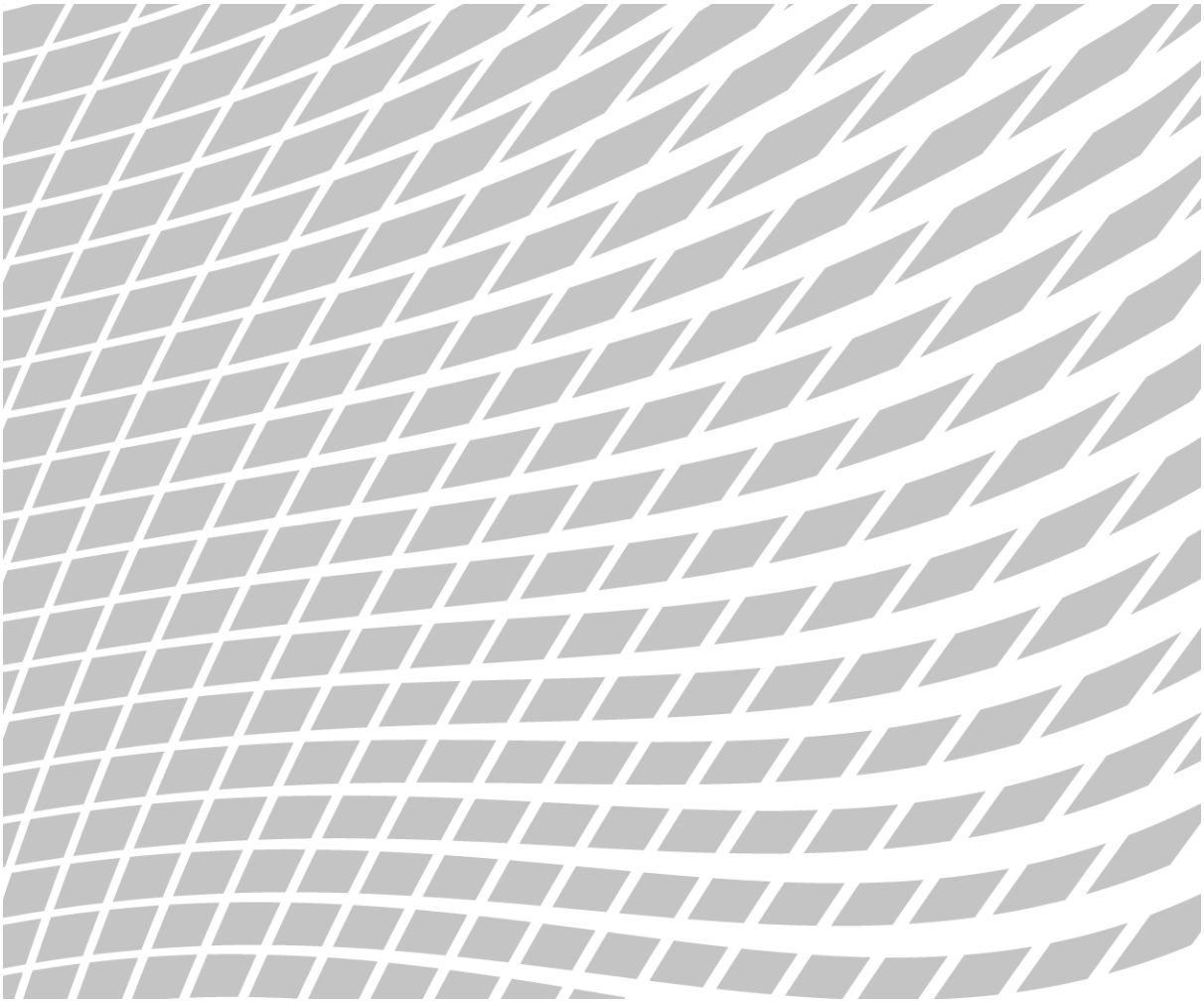
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Communication FINMA 31 (2011), 13 décembre 2011

Opérations de négoce non autorisées

Banques



Einsteinstrasse 2, 3003 Berne
Tél. +41 (0)31 327 91 00, fax +41 (0)31 327 91 01
www.finma.ch

A143616/00010/1069215

Table des matières

1 Introduction

Soucieuse de renforcer la prévention des opérations de négoce non autorisées et forte des récentes expériences engrangées en la matière, la FINMA a décidé de décrire de manière plus précise les modalités d'application des dispositions réglementaires actuelles relatives à la gestion des risques. Les récents événements qui se sont produits chez UBS ne font ici l'objet d'aucun commentaire.

Les risques opérationnels encourus dans le domaine du négoce sont souvent liés à des transactions dissimulées, non autorisées ou saisies de manière erronée, à la complexité des instruments financiers, aux nouveaux produits ou encore à la brusque augmentation du volume des échanges. Par le passé, ces risques ont maintes fois entraîné pour les banques d'investissement des pertes substantielles sur les opérations de négoce. S'agissant des prescriptions réglementaires relatives aux risques opérationnels, la FINMA renvoie aux circulaires FINMA 2008/21 « Risques opérationnels – banques », 2008/24 « Surveillance et contrôle interne – banques », 2008/7 « Outsourcing – banques » ainsi que 2010/1 « Systèmes de rémunération ».

Afin de décrire de manière plus précise les modalités d'application, la FINMA a préalablement identifié plusieurs domaines importants pour la mise en place d'un contrôle efficace et approprié des activités de négoce et, partant, pour la prévention des transactions non autorisées. Il s'agit de la direction et de la supervision de l'établissement au plus haut niveau, du système de contrôle interne, du *reporting* ainsi que de l'externalisation des fonctions de contrôle. Dans ce contexte, le risque lié aux transactions non autorisées dans le négoce ne se limite pas à certains secteurs d'activités, produits ou systèmes, mais concerne toutes les activités de négoce. Les établissements exercent des activités de négoce variées et l'on retrouve, par conséquent, une multiplicité d'organisations en matière de structures de contrôle et de gestion des risques. A cela s'ajoute la constante évolution des produits financiers et des segments d'affaires des banques. C'est la raison pour laquelle la liste d'exigences reprise ci-après n'est pas exhaustive. Elle récapitule néanmoins les attentes actuelles de la FINMA en matière de gestion des risques liés aux opérations de négoce non autorisées.

2 Direction et supervision de l'établissement

Le management à son plus haut niveau doit déterminer l'importance des risques induits par les opérations non autorisées par rapport aux autres risques de négoce. Il doit consacrer l'attention requise et sa capacité de gestion à l'identification, à l'évaluation et au contrôle de ces risques. Il lui incombe en particulier d'organiser les activités de négoce de telle sorte qu'il soit possible d'identifier, mesurer et contrôler efficacement et de manière appropriée les risques liés aux opérations de négoce non autorisées.

1. L'ampleur, la teneur et l'intensité des mesures de surveillance appliquées aux unités de négoce doivent être intégralement consignées dans des directives. Les procédures de contrôle doivent se dérouler de manière clairement distincte entre le *front office* et les unités de contrôle situées

en aval. Il convient particulièrement de déterminer clairement les responsabilités et les lignes de *reporting*.

2. L'efficacité des contrôles a la même importance que le suivi de la réalisation des objectifs financiers. A l'échelle des collaborateurs, des unités de négoce et des unités d'affaires, cela signifie que les indicateurs destinés à mesurer les activités de contrôle et leur qualité doivent faire partie intégrante du processus d'évaluation de la performance et du processus de rétribution qui en découle. Cela signifie également que lors de la fixation des objectifs annuels, il convient de mettre en balance les objectifs de rentabilité avec les risques encourus. Enfin, toute infraction matérielle aux règles doit faire l'objet d'une procédure disciplinaire et avoir des répercussions directes sur l'intensité des contrôles et sur les compétences attribuées en matière de contrôle.
3. L'évolution constante des marchés financiers justifie également de continuer à développer de manière prioritaire le système de contrôle proprement dit, en marge des contrôles courants.

3 Contrôles internes

Conformément aux principes et aux lignes directrices édictés par le management à son plus haut niveau, les contrôles internes jouent un rôle clé dans la gestion des risques issus des opérations de négoce non autorisées.

Système de contrôle interne

4. Le système de contrôle interne et le *management information system* doivent englober toute une série d'indicateurs concernant les transactions non autorisées. En cas de dépassement de seuils prédéfinis, ils doivent être capables d'alerter les unités de contrôle compétentes et de déclencher, en temps voulu, une réaction appropriée et efficace. Cet impératif implique de débloquer des ressources techniques et humaines suffisantes. La procédure de remontée relative aux messages d'alerte (*escalation*) doit par ailleurs être clairement réglementée.
5. A son niveau, chaque *trader* doit disposer d'un mandat fixant précisément les produits susceptibles d'être négociés et les stratégies pouvant être mises en œuvre. Le respect de ce mandat doit être contrôlé par une fonction indépendante. Le *trader* ne peut en aucun cas contrôler et autoriser lui-même des activités de négoce.
6. Afin de garantir une évaluation globale des performances des *traders*, les indicateurs relatifs au risque d'opérations non autorisées doivent être définis et contrôlés à l'échelon des *traders* avant d'être remontés sous forme agrégée à la direction du *front office*. L'évolution des indicateurs doit également faire l'objet d'une surveillance continue par les unités de contrôle situées en aval.
7. Le *front office* et les unités de contrôle doivent adopter une culture propre à favoriser chez leurs collaborateurs une attitude critique, responsable et professionnelle. A ce titre, il est indispensable que les unités de contrôle soient suffisamment dotées en personnel et que leurs collaborateurs disposent d'une formation suffisante pour bien comprendre les opérations de négoce assujetties à leur surveillance et qu'ils soient précisément informés de l'objectif poursuivi par chacun des contrôles effectués. Le but est qu'en cas d'anomalie, les activités de négoce concernées soient

soumises à un examen critique ciblé et sans concession. Il importe également d'instaurer une proximité physique entre les unités de négoce et celles de contrôle. Il s'agit d'un aspect dont les banques d'envergure internationale devront tenir particulièrement compte dans l'organisation du négoce.

8. L'instauration d'un tableau de bord en matière de contrôle est également fortement conseillée. Toutes les informations concernant les fonctions de contrôle d'une unité ou d'un département (Front Office, Operations, Finance, Risk, Compliance, Treasury, Human Resources, etc.) y seront régulièrement consignées. Il faut régler l'usage d'un tel tableau de bord de façon que l'évolution anormale de tel ou tel indicateur soit détectée et analysée et que le cas puisse être remonté de façon appropriée.

9. L'analyse régulière de l'efficacité des systèmes de contrôle revêt aussi une très grande importance. En effet, il est impératif de garantir une très haute qualité de contrôle mais également de vérifier en continu cette qualité. Par conséquent, soumettre l'efficacité des contrôles à un seul examen par an ne suffit pas. Il doit être assuré que les contrôles aient la portée prévue et soient conduits conformément à la fréquence fixée. Tout contrôle incomplet doit immédiatement être remonté. Pour déceler les éventuelles lacunes et autres points faibles, différents instruments d'aide peuvent être utilisés, tels que des analyses de scénarios, des revues régulières ou des tests grandeur nature de l'environnement de négoce (usurpation de mots de passe, utilisation non autorisée de profils d'utilisateur, établissement de documents fictifs ou de fausses écritures comptables). Les contrôles devront ensuite être adaptés en fonction des résultats de ces tests. Les mesures prises pour remédier aux lacunes observées doivent faire l'objet d'un contrôle de qualité rigoureux.

10. Le changement de collaborateurs, les restructurations et l'implémentation de nouveaux systèmes informatiques sont autant de moments critiques. Même en période de passage de l'ancienne à la nouvelle organisation ou de l'ancien système informatique au nouveau, il importe que tous les contrôles prévus soient exécutés selon la fréquence requise et conformément aux critères de qualité retenus. Le cas échéant, des mesures complémentaires temporaires devraient être prises. Cela vaut également pour le cas d'externalisation des activités de contrôle (voir le chapitre 5).

11. Le transfert de collaborateurs entre le *front office*, le middle office et le back office doit faire l'objet d'une réglementation particulière, afin de réduire à un minimum les risques d'opérations non autorisées. S'ils ne sont pas interdits, de tels transferts doivent en tout état de cause être consignés et faire l'objet de contrôles continus. Il convient également d'imposer un nombre minimal de jours de congé par an qui doivent être pris en un bloc. Enfin, les relations entre les *traders* et leurs contreparties de négoce doivent être surveillées de manière adéquate.

12. Les droits d'accès des *traders* aux systèmes boursiers, comptables et de règlement des transactions seront régulièrement contrôlés afin de vérifier leur conformité avec les mandats de négoce attribués.

Contrôles opérationnels

13. En principe, les montants nominaux des positions de négoce doivent faire l'objet d'une surveillance et de limites à la fois en termes bruts et en termes nets, même lorsque seules les positions nettes ont une signification sur le plan économique. En effet, le contrôle des montants nominaux bruts peut contribuer à détecter des schémas inhabituels ou des opérations non autorisées. Ce principe s'applique également aux indicateurs de risques proprement dits, qui doivent être mesurés, surveillés et limités séparément tant pour les positions longues que pour les positions courtes – et ce quand bien même seul le risque net revêt de l'importance économiquement parlant.
14. Les montants nominaux et les indicateurs de risques doivent être suivis non seulement en fin de journée mais aussi pendant la journée. Ils doivent également être soumis à des restrictions pendant la journée de négoce.
15. Lorsque les échanges atteignent des volumes considérables, il est important que les routines de contrôle, soutenues par l'IT, effectuent une présélection pour le management des transactions à contrôler afin d'affecter les ressources de contrôle selon une approche risque. En particulier, les opérations hors norme devraient être soumises en priorité à un contrôle détaillé et permanent. Il s'agit notamment des opérations conclues hors prix du marché, interrompues, modifiées, comptabilisées tardivement ou assorties de délais de paiement différés.
16. En principe, des confirmations doivent être activement sollicitées pour toutes les opérations, qu'elles soient internes ou externes. On contrôlera tout particulièrement les confirmations en suspens et l'on signalera les confirmations manquantes à l'échelon supérieur. Le *front office* ne doit pas intervenir dans le processus de confirmation ni tenter de l'influencer de manière inappropriée.
17. Il est également essentiel de mettre en place une procédure indépendante et performante de rapprochement des comptes, englobant tous les comptes, internes comme externes. Cela vaut aussi pour les comptes affectés à un but particulier (comptes d'attente) comme les écritures de correction de pertes et profits ou la comptabilisation de commissions et de rémunérations. En cas de divergence entre deux comptes, une procédure robuste doit prévoir une évaluation des risques et garantir que les écritures de correction ou l'apurement seront effectuées de manière adéquate et pertinente.
18. Toute ouverture ou clôture de comptes – y compris de comptes inactifs – doit être explicitement réglementée et faire l'objet de contrôles continus.
19. Une procédure de rapprochement identique sera appliquée aux appels de marge en relation avec des opérations couvertes. En cas d'incohérences, la procédure doit là aussi prévoir une évaluation des risques et garantir que l'apurement sera effectué de manière adéquate et pertinente.

Attribution des pertes et profits de négoce

20. L'attribution des pertes et des profits découlant des activités de négoce constitue un contrôle clé qui aide à mieux comprendre les risques liés à ces activités. A ce titre, il convient en particulier de s'assurer que les pertes ou les profits individuels de grande envergure seront soumis à une ana-

lyse appropriée au titre du contrôle des risques opérationnels. Toute fluctuation sensible des pertes et profits sur une période donnée (calculée en semaines, en mois ou en trimestres) doit également être remise en cause et retracée avec précision.

21. S'agissant des opérations conclues hors prix du marché, interrompues, modifiées, comptabilisées tardivement ou assorties de délais de paiement différés, leur impact sur les pertes et profits doit lui aussi être intégré dans les analyses quotidiennes et mensuelles.

4 Reporting interne

22. Le *reporting* interne devrait permettre de contrôler de manière appropriée les risques opérationnels dans le secteur du négoce. La direction du négoce doit disposer dans les plus brefs délais d'informations sur les indicateurs de risques opérationnels, ce qui nécessite entre autres le recours à des technologies de l'information performantes.
23. Le système de *reporting* des risques opérationnels doit être en mesure de générer des alertes automatiques dès que les indicateurs sélectionnés franchissent des seuils déterminés afin de prévenir sans délai la direction de tout incident majeur. Cette exigence impose notamment le stockage et l'analyse de toutes les pertes opérationnelles majeures issues d'opérations de négoce.
24. En plus de la surveillance et de l'analyse des indicateurs internes, le *reporting* concernant les risques opérationnels doit également rapporter et évaluer de manière systématique les alertes et autres notifications émanant de tiers (collaborateurs, bourses, courtiers, organismes de compensation, banques de dépôt, etc.).
25. Le *reporting*, et en premier lieu le tableau de bord en matière de contrôle, doivent permettre l'analyse dans leur globalité des pertes et profits, du besoin de liquidités et des risques, que ce soit au niveau d'une unité ou d'un secteur d'activité donné.

5 Externalisation

Le fait de déléguer les contrôles à des tiers (outsourcing au sens de la Circ.-FINMA 2008/7 « Outsourcing – banques », Cm 2 et 3) nécessite de prendre certaines précautions afin de garantir le déroulement ininterrompu et intégral de ces contrôles.

26. Il faut en particulier veiller à ce que les changements intervenant au sein du délégataire (changements de collaborateurs, restructurations, changements de système informatique) n'entravent pas la bonne exécution des contrôles.
27. La réalisation d'un seul examen annuel des prestations externalisées n'est pas suffisante pour garantir le déroulement ininterrompu et intégral des contrôles. Au contraire, il conviendra de soumettre les services de ces tiers à une surveillance et à une évaluation permanentes.

Nonobstant les autres dispositions de la Circ.-FINMA 2008/7 « Outsourcing – banques », l'externalisation des activités de contrôle doit être soumise aux principes suivants :

28. L'entreprise doit choisir, instruire et contrôler le délégataire avec diligence (Circ.-FINMA 2008/7 « Outsourcing – banques », Cm 21).
29. Les critères et les facteurs guidant le choix du délégataire et la collaboration avec celui-ci doivent être déterminés avant qu'une relation contractuelle soit nouée. Le choix du délégataire se fera après examen de ses capacités professionnelles ainsi que de ses ressources humaines et financières. Le délégataire doit présenter toutes garanties d'une activité d'outsourcing sûre et durable (Circ.-FINMA 2008/7 Outsourcing – banques, Cm 22).
30. Le système de contrôle interne de l'entreprise doit s'étendre au domaine d'activités transféré. L'entreprise désigne en son sein une personne chargée de la surveillance et du contrôle du délégataire. Les activités de celui-ci sont à surveiller et évaluer de façon suivie, de sorte que les mesures adéquates puissent être prises le cas échéant (Circ.-FINMA 2008/7 « Outsourcing – banques », Cm 24).