

保險業風險管理實務守則問答手冊修訂對照表

金管會 110 年 1 月 7 日金管保財字第 1090150432 號函同意備查

修訂條文	原條文	說明
<p><u>Q5.18 :</u></p> <p><u>本守則 5.4.2_11 所稱營運持續管理為何?董事會與內部稽核單位於營運持續管理之角色與職責為何?</u></p> <p><u>A :</u></p> <p><u>一、營運持續管理係指監督和落實營運韌性、持續性及對重大事件的因應能力，以保障員工、客戶的權益及公司產品與服務的管理程序。</u></p> <p><u>上述之營運韌性意指做好準備以適應不斷變化的環境及抵禦業務中斷並快速恢復的能力。</u></p> <p><u>二、董事會於營運持續管理之角色與職責，係依據本守則 3.2.1_1 辦理。</u></p> <p><u>三、稽核單位應查核及評估營運持續管理機制是否有效運作，適時提供改進建議，並列入定期查核範圍。</u></p>	NA	<p>一、 配合風險管理實務守則修訂，具體說明營運持續管理之內容。資料參考來源：美國聯邦金融檢查委員會之營運持續管理手冊 -FFIEC Information Technology Examination Handbook Business Continuity Management (https://ithandbook.ffiec.gov/it-bookslets/business-continuity-management.aspx):</p> <p>APPENDIX B – GLOSSARY</p> <ul style="list-style-type: none"> ● Business continuity management (BCM) : The process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services. ● Resilience: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. <p>二、 說明董事會與內部稽核單位之角色與職責，彰顯營運持續管理與內部控制及公司治理之連結關係。</p>

		<p>資料參考來源：</p> <p>(一) 保險業內部控制及稽核制度 實施辦法第 3 條、第 9 條； 保險業公司治理實務守則第 3 條。</p> <p>(二) 澳洲審慎監理總署 (Australian Prudential Regulation Authority, APRA) 之營運持續管理法令規定 (Prudential Standard CPS 232 Business Continuity Management) ... review the business continuity plan annually and periodically arrange for its review by the internal audit function or an appropriate external expert;</p> <p>(三) 美國聯邦金融檢查委員會之 營運持續管理手冊內關於董 事會和稽核單位之職責描 述： Page 5-7 Board oversight should include:</p> <ul style="list-style-type: none"> ● Assigning BCM responsibility and accountability. ● Allocating resources to BCM. ● Aligning BCM with the entity's business strategy and risk appetite. ● Reviewing business continuity operating results and performance through management reporting, testing, and auditing.
--	--	---

		<p>The board and senior management should engage internal audit (or an independent review) to assess the BCM design effectiveness, including policies and procedures, and the effectiveness of controls. Audit should report to the board and provide an assessment of management's ability to oversee and control risks related to continuity and resilience.</p> <p>Auditors should:</p> <ul style="list-style-type: none">● Evaluate the business impact analysis (BIA) and risk assessment for reasonableness, identification of critical functions, and the likelihood of different events and the potential impact on operations.● Evaluate controls for reliability, adequacy, and effectiveness regarding continuity and resilience.● Leverage SOC reports and other external artifacts from third-party service providers, as appropriate.● Compare the entity's inherent risk level and the effectiveness of risk mitigation against the entity's risk appetite.
--	--	---

		<ul style="list-style-type: none"> ● Verify whether test plans achieve the stated objectives. ● Monitor BCM testing to verify that issues (e.g., deviation from test plans and failed objectives) are appropriately identified and escalated. ● Assess the BCM program's effectiveness.
<p><u>Q5.19 :</u></p> <p><u>本守則所稱營運持續管理機制，具體應如何建立？</u></p> <p><u>A :</u></p> <p><u>營運持續管理機制之建立，除參考產壽險公會共擬之「保險業營運持續管理或緊急應變相關因應措施」或美國聯邦金融檢查委員會之營運持續管理手冊(FFIEC Information Technology Examination Handbook - Business Continuity Management)以外，亦可參考本國中央流行疫情指揮中心編訂之「企業因應嚴重特殊傳染性肺炎(COVID-19)疫情持續營運指引」以及該指引中所提到之「中小企業持續營運教戰手冊」。</u></p> <p><u>另可參酌以下所列之訂定方法，實際做法仍需視各公司狀況而訂。</u></p> <p><u>步驟 1. 發展營運衝擊分析 (Business impact analysis, BIA)，其中包含：</u></p> <p><u>a) 辨識所有業務之功能及其重要性</u></p>	<p>NA</p>	<p>參考美國聯邦金融檢查委員會之營運持續管理手冊提供建立營運持續管理機制之參考步驟。</p> <p>一、Page 9</p> <p>Management should develop a BIA that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies among business processes and systems, and assesses a disruption's impact through established metrics. The BIA should define recovery priorities and resource dependencies for critical processes.</p> <p>二、Page 3</p> <p>Conduct a risk assessment to identify risks and evaluate likelihood and impact of disruptions.</p> <p>三、Page 16</p> <p>Management should establish recovery objectives after determining a disruption's impact.</p> <p>另參考澳洲審慎監理總署</p>

b)分析各業務流程和各系統之間的相互依賴關係

c)評估業務中斷之衝擊

d)確認各項業務之恢復優先順序及關鍵業務運作所仰賴之資源

步驟 2. 辨識風險及評估風險事件導致業務中斷之可能性及影響程度。

風險事件例如：天災；流行疫病；軟體、電力或通訊系統失靈；惡意的人為活動（詐欺、竊盜、蓄意破壞、網路攻擊）；恐怖攻擊。

步驟 3. 考量公司之經營策略及營運目標後，訂定適當之營運中斷復原目標以反映公司整體所願意接受之營運中斷風險程度。

步驟 4. 依據上述步驟之結果，發展營運持續策略並建立營運持續計畫 (Business Continuity Plan)，其中包含應變機制和營運恢復之程序。

步驟 5. 就相關人員舉辦營運持續之教育訓練。

步驟 6. 執行演練及辦理測試，以確認各項步驟能達成預設的營運持續目標。

步驟 7. 定期檢視及更新營運持續計畫。

步驟 8. 營運持續管理機制之監控

(Australian Prudential Regulation Authority, APRA)之營運持續管理法令規定 (Prudential Standard CPS 232 Business Continuity Management)第 28 條：Recovery objectives are pre-defined goals for recovering critical business operations to a specified level of service (recovery level) within a defined period (recovery time) following a disruption.

四、Page 26

The board and senior management should develop effective strategies to meet resilience and recovery objectives. Management should develop business continuity plan(s) (BCP) with sufficient detail in relation to the entity's size and complexity. The BCP should address key business needs and incorporate inputs from all business units.

另參考澳洲審慎監理總署 (Australian Prudential Regulation Authority, APRA)之營運持續管理法令規定 (Prudential Standard CPS 232 Business Continuity Management)第 31 條：31. The BCP must document procedures and information that enable the institution to:

- (a) manage an initial business disruption (crisis management); and
- (b) recover critical business operations.

五、Page 35

<p><u>與報告。</u></p>		<p>Management should implement a business continuity training program for all stakeholders.</p> <p>六、Page 37</p> <p>The board and senior management should provide for appropriate exercises and tests to verify that business continuity procedures support business continuity objectives.</p> <p>七、Page 47</p> <p>Because risks and technology often change, management should regularly review and update the business continuity program to reflect the current environment.</p> <p>八、Page 3、49</p> <p>Monitor and report business continuity and resilience activities.</p> <p>The board should establish expectations for management's business continuity reporting, regularly monitor business continuity and resilience activities, and provide credible challenges to management.</p>
<p>Q5.20： 作業風險因子及辨識方法有哪些？可考量之項目為何 (5.4.3)? A: ...</p>	<p>Q5.18： 作業風險因子及辨識方法有哪些？可考量之項目為何 (5.4.3)? A: ...</p>	<p>僅項次更動。</p>
<p>Q5.21： 作業風險衡量是否有範例供參 (5.4.4)? A: ...</p>	<p>Q5.19： 作業風險衡量是否有範例供參 (5.4.4)? A: ...</p>	<p>僅項次更動。</p>
<p>Q5.22：</p>	<p>Q5.20：</p>	<p>僅項次更動。</p>

<p>作業風險管理工具中有關風險及控制自評是否有範例供參 (5.4.5_2)?</p> <p>A: ...</p>	<p>作業風險管理工具中有關風險及控制自評是否有範例供參 (5.4.5_2)?</p> <p>A: ...</p>	
<p>Q5.23 : 請舉例說明何者可設定為作業風險之關鍵風險指標? 使用關鍵風險指標 (KRI) 應注意之要點為何 (5.4.5_3)?</p> <p>A: ...</p>	<p>Q5.21 : 請舉例說明何者可設定為作業風險之關鍵風險指標? 使用關鍵風險指標 (KRI) 應注意之要點為何 (5.4.5_3)?</p> <p>A: ...</p>	<p>僅項次更動。</p>
<p>Q5.24 : 本守則 5.5.1 提到保險業進行商品設計及定價風險衡量時,可參酌之衡量方法,區分了壽險業及產險業,但有些商品類型同時存在於產壽險業,其適用時是否僅須依各業範圍適用,而不考慮商品的性質?</p> <p>A: ...</p>	<p>Q5.22 : 本守則 5.5.1 提到保險業進行商品設計及定價風險衡量時,可參酌之衡量方法,區分了壽險業及產險業,但有些商品類型同時存在於產壽險業,其適用時是否僅須依各業範圍適用,而不考慮商品的性質?</p> <p>A: ...</p>	<p>僅項次更動。</p>
<p>Q5.25 : 「資產配置計畫」項下提及「對可能發生之不利情勢,應制定適當之應變方案」。應變方案可否舉例說明之。(5.5.1)</p> <p>A: ...</p>	<p>Q5.23 : 「資產配置計畫」項下提及「對可能發生之不利情勢,應制定適當之應變方案」。應變方案可否舉例說明之。(5.5.1)</p> <p>A: ...</p>	<p>僅項次更動。</p>
<p>Q5.26 : 就實務守則 5.5.2_3「為求有效維護承保業務品質及降低潛在核保風險,保險業應就所經營之各項保險業務,分別制定相關之核保手冊。…」,其中「核保手冊」是否為專門用語?</p> <p>A: ...</p>	<p>Q5.24 : 就實務守則 5.5.2_3「為求有效維護承保業務品質及降低潛在核保風險,保險業應就所經營之各項保險業務,分別制定相關之核保手冊。…」,其中「核保手冊」是否為專門用語?</p> <p>A: ...</p>	<p>僅項次更動。</p>
<p>Q5.27 : 有關保險業之核保風險管理指標之設定方法為何 (5.5.2)?</p>	<p>Q5.25 : 有關保險業之核保風險管理指標之設定方法為何 (5.5.2)?</p>	<p>僅項次更動。</p>

A: ...	A: ...	
Q5.28 : 產險業如何進行巨災風險評估 (5.5.4)? A: ...	Q5.26 : 產險業如何進行巨災風險評估 (5.5.4)? A: ...	僅項次更動。
Q5.29 : 何謂巨災風險累積效應及相關性 (5.5.4)? A: ...	Q5.27 : 何謂巨災風險累積效應及相關性 (5.5.4)? A: ...	僅項次更動。
Q5.30 : 如何訂定巨災關鍵風險指標 (5.5.4_6)? A: ...	Q5.28 : 如何訂定巨災關鍵風險指標 (5.5.4_6)? A: ...	僅項次更動。
Q5.31 : 保險業之理賠風險控管機制如何運作 (5.5.5)? A: ...	Q5.29 : 保險業之理賠風險控管機制如何運作 (5.5.5)? A: ...	僅項次更動。
Q5.32 : 保險業如何評估理賠風險 (5.5.5)? A: ...	Q5.30 : 保險業如何評估理賠風險 (5.5.5)? A: ...	僅項次更動。
Q5.33 : 產險業是否訂定資產負債配合風險管理機制 (5.6)? A: ...	Q5.31 : 產險業是否訂定資產負債配合風險管理機制 (5.6)? A: ...	僅項次更動。
Q5.34 : 可如何管理資產負債配合風險 (5.6)?保險業負債現金流量和資產現金流量如何評估(5.6.2)?有關資產負債管理衡量方法可否加以說明(5.6.3)? A: ...	Q5.32 : 可如何管理資產負債配合風險 (5.6)?保險業負債現金流量和資產現金流量如何評估 (5.6.2)?有關資產負債管理衡量方法可否加以說明(5.6.3)? A: ...	僅項次更動。
Q5.35 : 本守則 5.7 其他風險所指為何? A: ...	Q5.33 : 本守則 5.7 其他風險所指為何? A: ...	僅項次更動。

