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

Guide pratique

relatif à la réalisation de l'**audit prudentiel** et destiné aux **sociétés d'audit** des banques, maisons de titres et groupes financiers

Édition du 2 février 2024

But

Le présent guide pratique est un document d'aide destiné aux sociétés d'audit prudentielles des banques, maisons de titres et groupes financiers en relation avec le traitement des formulaires d'enquête suivants relatif à l'audit prudentiel : l'analyse des risques, la stratégie d'audit standard et le rapport sur l'audit prudentiel. Il contient également des indications concernant la réalisation des audits prudentiels.

I. Généralités

- La structure du présent guide pratique ainsi que des formulaires susmentionnés se fonde sur la Circ.-FINMA 2013/3 « Activités d'audit ».
- La FINMA met à disposition de la société d'audit, pour chaque établissement à auditer, des documents d'enquête spécifiques par le biais de la plate-forme électronique de saisie et demande (ci-après « EHP »)[1]. Ainsi, la société d'audit procède directement à une saisie de l'analyse des risques, de la stratégie d'audit et du rapport sur l'audit prudentiel dans les documents électroniques mis à sa disposition par le truchement de l'EHP. La remise des formulaires se fait également électroniquement via la fonction correspondante de l'EHP; le rapport sur l'audit prudentiel doit être remis sous forme signée (cf. ch. IV. Rapport sur l'audit prudentiel).
- Seule la partie « niveau individuel » est remplie s'agissant des établissements sans aspect consolidé. En présence d'une structure de type maison-mère, la partie « surveillance consolidée » est également complétée, les aspects individuel et consolidé étant ainsi traités en principe dans un seul formulaire. En présence d'une structure atypique ou de type holding, seule la partie « surveil-

[1] cf. www.finma.ch > FINMA > Extranet > Plate-forme de saisie et de demande ; login: https://portal.finma.ch/auth-login/portal?lang=fr

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

lance consolidée » (niveau groupe) est remplie, étant précisé que deux formulaires au moins doivent être remis si l'on tient compte du formulaire établi au niveau individuel pour l'établissement autorisé. Les parties des formulaires qui doivent être remplies se fondent sur les options choisies pour traiter le formulaire (données de base).

- Dans l'éventualité où les formulaires déjà remis devaient faire l'objet d'adaptations ou de compléments, il est possible d'en faire état à la personne de contact de la FINMA. Les formulaires concernés se voient alors conférés le statut « en cours de correction » et doivent faire l'objet d'une nouvelle remise après finalisation de la saisie des adaptations/compléments.
- La société d'audit doit tenir compte des indications et explications figurant cas échéant dans les différents formulaires d'enquête lorsqu'elle procède à leur traitement.
- Les champs marqués d'un astérisque (*) sont obligatoires et doivent impérativement être complétés avant la remise du formulaire concerné.
- L'année d'audit doit être indiquée dans le formulaire d'enquête, sous la forme d'une saisie à quatre chiffres qui se rapporte au début de la période d'audit concernée.
- Des informations générales relatives à la plate-forme EHP, comme par ex. au traitement et à la remise des documents d'enquête, au statut de l'enquête ou à la gestion des accès sont disponibles sur le site web de la FINMA[2].

II. Analyse des risques des banques et maisons de titres

- Les risques pertinents au sein d'un domaine / champ d'audit doivent être décrits de manière concrète, en vertu de la situation spécifique de l'établissement et, si possible, en y incluant des données chiffrées (« **Description du risque** »).
- Si certains aspects de l'audit ne s'appliquent pas à un établissement donné, la société d'audit peut renoncer à traiter le domaine ou champ d'audit en question. Une justification est mentionnée dans la « **Description du risque** » et les indications « n/a » sont sélectionnés sous « **Ampleur / volume** ».
- En ce qui concerne le champ « **Ampleur / volume** », la société d'audit évalue dans quel(le) ampleur / volume l'établissement autorisé ou le groupe serait concerné si les risques identifiés devaient se concrétiser. Sous « **Probabilité d'occurrence** », la société d'audit donne une estimation subjective par risque identifié.
- Le rapport entre l'ampleur / volume et la probabilité d'occurrence du risque par domaine ou champ d'audit détermine le « **Risque inhérent (brut)** ».

[2] cf. www.finma.ch > FINMA > Extranet > Plate-forme de saisie et de demande > Pages d'aide

- Sous « **Risque de contrôle** », la société d'audit remet une estimation de l'adéquation et de l'efficacité des contrôles internes. Les prescriptions exposées aux Cm 80 ss Circ.-FINMA 13/3 sont applicables.
- Le rapport entre le risque inhérent (brut) et le risque de contrôle détermine le risque combiné (net) qui est rapporté sous « **Risque net** ». La détermination du risque net s'effectue dans le formulaire de manière automatique en fonction de la systématique du Cm 85 Circ.-FINMA 13/3.
- La société d'audit classe les risques en fonction du risque inhérent (« **Hiérarchie des risques (bruts, top 10)** ») ainsi que du risque net (« **Hiérarchie des risques (nets, top 10)** »). Pour ce faire, elle numérote les dix plus grands risques de 1 à 10 (1 = risque le plus important). Cette procédure ne concerne que les domaines et champs d'audit du niveau individuel.
- Dans la partie « surveillance consolidée », le segment « **éléments complémentaires** » est traité dans les cas ci-après :

  En présence d'une structure de type maison-mère, des informations sont saisies lorsque d'autres sociétés du groupe comportent des risques significatifs, en sus de l'entité pour laquelle l'analyse des risques est disponible au niveau individuel.

  Dans le cas d'une structure atypique ou de type holding, il y a lieu de prendre en compte les sociétés du groupe qui sont la source de risques d'affaires significatifs. Des renvois à des analyses des risques individuelles séparées sont possibles.

III. Stratégie d'audit des banques et maisons de titres

- Selon le Cm 106 Circ.-FINMA 13/3, la société d'audit procède à une estimation des coûts d'audit afférents à sa stratégie d'audit. Cette estimation est faite en distinguant (i) les coûts résultant directement de l'examen des domaines d'audit et (ii) les coûts généraux ne pouvant pas être attribués aux domaines d'audit (par ex. pour la planification de l'audit, les rapports, le contrôle de qualité). S'agissant des assujettis des catégories de surveillance 1 à 3, l'estimation des coûts d'audit pouvant être attribués aux domaines d'audit est établie pour chaque champ / domaine d'audit.
- Les audits effectués en lien avec des approches par un modèle interne soumis à autorisation en matière de risques opérationnels, de risque de crédit, de risque de contrepartie ou de marché doivent faire l'objet d'une distinction fondée sur les critères suivants : travaux d'audit pour de nouvelles autorisations de modèles (i), de modifications de modèles (ii) et de surveillance de modèles (iii). Dans le cadre du formulaire d'enquête portant sur la stratégie d'audit, seuls les travaux d'audit en matière de surveillance de modèles doivent être pris en considération. Ces derniers doivent être planifiés en tant que composantes de l'audit de base portant sur le domaine d'audit« Exigences de fonds

propres découlant des approches par un modèle internes autorisées par la FINMA et conditions d'autorisation pour ces approches ». Les coûts / heures d'audit estimé(e)s pour la surveillance de modèles doivent par ailleurs faire l'objet d'une indication supplémentaire détaillée sous « Part des heures/coûts pour la "surveillance de modèles" dans le cadre de l'audit de base ».

- Les établissements des catégories de surveillance 3 à 5 sont soumis en principe à l'application de la stratégie d'audit standard selon les Cm 87.1 ss Circ.-FINMA 13/3. Si une « **Intervention actuelle / planifiée** » dévie de la stratégie d'audit standard, ceci doit être indiqué et justifié (« **Justification de la stratégie d'audit** »).
- En ce qui concerne la « **Justification de la stratégie d'audit / brève description des secteurs à auditer** », la société d'audit décrit de manière sommaire ce qui est planifié dans les domaines / champs d'audit soumis à une intervention graduelle ainsi que les secteurs à auditer couverts à cet égard lors des interventions des trois années antérieures. Par principe, la société d'audit assure le respect de la périodicité.
- Dans le cas de **contrôles subséquents** selon le Cm 110 Circ.-FINMA 13/3, une indication ad hoc est requise dans le champ "Contrôle subséquent" relatif au domaine d'audit correspondant, et les lacunes concernées sont rapportées sous « **Justification de la stratégie d'audit / brève description des secteurs à auditer** ». Dans l'éventualité où le contrôle subséquent survient dans un domaine d'audit qui, selon l'analyse des risques et la stratégie d'audit, ne doit pas être soumis dans l'année concernée à une intervention, il y lieu de choisir l'option « aucune » sous « **Intervention actuelle / planifiée** ».
- Lors du premier audit suivant la prise en charge du mandat, la société d'audit doit déterminer selon sa libre appréciation l'étendue de l'audit et/ou sa périodicité, le cas échéant en prenant en compte les dispositions figurant ci-avant (indication sous « **Justification stratégie d'audit / brève description des secteurs à auditer** »).
- La société d'audit peut proposer à la FINMA des audits supplémentaires lorsqu'un établissement autorisé (y c. surveillance consolidée) présente des risques qui ne sont pas couverts par les domaines / champs d'audit prévus dans l'audit de base (indication sous « **Audits supplémentaires** »). La FINMA décide de la mise en œuvre et des modalités des audits supplémentaires. En outre, la FINMA peut elle-même ordonner des audits supplémentaires en cas de besoin.

Interventions après le 1er janvier 2024 (entrée en vigueur de la circulaire 2023/1 « Risques et résilience opérationnels – banques » de la FINMA et de la révision partielle du 7 décembre 2022 de la Circ.-FINMA 13/3)

- Les premières interventions relatives à la Circ.-FINMA 23/1 et à la Circ.-FINMA 13/3 partiellement révisée auront lieu à partir de l'**année d'audit 2024**.

- Les points d'audits concernant l'informatique et le traitement des données électroniques des clients ont été supprimés à la fin de l'année 2023. À partir de l'année d'audit 2024, il y a de nouveaux points d'audit concernant **la gestion des cyberrisques** et **la gestion des risques des données critiques**.
- Pour l'élaboration de l'analyse des risques et de la stratégie d'audit concernant le champ d'audit « **Gestion globale des risques opérationnels** » (PS.IOK.ORM) en 2024 et les années subséquentes, les interventions précédentes concernant le champ d'audit « Exigences qualitatives concernant la gestion des risques opérationnels » (PS.IOK.QOR) peuvent être prises en compte (en ce qui concerne les « dernières interventions » et le « risque de contrôle »).
- Pour l'élaboration de l'analyse des risques et de la stratégie d'audit concernant le champ d'audit « **Gestion des risques des données critiques** » (PS.IOK.DAT) en 2024 et les années subséquentes, les interventions précédentes concernant le champ d'audit « Traitement des données électroniques des clients » (PS.IOK.EKD) peuvent être prises en compte (en ce qui concerne les « dernières interventions » et le « risque de contrôle »). Le nouveau programme d'audit sur la gestion des risques des données critiques s'applique.
- Pour l'élaboration de l'analyse des risques et de la stratégie d'audit concernant le champ d'audit « **Gestion des cyberrisques** » (PS.IOK.CYB) en 2024 et les années subséquentes, les interventions précédentes concernant l'élément « Risques et contrôles informatiques / cyberrisques » du champ d'audit « Informatique (IT) » (PS.IOK.INF) peuvent être prises en compte (en ce qui concerne les « dernières interventions » et le « risque de contrôle »). Pour les établissements présentant un risque net « moyen », il appartient à la société d'audit de répartir sur les années d'audit 2024 à 2026 les interventions prévues pour l'année d'audit 2024 conformément à la stratégie d'audit standard. Pour les établissements présentant un risque net « élevé » ou « très élevé », la stratégie d'audit standard doit être appliquée. Le nouveau programme d'audit sur la gestion des cyberrisques s'applique.
- Pour l'élaboration de l'analyse des risques et de la stratégie d'audit concernant le champ d'audit « **Gestion des risques liés à la technologie de l'information et de la communication (risques TIC)** » (avec les nouveaux éléments : (a) stratégie TIC et gouvernance, (b) gestion des changements, (c) exploitation des TIC et (d) gestion des incidents) en 2024 et les années subséquentes, les interventions précédentes concernant le domaine d'audit « Informatique (IT) » (PS.IOK.INF) et les différents éléments du programme d'audit des points d'audits supprimés relatifs à l'informatique peuvent être pris en compte (en ce qui concerne les « dernières interventions » et le « risque de contrôle ») :

- Le nouvel élément « **Stratégie TIC et gouvernance** » se réfère à l'historique des interventions relatives à l'ancien élément du programme d'audit « Stratégie, organisation et gouvernance informatiques ».
- Le nouvel élément « **Gestion des changements** » se réfère à l'historique des interventions de l'élément du programme d'audit « Infrastructure IT et prestations de services IT ».
- Le nouvel élément « **Exploitation des TIC** » se réfère à l'historique des interventions de l'élément du programme d'audit « Infrastructure IT et prestations de services IT ».
- Aucun historique des interventions n'est disponible pour l'élément « **Gestion des incidents** ».

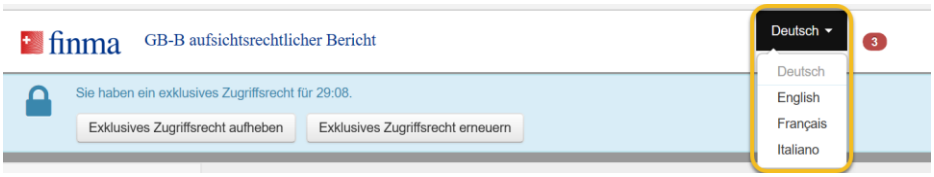
Il est possible que le recours à l'historique des interventions révèle un besoin d'intervention sur plusieurs des quatre éléments du champ d'audit « Gestion des risques TIC » en 2024. Le choix de l'un des quatre éléments pour l'intervention en 2024 est laissé à l'appréciation de la société d'audit sur la base de l'analyse des risques. Il sera procédé de la même manière les années subséquentes jusqu'à ce que le nouveau cycle de couverture progressive des quatre éléments soit établi sur quatre ans. Pour les établissements qui bénéficient d'une cadence d'audit réduite, un élément est couvert par année intermédiaire et par année d'audit (trois éléments par intervention pour les établissements avec une cadence d'audit réduite de trois ans).

- Pour le nouveau champ d'audit « **Résilience opérationnelle** » (PS.IOK.RES), la Circ.-FINMA 23/1 prévoit en partie des dispositions transitoires pouvant aller jusqu'à deux ans. Une première intervention peut avoir lieu à partir de 2024, à l'appréciation de la société d'audit et sur la base de son analyse des risques. Une intervention doit être effectuée au plus tard au cours de l'année d'audit 2027, c'est-à-dire la deuxième année après l'expiration du délai transitoire.

IV. Rapport sur l'audit prudentiel des banques et maisons de titres

- Conformément à l'art. 9 al. 2 OA-FINMA, le rapport d'audit est rédigé dans l'une des langues officielles. Dans des cas exceptionnels, l'établissement d'un rapport en anglais est possible sur demande de la société d'audit et après approbation de la FINMA. La langue du rapport peut être modifiée dans l'en-tête

du formulaire de saisie.



- Le rapport sur l'audit prudentiel doit présenter les résultats de l'audit de façon exhaustive, explicite et objective. L'auditeur responsable ainsi qu'un autre auditeur autorisé à signer le confirmement par leur signature (signature électronique qualifiée) sur le rapport (PDF) remis en annexe à l'envoi électronique via l'EHP. Si le rapport ne peut être signé au moyen d'une signature électronique qualifiée, il doit être imprimé, signé à la main et envoyé par voie postale à la FINMA (en plus de l'envoi électronique via l'EHP).
- Les irrégularités et recommandations conformément à l'art. 11 de l'ordonnance sur les audits des marchés financiers (OA-FINMA ; RS 956.161) doivent figurer sans exception dans la partie « **Résumé des résultats de l'audit** ». Elles font l'objet d'une notation (classification d'après les Cm 75.2 ss Circ.-FINMA 13/3).
- La société d'audit veille à ce que le rapport d'audit et les éventuels rapports complémentaires établis à l'intention de l'établissement autorisé (par ex. au sens d'une *management letter*) soient cohérents. Les constatations significatives figurant dans d'autres mandats/rapports sont également reprises dans le rapport d'audit. En principe, d'éventuels autres rapports adressés à l'établissement autorisé ne doivent pas être remis spontanément à la FINMA.
- Concernant l'établissement des rapports sur l'audit prudentiel pour les banques et les maisons de titres ainsi que leurs groupes financiers, quand une surveillance consolidée s'impose, il convient de joindre en « **Annexe** » les documents suivants[3]:
  - formulaire d'enquête LBA (enquête séparée) ;
  - présentation synoptique de la structure du groupe incluant les taux de participation (en prenant en considération les indications complémentaires en matière de surveillance consolidée, cf. chiffre 6.10 du rapport sur l'audit prudentiel des banques) ;
  - organigramme(s) (au moins avec l'indication des personnes responsables par secteur d'affaires ou par département).

[3] Une copie du rapport détaillé sur l'audit comptable conformément à l'art. 728*b* al. 1 CO (cf. annexe 18 Circ.-FINMA 13/3) est remise sous forme d'annexe de l'enquête séparée « Conduite d'un audit comptable ».

V. Indications concernant la réalisation des audits

- L'annexe au présent guide pratique fait état des bases juridiques qui doivent faire l'objet de l'audit de base. Elle ne contient généralement pas une énumération exhaustive des dispositions légales. Par ailleurs, l'annexe contient une présentation synoptique des Cm 87.1 à 102 Circ.-FINMA 13/3, lesquels stipulent les cycles d'audit applicables à chaque domaine / champ d'audit en fonction du risque net.
- En ce qui concerne certains domaines/champs d'audit, des « points d'audit standardisés » ont été élaborés. Ces derniers sont applicables chaque fois qu'une intervention a lieu dans un domaine / champ d'audit concerné. Lorsque certains aspects des points d'audit ne sont pas applicables, les réflexions y relatives doivent être consignées dans la documentation d'audit sous une forme compréhensible par un tiers. Les points d'audit ne constituent pas nécessairement une base décrivant de manière exhaustive les vérifications à exercer et les auditeurs doivent, si nécessaire, les compléter. Les travaux effectués et les constatations y relatives doivent être documentés de manière compréhensible par un tiers. Cette documentation peut être concrétisée sous une forme qui diffère des documents-modèles exposant les points d'audit, dans la mesure où elle contient toutes les indications figurant dans les documents-modèles précités.

Annexe : Bases juridiques de l'audit prudentiel / stratégie d'audit standard