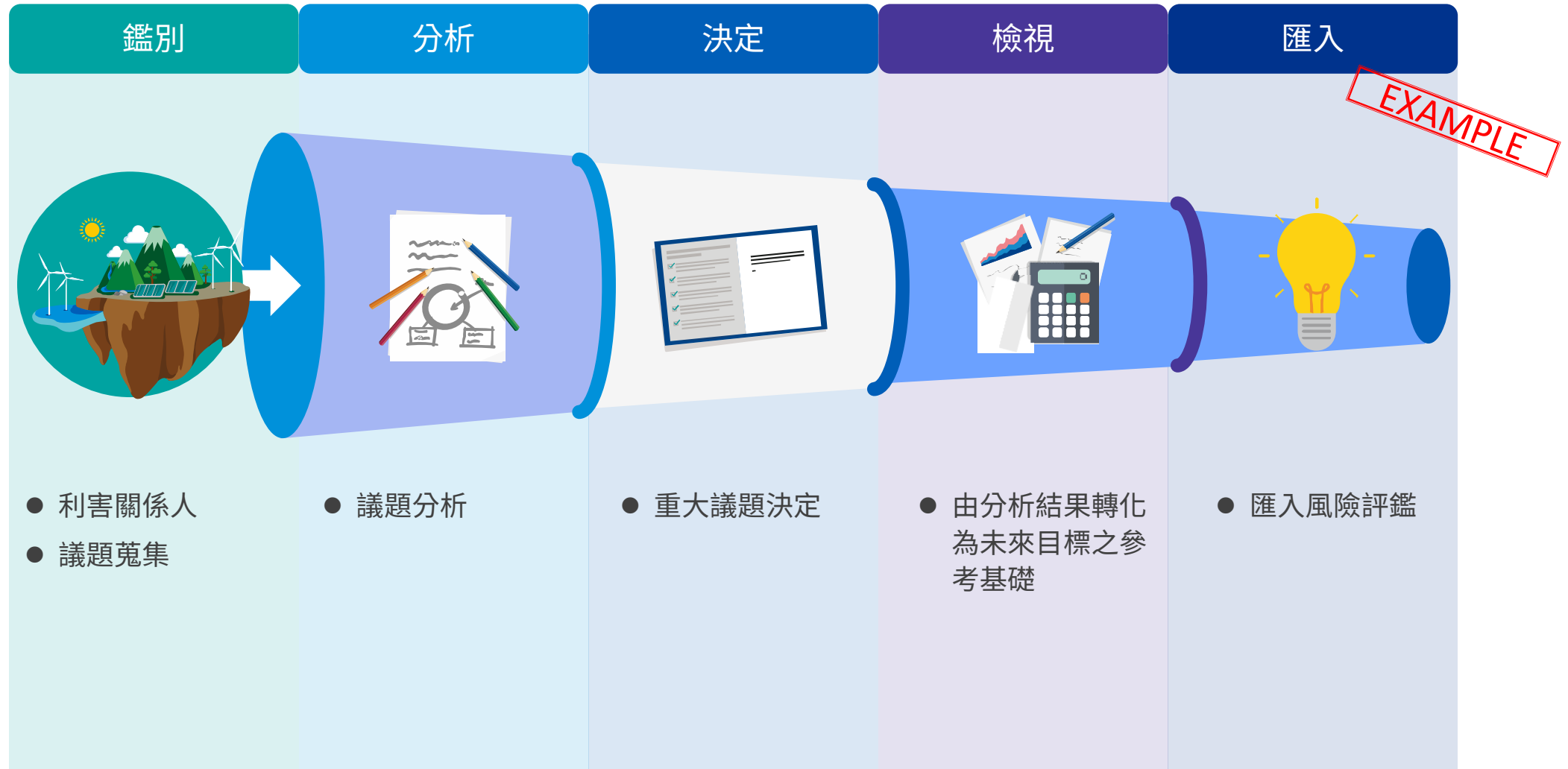
資料來源：[2024年全球風險報告環境風險佔長期風險半數，企業該如何行動？ - EDESG安得數治](#)

ISO 31000 風險管理架構

ISO 31000: 2018 Principles, framework and process



重大議題鑑別



風險評鑑



EXAMPLE

風險識別

- ① 內外部議題
- ② 法令法規
- ③ 利害關係人期望
- ④ 根因分析

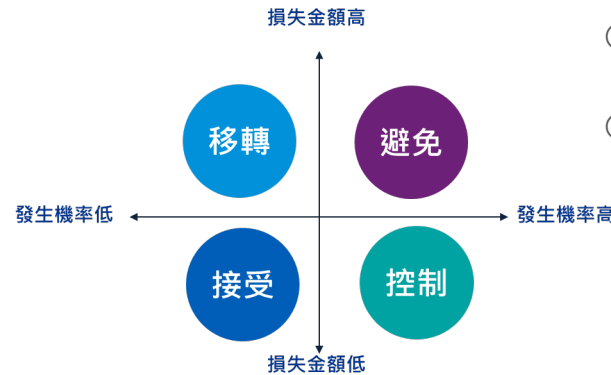
風險評估

- ① 固有風險：
 - 可能性
 - 衝擊
- ② 控制措施



風險值

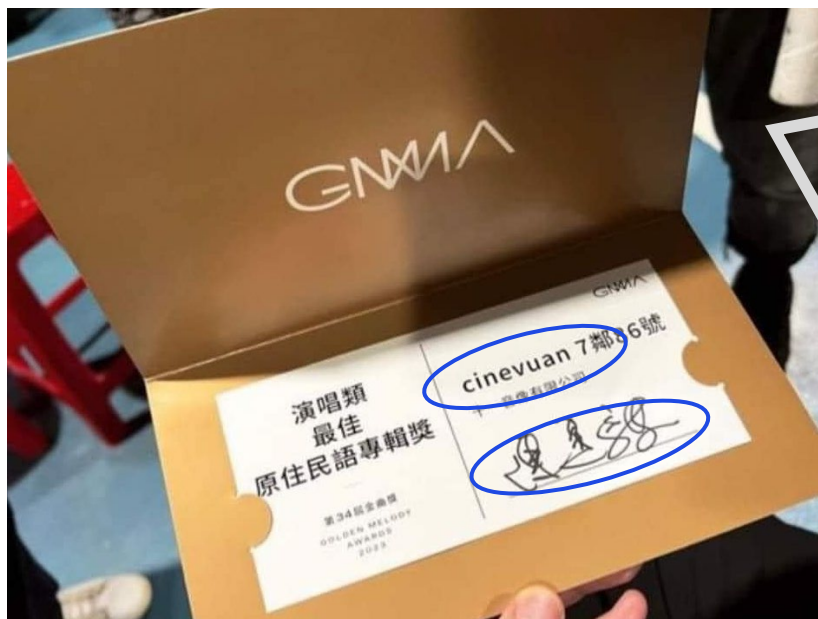
風險處理



風險監督

- ① 風險處理計畫及追蹤改善情形
- ② 現有風險、新/潛在風險

金曲獎頒錯獎事件



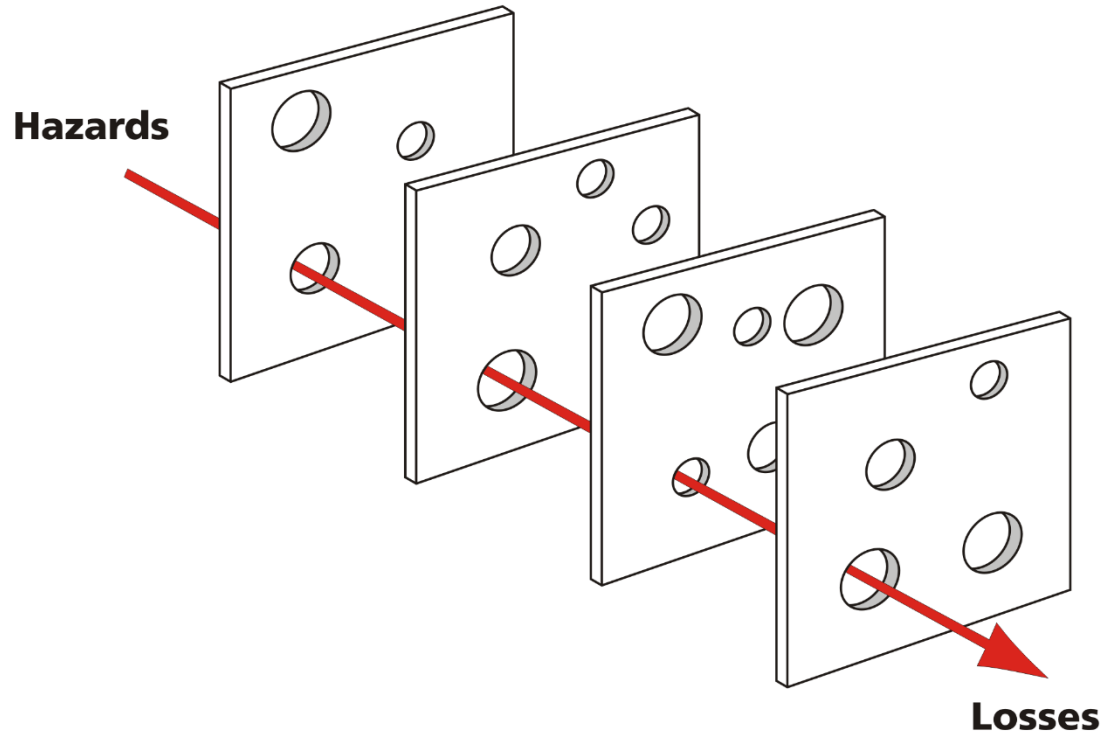
34屆金曲獎上發生頒錯獎烏龍事件，揭獎信封可看出評審陳建騏的簽名佔了整個信封四分之一。

頒獎人艾怡良第一時間以為得獎人是陳建騏，後來轉問司儀，殊不知司儀也不知道是誰，只好說出入圍者的名字陳健璋，最後才確認得獎者是啞啞。



乳酪理論

內控之重要性



紅色為風險，穿過數個孔後導致損失

導致嚴重事故發生從來都不是因為某個單獨的原因，而是多個問題同時出現。

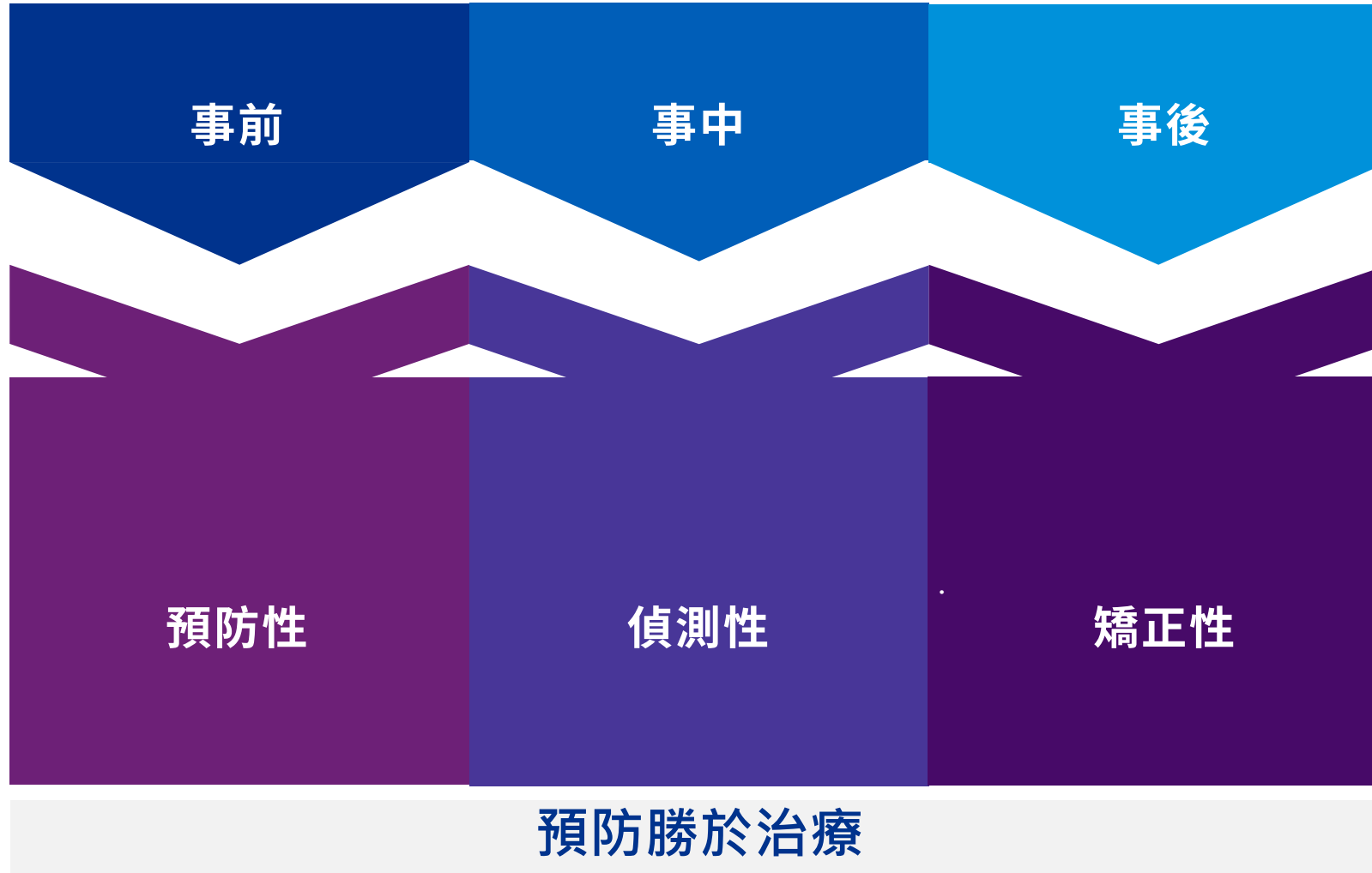
控制活動

- ✓ 政策規劃、執行、覆核及管理
- ✓ 營運表現的事後檢討
- ✓ 資訊的保護
- ✓ 責任區隔

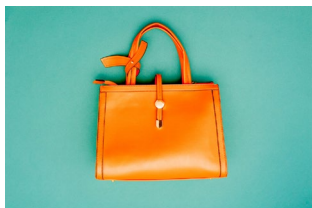
幫助管理階層確保指令被執行的政策及程序，在每個層級及職能中均會出現，且應配合環境變遷隨時修正。



控制方式



會計挪用公款 (1/2)

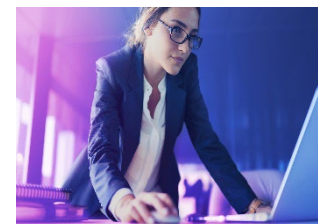


〈財經週報-神鬼會計〉身兼會計與出納她侵吞2億買800多個 ...

2023年2月5日 — 劉女業務侵占罪被判刑4年8月定讞，她供稱酷愛名牌包「就是喜歡、想買」；最終因廠商沒收到貨款，向另名同事核帳，劉女見事跡敗露才主動投案，交出名牌包給 ...

神鬼女會計！7年搬走台北律師公會6千多萬判刑4年

2022年11月29日 — 2020年北律改選理監事後，查帳發現李女涉長期挪用公款，李女自知紙包不住火，將2019年度挪用的640萬元公款繳還，但仍被依業務侵占罪起訴；北律回溯查帳， ...

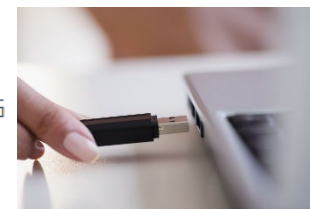


會計侵吞公款5百多萬元有罪老闆娘嗆聲也遭判刑

2018年1月9日 — 有公司的會計利用職務之便，侵吞公司款項達新臺幣五百多萬元，對此，臺中地方法院日前依詐欺取財罪、業務侵占罪，分別判處會計一年十個月、六個月的 ...

碧桂園30歲會計「挪用公款2億元」用途令人太傻眼

2023年8月27日 — 但是他卻挪用公款，將「泰安市碧桂園、碧桂園地產集團有限公司」兩個帳戶資金4800多萬元，轉進自己名下的帳戶。他並利用不法手段取得了4個「U盾」（USBKey ...



會計挪用公款 (2/2)



RISK

公司資產損失，財報不實表達

WHO

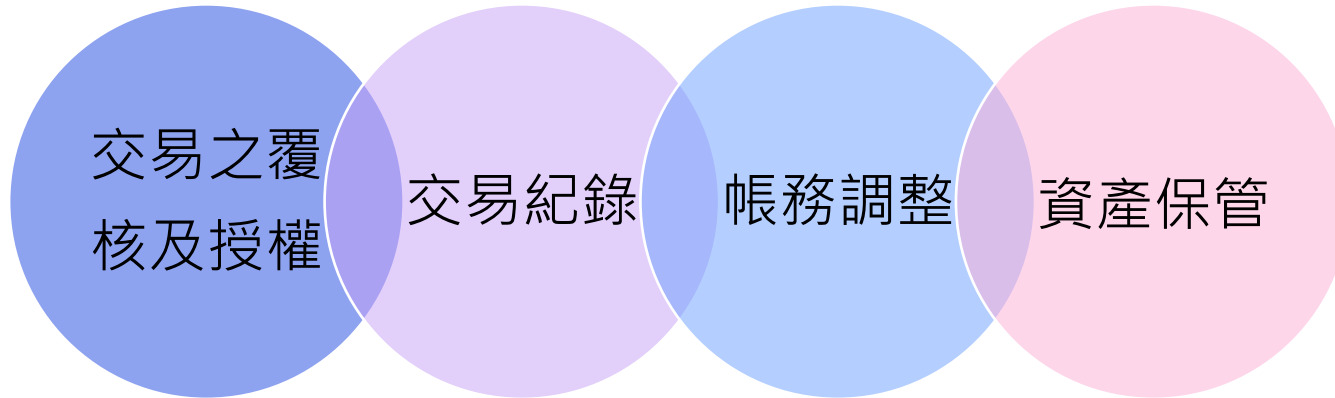
系統權限控管→誰可以執行入帳作業

WHO

職能劃分→權限是否依職務區分且符合最小化原則

職能分工

減少隱瞞錯誤及舞弊



- 管錢不管帳及印鑑
- 管貨不管錢
- 管貨不管帳
- 不能自始自終全面處理某項交易
- 不應有員工同時控制其中兩個以上之職能

行員竊取ATM現金



行員/又見行員監守自盜兆豐、華南銀2家今遭重罰800萬元

又見銀行員監守自盜！兆豐銀行有行員挪用ATM現鈔877萬元、華南銀行員利用客戶臨櫃繳稅款的時候挪用客戶存款236萬元，金管會今（2）日宣布2家銀行各...

2022年6月2日

如何避免？

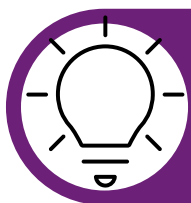
- 檢視內控機制及強化查核管理措施
- 增設ATM及時監控系統，遠端分組監看
- 抽查分行辦理ATM鈔箱補鈔或盤點作業，以掌握各分行ATM作業情況
- 確保分行落實「四眼原則」

四眼原則



- 一個特定的活動，如決策、交易等，必須得到至少兩個人的核准。
- 除可確定內容無誤，也可以促進授權及增加透明度。

系統權限管理 (1/2)



最小授權原則

中石化內鬼案！前總座蔡錫津竊營業秘密一審判1年2個月

2024年2月4日 — 中國石油化學公司2015年爆發內鬼案，前總座蔡錫津與同夥盜取公司10萬筆商業機密，不法重製利用中石化的營業秘密、保密資料及相關資源，違反營業秘密 ...

涉竊取Gogoro營業秘密 湛積共同創辦人追加起訴

以研發生產Gogoro電動機車聞名的睿能創意公司，發覺前主管林松慶離職後創辦湛積公司，帶走公司營業秘密，還挖走睿能員工，提告竊密；新北地檢署前年依...

2023年11月28日

Klook副總監涉竊取前東家KKday營業秘密 北檢今起訴3人

Klook副總監涉竊取前東家KKday營業秘密北檢今起訴3人 ... 2021年間，旅遊公司客遊公司Klook副總監陳鈞暘，涉嫌提供前東家客遊天國際旅行社股份有限公司KKday...

1 個月前

系統權限管理 (2/2)

01

- 共用特權帳號
- 特權帳號作業未有適當監控

02

同一資訊人員同時於應用系統、作業系統及資料庫持有跨系統層級之特權權限

04

開發人員擁有正式環境異動資料之權限

03

開發人員同時持有程式上線權限



特權帳號之固有風險

- 擁有的存取權限高
 - 可新增使用者帳號並規避權限管理機制
 - 逐步提升帳號權限或新增特權帳號
 - 可存取敏感資訊，並擁有高權限如新增、刪除、修改或複製
 - 可變更系統事件紀錄，影響稽核有效性



共用特權帳號之固有風險

- 增加識別身分的難度

預防性控制：最小授權原則，AP、DB/OS 特權帳號分持、暫時性授權等

偵測性控制：定期覆核特權帳號、及時/定期審查特權帳號異動或audit log等

書面制度

02

定期評估內容有效性



01

- 控制程序描述清楚
- 辦法間之流程不衝突

03

- 寫說做一致
- 落實執行

資訊控制

- 1 資訊部門與使用者部門權責之劃分
- 2 資訊處理部門之功能及職責劃分
- 3 系統開發及程式修改控制
- 4 編製系統文書之控制
- 5 程式及資料之存取控制
- 6 資料輸出入之控制
- 7 資料處理之控制
- 8 檔案及設備之安全控制
- 9 硬體及系統軟體之購置、使用及維護控制
- 10 系統復原計劃制度及測試程序之控制
- 11 資通安全檢查之控制

售價標示錯誤 (1/2)



樂桃航空促銷標錯價！大阪高雄只要643元台幣網友瘋搶

2023年10月21日 — 樂桃航空近期推出「萬聖節促銷活動」，飛日本機票單程未稅1440元起，昨天(20日)晚上8點開賣。不過有人發現「大阪到高雄」的幣值標錯，原本2980台幣 ...



雙11慘劇！馬卡龍甜點名店標錯價3千盒虧損450萬全認賠

4 天前 — ... 知名甜點工作室也推出馬卡龍禮盒雙11優惠活動，沒想到卻不慎標錯價，把優惠售價1780元標成300元，大批消費者瘋狂搶購，等到業者驚覺不對時已售出逾3千 ...



快訊 / 飛美頭等30萬變2萬5！國泰航空認標錯價照賣

2019年1月2日 — TVBS在元旦獨家報導，國泰航空越南飛北美，頭等艙竟然出現2萬5低廉價格，國泰航空也在官方Twitter認了，恭喜成功搶到限時快閃頭等和商務艙機票的幸運 ...

售價標示錯誤 (2/2)



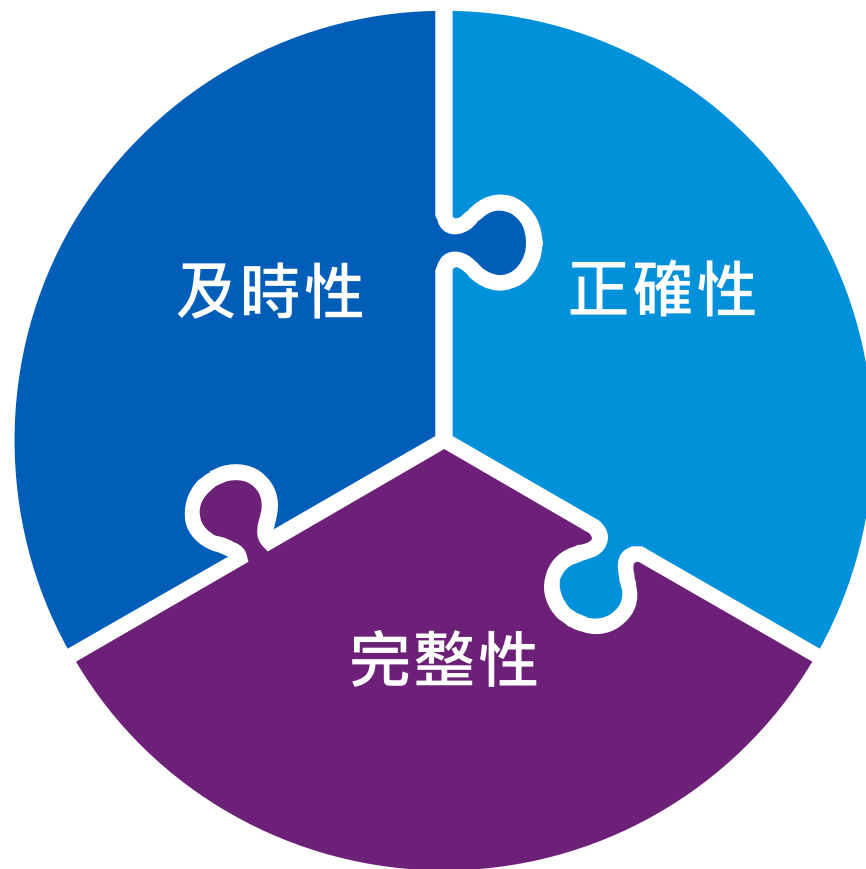
資訊與溝通

- ✓ 蒐集、產生及使用攸關且具品質之資訊
- ✓ 企業內部溝通：與董事會溝通、舉報熱線等
- ✓ 與外部之溝通：客戶、供應商、外部查核人員、主管機關、股東等

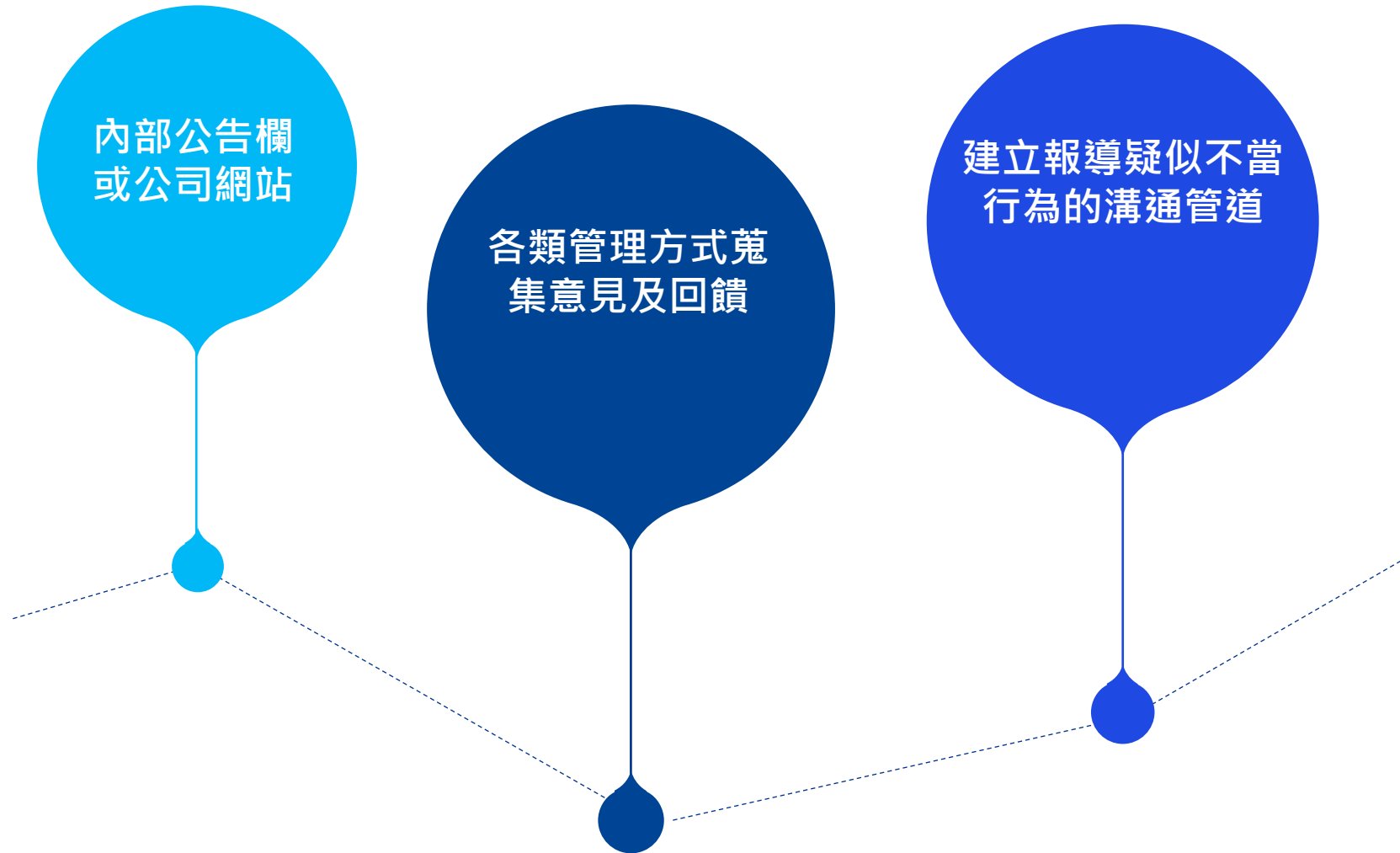
企業蒐集、產生及使用來自內部與外部之攸關、具品質之資訊，並確保資訊在企業內部及外部之間皆有效溝通。



資料品質



溝通管道



監督

- ✓ 例行的管理及監督活動
- ✓ 財務報表與營運資料對帳
- ✓ 定期與內部和外部單位溝通
- ✓ 內部稽核定期評估和建議

評估內部控制執行品質及績效之過程，在發現缺失前均已作適當處理。



內部稽核查核—以營業秘密為例



2024 年風險焦點：內部稽核之熱門議題

Figure 1:
Current risk levels vs. future risk levels – Asia Pacific

- Three areas share the highest risk level for Asia Pacific: cybersecurity, business continuity, and human capital.
- In the next 3 years, digital disruption and climate change are the risks expected to increase the most.



What are the top 5 risks your organization currently faces?

What are the top 5 risks your organization will face 3 years from now?



Note: The IIA's Risk in Focus Global Survey, Asia Pacific, n = 1,034. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 7:
Current audit effort vs. future audit effort – Asia Pacific



- Asia Pacific CAEs were most likely to choose cybersecurity as one of their top 5 areas for internal audit effort (66%).
- Second place was held by a wide variety of areas, including business continuity, regulatory change, and governance/corporate reporting.

What are the top 5 risks on which internal audit spends the most time and effort?

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?



Note: The IIA's Risk in Focus Global Survey, Asia Pacific, n = 1,034. Percentage who ranked the area as one of their top 5 for audit time and effort.

五大要素之應用



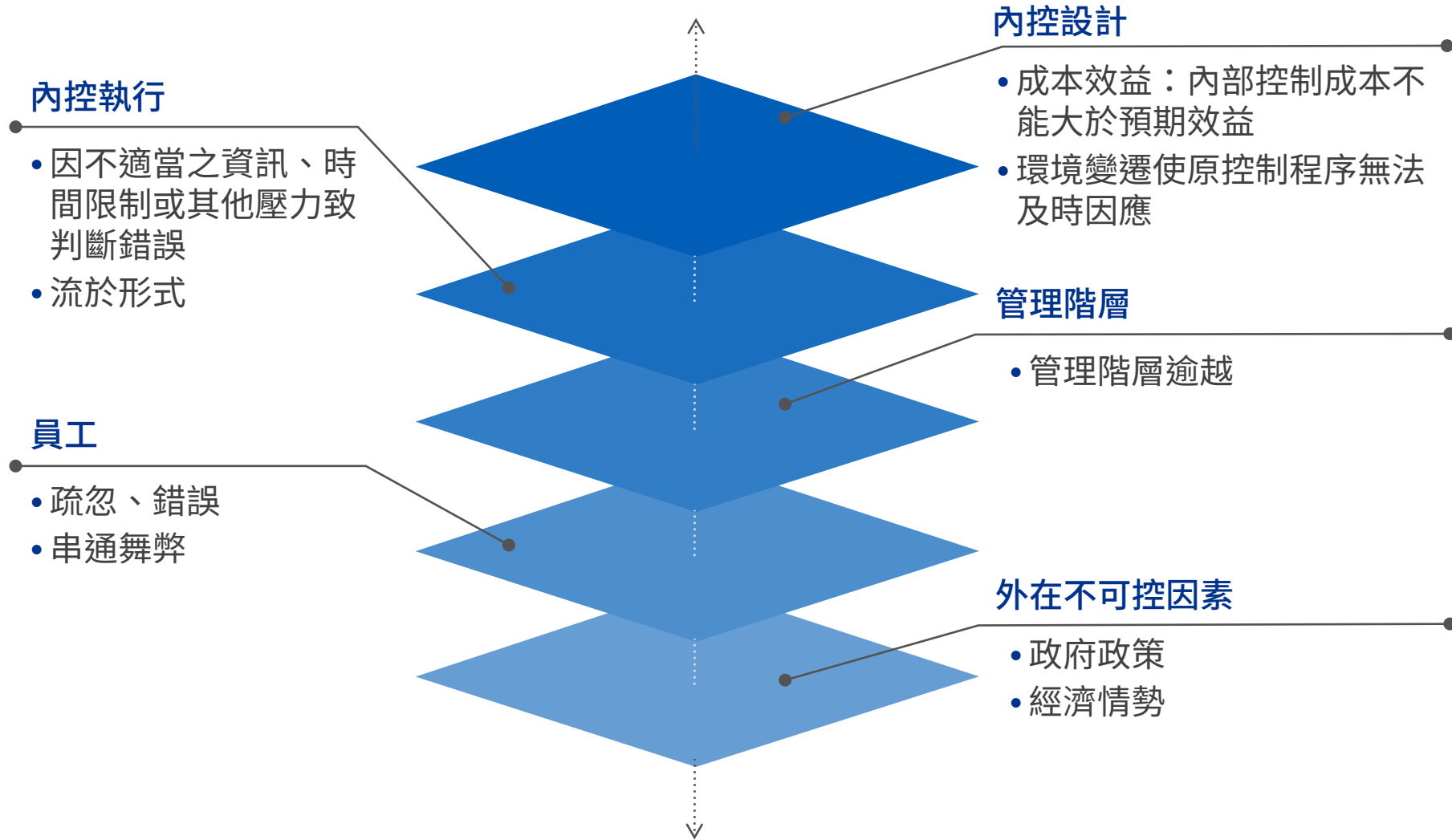
03

內部控制效益及限制

內部控制效益



內部控制限制



Q&A



Thank you



KPMG



本文所提及之一部分或全部服務，依相關獨立性規範，可能無法對KPMG之審計客戶及其關係企業提供服務。
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



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.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2023 KPMG, a Taiwan partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

Document Classification: KPMG Confidential