Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Circulaire 2017/xx
Gouvernance d'entreprise — assureurs

Gouvernance d'entreprise, gestion des risques et système de contrôle interne en matière d'assurance

Référence :	Circ.-FINMA 17/xx « Gouvernance d'entreprise — assureurs »
Date :	...
Entrée en vigueur :	1er janvier 2017
Concordance :	remplace la Circ.-FINMA 08/32 « Gouvernance d'entreprise — assureurs » et la Circ.-FINMA 08/35 « Révision interne – assureurs », toutes deux du 20 novembre 2008
Bases légales :	LFINMA art. 7 al. 1 let. b LSA art. 14, 22, 27, 67,68, 75, 76 OS art. 12–14, 16, 96–98*a*, 191, 195–196, 204

Destinataires																					
LB			LSA			LBVM		LPCC								LBA			Autres	
Banques	Groupes et congl. financiers	Autres intermédiaires	Assureurs	Groupes. et congl. d'assur.	Intermédiaires d'assur.	Bourses et participants	Négociants en valeurs mob.	Directions de fonds	SICAV	Sociétés en comm. de PCC	SICAF	Banques dépositaires	Gestionnaires de PCC	Distributeurs	Représentants de PCC étr.	Autres intermédiaires	OAR	IFDS	Entités surveillées par OAR	Sociétés d'audit	Agences de notation
			x	x																	

Laupenstrasse 27, 3003 Berne
Tél. +41 (0)31 327 91 00, fax +41 (0)31 327 91 01
www.finma.ch

Table des matières

I. But

Cette circulaire vise à concrétiser les dispositions de la loi sur la surveillance des assurances (LSA ; RS 961.01) concernant la gouvernance d'entreprise (*corporate governance*), la gestion des risques et le système de contrôle interne (SCI). 1

II. Champ d'application

La présente circulaire s'applique à toutes les entreprises d'assurance selon l'art. 2 al. 1 let. a et b LSA ainsi qu'aux groupes d'assurance et conglomérats d'assurance assujettis à la surveillance des groupes et des conglomérats selon l'art. 2 al. 1 let. d en rel. avec les art. 65 et 73 LSA. 2

Elle est applicable par analogie aux succursales suisses d'entreprises d'assurance ayant leur siège social à l'étranger (art. 2 al. 1 let. b LSA) et aux entreprises d'assurance autorisées à exploiter la branche d'assurance C3 (réassurance exercée par des captives). 3

Les Cm 16 à 28 concernant le conseil d'administration d'une entreprise d'assurance s'appliquent par analogie à l'organe d'administration de la société coopérative. 4

Lors de l'application de ces dispositions, il convient de tenir compte des spécificités, de la taille et de la complexité de l'unité concernée et de respecter le principe de proportionnalité. 5

III. Principes de gouvernance d'entreprise

L'entreprise d'assurance applique notamment les principes suivants de gouvernance d'entreprise à tous les échelons : 6

- attribution et documentation claires des tâches, compétences, responsabilités ainsi que de lignes de décision et de *reporting* ; 7
- séparation claire entre activités opérationnelles et activités de contrôle grâce à des mesures appropriées ; 8
- mise en place de processus de *reporting* et de communication internes afin de transmettre des informations à tous les organes pertinents de l'entreprise ; 9
- documentation des décisions importantes (y compris des mesures) ; 10
- mise en place d'un système de gestion des risques efficace au niveau de l'entreprise et d'un système de contrôle interne (SCI) performant, y compris les fonctions de contrôle (gestion des risques, *compliance*, révision interne), et vérification périodique de leur adéquation par une partie indépendante (interne ou externe) ; 11
- instauration de principes, de processus et de structures visant à assurer le respect des prescriptions légales, réglementaires et internes ; 12

- définition de principes, de processus et de structures destinés à identifier et éviter ou résoudre les conflits d'intérêts et les abus ; 13

- définition de principes concernant le comportement attendu des collaborateurs ; 14

- mise en place de processus garantissant que les personnes responsables de la haute direction, de la surveillance et du contrôle ainsi que de la direction opérationnelle de l'entreprise d'assurance possèdent durablement l'expérience professionnelle requise, les connaissances techniques et l'aptitude personnelle. 15

IV. Conseil d'administration

A. Composition

Dans son ensemble, le conseil d'administration doit notamment disposer, en plus d'un savoir suffisant en matière d'assurance, d'expériences professionnelles et de connaissances approfondies de la direction opérationnelle, du management stratégique, du pilotage des risques ainsi que des finances et de la comptabilité. 16

Chaque membre du conseil d'administration, en collaboration avec les autres membres, doit posséder des connaissances techniques ou des capacités pertinentes pour l'accomplissement des tâches du conseil d'administration. 17

Le conseil d'administration compte au moins trois membres. Leur nombre dépend de la taille, de la complexité et du profil de risque de l'entreprise d'assurance. 18

Le conseil d'administration est composé pour un tiers au moins de membres répondant aux critères d'indépendance énoncés ci-après. La FINMA peut autoriser des exceptions s'il existe de justes motifs. 19

Un membre du conseil d'administration est réputé indépendant s'il satisfait au moins aux critères suivants : 20

- il n'occupe pas d'autre fonction dans l'entreprise d'assurance et n'en a pas occupé au cours des deux dernières années ; 21

- il n'a pas occupé, au cours des deux dernières années, la fonction d'auditeur responsable de l'entreprise d'assurance au sein de la société d'audit ; et 22

- il n'entretient avec l'entreprise d'assurance aucune relation d'affaires qui, par sa nature ou son étendue, conduit à un conflit d'intérêts. 23

Une partie déterminante du conseil d'administration ne doit par ailleurs pas détenir de participation dans l'entreprise d'assurance ou, au cas où celle-ci appartiendrait à un groupe d'entreprises, ne doit pas exercer de fonction opérationnelle dans une autre entreprise du groupe, ou ne doit pas représenter le détenteur d'une participation. 24

B. Comités du conseil d'administration

Lorsque cela s'avère opportun, le conseil d'administration constitue des comités du conseil d'administration pour exercer efficacement ses tâches. 25

Les entreprises d'assurance des catégories de surveillance 2 et 3 mettent en place un comité d'audit et un comité des risques. Les entreprises d'assurance de la catégorie de surveillance 3 peuvent constituer un comité d'audit et des risques combiné. 26

Les comités d'audit et des risques sont constitués au moins pour un tiers de membres indépendants (cf. Cm 20 à 24). Le président du conseil d'administration ne préside ni le comité d'audit ni le comité des risques. 27

Dans leur globalité, les comités disposent des connaissances et expériences nécessaires dans leur domaine d'attribution respectif. Le président d'un comité doit satisfaire à des exigences plus élevées que les membres. 28

V. Système de gestion des risques et système de contrôle interne

A. Système de gestion des risques

L'entreprise d'assurance dispose d'un système de gestion des risques selon l'art. 96 OS, qui doit être documenté conformément à l'art. 97 OS. Les systèmes de limites pour les expositions au risque et les mécanismes de contrôle prévus à l'art. 97 al. 2 let. e visent à garantir que l'entreprise d'assurance agit dans le cadre de sa capacité de risque. 29

B. Système de contrôle interne

L'entreprise d'assurance met en place un système de contrôle interne afin de garantir une sécurité adéquate concernant les risques de la conduite des affaires, en particulier en ce qui concerne l'efficacité des processus opérationnels, la fiabilité du rapport financier et le respect des normes juridiques et des directives internes. 30

L'entreprise d'assurance définit des activités de contrôle au niveau de l'entreprise et des processus afin de garantir le respect et l'exécution des mesures ordonnées par le conseil d'administration et la direction dans le but de répondre aux principaux risques de la conduite des affaires. 31

Le conseil d'administration, la direction ainsi que les autres collaborateurs reçoivent toutes les informations dont ils ont besoin pour assumer leurs responsabilités concernant le système de contrôle interne. 32

L'entreprise d'assurance décrit son système de contrôle interne dans une documentation. Celle-ci est actualisée en permanence et inclut notamment : 33

- les directives internes de l'entreprise concernant le système de contrôle interne et les processus qui lui sont liés ; 34

- la description de l'organisation structurelle et fonctionnelle, y compris des tâches, compétences et responsabilités ; 35
- les exigences à l'égard du système de contrôle interne (notamment les objectifs, la dotation en ressources, la sensibilisation des collaborateurs) ; 36
- la description des activités de contrôle établies. 37

C. Fonctions de contrôle

L'entreprise d'assurance s'assure que chaque fonction de contrôle est libre de toute influence l'empêchant d'assurer ses missions de façon objective et indépendante. 38

La rémunération des collaborateurs des fonctions de contrôle doit être établie de manière à minimiser les conflits d'intérêts éventuels avec les unités d'affaires qu'ils surveillent ou contrôlent. 39

Les fonctions de contrôle ont un accès illimité à toutes les personnes et informations requises pour accomplir leurs tâches. 40

a) Fonction de gestion des risques

Le responsable de la fonction de gestion des risques procède régulièrement à une évaluation des risques importants de l'entreprise d'assurance et de l'adéquation du système de gestion des risques ; il en rend compte périodiquement (au moins une fois par an) au conseil d'administration. 41

b) Fonction de *compliance*

La fonction de *compliance* garantit l'identification des principales obligations juridiques et réglementaires de l'entreprise d'assurance et évalue les risques de *compliance* auxquels celle-ci est exposée. Elle analyse et évalue l'adéquation des directives, processus et contrôles mis en place par l'entreprise d'assurance afin d'éviter toute violation de la *compliance*. 42

Le responsable de la fonction de *compliance* procède périodiquement (au moins une fois par an) à une évaluation des risques de *compliance* importants de l'entreprise d'assurance ; il en rend compte au conseil d'administration. 43

c) Révision interne

La révision interne est directement subordonnée au conseil d'administration. Elle est indépendante des autres fonctions de contrôle de l'entreprise d'assurance aux plans organisationnel et opérationnel. Elle possède un droit de regard, d'information et d'examen illimité au sein de l'entreprise d'assurance. 44

La révision interne est organisée en conformité avec les normes professionnelles nationales et internationales de la révision interne[1] ; elle respecte ces normes dans le cadre de son activité. 45

La révision interne exerce ses activités sur la base d'une planification des audits périodique, fondée sur le risque. Le plan d'audit couvre une période de planification d'au moins un an et devrait inclure un aperçu de la planification pluriannuelle des audits. Le conseil d'administration approuve le plan d'audit ainsi que les changements importants qui y sont apportés. 46

Sur la base de la planification des audits, la révision interne vérifie à intervalles raisonnables tous les domaines d'activité et toutes les fonctions de l'entreprise d'assurance. 47

Au moins une fois par an, la révision interne établit un rapport à l'intention du conseil d'administration qui porte notamment sur les points suivants : 48

- le respect du plan d'audit approuvé par le conseil d'administration ainsi que les activités exécutées en complément du plan d'audit ; 49
- l'état de la mise en œuvre des mesures d'amélioration adoptées ; 50
- les circonstances qui entravent ou pourraient entraver l'indépendance, l'objectivité ou l'efficacité de la révision interne. 51

La révision interne rend compte par écrit au conseil d'administration, dans les meilleurs délais et de manière appropriée, de toutes les constatations importantes faites dans le cadre d'un audit. Les insuffisances graves doivent être immédiatement signalées au conseil d'administration. 52

La révision interne met son rapport au conseil d'administration et ses différents rapports d'audit à la disposition de la société d'audit selon l'art. 28 LSA. 53

Les tâches de la révision interne peuvent être externalisées en totalité ou en partie, sous réserve de l'approbation par la FINMA : 54

- à la révision interne de l'entité suprême du groupe, pour autant que l'entreprise d'assurance assujettie soit impliquée dans les processus de contrôle et de pilotage à l'échelle du groupe ; 55
- à une société d'audit agréée par l'Autorité fédérale de surveillance en matière de révision (ASR), indépendante de la société d'audit déjà mandatée par l'entreprise d'assurance selon l'art. 28 LSA ; 56
- à un prestataire externe, indépendant de la société d'audit déjà mandatée par l'entreprise d'assurance selon l'art. 28 LSA. 57

[1] Ligne de conduite de l'audit interne de l'Association suisse d'audit interne (ASAI) ou Normes internationales pour la pratique professionnelle de l'audit interne de l'Institute of Internal Auditors (IIA).

VI. Gestion des risques et système de contrôle interne en cas d'externalisation

Il y a externalisation si une entreprise d'assurance charge une autre entreprise (prestataire) d'assumer de façon autonome et durable une fonction ou une tâche en lien avec l'activité de l'entreprise d'assurance. 58

Les Cm 60 à 66 sont applicables à tous les types d'externalisation. 59

Les risques liés à une externalisation doivent être systématiquement identifiés, surveillés, quantifiés et pilotés. 60

Avant toute externalisation, l'entreprise d'assurance établit une analyse des risques qui présente les réflexions économiques et opérationnelles ainsi que les risques afférents de manière compréhensible. Une nouvelle analyse des risques est établie en cas de modification significative des conditions-cadres de l'externalisation afin de statuer sur sa poursuite ou sa cessation. 61

Lorsque plusieurs fonctions et/ou tâches sont externalisées au même prestataire, le risque de concentration doit être pris en compte en particulier. 62

Les risques liés à l'externalisation doivent être pris en compte dans le système de contrôle interne de l'entreprise d'assurance qui sous-traite. La sécurité des données, la protection des données ainsi que l'efficacité des processus opérationnels doivent en outre être garanties. 63

L'entreprise d'assurance qui externalise et la FINMA doivent pouvoir contrôler en tout temps les fonctions et/ou les tâches externalisées. 64

L'entreprise d'assurance désigne un responsable de la surveillance et du contrôle du prestataire. 65

L'entreprise d'assurance exige des rapports du prestataire afin de pouvoir surveiller d'une manière appropriée les fonctions et/ou les tâches externalisées. 66

VII. Disposition transitoire

Les Cm 18, 19 à 24 et 25 à 28 doivent être mise en oeuvre d'ici au 31 décembre 2019 au plus tard. La FINMA peut admettre des exceptions dans des cas particuliers justifiés. 67