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 2008/32
Gouvernance d'entreprise – assureurs

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

Référence :	Circ.-FINMA 08/32 « Gouvernance d'entreprise – assureurs »
Date :	20 novembre 2008
Entrée en vigueur :	1er janvier 2009
Dernière modification :	20 novembre 2008
Concordance :	remplace la Directive-OFAP 15/2006 « Gouvernance d'entreprise » du 21 novembre 2006
Bases légales :	LFINMA art. 7 al. 1 let. b, 29 LSA art. 14, 22, 27, 67, 75, 76 ainsi que les articles de l'ordonnance s'y rapportant

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																	

Einsteinstrasse 2, 3003 Berne
Tél. +41 (0)31 327 9100, Fax +41 (0)31 327 9101
www.finma.ch

Table des matières

I. Bases juridiques, but et champ d'application

A. Bases juridiques

La présente Circulaire repose sur les bases juridiques suivantes : les art. 14 et 22 de la Loi sur la surveillance des assurances (LSA ; RS 961.01) pour la gouvernance d'entreprise et la gestion des risques, l'art. 27 LSA pour le système interne de contrôle, les articles 67, 68, 75 et 76 LSA en ce qui concerne les groupes d'assurance et les conglomérats d'assurance, ainsi que sur les articles de l'ordonnance s'y rapportant. 1

B. But

La présente Circulaire a pour but de concrétiser les dispositions du droit de surveillance concernant la gouvernance d'entreprise (GE), la gestion des risques (GR) et le système interne de contrôle (SIC). Elle doit fixer, de manière résumée et en se fondant sur des principes, un standard minimum dans les domaines GE, GR et SIC pour les entreprises d'assurance, les groupes d'assurance et les conglomérats d'assurance soumis à la surveillance. 2

C. Champ d'application

Les présentes dispositions concernant la gouvernance d'entreprise (GE), la gestion des risques (GR) et le système interne de contrôle (SIC) sont valables pour toutes les entreprises d'assurance, tous les groupes d'assurance et tous les conglomérats d'assurance (ci après : entreprises) qui sont soumis à la surveillance des assurances suisse en vertu de l'art. 2, al. 1, let. a LSA, ainsi que, sur la base de décisions, en vertu des art. 2, al. 1, let. d et 65, respectivement 73 LSA. Pour les caisses-maladie exploitant des affaires soumises à la LCA, c'est la réglementation prévue par la « circulaire » n° 11/2006 de l'OFAP sur la nouvelle législation en matière d'assurance privée du 1er novembre 2006 qui est valable. Les présentes dispositions sont applicables par analogie aux succursales suisses d'entreprises d'assurance ayant leur siège social à l'étranger. Lors de l'application de ces dispositions, il convient de prendre en considération la complexité et la taille de l'entité concernée et de tenir compte du principe de la proportionnalité. 3

Pour la surveillance des groupes et des conglomérats, une mise en œuvre au niveau de la société faîtière du groupe suffit dès que les sociétés individuelles surveillées sont comprises dans les processus de contrôle et de commandement au niveau du groupe. 4

II. Définitions et objectifs

A. Définition et objectif de la gouvernance d'entreprise

La gouvernance d'entreprise comprend les principes et les structures sur la base desquels une entreprise est conduite et contrôlée. La gouvernance d'entreprise a pour but de réaliser un équilibre fonctionnel entre les divers organes de l'entreprise (« checks and balances »), une transparence suffisante des processus internes de l'entreprise, ainsi que l'harmonisation des objectifs de l'entreprise avec les attentes des divers groupes d'ayants droit. En font partie les preneurs d'assurance et les bénéficiaires de prestations, les propriétaires, l'autorité de surveillance, ainsi que les collaborateurs. La protection des preneurs d'assurance et des ayants droit revêt une signification particulière sous l'angle du droit de surveillance. 5

B. Définition de la gestion des risques

La gestion des risques porte sur les méthodes et les processus qui servent à l'identification et à l'évaluation des risques, à la mise au point de stratégies, de mesures de conduite en matière de risques et au contrôle et à l'établissement de rapports relatifs aux risques. 6

C. Définition du système interne de contrôle

Le système interne de contrôle (SIC) comporte les processus, les méthodes et les mesures prescrites au sein de l'entreprise et qui servent à garantir une sécurité adéquate concernant les risques de la conduite des affaires, en particulier en ce qui concerne l'efficacité des processus d'activité, la fiabilité du rapport financier et le respect des lois et des prescriptions. 7

D. Objectif de la gestion des risques et du système interne de contrôle

Une gestion appropriée des risques (art. 22 LSA, art. 96–98, ainsi que 195 et 196, al. 2 de l'Ordonnance de la surveillance [OS ; RS 961.011]) et un système interne de contrôle efficace (art. 27 LSA) garantissent que les risques potentiels soient reconnus et évalués à temps et que des mesures soient prises pour empêcher ou couvrir des risques importants et des cumuls de risques (art. 96 OS). 8

III. Dispositions concernant la gouvernance d'entreprise

A. Principes généraux de la gouvernance d'entreprise

Les entreprises se conforment aux principes suivants de la gouvernance d'entreprise et prennent les mesures nécessaires à leur transposition : 9

- documentation claire des structures de gouvernance d'entreprise et des processus de reporting existants, concernant par exemple les statuts, les règlements d'organisation ainsi que les règlements des comités institués (cf. art. 4, al. 2, let. a et b LSA, ainsi que l'art. 191 OS) ;

- respect des bases juridiques et des exigences réglementaires déterminantes pour l'activité de l'entreprise ;

- intégrité et comportement éthique, ainsi que culture de responsabilité, par exemple par
  - la prescription de directives et d'instructions qui invitent les collaborateurs de l'entreprise à un comportement éthique ;
  - la détermination de systèmes de rémunération et d'incitation appropriés, qui servent les intérêts et la réalisation durables des buts de l'entreprise et encouragent un comportement éthique ;
  - le recrutement de collaborateurs sur la base des qualifications nécessaires.

- respect de principes visant à éviter les conflits d'intérêts et les abus. Les entreprises édictent à cet effet des directives internes, notamment dans le domaine des placements de capitaux et des instruments de garantie. Pour ces derniers, le code de déontologie dans le domaine de la prévoyance professionnelle s'applique par analogie en tant que norme mi-

nimum ;

- institution d'une fonction de conformité, si cela est approprié eu égard à l'étendue et à la complexité des affaires ;

- sensibilisation périodique et aux échelons appropriés concernant la gouvernance d'entreprise, p.ex. par la formation ;

- indépendance de la révision interne en tant que fonction de contrôle importante pour la surveillance de l'activité (art. 27, al. 1, 2ème phrase LSA) ;

- création d'un environnement approprié, dans lequel l'actuaire responsable peut accomplir ses tâches (cf. art. 4, al. 2, let. h, 23–24 LSA, 99 OS, ainsi que 2–4 OS-FINMA).

B. Conseil d'administration

Les principes de gouvernance d'entreprise suivants sont valables pour le conseil d'administration (ils doivent être transposés par analogie à l'organe d'administration pour les sociétés coopératives) : 10

- le conseil d'administration est responsable en particulier de la haute direction, de l'organisation et de la surveillance de l'entreprise (art. 716a, al. 1 CO; cf. aussi art. 894 ss CO) et doit être composé de façon à pouvoir globalement assumer ces tâches (art. 12, al. 1, 1ère demi-phrase OS); cela implique notamment un temps disponible adéquat ;

- globalement, le conseil d'administration doit disposer, en plus des connaissances spécialisées dans le domaine, du savoir stratégique nécessaire en matière d'assurance afin d'être en mesure d'accomplir ses tâches de surveillance et de haute direction de l'entreprise, en particulier de pouvoir comprendre et apprécier les affaires, les processus et les risques de l'entreprise (art. 12, al. 2, 2ème demi-phrase OS) ;

- les membres du conseil d'administration doivent offrir la garantie d'une activité irréprochable en disposant de connaissances spécialisées convenables (voir plus haut), d'une expérience appropriée (Fitness) ainsi que d'une bonne réputation (Properness) (art. 14 et 67 LSA) ;

- les membres du conseil d'administration règlent leurs relations personnelles et d'affaires de façon à ce que les conflits d'intérêts avec l'entreprise soient évités dans la mesure du possible ;

- le président du conseil d'administration ne doit en principe pas être en même temps président de la direction (interdiction de la double fonction selon l'art. 13 OS) ;

- dans le cadre de sa compétence organisationnelle légale et selon l'importance et la complexité des affaires, le conseil d'administration désigne des comités du conseil d'administration afin d'améliorer la conduite et le contrôle (par ex. un Audit-Committee, un Nomination-Committee ou un Compensation-Committee) ;

- le conseil d'administration prend les mesures permettant la transposition des principes de la présente Circulaire dans l'entreprise.

C. Direction

Les principes de gouvernance d'entreprise suivants sont valables pour la direction (ils s'appliquent par analogie aux sociétés coopératives ayant des structures organisationnelles analogues) : 11

- les membres de la direction doivent offrir la garantie d'une activité irréprochable en disposant de connaissances spécialisées convenables, d'une expérience appropriée (Fitness) ainsi que d'une bonne réputation (Properness) (art. 14 et 67 LSA) ;

- les membres de la direction doivent avoir les connaissances nécessaires à la conduite des secteurs de l'entreprise qui leur sont subordonnés, ainsi qu'une expérience appropriée (art. 14, al. 1 OS) ;

- la direction de l'entreprise doit informer sans délai la FINMA de tous les faits susceptibles de concerner la surveillance (art. 29, al. 2 LFINMA ; voir aussi la Circ.-FINMA 08/25 « Obligation de renseigner – assureurs ») ;

- les membres de la direction règlent leurs relations personnelles et d'affaires de façon à ce que les conflits d'intérêts avec l'entreprise soient évités dans la mesure du possible.

IV. Dispositions concernant la gestion des risques et le système interne de contrôle

A. Principes généraux

- L'entreprise garantit une gestion des risques appropriée à l'activité pour tous les risques principaux et la documente (art. 22 LSA, art. 96 et 97 OS) ; 12

- l'entreprise instaure un système interne de contrôle approprié à l'activité et efficace (art. 27 LSA) ; 13

- l'entreprise définit la portée et l'opportunité des structures, des processus internes, de l'organisation interne ainsi que de la responsabilité et la répartition des tâches entre la gestion des risques et le système interne de contrôle ; 14

- l'entreprise examine périodiquement les processus dans le domaine de la gestion des risques et dans le système interne de contrôle et procède à temps aux adaptations importantes ; 15

- l'entreprise veille à ce qu'elle dispose de ressources suffisantes pour la gestion des risques et pour le système interne de contrôle, elle définit le processus d'établissement des rapports. L'entreprise sensibilise les collaborateurs conformément à leur niveau hiérarchique en ce qui concerne les tâches et les responsabilités en relation avec la gestion des risques et le système interne de contrôle, par exemple par la formation ; 16

- l'entreprise élabore des stratégies de risque appropriées à sa taille et à sa complexité, en tenant compte de l'appétit et de la tolérance au risque. La tolérance au risque est limitée par la diminution économique de valeur qu'une entreprise est disposée à supporter ou peut supporter sur la base de mesures adéquates. Elle dépend des ressources existantes (capi- 17

tal, ressources humaines, informatique) et dicte les limites de risque. L'appétit au risque se comprend comme le risque qu'une entreprise veut assumer dans le cadre de ses possibilités ;

- les processus de gestion des risques et de système interne de contrôle se composent des éléments suivants : 18
  - la reconnaissance et l'évaluation des risques (B.) ;
  - les mesures pour la maîtrise des risques et les activités de contrôle (C.) ;
  - l'information et la documentation (D.) ;
  - la surveillance aux fins de constatation de manquements et les mesures correctives (E.).

B. Reconnaissance et évaluation des risques

- L'entreprise prend des mesures appropriées concernant la reconnaissance et l'évaluation des risques ; 19
- une part importante du processus de reconnaissance des risques consiste en une classification des risques principaux ; 20
- la reconnaissance et l'évaluation des risques doivent être effectuées régulièrement ; 21
- il s'agit d'identifier et d'évaluer les risques principaux ; 22
- les méthodes de reconnaissance et d'évaluation des risques doivent être réexaminées régulièrement et adaptées au besoin ; 23
- la reconnaissance et l'évaluation des risques doivent prendre en considération le dernier état de la science, en particulier pour ce qui concerne les méthodes économiques et actuarielles ; 24
- la reconnaissance et l'évaluation des risques doivent comporter une réflexion prospective. 25

C. Mesures de maîtrise des risques et activités de contrôle

- L'entreprise prend des dispositions appropriées concernant les mesures de maîtrise des risques et les activités de contrôle (comme par exemple directives et contrôles concernant l'Underwriting, les investissements, la réassurance, les provisions techniques, la gestion des sinistres, etc.) ; 26
- les mesures pour la maîtrise des risques doivent être compatibles avec l'appétit au risque et la tolérance au risque définis au sein de l'entreprise ; 27
- les activités de contrôle doivent garantir que les mesures définies sont observées. Un rapport est établi périodiquement au sujet des limites et des mesures importantes qui n'ont pas été respectées, ainsi que de la transposition des mesures correctives prises ; 28
- les risques principaux doivent être surveillés ; 29

- les méthodes relatives aux mesures de maîtrise des risques et aux activités de contrôle doivent être réexaminées régulièrement et, au besoin, adaptées ; 30

- les dispositions concernant les mesures de maîtrise des risques et les activités de contrôle doivent prendre en considération le dernier état de la science, en particulier en ce qui concerne les méthodes économiques et actuarielles ; 31

- afin d'éviter des conflits d'intérêts, il doit y avoir une séparation appropriée des fonctions entre l'activité opérationnelle et celle de contrôle. 32

D. Information et documentation

- Les objectifs de la gestion des risques et du système interne de contrôle doivent être communiqués au sein de l'entreprise à temps et de manière adaptée aux destinataires. 33

- Les informations sont adressées aux preneurs de décisions correspondants. Les processus d'information et d'escalade sont définis. 34

- Les collaborateurs doivent recevoir toutes les informations nécessaires pour pouvoir assumer les responsabilités exigées en matière de gestion des risques et de système interne de contrôle. 35

- Documentation concernant la gestion des risques et le système interne de contrôle : 36

    - la gestion des risques et le système interne de contrôle doivent être documentés ;

    - la documentation porte notamment sur :
        - l'organisation, y compris les tâches, les compétences et les responsabilités ;
        - les exigences concernant la gestion des risques et le système interne de contrôle ;
        - la stratégie en matière de risques, y compris la tolérance au risque ;
        - les procédures d'identification des risques principaux, ainsi que la présentation des méthodes, instruments et processus en vue de leur identification, de leur mesurage et de leur surveillance ;
        - la présentation de systèmes de limites en vigueur en ce qui concerne les expositions au risque, ainsi que des mécanismes de contrôle ;
        - les directives internes de l'entreprise concernant la gestion des risques, le système interne de contrôle et les processus qui leur sont liés.

    - la documentation doit être actualisée lors d'adaptations.

- Rapports internes concernant les risques (art. 96, al. 2, let. e OS) : 37

    - les rapports indiquent la situation actuelle en matière de risques et les concentrations de risques, ainsi que les méthodes, instruments et procédures qui ont conduit à ces estimations ;

    - les rapports doivent être adressés en temps utile aux preneurs de décisions correspondants ;

    - les rapports contiennent des déclarations relatives à l'efficacité et aux points faibles

de la gestion des risques et du système interne de contrôle.

- Transparence interne et externe : L'entreprise renseigne régulièrement les divers groupes de destinataires sur : 38
  - la gouvernance d'entreprise ;
  - le genre de gestion des risques et de système interne de contrôle.

E. Surveillance à des fins de constatation de manquements et mesures correctives (Monitoring)

L'entreprise apprécie d'une part l'existence et le fonctionnement des éléments constitutifs de la gestion des risques et du système interne de contrôle et, d'autre part, l'amélioration de la qualité au cours du temps. 39