「上市上櫃公司風險管理實務守則」總說明

鑒於企業經營所面臨之風險日益複雜，為協助企業辨識未來可能產生之挑戰並適當因應，以健全企業穩健經營，經參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018及我國金融保險業之「風險管理實務守則」等規定訂定本守則，俾供上市上櫃公司遵循辦理，以符合國際潮流。

本守則共計二十九條，要點臚列如下：

一、本守則訂定目的。(第一條)

二、明訂企業風險管理目標。(第二條)

三、明訂企業風險管理原則。(第三條)

四、為落實政策，企業應訂定風險管理政策與程序及訂定時應注意事項。(第四條)

五、企業風險管理政策與程序之審查、施行及揭露規範。(第五條)

六、企業推動風險管理相關作為，應建置完善的風險治理與管理架構。(第六條)

七、明訂強化企業風險文化之可實施具體作為。(第七條)

八、明訂企業風險治理與管理單位之資源提供與協調整合職責。(第八、九條)

九、明訂企業風險管理組織架構之組成原則及相關職責角色。(第十條至第十六條)

十、明訂風險管理程序步驟及其作法。(第十七條至第二十五條)

十一、為落實推動企業風險管理，明訂公司應針對風險管理執行之過程及其結果適當記錄，並建立相關報導機制，以協助高階管理階層和治理單位進行相關風險決策，並履行其風險管理職責。(第二十六、二十七條)

十二、為落實推動企業風險管理，明訂公司應強化企業執行風險管理相關資訊之揭露。(第二十八條)

十三、明訂企業應隨時注意國內外規範發展，並據以檢討修正其風險管理機制。(第二十九條)

上市上櫃公司風險管理實務守則

條　　文	說　　明
第一章　總則 第一條（訂定目的） 為協助上市上櫃公司建立完善之風險管理制度，穩健經營業務朝企業永續發展目標邁進，臺灣證券交易所股份有限公司及財團法人中華民國證券櫃檯買賣中心爰共同制定本守則，以資遵循。 上市上櫃公司宜參照本守則相關規定訂定公司本身之風險管理政策與程序，以強化風險管理制度。	為協助公司建立完善之風險管理制度，並健全穩健經營，爰訂定本守則，並鼓勵上市上櫃公司參照訂定風險管理政策與程序。
第二條（企業風險管理目標） 企業風險管理之目標旨在透過完善的風險管理架構，考量可能影響企業目標達成之各類風險加以管理，並透過將風險管理融入營運活動及日常管理過程，達成以下目標： 一、實現企業目標； 二、提升管理效能； 三、提供可靠資訊； 四、有效分配資源。	參考國際企業風險管理相關規範 COSO ERM 2017、ISO 31000:2018，及我國「行政院及所屬機關風險管理及危機處理作業手冊」，明訂企業風險管理目標。
第三條（企業風險管理原則） 上市上櫃公司建立風險管理制度，宜依下列原則為之： 一、整合性：將風險管理視為所有活動的一部分。 二、結構化和全面性：以結構化和全面性的方式推動風險管理，獲得一致且具可比較性的結果。 三、客製化：依據企業所屬環境、規模、業務特性、風險性質與營運活動，制定適切的風險管理框架與流程。 四、包容性：將利害關係者的需求與期望納入考量，提高並滿足利害關係者對企業風險管理的	參酌國際企業風險管理規範 ISO 31000:2018 提出之八大風險管理原則，明訂企業於規劃風險管理架構及相關管理程序之核心原則。

條　　文	說　　明
瞭解與期待。 五、動態：適當並及時預測、監控、掌握和回應企業內部和外部環境的變化。 六、有效資訊利用：依據歷史、當前的資訊及未來趨勢，作為建構風險管理的基礎，並將資訊及時、清晰地提供利害關係人參考。 七、人員與文化：提升治理與管理單位對風險管理之重視程度，並透過各層級人員完善的風險管理相關培訓機制，提升企業整體之風險意識與文化，將風險管理視為公司治理與日常作業的一部分。 八、持續改進：透過學習與經驗，不斷改善風險管理與相關作業流程。	
第四條（建立風險管理政策與程序） 上市上櫃公司應考量公司及其子公司整體之規模、業務特性、風險性質與營運活動，訂定適用之風險管理政策與程序，並至少涵蓋以下項目： 一、風險管理目標； 二、風險治理與文化； 三、風險管理組織架構與職責； 四、風險管理程序； 五、風險報導與揭露。 上述風險管理政策與程序應依據公司內、外在環境之變遷隨時檢討，俾確保該制度之設計與執行持續有效。	參酌國際企業風險管理規範 COSO ERM 2017、ISO 31000:2018、我國金融保險業之「風險管理實務守則」，及「行政院及所屬機關風險管理及危機處理作業手冊」規範，為落實推動風險管理，明訂企業應訂定風險管理政策與程序，並說明應規範項目及注意事項。
第五條（風險管理政策與程序之審查與施行） 公司訂定之風險管理政策與程序應由公司指派之風險治理單位進行審查，並經董事會核定後實施。 相關政策與程序應於公司網站或公開資訊觀測站中進行揭露。	參酌我國金融保險業之「風險管理實務守則」規範，為確保風險管理政策與程序相關內容之適切性及有效性，明訂風險管理政策與程序之審查及施行規範，並要求揭露相關資訊提供利害關係者參考，以強化企業資訊揭露內容。

條　　文	說　　明
第二章　風險治理與文化 第六條（建置完善的風險治理與管理架構） 上市上櫃公司宜考量公司規模、業務特性、風險性質與營運活動,建置完善的風險治理與管理架構,透過董事會、功能性委員會及高階管理階層的參與,使風險管理與公司之策略、目標產生連結,定調公司重大風險項目,提升風險辨識結果之全面性、前瞻性與完整性,並向下宣導及展開對應之風險控管與因應,以合理確保公司策略目標之達成。	參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018,及我國金融保險業之「風險管理實務守則」,完善的風險治理與管理架構是確保企業風險管理落實與發揮功效的基石,爰明訂企業應建置完善的風險治理與管理架構,以落實推動企業風險管理之執行。
第七條（深化風險文化） 上市上櫃公司宜推動由上而下的風險管理文化,透過治理單位與高階管理階層明確的風險管理聲明與承諾、設置並支持風險管理單位、提供全體員工風險管理相關專業訓練等方式,將風險管理意識融入至日常決策及營運活動中,形塑全方位的企業風險管理文化。	參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018,及我國金融保險業之「風險管理實務守則」,風險文化為企業是否能有效推動並發揮風險管理之關鍵要素,爰明訂企業強化風險文化之可實施具體作為。
第八條（提供足夠資源與支持） 上市上櫃公司之風險治理與管理單位應重視與支持風險管理,提供適切資源使其有效運作,並對風險管理有效運作負責。	參酌國際企業風險管理規範 ISO 31000:2018,明訂風險治理與管理單位應確保分配足夠必要之資源,使風險管理有效運作。
第九條（整合與協調） 上市上櫃公司推動風險管理應整合公司內各單位職責,全體共同推動執行,透過各單位間之溝通、協調與聯繫,落實整體業務之風險管理。	參酌國際企業風險管理規範 ISO 31000:2018,風險管理為所有企業活動的一部分,執行風險管理應依據組織結構、目標、複雜性、各單位職責進行整合以落實整體業務之風險管理目標。
第三章　風險管理組織架構與職責 第十條（風險管理組織架構） 上市上櫃公司除以董事會作為風險管理最高治	為確保風險管理之落實,明訂公司應建立完善之風險管理組織架構,包含治理單位、風險管理委員會及推動與執行單位,並明訂各單

條　　文	說　　明
理單位外，得考量公司規模、業務特性、風險性質與營運活動，設置隸屬於董事會之風險管理委員會，並指派適當風險管理推動與執行單位。	位之職責角色。
第十一條（設置風險管理委員會） 上市上櫃公司為健全與強化風險管理機能，宜考量公司規模、業務特性、風險性質與營運活動，設置隸屬於董事會之風險管理委員會，進行風險管理相關運作機制之監督，且該委員會過半數成員宜由獨立董事擔任，並由獨立董事擔任主席。 風險管理委員會應對董事會負責，並將所提議案交由董事會決議。 風險管理委員會應訂定組織規程，並經由董事會決議通過。組織規程之內容應包括委員會之人數、任期、職權事項、議事規則、行使職權時公司應提供之資源等事項。 上市上櫃公司亦得考量其規模大小，以其他功能性委員會或工作小組形式，替代風險管理委員會之職能。	明訂風險管理委員會之設置及組成原則。
第十二條（設置風險管理推動與執行單位） 上市上櫃公司應指定或設置適當的風險管理推動與執行單位，負責規劃、執行與監督風險管理相關事務。該單位得考量公司規模、業務特性、風險性質與營運活動，指派專責單位或以任務編組方式組成。	明訂風險管理推動與執行單位之設置及組成原則。
第十三條（董事會之職責角色） 董事會之職責角色如下： 一、核定風險管理政策、程序與架構； 二、確保營運策略方向與風險管理政策一致； 三、確保已建立適當之風險管理機制與風險管理文化； 四、監督並確保整體風險管理機制之有效運作；	明訂董事會於企業風險管理中之職責角色。

條　　文	說　　明
五、分配與指派充足且適當之資源，使風險管理有效運作；	
第十四條（風險管理委員會之職責角色） 風險管理委員會之職責角色如下： 一、審查風險管理政策、程序與架構，並定期檢討其適用性與執行效能； 二、核定風險胃納(風險容忍度)，導引資源分配； 三、確保風險管理機制能充分處理公司所面臨之風險，並融合至日常營運作業流程中； 四、核定風險控管的優先順序與風險等級； 五、審查風險管理執行情形，提出必要之改善建議，並定期(至少一年一次)向董事會報告； 六、執行董事會之風險管理決策。	明訂風險管理委員會於企業風險管理中之職責角色。
第十五條（風險管理推動與執行單位之職責角色） 風險管理推動與執行單位之職責角色如下： 一、擬訂風險管理政策、程序與架構； 二、擬訂風險胃納(風險容忍度)，並建立質化與量化之量測標準； 三、分析與辨識公司風險來源與類別，並定期檢討其適用性； 四、定期(至少一年一次)彙整並提報公司風險管理執行情形報告； 五、協助與監督各部門風險管理活動之執行； 六、協調風險管理運作之跨部門互動與溝通； 七、執行風險管理委員會之風險管理決策； 八、規劃風險管理相關訓練，提升整體風險意識與文化。	明訂風險管理推動與執行單位於企業風險管理中之職責角色。

條　　文	說　　明
第十六條（營運單位之職責角色） 各營運單位之職責角色如下： 一、負責所屬單位之風險辨識、分析、評量與回應，並於必要時建立相關危機管理機制； 二、定期提報風險管理資訊予風險管理推動與執行單位； 三、確保所屬單位風險管理及相關控制程序有效執行，以符合風險管理政策。	明訂各營運單位於企業風險管理中之職責角色。
第四章　風險管理程序 第十七條（風險管理程序） 風險管理政策應包含風險管理程序，且風險管理程序應至少包含：風險辨識、風險分析、風險評量、風險回應，及監督與審查機制五大要素，並載明各要素實際執行之程序與方法。	參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018，及我國金融保險業之「風險管理實務守則」，明訂風險管理程序應涵蓋項目。
第十八條（分析與辨識公司風險來源與類別） 風險來源與類別一般可歸納為以下構面，主要包含：策略風險、營運風險、財務風險、資訊風險、法遵風險、誠信風險、其他新興風險(如：氣候變遷或傳染病相關風險)等。 風險管理推動與執行單位宜依據公司規模、所屬產業、業務特性、營運活動，並考量企業永續（含氣候變遷)各面向規範重點進行全方位風險分析，分析與辨識公司適用之風險來源與類別，定義公司自身之風險類別，針對各風險類別展開相關細部風險情境辨識，並定期檢討其適用性。	為協助企業以系統化之方式對各風險類別進行通盤的思考及分析，明訂企業於分析與辨識風險時可考量之風險類別，並應將企業永續面向納入考量。

條　　文	說　　明
第十九條（風險辨識） 各營運單位應依據公司策略目標及董事會核定之風險管理政策與程序，就其所屬單位之短、中、長程目標與業務執掌進行風險辨識。 風險辨識宜採用各種可行之分析工具及方法(如：流程分析、情境分析、問卷調查、PESTLE 分析等)，依據以往經驗及資訊，並考量內、外部風險因子、利害關係者關注重點等，透過「由下而上」及「由上而下」的分析討論，結合策略風險與營運風險，全面辨識可能導致公司目標無法達成、造成公司損失或負面影響之潛在風險事件。	參酌國際企業風險管理相關規範 COSO ERM 2017 及 ISO 31000:2018，明訂企業執行風險辨識之相關程序及方法。
第二十條（風險分析） 風險分析主要係針對已辨識風險事件之性質及特徵進行瞭解，並分析其發生機率及影響程度，據以計算風險值。 各營運單位應針對已辨識出之風險事件，考量現有相關管控措施之完整性、過往經驗、同業案例等，分析風險事件之發生機率與影響程度，據以計算風險值。	參酌國際企業風險管理相關規範 COSO ERM 2017 及 ISO 31000:2018，明訂企業執行風險分析之相關程序方法。
第二十一條（風險分析量測標準） 風險管理推動與執行單位宜依據公司風險特性擬訂適切的量化或質化量測標準，作為風險分析之依據。 質化之量測標準係指透過文字描述，表達風險事件之發生機率及影響程度；量化之量測標準則係指透過具體可計算之數值指標(如：天數、百分比、金額、人數等)，表達風險事件之發生機率與影響程度。	為協助企業針對已辨識出之風險發生的可能性及所產生之負面衝擊程度進行分析，參酌國際企業風險管理相關規範 COSO ERM 2017 及 ISO 31000:2018，明訂企業宜擬訂風險分析相關量測標準，做為評估風險等級之準則依據，以協助企業了解各項風險之排序及可能造成之影響。
第二十二條（風險胃納） 風險管理推動與執行單位宜擬訂風險胃納(風	參酌國際企業風險管理相關規範 COSO ERM 2017、ISO 31000:2018，及我國金融保險業之「風險管理實

條　　文	說　　明
險容忍度)，提報風險管理委員會進行核定，以決定公司可承受之風險限額。並依據風險胃納研議各風險值對應之風險等級，及各風險等級之風險回應方式，作為後續風險評量及風險回應之依據。	務守則」，明訂企業宜依據組織整體願意接受之風險程度擬訂風險胃納，及相應的風險管理策略。
第二十三條（風險評量） 風險評量的目的是提供企業作為決策之依據，透過將風險分析結果與風險胃納加以比對，決定需優先處理之風險事件，並作為後續擬訂回應措施選擇之參考依據。 各營運單位應依據風險分析結果，對照經風險管理委員會核定之風險胃納，依據風險等級規劃與執行後續風險回應方案。 相關風險分析與評量結果應確實記錄，並提報風險管理委員會進行核定。	參酌國際企業風險管理相關規範COSO ERM 2017及ISO 31000:2018，明訂企業執行風險評量之相關程序方法，及應考量與注意事項。
第二十四條（風險回應） 針對風險回應應訂定相關處理計畫，確保相關人員充分理解與執行，並持續監控相關處理計劃之執行情形。 企業應考量企業策略目標、內、外部利害關係人觀點、風險胃納及可用資源，來擇定風險回應方式，使風險回應方案在實現目標與成本效益之間取得平衡。	參酌國際企業風險管理相關規範COSO ERM 2017及ISO 31000:2018，說明企業執行風險回應之相關程序方法，及應考量與注意事項。
第二十五條（風險監督與審查） 風險監督與審查機制應於風險管理程序中明確定義，以確實審查風險管理流程及相關風險對策是否持續有效運作，並將相關審查結果納入績效衡量與報告事項中。 風險管理應與組織中關鍵流程進行連結，以有	參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018，明訂企業執行風險監督與審查之相關程序方法，及應考量與注意事項。

條　　文	說　　明
效監督與提升風險管理落實實施之效益。	
第五章　風險報導與揭露 第二十六條（風險紀錄） 風險管理執行之過程及其結果均應通過適當的機制進行紀錄、審查與報告，並妥善留存備查，包含風險管理流程中之風險辨識、風險分析、風險評量、風險回應措施、相關資訊來源及風險評估結果等。	參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018，及我國金融保險業之「風險管理實務守則」，明訂企業實施風險管理之相關文件應予文件化保存備查。
第二十七條（風險報導） 風險報導為公司治理中不可或缺的一部分，宜考量不同利害關係者及其特定的資訊需求和要求、報導的頻率與時效性、報導方法、資訊與組織目標和決策的相關性，以協助高階管理階層和治理單位進行相關風險決策並履行其風險管理職責。 風險管理推動與執行單位應彙整各單位所提供之風險資訊，定期出具風險管理相關報告予風險管理委員會及董事會，並建置動態管理與報導機制，以確實督導風險管理之有效執行。	參酌國際企業風險管理相關規範COSO ERM 2017、ISO 31000:2018，及我國金融保險業之「風險管理實務守則」，明訂企業宜規劃完善的風險報導流程與內容，以協助高階管理階層和治理單位進行相關風險決策並履行其風險管理職責。
第二十八條（資訊揭露） 上市上櫃公司應於公司網站或公開資訊觀測站中揭露下列風險管理相關資訊，提供外部利害關係人參考，並持續更新。 具體應揭露項目包含： 一、風險管理政策與程序； 二、風險治理與管理組織架構； 三、風險管理運作與執行情形(包含向董事會及委員會報告之頻率與日期)。	為強化企業風險管理資訊之揭露，爰明訂公司應揭露其風險管理相關資訊。
第六章　附則 第二十九條（注意國內外發展） 上市上櫃公司應隨時注意國內與國際企業風	推動完善之風險管理為國際趨勢，明訂公司應隨時注意國內外風險管理相關規範之發展，據以檢討

條　　文	說　　明
險管理機制之發展，據以檢討改進公司所建置之風險管理架構，以提升公司治理成效。	改進公司訂定之風險管理架構。