

# 建立內部控制制度核心原則

## 1. 總則

- 1.1 本核心原則之目的，係為促使企業有效設計及執行其內部控制制度，因應瞬變之經營環境，強化董事會與管理階層之公司治理與經營決策，降低風險至可接受水準，以協助企業達成永續經營目標，進而提高資本市場之資訊透明度，維護利害關係人之權益。
- 1.2 公開發行公司、金融相關機構、中小型企業及其他單位，依據證券交易法、期貨交易法、金融控股公司法、銀行法、保險法、證券投資信託及顧問法、票券金融管理法、信託業法、信用合作社法或其他相關法令規定設計及執行內部控制制度，可參考本核心原則。
- 1.3 內部控制係指一種過程，由企業董事會、管理階層與其他成員負責設計及執行，以合理確認營運、報導與遵循等相關目標之達成。

內部控制之三個目標如下：

- (1).營運目標：營運之效果及效率，包括達成營運與財務績效目標及維護資產安全。
- (2).報導目標：企業內部與外部財務報導及非財務報導具可靠性、及時性、透明性或符合相關規範。
- (3).遵循目標：相關法令規章之遵循。

### 1.4 企業內部控制制度之組成要素：

- (1).控制環境：控制環境係企業設計及執行內部控制制度之基礎。董事會與高階管理階層應對內部控制之重要性建立內部行為

準則，包括訂定董事行為準則、員工行為準則等事項。控制環境包括企業之誠信與道德價值、董事會治理監督責任、組織結構、權責分派、人力資源政策、績效衡量及獎懲等。

- (2).風險評估：風險評估之先決條件為確立各項目標，並與企業不同層級單位相連結，同時需考慮企業目標之適合性。風險評估要求管理階層應考量企業外部環境與商業模式改變之影響，以及可能發生之舞弊情事。
  - (3).控制作業：控制作業係指企業依據風險評估結果，採用適當政策與程序之行動，將風險控制在可承受範圍之內。控制作業之執行遍及企業所有層級、業務流程內之各個階段、所有科技環境等範圍；控制作業可具有預防性或偵測性之功能，亦可涵蓋一系列人工化與自動化作業，諸如授權、核准、驗證、調節、績效複核等。
  - (4).資訊與溝通：資訊與溝通係指企業蒐集、產生及使用來自內部與外部之攸關、具品質之資訊，以支持內部控制其他組成要素之持續運作，並確保資訊在企業內部以及企業與外部之間皆能進行有效溝通。
  - (5).監督作業：監督作業係指企業依據法律規定及企業相關規範，進行持續性評估、個別評估或兩者兼用，以確定內部控制制度之各組成要素是否已經存在及持續運作；對於所發現之內部控制制度缺失，應向適當層級之管理階層與董事會溝通，並及時改善。
- 1.5 企業內部控制制度係包括內部控制之目的、原則、政策、程序，內部稽核人員之資格條件與應遵循及執行之事項。
- 1.6 企業設計及執行有效內部控制制度之要件：

(1).五大組成要素能整體運作。

「整體運作」係指企業合理確認五大組成要素可共同將無法達成某項目標之風險降低至可接受水準。

(2).各組成要素及各攸關原則已經存在且持續運作。

「已經存在」係指在設計及執行內部控制制度以達成特定目標時，確定各組成要素與各項攸關原則已經存在；「持續運作」係指在運作及管理內部控制制度以達成特定目標時，確定各組成要素及各攸關原則持續運作。

(3).當企業發生一個內部控制重大缺失時，不可判定其已符合有效內部控制制度之要求。

(4).定期檢視內部控制制度，應考量企業經營規模、業務範圍、競爭狀況及風險水準等因素，並隨情況之變化適時調整。

(5).考量設計及執行內部控制制度之效益與成本。

## **2. 控制環境**

2.1 董事會與高階管理階層公開展現企業對於誠信與道德價值之承諾。

2.1.1 高層訂定內部行為準則

董事會與高階管理階層透過其指令、行動及行為，展現誠信與道德價值，以支持內部控制制度運作之重要性。

2.1.2 建立行為準則

董事會與高階管理階層對於誠信與道德價值之期望，明確訂定於企業之行為準則，並使企業所有階層與外包服務提供者及商業合作夥伴瞭解。

2.1.3 評估行為準則之遵循情形

建立各種流程，以評估個人與團隊遵循企業行為準則之表現。

#### 2.1.4 及時處理與規定不符之行為

以及時且一致之方式，辨識與補救偏離企業行為準則之情形。

### 2.2 董事會對於內部控制制度之設計及執行，行使獨立之監督權，並定期評估其成效。

#### 2.2.1 建立監督責任

董事會應辨識及接受各界對其之要求與期望，建立監督責任。

#### 2.2.2 運用攸關之專長

董事會宜明文規定、維持及定期評估董事會成員所需之知識與技能，俾使其能向高階管理階層提出追根究柢之問題，並採取對應行動。

#### 2.2.3 獨立運作

董事會應擁有足夠之成員，其獨立於管理階層，並可客觀進行評估與制定決策。

#### 2.2.4 對內部控制制度進行監督

董事會對於管理階層所設計及執行之內部控制制度維持監督責任：

- (1).控制環境：要求管理階層負責建立誠信與道德價值、監督架構、職權與責任、能力之期望及課責性<sup>2</sup>。
- (2).風險評估：監督管理階層對目標達成之風險評估能力，包括重大改變、舞弊及管理階層逾越內部控制之潛在影響。
- (3).控制作業：監督高階管理階層設計及執行控制作業。
- (4).資訊與溝通：分析及討論與企業達成目標相關之資訊。
- (5).監督作業：評估與監督有關監督作業之性質及範圍、管理階

---

<sup>2</sup>課責性：賦予其責任並檢視是否落實

層之評估及缺失改善。

2.3 管理階層在董事會監督下，建立企業達成各目標之組織結構、呈報體系，及適當權限與責任。

2.3.1 考量企業之所有組織結構

管理階層與董事會宜考量支持各目標達成之組織結構（包括企業個別單位、企業整體、銷售通路及外包服務提供者）。

2.3.2 建立呈報體系

管理階層設計及評估企業架構之呈報體系，以促成職權與責任之行使，及加速企業活動管理資訊系統之運作。

2.3.3 定義、分派及限制職權與責任

管理階層與董事會授予職權、界定責任，及利用適當之程序與科技以分派責任，且於企業不同層級進行必要之職能分工：

- (1).董事會：保留制定重要決策之權力，並複核管理階層對於職權與責任之分派及限制。
- (2).高階管理階層：建立指令、指引與控制，以促使管理階層及其他人員瞭解並履行其內部控制之責任。
- (3).管理階層：引導及幫助企業及其下屬單位之員工執行高階管理階層之指令。
- (4).員工：瞭解企業之行為準則、達成目標之風險、企業個別層級有關之控制作業、預期之資訊與溝通，及與達成目標相關之監督作業。

2.4 企業為配合目標之達成，應延攬、培養及留用有能力之人才。

2.4.1 建立政策與實務

政策與實務宜反映達成目標所需能力之期望。

2.4.2 評估能力及提出缺點

評估企業及外包服務提供者執行既定政策與實務運作之能力；如有缺點，亦須提出。

#### 2.4.3 延攬、培養及留用人才

提供指導與訓練，延攬、培養及留用足夠有能力之人才與外包服務提供者，以支持其達成目標。

#### 2.4.4 規劃及準備接班人選

對於內部控制之主要負責人員，訂定接班人計畫。

### 2.5 要求個人對內部控制負責以達成目標。

#### 2.5.1 透過結構及權責強化課責性

建立機制溝通及要求各級人員對內部控制之執行負責，並採取必要之改善。

#### 2.5.2 建立績效衡量指標、誘因與獎勵措施

管理階層與董事會建立適合於企業所有階層之績效衡量指標、誘因與其他獎勵措施，以適當反映各層面績效及行為準則，並考量短期與長期目標之達成。

#### 2.5.3 評估績效衡量指標、誘因及獎勵措施與達成目標之持續攸關性

管理階層與董事會將各種誘因及獎勵措施，與達成目標之內部控制責任密切配合。

#### 2.5.4 考量壓力是否過大

管理階層與董事會宜於分派職責、訂定績效衡量指標及評估績效時，評估及調整與達成目標有關之壓力。

#### 2.5.5 評估績效及獎懲個人

管理階層與董事會宜評估內部控制執行之責任，包括遵循行為準則及期望之能力水準，並適當給與獎勵或懲處。

### 3. 風險評估

3.1 企業明確界定目標，以辨識及評估與目標相關之風險。

#### 3.1.1 遵循適當之會計準則

財務報導目標應與企業所適用之會計原則一致，企業應依經營情況選擇適當之會計原則。

#### 3.1.2 考慮重大性

管理階層應考慮財務報表表達之重大性，並訂定重大性判斷原則。

#### 3.1.3 反映企業活動

外部報導應反映顯示交易與事件之特性及聲明。

3.2 企業辨識其達成整體目標之風險，並分析各項風險，以作為決定執行風險管理之基礎。

#### 3.2.1 風險評估涵蓋企業、子公司、部門、營運及其他單位

企業辨識及評估風險時，範圍涵蓋與達成目標攸關之企業、子公司、部門、營運及其他單位之風險。

#### 3.2.2 分析內部及外部因素

企業於風險辨識時，同時考量內部與外部因素，及其對達成目標之影響。

#### 3.2.3 適當之管理階層參與

企業建立有效之風險評估機制，包括適當管理階層之參與。

#### 3.2.4 評估已辨識風險之重大性

已辨識風險係透過風險分析過程所產生之結果，包括評估該風險之潛在重大性。

#### 3.2.5 決定如何回應風險

風險評估包括考量如何管理風險，及是否接受、規避、降低或分擔風險。

3.3 企業評估達成目標之風險時，應考量可能發生之舞弊。

3.3.1 考量各種舞弊類型

評估舞弊需考量不實報導、可能之資產損失，及從舞弊與不當行為所導致之貪腐。

3.3.2 評估誘因與壓力

評估舞弊風險宜考量誘因與壓力。

3.3.3 評估機會

舞弊風險之評估宜考量未經授權取得、使用或處分資產，竄改企業報導紀錄，或從事其他不當行為等之機會。

3.3.4 評估態度與合理化

舞弊風險之評估宜考量管理階層及其他人員從事或合理化其不當行為。

3.4 企業辨識及評估可能對內部控制制度產生重大影響之各項改變。

3.4.1 評估外部環境之改變

風險辨識需考量法令、經濟及當地實質環境之改變。

3.4.2 評估商業模式之改變

企業考量其新業務、現行業務之重大改變、取得或分割之業務、對外國地區之依賴程度及新科技之潛在影響，調整其內部控制制度。

3.4.3 評估管理階層之變動

企業宜考量管理階層之變動，對內部控制制度態度與哲學之改變。

## 4. 控制作業

4.1 企業選擇及建立控制作業，以降低達成目標之風險至可接受水準。

4.1.1 整合風險評估



控制作業有助於確保處理及降低風險之回應措施能落實執行。

#### 4.1.2 考量企業之特定因素

管理階層選擇及建立控制作業，考量企業之經營環境、複雜性、營運性質與範圍，及企業之特性。

#### 4.1.3 決定攸關之業務流程

管理階層決定需制定控制作業之攸關業務流程。

#### 4.1.4 評估控制作業類型之組合

控制作業包括作業範圍之各類控制，其可能採用一種或數種方法以降低風險，如同時考量人工化及自動化控制、預防與偵測控制。

#### 4.1.5 考量各作業適用於不同階層

管理階層應考量企業內不同階層之控制作業。

#### 4.1.6 強調職能分工

管理階層針對不相容或不適當之職能分工，應選擇及建立替代性之控制作業。

### 4.2 企業運用科技選擇及建立一般控制作業，以支持目標之達成。

#### 4.2.1 決定業務流程使用科技與科技一般控制間之依賴性

管理階層瞭解並判斷業務流程、自動化控制作業、科技一般控制三者間之依賴性及關聯性。

#### 4.2.2 建立與科技基礎架構有關之控制作業

管理階層選擇、建立及執行科技基礎架構之控制作業，以確保科技處理之完整性、正確性與可用性。

#### 4.2.3 建立與安全管理過程有關之控制作業

管理階層選擇、建立及執行控制作業，用於限制科技使用者之權限時，使用者之權限與其工作職責需相符，以保護企業之資產免受外部威脅。

#### 4.2.4 建立與科技購置、發展及維護過程有關之控制作業

管理階層選擇、建立及執行購置、發展及維護科技之控制作業與基礎架構，以達成管理階層訂定之目標。

#### 4.3 企業透過所建立之政策及程序，建置其控制作業。

##### 4.3.1 建立政策與程序，以支持管理階層之指令

管理階層透過建立之政策與程序，建置業務流程及員工例行活動之控制作業。

##### 4.3.2 確立執行政策與程序之責任及課責性<sup>2</sup>

管理階層對於風險所在之業務單位管理者（或其他指定人員）之控制作業，確立其責任及課責性<sup>2</sup>。

##### 4.3.3 及時執行

負責人員依政策與程序規定，及時執行控制作業。

##### 4.3.4 採取改善行動

權責人員因執行控制作業發現缺失，應立即調查並追蹤改善。

##### 4.3.5 指派適任人員執行

由充分授權之適任人員持續專注並盡責執行控制作業。

##### 4.3.6 重新評估政策與程序

管理階層定期複核控制作業，以確認其持續攸關，並於必要時更新。

## 5. 資訊與溝通

#### 5.1 企業蒐集、產生及使用攸關且具品質之資訊，以支持內部控制制度之持續運作。

##### 5.1.1 辨識需要之資訊

以適當流程辨識需要之資訊，支持內部控制制度其他組成要素之運作及企業目標之達成。

---

<sup>2</sup>課責性：賦予其責任並檢視是否落實

#### 5.1.2 擷取內部與外部之資料來源

資訊系統能擷取內部與外部之資料來源。

#### 5.1.3 處理攸關資料成為資訊

資訊系統處理及轉換攸關資料成為資訊。

#### 5.1.4 維持處理過程之品質

資訊系統產生之資訊係及時、最新、正確、完整、可取得、受保護，及可證實與保存。資訊需經複核以評估其在支持內部控制制度組成要素方面具攸關性。

#### 5.1.5 考量成本與效益

溝通資訊之性質、數量與精確度符合成本效益原則，並支持目標之達成。

### 5.2 企業內部溝通之資訊須支持內部控制之運作，前揭資訊包括內部控制之目標與責任。

#### 5.2.1 溝通內部控制資訊

訂定資訊溝通之流程，使所有人員瞭解並履行其內部控制責任。

#### 5.2.2 與董事會溝通

管理階層與董事會進行溝通，使雙方取得所需資訊，以履行其對於企業目標之責任。

#### 5.2.3 提供個別之內部溝通方式

設置個別之溝通管道（如舉報熱線），當正常管道失效或無效時，可啟用匿名或保密之溝通方式。

#### 5.2.4 選擇攸關之內部溝通方式

溝通方式須考量時機、對象及資訊之性質。

### 5.3 企業與外部人士溝通影響內部控制持續運作之相關事項。

#### 5.3.1 建立由內向外之溝通

訂定與外部人士溝通攸關且及時資訊之程序，對象包括股

東、合作夥伴、業主、主管機關、客戶、金融分析師及其他外部人士。

### 5.3.2 建立由外向內之溝通

公開溝通管道，允許來自客戶、消費者、供應商、外部審計人員、主管機關、金融分析師，及其他人士之建議，提供管理階層與董事會相關資訊。

### 5.3.3 外部意見提報董事會

來自外部人士之評估意見，提董事會進行報告。

### 5.3.4 提供個別之外部溝通方式

設置個別之溝通管道（如舉報熱線），當正常管道失效或無效時，可啟用匿名或保密之溝通方式。

### 5.3.5 選擇攸關之外部溝通方式

溝通方式須考量時機、對象、溝通性質，及符合法律、規章、與誠信之要求及期望。

## 6. 監督作業

### 6.1 企業選擇、建立及執行持續性或個別評估，以確定內部控制制度組成要素是否已經存在及持續運作。

#### 6.1.1 考量持續性及個別評估之組合

管理階層平衡運用持續性及個別評估。

#### 6.1.2 考量變動情形

管理階層選擇及建立持續性及個別評估，需考量業務及業務流程之變動情形。

#### 6.1.3 建立基準

以內部控制制度之設計及現況，作為建立持續性及個別評估之基準。

#### 6.1.4 任用有經驗人員

執行持續性及個別評估之人員，須具備充分知識及瞭解被評

估之事項。

#### 6.1.5 整合業務流程

持續性評估與業務流程結合，並隨環境變化調整。

#### 6.1.6 調整範圍與頻率

管理階層依據風險高低調整個別評估之範圍與頻率。

#### 6.1.7 客觀評估

定期執行個別評估，以提供客觀之回饋。

### 6.2 企業及時評估內部控制制度缺失，並與負責採取改善行動者溝通，包括向高階管理階層及董事會報告。

#### 6.2.1 評估結果

管理階層、董事會及其他適當人員妥善分析處理持續性及個別評估之結果。

#### 6.2.2 溝通缺失

向負責採取改善行動者、高階管理階層、董事會等適當人員溝通所發現之缺失。

#### 6.2.3 監督改善行動

管理階層追蹤缺失是否於時效內改善。