企業風險管理

- 永續經營的重要關鍵

主講人：王怡心 博士

CPA CGAP CIA CRMA

台北大學會計學系教授

中華民國內部稽核協會理事長

Taipei 2013

Taiwan

大綱

1.ERM 與 COSO

2.ISO 31000發展

3.ERM 對內部稽核之影響

4.結語

ERM與COSO

Taipei 2013

Taiwan

企業風險管理發展
-與COSO報告和沙賓法案相關

Treadway 委員會

- 美國會計師公會**AICPA** (American Institute of Certified Public Accountants)、
- 美國會計學會**AAA** (American Accounting Association)、
- 內部稽核協會**IIA** (Institute of Internal Auditors)、
- 管理顧問協會**IMA** (Institute of Management Accountants)、
- 財務主管協會**FEI** (Financial Executive Institute)等五個專業單位乃共同贊助組成「不實財務報導全國調查委員會」

(National Commission on Fraudulent Financial Reporting，簡稱Treadway委員會)

- 主要目的:

在探討如何解決企業日益嚴重的**不實財務報告**問題

ACIIA Taipei 2013

IIA Taiwan

Treadway 委員會成立 COSO

COSO 成立後，於1992年發佈

「內部控制：整合架構」(Internal Control – Integrated Framework)，

提出內部控制的定義與五項組成要素

(控制環境、風險評估、控制作業、資訊與溝通、監督)之內部控制整合架構。

Taipei 2013

Taiwan

沙賓法案 404 條款

沙賓法案出現的背景，源於2001年安隆(Enron)與世界通訊(WorldCom)案等一連串的會計醜聞。

404條款之立法目的，為了使大眾更易於察覺到企業的欺詐行為，並確保企業財務報導的可靠性。

要求企業必須針對企業的內部控制進行自行評估，再由會計師對企業內部控制及管理階層自行評估的結果加以審查，並將審查結果向證管會申報。

COSO 2004 ERM 報告

企業風險管理-整合架構

(Enterprise Risk Management – Integrated Framework，簡稱

COSO ERM報告)，係COSO於2004年9月為因應沙賓法案規定而發佈。

COSO 2004 企業風險管理組成要素

- COSO ERM在保持COSO報告內部控制五個組成要素的基礎上，將**控制環境**要素，細分為**內部環境**、**目標設定**，**風險評估分為事項辨識**、**風險評估**、**風險回應**，

  1.內部環境

  2.目標設定

  企業先有目標，管理階層辨識**影響**目標達成的**潛在事件**

  3.**事項辨識**

  管理階層辨識影響企業目標達成的內部和外部事件，區分**風險**和**機會**，並把機會導回到**策略**制訂過程

COSO 2004 企業風險管理組成要素

4.風險評估

風險評估使管理階層瞭解**潛在事件**如何影響企業目標的達成

5.風險回應

分為「避免風險」、「降低風險」、「分攤風險」和「接受風險」四類

6.控制作業

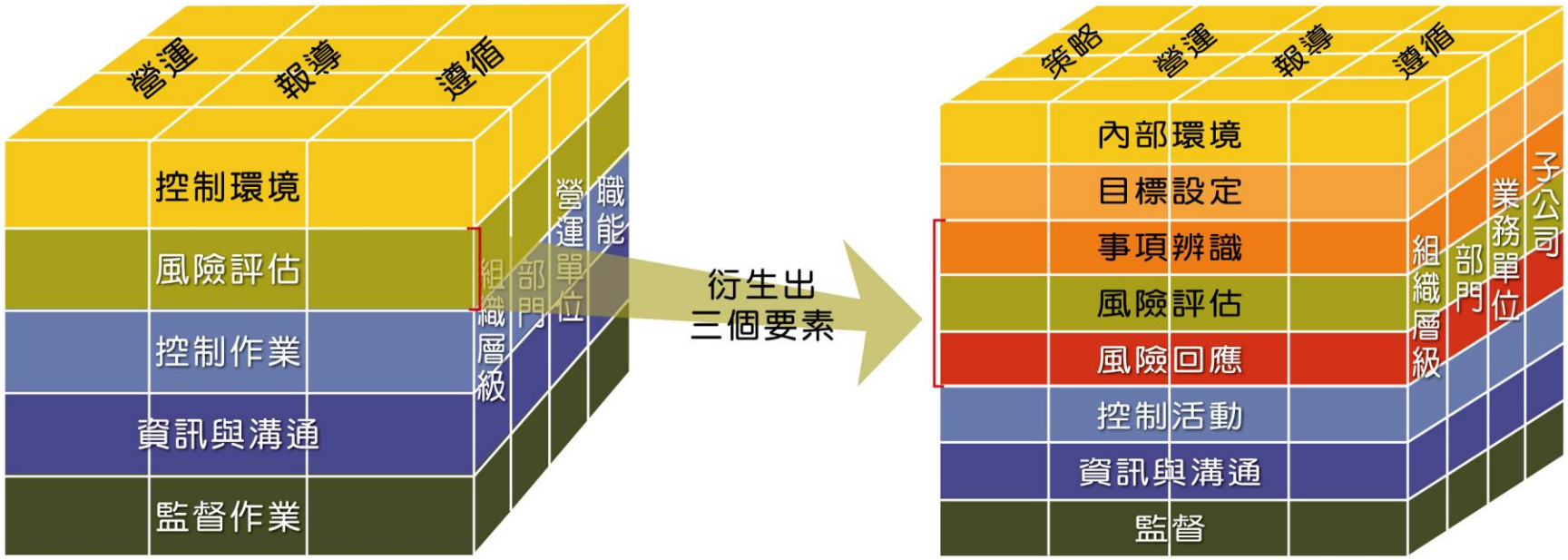
控制作業是企業**控制風險**以達成其目標而執行的過程

7.資訊與溝通

8.監督

評估風險管理制度設計及執行品質的一種過程

ERM架構更關注於風險



ERM架構更加關注於風險，其延伸內部控制架構的**風險評估**要素，而產生三個要素：事項辨識、風險評估及風險回應。

ERM目標:策略、營運、報導、遵循

- 內部控制關注於如何達成機構的目標。

- ERM關注於如何建立策略目標來創造、維持並實現機構價值。
- ERM較具前瞻性，考量如何規避風險以降低損失，或接受新風險來提高價值。

ERM適用於專案計畫：

設定明確的策略目標－以2013 ACIIA為例

研討會主題-
王道治理：政府治理與公司治理

2013 ACIIA CONFERENCE
Taipei 2013

Wangdao Governance
Creating Social Value

分組場次主題

春耕：**Emerging Issues**
夏耘：**Current Issues**
秋收：**Best Practices**
冬藏：**Self Assessment**

Taipei 2013

Taiwan

來自20個
國家代表

2014.11.03-11.05

約1,200位
與會者

圓山飯店

2013 ACIIA 各國代表團體照

2013 ACIIA 歡迎酒會

2013 ACIIA 開幕典禮

2013 ACIIA 迎賓晚會

ISO 31000發展

Taipei 2013

Taiwan

ISO 31000 源起

- 面對接踵而來的全球金融風暴、各地頻傳的氣候異常現象等，企業無時無刻不在面臨經營時的風險。國際標準化組織ISO於2009年11月15日正式公告的標準ISO 31000:2009風險管理-原則與指導綱要(Risk Management – Principles and guidelines)。
- ISO 31000是第一個國際認可的風險管理標準，可於任何產業或部門、組織使用，透過戴明博士的PDCA管理循環的模式，進行風險管理工作。

「危機」

危險　還是　機會

危機是由危險及機會兩個字構成，風險管理做的好，就能將危險轉換成機會。

ACIIA Taipei 2013

IIA Taiwan

影片介紹：化風險為利基

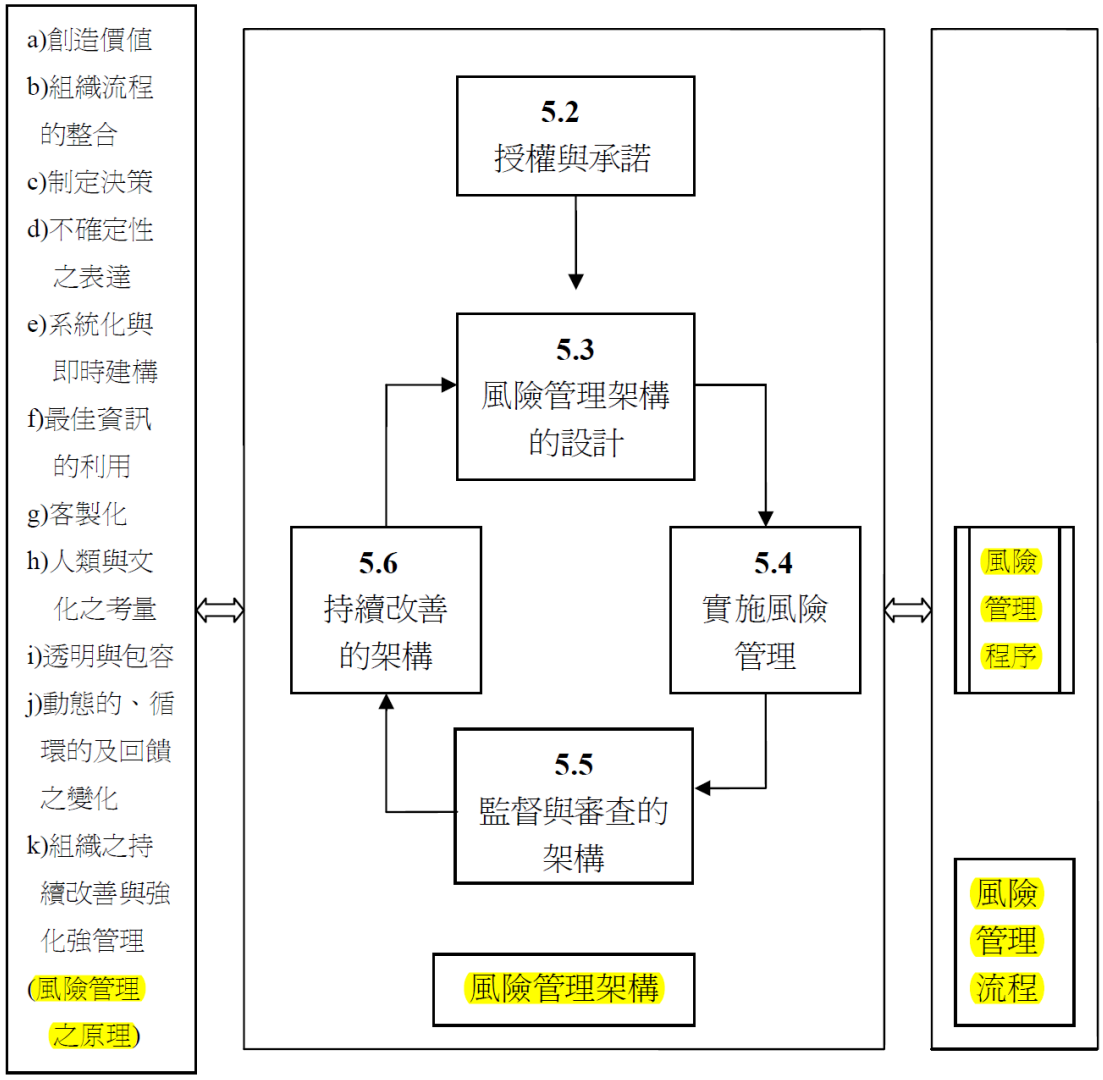
Taipei 2013

Taiwan

ISO 31000 特色

- ISO 31000有三個特點：
  - 是一個全面的自上而下的方法。
  - 風險管理作為一個管理任務（而不是僅僅作為一個過程）。
  - 是一個普遍持有的基本標準。

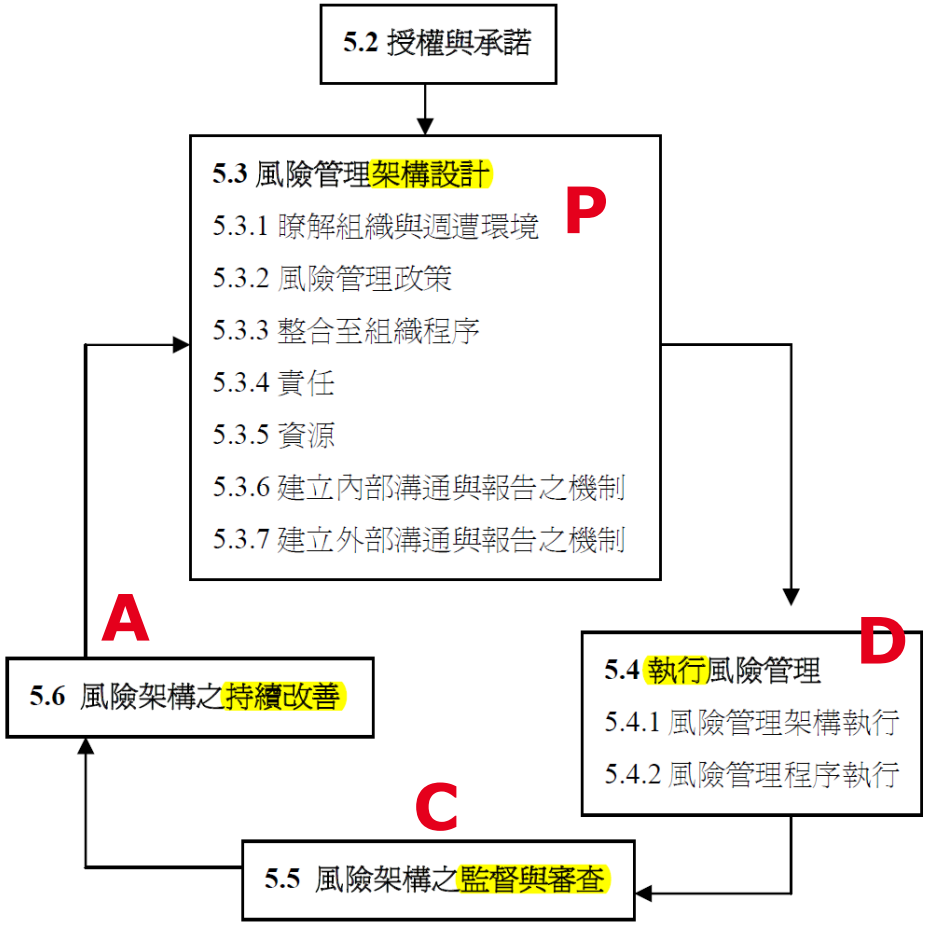
風險管理之原理、架構及過程



風險管理可以協助組織對未來可能發生活動的**不確定性**與**可能的衝擊**提供決策參考，並評估可採行的因應措施。

Taiwan

風險管理架構



ISO 31000風險管理的架構，是透過P-D-C-A管理循環的模式。企業在開始設計與完成風險管理架前，須瞭解組織的內外部環境因素，訂定風險管理政策，並建立風險溝通的模式。同時擬定風險發展執行計畫與程序，經由監督與審查機制，使組織的風險管理達到持續改善的終極目標。

Taiwan

ISO 31000 風險管理的影響

- 運用ISO 31000，
  - 企業可有效改善對威脅風險的辨識程度；
  - 為決策與規劃建立可靠的基礎；
  - 改善營運的有效性和效率性；
  - 強化失誤預防的改善和意外事件的管理；
  - 有效地配置和使用資源。

ERM對內部稽核之影響

Taipei 2013

Taiwan

以COSO ERM為基礎之內部稽核

- 以COSO ERM為基礎之稽核計畫
  - 於稽核範疇中納入COSO ERM目標
  - 確保內部稽核之風險評估與組織之風險評估相結合
- 確認性與諮詢性服務
  - 確認性服務需考量企業風險管理
  - 諮詢性服務可改善企業風險管理之效益

規劃及實施COSO ERM內部稽核計畫

- 設計規劃：應用相關指引，以結構化、具原則性之方法來實施COSO ERM。
- 決定風險標準：考量哪些類型之風險。
- 風險評核：包括風險辨識、風險分析及風險評估。
- 風險處理：描述風險情況及研擬風險處理計畫。
- 監督COSO ERM系統：界定COSO ERM監督範圍與權責。
- 風險管理報導：強調風險管理報導之重要性，並包括內部報導與外部報導。

結　語

Taipei 2013

Taiwan

結　　語

- 成功落實COSO ERM是靠逐漸之進化，而非革命。
  - COSO ERM較具前瞻性，需考量如何規避風險以降低損失，或接受新風險來提高價值。
  - 善用ISO 31000:2009風險管理-原則與指導綱要，進行風險管理工作。
  - 內部稽核於企業風險管理過程，對每一階段均有其角色之扮演。

Taipei 2013

Taiwan