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** (guide pratique audit prudentiel banques)

Édition du 10 mars 2025

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 complémentaires concernant les principes d'audit et la réalisation des audits prudentiels.

I. Généralités

La structure du présent guide pratique ainsi que des formulaires susmentionnés l'analyse des risques, la stratégie d'audit standard et le rapport sur l'audit prudentiel se fonde sur l'ordonnance de la FINMA du 31 octobre 2024 sur l'audit prudentiel (ordonnance FINMA sur l'audit prudentiel ; RS *956.161.1*) et sur la circulaire FINMA 2025/1 « Activités d'audit ».

La FINMA met à disposition de la société d'audit, pour chaque établissement à auditer, les modèles à utiliser sous la forme de formulaires d'enquête par le biais de la plate-forme électronique de saisie et de demande de la FINMA (ci-après « EHP »)[1]. Ainsi, la société d'audit saisit l'analyse des risques, la stratégie d'audit et le rapport sur l'audit prudentiel directement dans les formulaires d'enquête mis à

[1] www.finma.ch > FINMA > Échange numérique avec la FINMA > EHP : transmettre des demandes, des déclarations et des données ou annoncer le changement de BVA > Accès à EHP disponible > Vers le login EHP

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

sa disposition par le biais de la plate-forme EHP. La remise des formulaires d'enquête se fait également par voie électronique au moyen de la fonction correspondante d'EHP.

Seule la partie « niveau individuel » des formulaires d'enquête correspondants 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 d'enquête. En présence d'une structure atypique ou de type holding, seule la partie « surveillance consolidée » (niveau du groupe) est remplie, étant précisé que deux formulaires d'enquête au moins doivent être remis si l'on tient compte du formulaire établi au niveau individuel pour le titulaire d'autorisation. Les parties des formulaires d'enquête qui doivent être remplies sont affichées en fonction des options choisies pour traiter le formulaire (données de base).

Dans l'éventualité où les formulaires d'enquête déjà remis devaient faire l'objet d'adaptations ou de compléments, il convient d'en faire état à la personne de contact de la FINMA. Les formulaires d'enquête concernés se voient alors conférer le statut « en cours de correction » et doivent être à nouveau envoyés dans les délais après les adaptations/compléments.

La société d'audit doit également tenir compte des éventuelles indications et explications figurant 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.

Si l'année d'audit est requise dans le formulaire d'enquête, elle doit être indiquée sous la forme d'un nombre à quatre chiffres et doit se référer au début de la période d'audit concernée.

Des informations générales relatives à la plate-forme EHP, telles que le traitement et la remise d'un formulaire d'enquête, le statut d'une enquête ou la gestion des accès sont disponibles sur le site Internet de la FINMA[2].

[2] Cf. www.finma.ch > FINMA > Échange numérique avec la FINMA > EHP : transmettre des demandes, des déclarations et des données ou annoncer le changement de BVA

II. Analyse des risques

II.1 Description des risques

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 sélectionnées sous « **Ampleur / volume** ».

II.2 Classification des risques

En ce qui concerne le champ **« Ampleur / volume »**, la société d'audit évalue dans quel(le) ampleur / volume le titulaire d'autorisation 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 / le volume et la probabilité d'occurrence du risque par domaine ou champ d'audit détermine le **« Risque inhérent (brut) »**. Les prescriptions de l'art. 6 al. 1 en relation avec celles de l'annexe 1 de l'ordonnance FINMA sur l'audit prudentiel s'appliquent.

Sous **« Risque de contrôle »**, la société d'audit donne une estimation de l'adéquation et de l'efficacité des contrôles internes. Les prescriptions de l'art. 6 al. 2 en relation avec celles de l'annexe 2 de l'ordonnance FINMA sur l'audit prudentiel s'appliquent.

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 d'enquête de manière automatique en fonction de la systématique de l'art. 6 al. 3 en relation avec l'annexe 3 de l'ordonnance FINMA sur l'audit prudentiel.

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

III.1 Règles générales

Les établissements des catégories de surveillance 3 à 5 sont soumis en principe à l'application de la stratégie d'audit standard selon l'art. 32 al. 2 à 4 de l'ordonnance FINMA sur l'audit prudentiel (cf. modèle « Stratégie d'audit standard »). Si une **« Intervention actuelle / planifiée »** de la stratégie d'audit standard propre à l'établissement dévie de la stratégie 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 pour 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 l'art. 15 de l'ordonnance FINMA sur l'audit prudentiel, 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 »**.

La société d'audit peut proposer à la FINMA des audits supplémentaires lorsqu'un titulaire d'autorisation (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 ordonner elle-même des audits supplémentaires en cas de besoin (cf. Cm 4 Circ.-FINMA 25/1).

III.2 Estimation des coûts d'audit

Conformément à l'art. 33 al. 2 de l'ordonnance FINMA sur l'audit prudentiel, la société d'audit procède à une estimation des coûts d'audit afférents à sa stratégie d'audit. Cette estimation est faite en distinguant :

- les coûts résultant directement de l'examen des domaines ou champs d'audit, et
- les coûts généraux ne pouvant pas être attribués aux domaines ou champs d'audit (par ex. coûts liés à la planification de l'audit, aux rapports, à l'assurance de la qualité).

S'agissant des assujettis des catégories de surveillance 1 à 3, l'estimation des coûts d'audit pouvant être attribués aux domaines ou champs d'audit est établie pour chaque domaine ou champ d'audit.

Les coûts / heures d'audit estimé(e)s pour l'audit de 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 ».

III.3 Règles spécifiques pour certains domaines et champs d'audit

La périodicité de l'audit et l'étendue d'audit prévus à l'art. 30 de l'ordonnance FINMA sur l'audit prudentiel ne s'appliquent pas aux domaines et champs d'audit indiqués ci-après.

III.3.1 Exigences de fonds propres découlant des approches par modèles internes autorisées par la FINMA et conditions d'autorisation pour ces approches

Couverture graduelle des thèmes sur quatre ans. La couverture s'effectue en principe avec l'étendue d'audit « revue critique » en cas de risque net « faible » et avec l'étendue d'audit « audit » en cas de risque net « moyen » à « très élevé ». Pour les structures de modèle simples, la société d'audit peut se limiter à un audit global unique (étendue « audit ») des différents thèmes sur une période de quatre ans.

Les audits effectués en lien avec des approches par modèles internes 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), des modifications de modèles (ii) et la surveillance de modèles (iii). Dans le 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 modèles internes autorisées par la FINMA et conditions d'autorisation pour ces approches ».

III.3.2 Organisation interne et système de contrôle interne

Couverture graduelle des thèmes sur six ans avec une étendue d'audit laissée à l'appréciation de la société d'audit.

III.3.3 Gestion des risques TIC

Couverture graduelle des thèmes sur quatre ans avec une étendue d'audit laissée à l'appréciation de la société d'audit.

III.3.4 Externalisation

Couverture graduelle de chacun des thèmes sur six ans avec une étendue d'audit laissée à l'appréciation de la société d'audit. Une intervention avec l'étendue « audit » a lieu la première année pour les conventions d'externalisation nouvellement reçues.

III.3.5 Révision interne (établissement individuel) et révision interne de groupe (niveau du groupe)

Les champs d'audit Révision interne (établissement individuel) et révision interne de groupe (niveau du groupe) sont soumis à une revue critique annuelle.

III.3.6 Respect des prescriptions en matière de lutte contre le blanchiment d'argent (établissement individuel) et mesures de lutte contre le blanchiment d'argent à l'échelle du groupe (niveau du groupe)

En cas de risque net « élevé » ou « très élevé », une intervention avec l'étendue d'audit « audit » a lieu chaque année. En cas de risque net « moyen », une intervention avec l'étendue d'audit « audit » a lieu au moins tous les 2 ans. En cas de risque net « faible », une intervention avec l'étendue d'audit « audit » a lieu au moins tous les 3 ans.

III.3.7 Gouvernance d'entreprise au niveau du groupe

Revue critique annuelle.

III.3.8 Fonctions de groupe pour le contrôle et la réduction des risques

Revue critique annuelle. En cas de risque net « très élevé », une intervention avec l'étendue d'audit « audit » a lieu chaque année.

III.4 Audit réalisé en lien avec la circulaire FINMA 2023/1 « Risques et résilience opérationnels – banques » – règlementation provisoire

Les interventions effectuées en lien avec la Circ.-FINMA 23/1 ont lieu depuis **l'année d'audit 2024**.

Les points d'audit concernant l'informatique et le traitement des données électroniques des clients ont été supprimés à la fin de l'année 2023. Depuis 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), 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), 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 »).

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), 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.

Pour l'élaboration de l'analyse des risques et de la stratégie d'audit concernant le champ d'audit **« Gestion des 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 comme suit (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 » sur une année d'audit. Le choix de l'un des quatre éléments par année d'audit 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 depuis 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. Principes d'audit

Les audits doivent se fonder sur l'ordonnance FINMA sur l'audit prudentiel et la Circ.-FINMA 25/1. Les normes d'audit nationales et internationales relatives à l'audit des comptes ne font pas foi pour l'audit prudentiel.

Les exigences relatives à l'assurance de la qualité (art. 12 ordonnance FINMA sur l'audit prudentiel) s'appliquent entre autres à la planification et au programme de l'audit, à la délégation de tâches en fonction des compétences à des collabora-

teurs qualifiés, à la mise à disposition des informations requises pour l'audit, à l'instruction des équipes d'audit et à leur surveillance et enfin à une gestion du temps adéquate.

V. Rapport sur l'audit prudentiel

L'établissement des rapports est régi par les art. 22 à 28 ordonnance FINMA sur l'audit prudentiel. La FINMA fournit ci-après des explications complémentaires à ce sujet.

La vue d'ensemble des conditions générales de l'audit contient en particulier l'étendue et la période de l'audit, le nom des personnes essentielles impliquées dans l'audit (personnes occupant une fonction d'encadrement et de coordination et spécialistes de l'informatique, de la fiscalité, de l'évaluation, etc.), la période durant laquelle les travaux d'audit ont eu lieu ainsi que la procédure choisie, l'ampleur de la prise en compte de travaux de tiers, la confirmation du respect de la stratégie d'audit, la mention des difficultés rencontrées lors de l'audit et la confirmation que l'assujetti a mis toutes les informations requises à disposition en temps utile et avec la qualité nécessaire.

Les irrégularités et recommandations doivent figurer sans exception dans la partie **« Résumé des résultats de l'audit »**. Elles font l'objet d'une notation (classification selon les art. 25 et 26 de l'ordonnance FINMA sur l'audit prudentiel).

La présentation des irrégularités et recommandations comprend les délais de la société d'audit pour la correction ou la mise en œuvre ainsi que les mesures déjà prises ou à prendre par l'assujetti pour remédier à l'irrégularité ou pour mettre en œuvre la recommandation. Seules les irrégularités et recommandations pour lesquelles la société d'audit avait prévu ses propres contrôles d'audit selon la stratégie d'audit doivent être traitées.

La présentation des faiblesses matérielles révélées par des tiers contient également les faiblesses révélées par la révision interne si la société d'audit ne s'appuie pas sur les travaux de la révision interne.

Il incombe à la société d'audit de vérifier systématiquement le rétablissement de la situation selon l'art. 27 al. 2 de la loi sur la surveillance des marchés financiers (RS *956.1*). Dans le cas des établissements ayant une cadence d'audit réduite selon l'art. 31 de l'ordonnance FINMA sur l'audit prudentiel, cette vérification est en principe reportée à la prochaine intervention prévue.

La présentation des changements importants chez l'assujetti concerne en particulier le propriétaire ou les propriétaires, les organes, le modèle d'affaires, les relations avec d'autres entreprises et l'orientation stratégique.

Les irrégularités et recommandations doivent être émises indépendamment de l'étendue d'audit utilisée et de l'avancement de leur résolution.

Conformément à l'art. 9 al. 2 de l'ordonnance du 5 novembre 2014 sur les audits des marchés financiers (RS *956.161*), 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 d'enquête.

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 confirment par leur signature (signature électronique qualifiée) sur le rapport d'audit (PDF) remis en annexe à l'envoi électronique par 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 par EHP).

La société d'audit veille à ce que le rapport d'audit et les éventuels rapports complémentaires établis à l'intention du titulaire d'autorisation (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 au titulaire d'autorisation 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 »** au moins 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 est remise chaque année sous forme d'annexe de l'enquête séparée « Conduite d'un audit comptable ».

VI. 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 pas une énumération exhaustive des dispositions légales. Par ailleurs, l'annexe contient une présentation synoptique de la périodicité de l'audit et de l'étendue d'audit selon les art. 30 et 32 al. 4 de l'ordonnance FINMA sur l'audit prudentiel.

En ce qui concerne certains champs ou domaines d'audit, des points d'audit standardisés selon l'art. 16 de l'ordonnance FINMA sur l'audit prudentiel ont été conçus. Ces derniers sont applicables chaque fois qu'une intervention a lieu dans un champ ou domaine d'audit concerné. Si les travaux d'audit indiqués ne sont pas réalisés dans leur intégralité, il convient d'inscrire une explication significative dans les documents de travail. Les points d'audit ne constituent pas nécessairement une base décrivant de manière exhaustive les vérifications à effectuer et les auditeurs doivent, si nécessaire, les compléter. Il est de la responsabilité de l'équipe d'audit d'adapter le programme d'audit standard à la situation de l'établissement audité (taille, modèle d'affaires, organisation, processus, exposition aux risques, etc.). Les travaux d'audit réalisés 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 lesdits documents-modèles.

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