

# 保險業建立風險導向內部稽核制度實務守則

金融監督管理委員會111年10月27日金管檢保字第11106101874號函核復修正後同意備查

## ( 依據 )

- 一、本實務守則係依據金融監督管理委員會111年10月27日金管檢保字第11106101871號令辦理。

## ( 目的 )

- 二、保險業實施風險導向內部稽核制度，係透過風險評估之方法，審慎評估稽核範疇內各個受查主體之風險，並依據評估結果決定稽核任務之查核重點、範圍、方法、稽核程序及查核頻率，將稽核資源做最有效的配置，聚焦於重要風險並加強查核深度，提升內部稽核執行效益，以有效協助保險業完善內部控制制度及強健企業體質。

## ( 風險導向內部稽核制度實施方法 )

- 三、為確保內部稽核之品質與有效性，保險業實施風險導向內部稽核制度，應具備明確之內部控制三道防線架構，內部稽核並應建立以下機制：
  - (一) 內部稽核風險評估之程序與方法。
  - (二) 內部稽核品質評核機制。

## ( 訂定風險評估程序 )

- 四、內部稽核應建立風險評估之程序與方法，以辨識並評估各受查主體所面臨之風險，並定期驗證風險評估因子或指標及各項控制措施之有效性。

## 五、確認風險評估範圍：

內部稽核應依據保險業所經營業務範圍及單位組織，以及主管機關法令規範，辨識應辦理風險評估之受查主體，以確保風險評估範圍能完整涵蓋保險業整體營運範疇。

內部稽核得以單位組織、產品、業務、作業流程或其他構面訂定受查主體。

## 六、風險評估因子與方法：

(一) 內部稽核應就各受查主體所面臨之固有風險、控制措施有效性進行評估後，確認受查主體之風險評估結果（即剩餘風險），並據以決定年度稽核計畫。所稱固有風險、控制措施與剩餘風險定義如下：

- 1.固有風險：在管理階層尚未採取任何行動來改變風險發生的可能性或其影響之情況下，達成目標之風險。
- 2.控制措施：管理階層為管理風險及增加達成既定目標之可能性，而採取之任何行動。管理階層負責規劃、組織及指揮執行足夠之行動，以合理保證目的及目標之達成。
- 3.剩餘風險：管理階層在設計及執行控制措施後，仍留下來無法達成組織目標之風險。

(二) 固有風險之評量：

- 1.內部稽核應依據所屬保險業之經營形態與發展策略目標，擬訂適合之固有風險評估因子。風險評估因子之訂定可參酌保險業風險管理實務守則所列舉之主要風險類型，並應描述評估各風險類型時應考量之因素（所述因素應能顯著代表各風險之表徵）。
- 2.依前項有關之固有風險因子，就受查主體發生風險事項之可能性與嚴重程度評估其固有風險：
  - 1) 發生可能性：評估風險事件在可預期的未來中發生之可能性。
  - 2) 嚴重程度：評估風險事件發生對財務、商譽及營運服務可能造成之影響。
  - 3) 依據前二項構面評估固有風險，評估結果至少應區分為高、中、低等三個風險等級。

(三) 控制措施有效性之評量：

- 1.以持續或個別評估的方式確認各受查主體之控制措施是否存在且發揮功效，並就控制措施設計及執行之有效性至少區分為高、中、低三個等級。
- 2.控制措施有效性評估至少應包含下列資訊：
  - 1) 主要業務之內部控制運作情形。

- 2) 外部檢查意見，包含主管機關、會計師、母公司稽核單位及其他外部檢查。
- 3) 內部檢查意見，包含內部稽核、第二道防線法令遵循及風險監控結果、自行查核及內部控制制度聲明書所列應加強辦理改善事項。
- 4) 主管機關裁罰及重大風險事件之發生及處理。
- 5) 缺失追蹤改善及重覆發生情形。

3.運用前項評估資訊時，應考量相關資料之時效性。

(四) 風險評估結果(剩餘風險)：

- 1.內部稽核單位依據固有風險及控制措施有效性之評估結果(即固有風險經執行控制措施後之剩餘風險)，確認各受查主體之綜合風險評估最終結果，並至少區分為高、中、低三個等級。
- 2.內部稽核應訂定受查主體之綜合風險評估結果與查核頻率連結之標準，就風險等級為高者，應至少每年執行一次或一次以上查核；就風險等級為低者，至少每三年執行一次查核。

(五) 內部稽核辦理風險評估，應考量主要利益關係人(Stake holder)對保險業可能面臨之重大及潛在風險之意見，包含主管機關、董事會及審計委員會、高階管理階層、風險管理與法令遵循單位等。

七、內部稽核應依據其所訂定之評估方法，每年至少執行一次風險評估。執行風險評估時應指定合適之稽核人員辦理，並指派資深稽核人員覆核其評估結果後，呈總稽核核准。

八、內部稽核所訂定之風險評估程序與方法，以書面交付監察人或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。風險評估程序與方法並應經董事會通過；修正時，亦同。

內部稽核對受查主體有縮減或整併及風險評估方法論等有大幅變更者，經評估後屬整體風險導向內部稽核制度之重大改變，應提報董事會通過。

九、內部稽核辦理風險評估應留存記錄並至少保存五年，包含確認風險評估範

圖與受查主體、辨識與評量風險、訂定稽核計畫等過程，以及有關核准記錄。

( 訂定內部稽核計畫 )

十、內部稽核應依據風險評估結果進行年度稽核計畫之規劃，包含受查主體、頻率、範圍及查核方式，並另依據主管機關其他個別指定事項，彙總訂定年度稽核計畫。

十一、受查主體若有主管機關要求年度辦理之查核範圍，則無論風險評估結果所對應之查核頻率為何，均應依主管機關要求納入年度稽核計畫。

十二、內部稽核應於年度稽核計畫擬訂完成後，檢附年度稽核計畫及風險評估結果，呈總稽核就主管機關監理重點及保險業經營策略目標，審閱整體年度稽核計畫與風險評估結果之妥適性，並做必要之調整。

十三、年度稽核計畫應併同內部稽核單位風險評估結果以書面交付監察人或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。年度稽核計畫並應經董事會通過；修正時，亦同。

( 定期檢視風險評估結果與內部稽核計畫 )

十四、內部稽核應定期就整體外部環境或內部業務發展變化檢視風險評估結果，以即時反應受查主體之風險，並據以決定是否修訂年度稽核計畫。

十五、內部稽核應依據其所制定之風險評估方法，持續蒐集內、外部監控資訊，如：國內、外主管機關監理重點與重要法令及金融環境變化、經營策略目標與重要政策變化、業務營運管理資訊與重要監控指標、主要利益關係人意見、以及重大風險事件發生情形等，俾確保風險評估過程能充分考量內、外部環境風險變化。

( 內部稽核品質評核機制 )

十六、內部稽核應訂定品質評核機制，以定期確認內部稽核業務執行是否確實遵循有關內部稽核制度與程序，並符合主管機關法令規範。

十七、內部稽核品質評核內容應涵蓋下列項目：

- (一) 稽核策略與目標之訂定與執行。
- (二) 稽核制度及程序之設計與運作。
- (三) 組織編制與稽核資源配置。
- (四) 人員專業之適足性及持續訓練。
- (五) 稽核方法與工具之持續精進與研發。
- (六) 對主管機關法令規範遵循情形。
- (七) 前次品質評核應改善事項。

十八、內部稽核辦理品質評核，得採內部自我評核或外部機構評核方式辦理：

(一) 評核方式：

1. 內部自我評核：由內部稽核單位或金融控股公司或金融機構之集團(母公司)指定人員，每年度至少辦理一次自我評核，負責辦理評核人員應不得檢查自身經辦之業務，內部稽核單位並應至少每五年委請外部機構驗證其評核結果。
2. 外部機構評核：由內部稽核單位委請外部機構辦理評核，應至少每五年辦理一次。

(二) 內部稽核單位委請負責辦理驗證或評核之外部機構，不得為其財務簽證會計師。

(三) 內部稽核應就所採行之評核方式，及外部機構之資格與獨立性，以書面交付監察人或審計委員會核議，未設審計委員會者，應送獨立董事。評核方式及選定之外部機構應經董事會通過。

前項各款所稱之外部機構，由中華民國人壽保險商業同業公會及中華民國產物保險商業同業公會(以下簡稱產、壽險公會)認定之。

十九、內部稽核應依據評核結果，就可能影響內部稽核整體運作事項擬訂改善計畫，總稽核應負責督導改善計畫之確實執行。

內部稽核品質評核結果與改善計畫應以書面交付監察人或審計委員會，未設審計委員會者，應送獨立董事。內部稽核品質評核結果與改善計畫並應提報董事會備查。

(本實務守則修訂核准層級)

二十、本實務守則由產、壽險公會共同訂定，經各該公會理事會決議通過，並報經主管機關備查後施行；修正時，亦同。

## 保險業建立風險導向內部稽核制度實務守則條文對照說明

條文內容	說明
<p>( 依據 )</p> <p>一、本實務守則係依據金融監督管理委員會111年10月27日金管檢保字第11106101871號令辦理</p>	<p>說明本實務守則訂定依據</p>
<p>( 目的 )</p> <p>二、保險業實施風險導向內部稽核制度，係透過風險評估之方法，審慎評估稽核範疇內各個受查主體之風險，並依據評估結果決定稽核任務之查核重點、範圍、方法、稽核程序及查核頻率，將稽核資源做最有效的配置，聚焦於重要風險並加強查核深度，提升內部稽核執行效益，以有效協助保險業完善內部控制制度及強健企業體質。</p>	<p>說明保險業建立風險導向內部稽核制度之目的。</p> <p>所稱稽核範疇(audit universe)，係指一份涵蓋所有可能進行受查主體(auditable entity)的清單。</p>
<p>( 風險導向內部稽核制度實施方法 )</p> <p>三、為確保內部稽核之品質與有效性，保險業實施風險導向內部稽核制度，應具備明確之內部控制三道防線架構，內部稽核並應建立以下機制：</p> <ol style="list-style-type: none"> <li>1 內部稽核風險評估之程序與方法。</li> <li>2 內部稽核品質評核機制。</li> </ol>	<ol style="list-style-type: none"> <li>1.明確訂定保險業為實施風險導向內部稽核制度，應建立之有關機制，以確保：             <ol style="list-style-type: none"> <li>(1)風險評估有明確且標準之方法與程序。</li> <li>(2)有關機制能持續有效的運作。</li> </ol> </li> <li>2.內部稽核可參採內部控制各道防線之風險管理及控制功能運作結果等資訊，提供獨立客觀及攸關的確認，以建立內部稽核風險評估之程序與方法。</li> </ol>
<p>( 訂定風險評估程序 )</p> <p>四、內部稽核應建立風險評估之程序與方法，以辨識並評估各受查主體所面臨之風險，並定期驗證風險評估因子或指標及各項控制措施之有效性</p>	
<p>五、確認風險評估範圍：</p> <p>內部稽核應依據保險業所經營業務範圍及單位組織，以及主管機關法令規範，辨識應辦理風險評估之受查主體，以確保風險評估範圍能完整涵蓋保險業整體營運範疇。</p> <p>內部稽核得以單位組織、產品、業務、作業流程或其他構面訂定受查主體。</p>	<p>說明辦理風險評估首要應確認評估範圍涵蓋完整，符合「保險業內部控制及稽核制度實施辦法」規定。</p> <p>內部稽核係依據企業經營業務及單位組織辨識應辦理風險評估之受查主體。內部稽核可依據實際需要，就單位組織、產品、業務、流程或其他構面，個別或合併訂定受查主體。</p>
<p>六、風險評估因子與方法：</p> <p>( 一 ) 內部稽核應就各受查主體所面臨之</p>	<p>內部稽核衡量受查主體之風險應包含固</p>

固有風險、控制措施有效性進行評估後，確認受查主體之風險評估結果（即剩餘風險），並據以決定年度稽核計畫。所稱固有風險、控制措施與剩餘風險定義如下：

- 1.固有風險：在管理階層尚未採取任何行動來改變風險發生的可能性或其影響之情況下，達成目標之風險。
- 2.控制措施：管理階層為管理風險及增加達成既定目標之可能性，而採取之任何行動。管理階層負責規劃、組織及指揮執行足夠之行動，以合理保證目的及目標之達成。
- 3.剩餘風險：管理階層在設計及執行控制措施後，仍留下來無法達成組織目標之風險。

(二) 固有風險之評量：

- 1.內部稽核應依據所屬保險業之經營形態與發展策略目標，擬訂適合之固有風險評估因子。風險評估因子之訂定可參酌保險業風險管理實務守則所列舉之主要風險類型，並應描述評估各風險類型時應考量之因素（所述因素應能顯著代表各風險之表徵）。
- 2.依前項有關之固有風險因子，就受查主體發生風險事項之可能性與嚴重程度評估其固有風險：
  - 1) 發生可能性：評估風險事件在可預期的未來中發生之可能性。
  - 2) 嚴重程度：評估風險事件發生對財務、商譽及營運服務可能造成之影響。
  - 3) 依據前二項構面評估固有風險，評估結果至少應區分為高、中、低等三個風險等級。

(三) 控制措施有效性之評量：

- 1.以持續或個別評估的方式確認各受查主體之控制措施是否存在且發揮功效，並就控制措施設計及執行之有效性至少區分為高、中、低三個等級。
- 2.控制措施有效性評估至少應包含下列資訊：
  - 1) 主要業務之內部控制運作情形。

有風險、控制措施有效性及確認剩餘風險。<參考國際IIA內部稽核準則及實務諮詢指引與範例、COSO定義>

說明內部稽核應事先訂定固有風險評估因子，以做為衡量各受查主體固有風險之參考。

固有風險應以發生可能性及嚴重程度兩個方向進行衡量，其評估結果至少應區分為高、中、低三個風險等級俾利識別。<參考國際IIA內部稽核準則及實務諮詢指引與範例>

控制措施有效性評估結果至少應區分為高、中、低三個等級俾利識別。<參考國際IIA內部稽核準則及實務諮詢指引與範例>

控制有效性評估項目至少應包含「保險業內部控制及稽核制度實施辦法」規範之內部稽核應確認事項。



<p>2) 外部檢查意見，包含主管機關、會計師、母公司稽核單位及其他外部檢查。</p> <p>3) 內部檢查意見，包含內部稽核、第二道防線法令遵循及風險監控結果、自行查核及內部控制制度聲明書所列應加強辦理改善事項。</p> <p>4) 主管機關裁罰及重大風險事件之發生及處理。</p> <p>5) 缺失追蹤改善及重覆發生情形。</p> <p>3. 運用前項評估資訊時，應考量相關資料之時效性。</p> <p>(四) 風險評估結果(剩餘風險)：</p> <p>1. 內部稽核單位依據固有風險及控制措施有效性之評估結果(即固有風險經執行控制措施後之剩餘風險)，確認各受查主體之綜合風險評估最終結果，並至少區分為高、中、低三個等級。</p> <p>2. 內部稽核應訂定受查主體之綜合風險評估結果與查核頻率連結之標準，就風險等級為高者，應至少每年執行一次或一次以上查核；就風險等級為低者，至少每三年執行一次查核。</p> <p>(五) 內部稽核辦理風險評估，應考量主要利益關係人(Stake holder)對保險業可能面臨之重大及潛在風險之意見，包含主管機關、董事會及審計委員會、高階管理階層、風險管理與法令遵循單位等。</p>	<p>內部稽核於運用相關評估資訊，應考量所取用資訊之時效，俾確認其是否仍具參考價值。</p> <p>綜合風險評估結果(剩餘風險)至少應區分為高、中、低三個風險等級俾利識別。</p> <p>參考金融監督管理委員會109.2.13金管檢銀字第1090604016號函說明二(一)。</p> <p>內部稽核辦理風險評估應考量主要利益關係人對保險業可能面臨之重大及潛在風險之意見，包含主管機關、董事會及審計委員會、高階管理階層、風險管理與法令遵循單位。&lt;參考國際IIA內部稽核準則及實務諮詢指引與範例&gt;</p>
<p>七、內部稽核應依據其所訂定之評估方法，每年至少執行一次風險評估。執行風險評估時應指定合適之稽核人員辦理，並指派資深稽核人員覆核其評估結果後，呈總稽核核准。</p>	<p>內部稽核應依據組織分工及風險評估方法，對指定合適之人員所辦理之風險評估，應經審慎之覆核及核准程序。</p>
<p>八、內部稽核所訂定之風險評估程序與方法，以書面交付監察人或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。風險評估程序與方法並應經董事會通過；修正時，亦同。</p> <p>內部稽核對受查主體有縮減或整併及風險評估方法論等有大幅變更者，經評估後屬整體風險導向內部稽核制度之重大改變，</p>	<p>內部稽核風險評估程序與方法之核准層級應比照「保險業內部控制及稽核制度實施辦法」規定年度稽核計畫之核准層級。</p>

應提報董事會通過。	
九、內部稽核辦理風險評估應留存記錄並至少保存五年，包含確認風險評估範圍與受查主體、辨識與評量風險、訂定稽核計畫等過程，以及有關核准記錄。	內部稽核應就風險評估之過程留存清楚完整之記錄，以備內部稽核品質確保之驗證。
(訂定內部稽核計畫) 十、內部稽核應依據風險評估結果進行年度稽核計畫之規劃，包含受查主體、頻率、範圍及查核方式，並另依據主管機關其他個別指定事項，彙總訂定年度稽核計畫。	內部稽核除依據風險評估結果訂定年度稽核計畫，並應包含主管機關來函要求列入年度稽核計畫項目。
十一、受查主體若有主管機關要求年度辦理之查核範圍，則無論風險評估結果所對應之查核頻率為何，均應依主管機關要求納入年度稽核計畫。	受查主體之查核範圍應符合主管機關規定事項。
十二、內部稽核應於年度稽核計畫擬訂完成後，檢附年度稽核計畫及風險評估結果，呈總稽核就主管機關監理重點及保險業經營策略目標，審閱整體年度稽核計畫與風險評估結果之妥適性，並做必要之調整。	總稽核應就主管機關監理重點及整體保險業經營策略，審閱年度稽核計畫及風險評估結果，並做必要之修正。
十三、年度稽核計畫應併同內部稽核單位風險評估結果以書面交付監察人或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。年度稽核計畫並應經董事會通過；修正時，亦同。	年度稽核計畫應依據「保險業內部控制及稽核制度實施辦法」規定呈報核准，風險評估結果亦應併同呈送，俾強化其與年度稽核計畫之連結。
(定期檢視風險評估結果與內部稽核計畫) 十四、內部稽核應定期就整體外部環境或內部業務發展變化檢視風險評估結果，以即時反應受查主體之風險，並據以決定是否修訂年度稽核計畫。	規範內部稽核於年度稽核計畫核准後，應定期檢視受查主體之風險變化(如：併購、重要或新業務/產品/服務/系統)，並視需要修訂稽核計畫，以確保計畫能因應風險變化適時調整。
十五、內部稽核應依據其所制定之風險評估方法，持續蒐集內、外部監控資訊，如：國內、外主管機關監理重點與重要法令及金融環境變化、經營策略目標與重要政策變化、業務營運管理資訊與重要監控指標、主要利益關係人意見、以及重大風險事件發生情形等，俾確保風險評估過程能充分考量內、外部環境風險變化。	持續性監控資訊蒐集之資料範圍應包含下列項目： (1) 國內、外主管機關監理重點與趨勢、重要法令及金融環境變化。 (2) 短、中、長期經營策略目標與重要政策變化。 (3) 業務營運及管理資訊、重要業務監控指標與重大風險事件發生情形。 (4) 二道防線(含：風險管理、法令遵循、業務管理等單位)對一道防線之監控管理資訊。 (5) 主要利益關係人意見。

<p>( 內部稽核品質評核機制 )</p> <p>十六、 內部稽核應訂定品質評核機制，以定期確認內部稽核業務執行是否確實遵循有關內部稽核制度與程序，並符合主管機關法令規範。</p>	<p>為確保內部稽核實施風險導向稽核制度之品質與有效性，內部稽核應訂定內部稽核品質評核機制。</p>
<p>十七、 內部稽核品質評核內容應涵蓋下列項目：</p> <ol style="list-style-type: none"> <li>1 稽核策略與目標之訂定與執行。</li> <li>2 稽核制度及程序之設計與運作。</li> <li>3 組織編制與稽核資源配置。</li> <li>4 人員專業之適足性及持續訓練。</li> <li>5 稽核方法與工具之持續精進與研發。</li> <li>6 對主管機關法令規範遵循情形。</li> <li>7 前次品質評核應改善事項。</li> </ol>	<p>內部稽核品質評核範圍應涵蓋整體內部稽核單位之運作執行情形。</p>
<p>十八、 內部稽核辦理品質評核，得採內部自我評核或外部機構評核方式辦理：</p> <p>( 一 ) 評核方式：</p> <ol style="list-style-type: none"> <li>1.內部自我評核：由內部稽核單位或金融控股公司或金融機構之集團(母公司)指定人員，每年度至少辦理一次自我評核，負責辦理評核人員應不得檢查自身經辦之業務，內部稽核單位並應至少每五年委請外部機構驗證其評核結果。</li> <li>2.外部機構評核：由內部稽核單位委請外部機構辦理評核，應至少每五年辦理一次。</li> </ol> <p>( 二 ) 內部稽核單位委請負責辦理驗證或評核之外部機構，不得為其財務簽證會計師。</p> <p>( 三 ) 內部稽核應就所採行之評核方式，及外部機構之資格與獨立性，以書面交付監察人或審計委員會核議，未設審計委員會者，應送獨立董事。評核方式及選定之外部機構應經董事會通過。</p> <p>前項各款所稱之外部機構，由中華民國人壽保險商業同業公會及中華民國產物保險商業同業公會(以下簡稱產、壽險公會)認定之。</p>	<p>規範內部稽核單位辦理品質評估得以內部自我評核或外部機構評核方式辦理。&lt;參考國際IIA內部稽核準則及實務諮詢指引與範例&gt;</p>
<p>十九、 內部稽核應依據評核結果，就可能影響</p>	<p>內部稽核應依據前項評核結果，辨識應</p>

<p>內部稽核整體運作事項擬訂改善計畫，總稽核應負責督導改善計畫之確實執行。</p> <p>內部稽核品質評核結果與改善計畫應以書面交付監察人或審計委員會，未設審計委員會者，應送獨立董事。內部稽核品質評核結果與改善計畫並應提報董事會備查。</p>	<p>改善事項及提出改善計畫。</p> <p>內部稽核自我評核結果及改善計畫應向監察人或審計委員會報告(未設審計委員會者，應向獨立董事報告)後，提報董事會核備，並持續追蹤改善。&lt;參考國際IIA內部稽核準則及實務諮詢指引與範例&gt;</p>
<p>(本實務守則修訂核准層級)</p> <p>二十、本實務守則由產、壽險公會共同訂定，經各該公會理事會決議通過，並報經主管機關備查後施行；修正時，亦同。</p>	