**Points d’audit concernant l’organisation interne et le système de contrôle interne**

**Vue d'ensemble**

|  |  |
| --- | --- |
| **Sujet :** | **Organisation interne et système de contrôle interne** |
| **Eléments couverts / Etendue d'audit :** | Eléments couverts : [xx]  Etendue d'audit : [Audit / Revue critique][[1]](#footnote-1) |
| **Bases légales :**  (liste non exhaustive) | Art. 3 al. 2 let. a, cbis et d de la loi sur les banques (LB)  Art. 9 et 11 de la loi sur les établissements financiers (LEFin)  Art. 9-12 de l'ordonnance sur les banques (OB)  Art. 12 et 66-68 de l’ordonnance sur les établissements financiers (OEFin)  Circulaire 2017/1 « Gouvernance d'entreprise – banques » de la FINMA (Circ.-FINMA 17/1, Cm 1-61 & 63 & 98-105)  Circulaire 2010/1 « Systèmes de rémunération de la FINMA » (Circ.-FINMA 10/1)[[2]](#footnote-2)  Circulaire 2016/1 « Publication – banques » de la FINMA (Circ.-FINMA 16/1, Cm 20, 41.1 & annexe 4) |
| **Visas :** | |  |  |  |  | | --- | --- | --- | --- | | **Visa :** | **Nom :** | **Fonction :** | **Date :** | | Préparateur : | [Nom] | [Assistant / Senior / Manager / Senior Manager / Partner] | [JJ.MM.AAAA] | | Reviewer : | [Nom] | [Senior / Manager / Senior Manager  / Partner] | [JJ.MM.AAAA] | |

**Le présent document est un programme de travail standard** **qui s’applique en principe lors de toute intervention pour chaque élément couvert de ce champ d’audit, conformément à la stratégie d'audit en la matière (Circ.-FINMA 13/3, Cm 28 ss). Il est de la responsabilité de l'équipe d'audit d'adapter le programme de travail standard à la situation de chaque établissement audité (taille, modèle d’affaires, organisation, processus, exposition aux risques, etc.). Si le contrôle effectué ne prend pas en compte toutes les procédures prescrites, une justification doit être fournie dans le document de travail. Les points d’audit marqués d’un astérisque (\*) ne s’appliquent pas aux banques des catégories de surveillance 4 et 5.**

**Conclusion globale**

| **Thème :** | **Information / Description :** |
| --- | --- |
| Eléments devant être couverts progressivement sur une période de six ans (y compris étendue d'audit) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Eléments :** | **20XX-2** | **20XX-1** | **20XX** | **20XX+1** | **20XX+2** | **20XX+3** | | Adéquation de l'organisation interne globale (structure organisationnelle, séparation des fonctions, descriptions de poste, responsabilités et compétences) | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | | Adéquation des directives internes (structure, clarté, caractère actuel, révision périodique, processus d'approbation, etc.) | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | | Adéquation du système de contrôle interne (méthodes d'identification, d'évaluation, de mesure, de surveillance et de *reporting* des risques, mise en œuvre de contrôles) | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | | Mesures visant à limiter les conflits d'intérêts de façon adéquate (systèmes de rémunération inclus) | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | | *Reporting* interne (contenu, destinataires, périodicité, processus de remontée de l'information, etc.) et publication relative à la gouvernance d’entreprise | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | | Politique des risques et lignes directrices pour la gestion des risques à l'échelle de l'établissement | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | [A / RC / –] | |
| Conclusion globale | |  |  | | --- | --- | | **Confirmation dans le rapport d'audit :** | **Conclusion :** | | Confirmation que les prescriptions et principes de la gouvernance d'entreprise ont été respectés, et que les domaine « organisation interne » et « système de contrôle interne » étaient structurés de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts). | **Oui** (Audit / Revue critique) / **Non** | | Confirmation de l'existence d'une séparation adéquate entre l'organe responsable de la haute direction et la direction opérationnelle (sur la base des constatations relatives aux éléments effectivement couverts). | **Oui** (Audit / Revue critique) / **Non** | |
| Résumé des résultats de l’audit / irrégularités et recommandations (voir détails ci-dessous) | [Résumé des résultats de l’audit / irrégularités et recommandations] |
| Domaines d'audit, résultats et travaux de la révision interne utilisés par la société d'audit (y compris la propre évaluation de la société d'audit) | [Description] |

**Programme de travail – Organisation interne et système de contrôle interne – Adéquation de l'organisation interne globale**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit » :** | **Procédures mises en œuvre / Constatations** | **Réf. doc. de travail** |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | **Adéquation de l'organisation interne**  (structure organisationnelle)  Art. 3 al. 2 let. a et d LB / art. 9-11 OB & art. 9 LEFin / art. 12, 66 OEFin | *Evaluer l'adéquation de la structure organisationnelle compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Se procurer les statuts, les règlements d'organisation, les accords de partenariat ou les règlements relatifs aux partenariats ainsi que l'organigramme englobant tous les sites géographiques.  Evaluer si le champ d’activité et son étendue géographique correspondent aux capacités financières et à l’organisation administrative.  Evaluer si l’établissement est effectivement dirigé depuis la Suisse et si les membres de la direction exercent réellement et de manière responsable leur fonction dirigeante.  Evaluer si l’organe responsable de la haute direction de la banque compte au moins trois membres. | Evaluer si les informations contenues dans les statuts, les règlements d'organisation et l'organigramme correspondent aux activités commerciales et à la dimension géographique des activités commerciales. |  |  |
| Sur la base de l'organigramme obtenu, identifier les services responsables et évaluer l'adéquation de l'organisation des fonctions clés (intégration fonctionnelle et hiérarchique, lignes de *reporting* hiérarchiques, etc.). |  |  |  |
|  | **Adéquation de l'organisation interne**  (séparation des fonctions) | *Evaluer l'adéquation globale de la séparation des fonctions compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Pour les banques : évaluer si les membres de l'organe responsable de la haute direction (par ex. CA) sont séparés de la direction sur le plan de l'organisation (art. 3 al. 2 let. a LB & art. 11 OB). |  |  |  |
| Evaluer l'indépendance organisationnelle entre les services qui prennent des risques et ceux qui surveillent les risques (par ex., séparation appropriée des fonctions entre les activités de crédit, de négoce, de gestion d’actifs et d'exécution des transactions au sein de l'établissement [art. 12 OB / art. 67 OEFin]). |  |  |  |
|  | **Adéquation de l'organisation interne**  (descriptions de poste) | *Evaluer l'adéquation globale des descriptions de poste compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Evaluer si les descriptions de poste du personnel clé sont disponibles et établies sur la base de principes uniformes et adéquats (forme, contenu, autorisation, processus de contrôle). | Sélectionner un échantillon approprié de descriptions de poste ou de tout autre document approprié relatif au personnel clé et évaluer si les points suivants sont abordés de façon détaillée :   * description des responsabilités * description des compétences * définition des lignes de *reporting* * définition des lignes de remontée de l'information (*escalation*) * autorisation de la description de poste * caractère actuel des informations fournies.   Comparer et évaluer en détail l'adéquation des descriptions de poste eu égard aux activités effectives des collaborateurs sur la base d'un échantillon. |  |  |
|  | **Adéquation de l'organisation interne**  (responsabilités et compétences [*checks* & *balances*]) | *Evaluer l'adéquation globale des responsabilités et des compétences compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Evaluer si l'établissement a défini les responsabilités et les compétences de ses fonctions clés dans des lignes directrices écrites qui sont accessibles à ces fonctions et connues de ces dernières. |  |  |  |
|  |  | Evaluer si l'organe responsable de la haute direction ainsi que la direction disposent des compétences de gestion suffisantes ainsi que des connaissances techniques et de l'expérience nécessaires dans les secteurs bancaire et financier. Evaluer si l'organe responsable de la haute direction est composé de manière suffisamment diversifiée (Circ.-FINMA 17/1, Cm 16 et 51) |  |  |  |
|  |  | Evaluer si l'organe responsable de la haute direction respecte les principes en matière d'indépendance et est composé pour un tiers au moins de membres indépendants (Circ.-FINMA 17/1, Cm 17 à 25) |  |  |  |
|  |  | Evaluer si l'organe responsable de la haute direction observe les principes de la gestion du mandat et, à cet effet, s'assure que chaque membre consacre suffisamment de temps à son mandat, détermine ou approuve les profils d'exigences qui relèvent de ses compétences et procède à une évaluation au moins annuelle de ses propres performances (Circ.-FINMA 17/1, Cm 26 à 28) |  |  |  |
|  | **Adéquation de l'organisation interne**  (Répartition des tâches et comités) | *Evaluer l'adéquation générale s'agissant de la répartition des tâches et de la création de comités* *compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment* |  |  |  |
|  | Evaluer si le président de l'organe responsable de la haute direction assume la représentation tant à l'intérieur qu'à l'extérieur de l'entreprise et s'il marque de façon déterminante la stratégie, la communication et la culture de l'entreprise (Circ.-FINMA 17/1, Cm 30). |  |  |  |
|  |  | Si un comité d’audit est constitué, évaluer si celui-ci se démarque suffisamment, au niveau de la composition, des autres comités, si la majorité des membres du comité d'audit et du comité des risques sont indépendants et si les autres prescriptions en matière d'organisation ont été observées (Circ.-FINMA 17/1, Cm 32 à 33) |  |  |  |
|  |  | **\*** Evaluer si tant un comité d'audit qu'un comité des risques ont été instaurés (étant précisé que les établissements appartenant à la catégorie de surveillance 3 ont la faculté d'instaurer un comité mixte) et si ces comités ont assuré un *reporting* approprié à l'organe responsable de la haute direction (Circ.-FINMA 17/1, Cm 31) |  |  |  |
|  |  | Applicable aux établissements d'importance systémique: évaluer si un comité des rémunérations et des nominations a été instauré au moins au niveau groupe (Circ.-FINMA 17/1, Cm 31) |  |  |  |
|  |  | Evaluer si les tâches qui incombent au comité d'audit (Circ.-FINMA 17/1,Cm 34 à 39) ont été assumées de manière appropriée par l’organe compétent (comité d’audit ou organe responsable de la haute direction). | Examen des procès-verbaux et des rapports afin d'apprécier les travaux assumés par l’organe compétent (comité d’audit ou organe responsable de la haute direction). |  |  |
|  |  | Evaluer si les tâches qui incombent au comité des risques (Circ.-FINMA 17/1, Cm 40 à 46) ont été assumées de manière appropriée par l’organe compétent (comité des risques ou organe responsable de la haute direction). | Examen des procès-verbaux et des rapports afin d'apprécier les travaux assumés par l’organe compétent (comité des risques ou organe responsable de la haute direction). |  |  |

**Programme de travail – Organisation interne et système de contrôle interne – Adéquation des directives internes**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit » :** | **Procédures mises en œuvre / Constatations** | **Réf. doc. de travail** |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | **Adéquation du concept-cadre des directives / lignes directrices internes**  (structure, clarté, caractère actuel, revue périodique, processus d'approbation, etc.) | *Evaluer l'adéquation globale du concept-cadre des directives / lignes directrices internes compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Se procurer une vue d'ensemble de toutes les directives / lignes directrices internes disponibles et évaluer si les aspects significatifs des activités des entités sont abordés de manière adéquate. | Sélectionner un échantillon approprié de directives / lignes directrices clés internes, et déterminer si elles couvrent correctement les aspects pertinents des activités de l’établissement et si elles ont été approuvées par l'organe compétent. |  |  |
| Au moyen d'enquêtes, évaluer le processus de définition, de révision, de mise à jour et d'approbation des directives / lignes directrices internes, et évaluer si ce processus est adéquat (conception). | Effectuer un test de l'efficacité de fonctionnement des contrôles clés identifiés concernant le processus de définition, de révision, de mise à jour et d'approbation des lignes directrices. |  |  |
|  |  |  |  |
|  |  | Au moyen d'enquêtes et par l'examen de documents appropriés (lignes directrices, directives, manuels, etc.), évaluer l'adéquation globale des principes établis par l'établissement pour identifier les besoins en matière de modification des directives existantes ou d'établissement de nouvelles directives (suite à la modification de la stratégie ou des processus, à l'évolution de la réglementation, etc.). | Par l'examen de documents appropriés, évaluer le respect, par l'établissement, des principes internes concernant la modification des directives existantes et/ou l'établissement de nouvelles directives, sur la base d'un échantillon. |  |  |

**Programme de travail – Organisation interne et système de contrôle interne – Adéquation du système de contrôle interne**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit » :** | **Procédures mises en œuvre / Constatations** | **Réf. doc. de travail** |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | **Adéquation du système de contrôle interne**  (méthodes d'identification, d'évaluation, de mesure, de surveillance et de *reporting* des risques ; mise en œuvre de contrôles) | *Evaluer l'adéquation des méthodes d'identification, d'évaluation, de mesure, de surveillance et de reporting des risques compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Evaluer si l'organe responsable de la haute direction détermine la stratégie commerciale et réglemente de manière adéquate l'établissement de lignes directrices et de processus relatifs à l'identification, l'évaluation, la mesure, la surveillance et le *reporting* des risques dans le but d'une gestion des risques efficace et du pilotage de l’ensemble des risques (Circ.-FINMA 17/1, Cm 10). |  |  |  |
| Evaluer si l'organe responsable de la haute direction assume effectivement ses tâches concernant l'organisation, la situation financière ainsi que la dotation suffisante de l'établissement au niveau des ressources humaines et autres (notamment la nomination et la révocation des membres des comités) (Circ.-FINMA 17/1, Cm 11 à 13) |  |  |  |
| Evaluer si l'organe responsable de la haute direction s'assure que tous les risques significatifs sont identifiés, limités et surveillés dans l'établissement au moyen de contrôles internes intégrés dans le système d'analyse et de surveillance systématiques des risques (caractère approprié de l'environnement de contrôle et de risque) (Circ.-FINMA 17/1, Cm 14). |  |  |  |
| Evaluer, sur la base des procès-verbaux de l'organe responsable de la haute direction, si cette instance exerce effectivement la haute surveillance sur la direction (Circ.-FINMA 17/1, Cm 14) |  |  |  |
| Evaluer si des procédures appropriées existent afin que les collaborateurs de tous les niveaux hiérarchiques connaissent et comprennent leurs tâches et responsabilités en matière de contrôle interne. |  |  |  |
| Evaluer si l'organe responsable de la haute direction a statué sur les changements importants apportés à la structure et aux investissements (Circ.-FINMA 17/1, Cm 15). |  |  |  |
| Evaluer si l'organe responsable de la haute direction discute régulièrement avec la direction de son appréciation de l'adéquation et de l'efficacité des contrôle internes. | Examiner les procès-verbaux des séances tenues avec la direction et/ou des séances de l'organe responsable de la haute direction ou de ses comités et évaluer l'adéquation des discussions concernant l'appréciation de l'adéquation et de l'efficacité des contrôles internes et des décisions prises à ce sujet. |  |  |
| Evaluer si la direction met en œuvre les instructions de l'organe responsable de la haute direction au niveau de l'activité opérationnelle, en conformité avec la stratégie commerciale, ainsi qu'en matière d'instauration, de maintien et de suivi régulier des contrôles internes (Circ.-FINMA 17/1, Cm 47 à 50)  La direction est responsable :   * de la conduite des affaires courantes, du pilotage opérationnel des revenus et des risques ainsi que de la représentation de l'établissement vis-à-vis des tiers dans le secteur opérationnel; * de la formulation de propositions concernant les affaires qui relèvent de la compétence ou nécessitent l'approbation de l'organe responsable de la haute direction et de l'édiction de prescriptions visant à régler l'exploitation commerciale opérationnelle; * de la conception et de l'entretien de processus internes adaptés, d'un système d'information du management approprié (MIS) et d'un SCI ainsi qu'une infrastructure technologique adéquates. | Examiner la documentation relative à la vérification de l'adéquation du SCI et évaluer l'adéquation des discussions et des décisions prises. |  |  |
| Evaluer l'adéquation globale du système de contrôle interne (conception) compte tenu des aspects suivants :   * principes de documentation * taille et complexité de l'établissement * respect du principe des 4 yeux * *reporting* (résultats, problématiques) * processus d'autorisation. | Sélectionner un échantillon de la documentation relative au SCI et évaluer si les directives établies par l'établissement au sujet de la documentation, de la prise en compte du principe des 4 yeux, du *reporting* et du processus d'autorisation ont été respectées et si les contrôles définis ont été exécutés (efficacité de fonctionnement). |  |  |
| Acquérir une compréhension du processus de mise à jour de la documentation relative au système de contrôle interne et évaluer s'il est approprié pour identifier les changements et pour tenir à jour le système de contrôle interne (conception). | Sélectionner un échantillon de la documentation relative au SCI et évaluer si les directives établies par l'établissement concernant les processus de mise à jour et d'autorisation ont été respectées et si les contrôles définis ont été exécutés (efficacité de fonctionnement). |  |  |

**Programme de travail – Organisation interne et système de contrôle interne – Mesures visant à limiter les conflits d'intérêts de façon adéquate**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit » :** | **Procédures mises en œuvre / Constatations** | **Réf. doc. de travail** |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | **Mesures visant à limiter les conflits d'intérêts de façon adéquate** | *Evaluer si l'organisation interne a été conçue de manière afin de limiter les conflits d'intérêts de façon adéquate compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* | Se procurer des documents sur les déficiences essentielles identifiées (fraude due au contournement des contrôles, par ex.) et évaluer la façon dont l'établissement a traité ces déficiences (*reporting*, solutions apportées, etc.). |  |  |
| Evaluer si les lignes directrices et les directives internes de l'établissement donnent des instructions sur la façon d'éviter et de gérer les conflits d'intérêts. |  |  |  |
| Evaluer si l'organe responsable de la haute direction s’assure que la gestion des conflits d'intérêts soit réglée (Circ.-FINMA 17/1, Cm 29).  Lorsque des conflits d'intérêts ne peuvent être évités, évaluer si l'établissement a pris des mesures afin de les gérer correctement. | Enquêter afin d’évaluer si des conflits d'intérêts n'ont pu être évités et évaluer si les mesures prises sont/ont été appropriées, sur la base d'un échantillon. |  |  |
| Evaluer si l'organe responsable de la haute direction veille à ce que la pression éventuellement exercée sur les collaborateurs de tout échelon hiérarchique pour la réalisation d’objectifs ne puisse pas conduire à contourner les mécanismes de contrôle. L'organe responsable de la haute direction fait en sorte que les systèmes de rémunérations ne créent pas d'incitations en matière de conflits d'intérêts ou au non-respect des mécanismes de contrôle (Circ.-FINMA 17/1, Cm 13 & 63). | Examiner les directives correspondantes définies par le CA et évaluer si elles sont respectées. |  |  |
| Evaluer si la direction veille à une séparation appropriée des fonctions et évite l’attribution de responsabilités conflictuelles. Dans les cas où le principe de séparation des fonctions ne peut être pleinement appliqué du fait de la taille de l'établissement, elle attache une importance particulière à un renforcement conséquent de la responsabilité de conduite des instances hiérarchiques. |  |  |  |
| Evaluer les procédures adoptées par l'établissement pour identifier les conflits d'intérêts potentiels (y compris, par ex., la politique en matière de « lancement d’alertes » et les procédures applicables en la matière). | Enquêter afin d’évaluer si des conflits d'intérêts ont été signalés et procéder à une évaluation de leur gestion, sur la base d'un échantillon. |  |  |
|  | **Systèmes de rémunération[[3]](#footnote-3)** | *Evaluer si l'organisation interne a été conçue de façon adéquate s'agissant des systèmes de rémunération compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Acquérir une compréhension du concept-cadre des systèmes de rémunération de l'établissement et le documenter. |  |  |  |
| Evaluer si l'établissement a globalement tenu compte des principes relatifs aux conflits d'intérêts définis dans la Circ.-FINMA 10/1. | Sélectionner un échantillon approprié de personnes clés et évaluer si les systèmes de rémunération (salaires, bonus et honoraires, par ex.) sont conçus de manière à éviter de façon adéquate toute incitation susceptible de provoquer des conflits d'intérêts ou de conduire au non-respect des mécanismes de contrôle (notamment Circ.-FINMA 17/1, Cm 63). |  |  |

**Programme de travail – Organisation interne et système de contrôle interne – *Reporting* interne et publication relative à la gouvernance d’entreprise**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit » :** | **Procédures mises en œuvre / Constatations** | **Réf. doc. de travail** |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | ***Reporting* interne**  **Contenu** | *Evaluer si un concept-cadre adéquat a été conçu pour le reporting interne compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Acquérir une compréhension de la conception du concept-cadre pour le *reporting* concernant l'organisation interne et le SCI dans son ensemble, y compris les lignes de *reporting* hiérarchiques, le contenu et la périodicité du *reporting*, et documenter cette conception. |  |  |  |
| Examiner l'ensemble du *reporting* effectué à l'intention de l'organe responsable de la haute direction et de la direction. Sur la base d'un échantillon, évaluer s'il contient tous les aspects pertinents compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation. | Sur la base d'un échantillon, examiner les rapports établis à l'intention de l'organe responsable de la haute direction et de la direction et tester les procédures et les contrôles mis en œuvre pour s'assurer que les rapports sont exacts, complets et fiables. |  |  |
|  | ***Reporting* interne**  **Destinataires et périodicité** | *Evaluer si les destinataires et la périodicité du reporting interne concernant l'organisation interne et le SCI ont été définis de façon adéquate compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Evaluer si le *reporting* interne concernant l'organisation interne et le SCI est adressé aux bons destinataires et est effectué à une périodicité convenable compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation. | Evaluer en détail si les lignes hiérarchiques de *reporting* sont adéquates compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation. |  |  |
|  | ***Reporting* interne**  **Processus de remontée de l'information (*escalation*)** | *Evaluer si les processus de remontée de l'information ont été conçus de façon adéquate compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Acquérir une compréhension des processus de remontée de l'information mis en œuvre pour 1) assurer en temps voulu le *reporting* sur la défaillance des contrôles et sur d'autres problématiques du système de contrôle interne et pour 2) s'assurer que ces rapports soient remis aux bons destinataires. | Sélectionner un échantillon de défaillances de contrôle majeures et examiner si ces défaillances ont été communiquées aux bons destinataires et si l'établissement a pris les mesures qui s'imposaient. |  |  |
|  | **Publication relative à la gouvernance d’entreprise**  **(Circ.-FINMA 16/1, Cm 14.1, 20, 41.1 et annexe 4)[[4]](#footnote-4)** | *Evaluer si les obligations en matière de publication relative à la gouvernance d’entreprise ont été remplies de manière adéquate compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation.* |  |  |  |
| Examen de la publication relative à la gouvernance d’entreprise. Evaluer si les informations requises selon la Circ.-FINMA 16/1, Cm 1 à 6 de l’annexe 4 ont été publiées, expliquées de manière adéquate et si les modifications substantielles ont été mises à jour dans les trois mois sur le site Internet. | Examiner si les informations requises selon la Circ.-FINMA 16/1, Cm 1 à 6 de l’annexe 4 ont été rendues publiques de manière exhaustive et adéquate. |  |  |
| **\*** Evaluer si les informations requises selon la Circ.-FINMA 16/1, Cm 7 à 13 de l’annexe 4 ont été publiées, expliquées de manière adéquate et si les modifications substantielles ont été mises à jour dans les trois mois sur le site Internet. | **\*** Examiner si les informations requises selon la Circ.-FINMA 16/1, Cm 7 à 13 de l’annexe 4 ont été rendues publiques de manière exhaustive et adéquate. |  |  |

**Programme de travail – Organisation interne et système de contrôle interne – Politique des risques et lignes directrices pour la gestion des risques à l'échelle de l'établissement**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit » :** | **Procédures mises en œuvre / Constatations** | **Réf. doc. de travail** |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | ***Politique des risques et lignes directrices pour la gestion des risques à l’échelle de l’établissement***  Art. 12 al. 2 OB et art. 68 OEFin | *Evaluer si une politique des risques et des lignes directrices adéquates ont été conçues pour la gestion des risques à l'échelle de l'établissement compte tenu de la taille de l’établissement ainsi que de la complexité de son activité et de son organisation, notamment :* |  |  |  |
| Evaluer si la politique des risques et les lignes directrices pour la gestion des risques à l’échelle de l’établissement ont été élaborées par la direction et adoptées par l'organe responsable de la haute direction (Circ.-FINMA 17/1, Cm 52) |  |  |  |
|  |  | Evaluer si la politique des risques et les lignes directrices pour la gestion des risques à l’échelle de l’établissement englobent la tolérance au risque ainsi que les limites correspondantes en matière de risques dans toutes les catégories de risques importantes (Circ.-FINMA 17/1, Cm 53) | Examen détaillé de la politique des risques et des lignes directrices pour la gestion des risques à l’échelle de l’établissement. Evaluation de la réglementation appropriée de la tolérance au risque ainsi que des limites correspondantes en matière de risques dans toutes les catégories de risques, et de l’application effective dans le cadre opératif de surveillance des risques. |  |  |
|  |  | Evaluer si la compétence et la procédure pour l'autorisation d'opérations risquées ont été fixées dans un règlement ou dans des directives internes (art. 12 OB). |  |  |  |
|  |  | **\*** Evaluer si les aspects pertinents (selon la Circ.-FINMA 17/1, Cm 54 à 59) ont bien été pris en compte dans la politique des risques et les lignes directrices pour la gestion des risques à l’échelle de l’établissement.  Obligation supplémentaire pour les établissements d'importance systémique : prise en compte des prescriptions additionnelles, notamment au sujet de l'architecture des données et de l'infrastructure informatique (Circ.-FINMA 17/1, Cm 59, dernière phrase). | **\*** Examen détaillé de la politique des risques et des lignes directrices pour la gestion des risques à l’échelle de l’établissement, et vérification si les aspects pertinents, compte tenu de la taille de l'établissement ainsi que de la complexité de son activité et de son organisation, ont bien été pris en compte et s'ils sont effectivement appliqués dans le cadre opératif de surveillance des risques. |  |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Circ.-FINMA 13/3, Cm 33 et 34 [↑](#footnote-ref-1)
2. Spécifiée uniquement dans l'audit de base des établissements de la catégorie 1 [↑](#footnote-ref-2)
3. Les points d’audit relatifs aux systèmes de rémunération ne s’appliquent qu’aux établissements visés dans la Circ.-FINMA 10/1, Cm 6. [↑](#footnote-ref-3)
4. Ne s’applique pas aux établissements visés aux art. 47*a* à 47*e* OFR. Ces derniers peuvent limiter leur publication aux chiffres clés qui leur sont applicables. Cf. Circ.-FINMA 16/1, Cm 8.1. [↑](#footnote-ref-4)