**Points d’audit concernant les fonctions centrales de contrôle et de limitation des risques**

**Vue d'ensemble**

|  |  |
| --- | --- |
| **Champs d’audit :** | **Fonctions centrales de contrôle et de limitation des risques (fonction de contrôle des risques, fonction *compliance*)** |
| **Étendue d'audit :** | [Audit / Revue critique][[1]](#footnote-2) |
| **Bases légales :**  (liste non exhaustive) | Art. 3 al. 2 let. a de la loi du 8 novembre 1934 sur les banques (LB ; RS *952.0*)  Art. 12 al. 2 à 4 de l'ordonnance du 30 avril 2014 sur les banques (OB ; RS *952.02*)  Art. 9 de la loi fédérale du 15 juin 2018 sur les établissements financiers (LEFin ; RS *954.1*)  Art. 12 al. 4, 68 et 73 de l’ordonnance du 6 novembre 2019 sur les établissements financiers (OEFin ; RS *954.11*)  Cm 62 à 81 de la circulaire FINMA 2017/1 « Gouvernance d'entreprise – banques » |
| **Visas :** | |  |  |  |  | | --- | --- | --- | --- | | **Visa :** | **Nom :** | **Fonction :** | **Date :** | | Auditeur : | [Nom] | [Assistant / Senior / Manager / Senior Manager / Partner] | [JJ MMMM AAAA] | | Réviseur : | [Nom] | [Senior / Manager / Senior Manager  / Partner] | [JJ MMMM AAAA] | |

**Le présent document est un programme de travail standard** **qui s’applique en principe lors de toute intervention dans ce champ d’audit conformément à la stratégie d'audit. 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 :** |
| --- | --- |
| Conclusion globale | |  |  | | --- | --- | | **Confirmation dans le rapport d'audit :** | **Conclusion :** | | Confirmation que les ressources techniques et personnelles de la fonction de *compliance* étaient suffisantes et qu’elle a assumé effectivement ses responsabilités. | ***Oui*** *(Audit / Revue critique) /* ***Non*** | | Confirmation que les ressources techniques et personnelles de la fonction de contrôle des risquesétaient suffisantes et qu’elle a assumé effectivement ses responsabilités. | ***Oui*** *(Audit / Revue critique) /* ***Non*** | | Confirmation que le positionnement dans l’organisation de ces fonctions et le mode de rémunération n’ont pas généré de conflits d’objectifs. | ***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 – Fonction de *compliance***

| **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** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the technical and personnel resources of the compliance function were adequate and it actually assumed responsibility“.*  *„Bestätigung, dass die technischen und personellen Ressourcen bei der Funktion Compliance ausreichend waren und dass diese ihre Verantwortung effektiv wahrgenommen hat“.*  *„Confirmation que les ressources techniques et personnelles de la fonction de compliance étaient suffisantes et qu’elle a assumé effectivement ses responsabilités“.* | | | | | |
|  | **Ressources humaines** | *Déterminer si les ressources humaines de la fonction de compliance sont adéquates compte tenu de la taille de l'établissement, de la complexité de son activité et de son organisation ainsi que du risque de* compliance *auquel il est exposé (Cm 64 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Acquérir une compréhension globale de la fonction de *compliance* de l'établissement, du nombre de ses collaborateurs et des tâches attribuées. |  |  |  |
| Se procurer par exemple les CV, les descriptions de poste des personnes clés / du personnel clé de la fonction de *compliance* et évaluer leur savoir-faire. |  |  |  |
|  | **Ressources techniques** | *Déterminer si les ressources techniques de la fonction de compliance sont adéquates compte tenu de la taille de l'établissement, de la complexité de son activité et de son organisation ainsi que du risque de* compliance *auquel il est exposé (Cm 64 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Évaluer l’adéquation des ressources techniques, par exemple au moyen d’une liste des applications de technologies de l'information et des autres outils utilisés par la fonction de *compliance*, y compris le nom du système, une description de son but et sa date de mise en œuvre. |  |  |  |
|  | **Prise de responsabilités** | *Évaluer si la fonction de* compliance *assume ses responsabilités compte tenu de la taille de l'établissement, de la complexité de son activité et de son organisation ainsi que du risque de* compliance *auquel il est exposé (Cm 77 à 81 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Évaluer si les directives internes établies par l'établissement pour la fonction de compliance sont en conformité avec la Circ.-FINMA 17/1 et sont appropriées étant donné les modifications récentes et celles prévues de la situation générale, des contrôles et de l'organisation de l'établissement. |  |  |  |
| Évaluer si la fonction de *compliance* procède, au moins une fois par an, à l'évaluation du risque de *compliance* lié aux activités d’affaires et, sur la base de celle-ci, élabore un plan d'action axé sur le risque, qui doit être approuvé par la direction et être remis à la révision interne (Cm 78 Circ.-FINMA 17/1). | Examiner le plan d'action axé sur le risque et évaluer son adéquation / exhaustivité. |  |  |
| Déterminer si la fonction de *compliance* informe l'organe responsable de la haute direction – au moins une fois par an – sur l'évaluation du risque de *compliance* et sur l'activité de la fonction de *compliance* (Cm 80 Circ.-FINMA 17/1). | Examiner les rapports annuels remis à l'organe de la haute direction (avec copie à la révision interne et à la société d'audit) et évaluer leur adéquation / exhaustivité. |  |  |
| Se procurer, examiner et évaluer les éléments probants selon lesquels la fonction de compliance assume effectivement ses autres responsabilités (remise en temps utile de rapports aux fonctions correspondantes i) sur les modifications importantes de l'évaluation des risques de *compliance* et ii) les manquements graves constatés en matière de compliance) (Cm 79 et 81 Circ.-FINMA 17/1). |  |  |  |
| Identifier et documenter les contrôles internes réalisés par la fonction de *compliance* et évaluer leur efficacité conceptuelle / exhaustivité. | Effectuer des tests de contrôles afin de confirmer l'efficacité de fonctionnement des contrôles internes effectués par la fonction de *compliance*. |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the organizational set-up of the compliance function and the compensation system did not lead to a conflict of interest“.*  *„Bestätigung, dass die organisatorische Anordnung der Funktion Compliance und das Entschädigungssystem keine Zielkonflikte herbeiführten“.*  *“Confirmation que le positionnement de la fonction de compliance dans l’organisation et le mode de rémunération n’ont pas généré de conflits d’objectifs”* | | | | | |
|  | **Positionnement dans la structure organisationnelle et prévention des conflits d'intérêts** | *Déterminer si le positionnement de la fonction de compliance dans la structure organisationnelle est adéquat compte tenu de la taille de l’établissement ainsi que de la complexité de ses activités et de son organisation, et s'il n'a pas généré de conflits d'intérêts et si elle indépendante des unités d'affaires génératrices de revenus (Cm 62 à 68 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Déterminer si le positionnement de la fonction de *compliance* dans la structure organisationnelle est en conformité avec la Circ.-FINMA 17/1 – en particulier sous l'angle de la prévention des conflits d'intérêts et de l'indépendance envers les unités d'affaires génératrices de revenus – et est approprié étant donné les modifications récentes et celles prévues de la situation générale, des contrôles et de l'organisation de l'établissement (Cm 60 à 64 Circ.-FINMA 17/1). |  |  |  |
| Identifier le (ou les) membre(s) de la direction ayant été désigné(s) responsable(s) de la fonction de *compliance* et évaluer si cette fonction dispose d'un droit illimité à l'information, à son accès et à sa consultation en sa qualité d'instance de contrôle indépendante (Cm 64 et 65 Circ.-FINMA 17/1). |  |  |  |
| Déterminer si le système de rémunération des collaborateurs de la fonction de *compliance* (salaires, bonus, honoraires, par ex.) ne crée pas des incitations susceptibles de générer un conflit d'intérêts (Cm 63 Circ.-FINMA 17/1). | Appliquer des contrôles de substance afin de confirmer que la rémunération des collaborateurs de la fonction de *compliance* ne dépend pas du résultat de produits ou de transactions spécifiques. |  |  |
|  |  | Évaluer si la fonction *compliance* (instance de contrôle indépendante) dispose d'un accès direct à l'organe responsable de la haute direction (Cm 66 Circ.-FINMA 17/1) |  |  |  |
|  |  | **\*** Évaluer si une fonction de *compliance* autonome en qualité d'instance de contrôle indépendante a été instaurée (Cm 67 Circ.-FINMA 17/1) |  |  |  |

**Programme de travail – Fonction de contrôle des risques**

| **N°** | **Thème :** | **Procédures pour l'étendue d'audit « revue critique » :** | **Procédures supplémentaires pour l'étendue d'audit « audit »:** | **Procédures mises en œuvre / Constatations** | **Réf. progr. de travail** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the technical and personnel resources of the risk control function were adequate and it actually assumed responsibility“.*  *„Bestätigung, dass die technischen und personellen Ressourcen bei der Funktion Risikokontrolle ausreichend waren und dass diese ihre Verantwortung effektiv wahrgenommen hat“.*  *„Confirmation que les ressources techniques et personnelles de la fonction de contrôle des risques étaient suffisantes et qu’elle a assumé effectivement ses responsabilités“.* | | | | | |
|  | **Ressources humaines** | *Déterminer si les ressources humaines de la fonction de contrôle des risques sont adéquates compte tenu de la taille de l’établissement, de la complexité de ses activités et de son organisation ainsi que de son profil de risque, notamment :* |  |  |  |
| Acquérir une compréhension globale de la fonction de contrôle des risques de l'établissement, du nombre de ses collaborateurs et des tâches attribuées. |  |  |  |
| Se procurer par exemple les CV, les descriptions de poste des personnes/employés clés de la fonction de contrôle des risques et évaluer leur savoir-faire. |  |  |  |
|  | **Ressources techniques** | *Déterminer si les ressources techniques de la fonction de contrôle des risques sont adéquates compte tenu de la taille de l’établissement, de la complexité de ses activités et de son organisation ainsi que de son profil de risque (Cm 64 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Évaluer l’adéquation des ressources techniques, par exemple au moyen d’une liste des applications de technologies de l'information et des autres outils utilisés par la fonction de contrôle des risques, y compris le nom du système, une description de son but et la date de sa mise en œuvre. |  |  |  |
|  | **Prise de responsabilités** | *Évaluer si la fonction de contrôle des risques assume ses responsabilités compte tenu de la taille de l'établissement, de la complexité de son activité et de son organisation ainsi que du profil de risques de l’établissement (Cm 69 à 76 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Évaluer si les directives internes établies par l'établissement pour la fonction de contrôle des risques sont en conformité avec la Circ.-FINMA 17/1 et sont appropriées étant donné les modifications récentes et celles prévues de la situation générale, des contrôles et de l'organisation de l'établissement. |  |  |  |
| Se procurer, examiner et évaluer les éléments probants selon lesquels la fonction de contrôle des risques assure le caractère systématique de la surveillance et de l'établissement de rapports sur des positions-risque individuelles et agrégées (y.c. tests de résistance et analyses de scénarios[[2]](#footnote-3)), la mise en œuvre appropriée des dispositions relatives à l'agrégation des données (établissements des catégories de surveillance 1 à 3) ainsi que la surveillance du profil de risque (tolérance au risque et limites fixées en matière de risques) (Cm 69 à 71 Circ.-FINMA 17/1) |  |  |  |
| Déterminer si la fonction de contrôle des risques assume effectivement ses responsabilités en matière de définition et d'application de bases et de méthodes pour la surveillance et la mesure des risques (Cm 72 Circ.-FINMA 17/1). |  |  |  |
| Évaluer si le contrôle des risques est impliqué de manière appropriée dans le développement de nouveaux types de produits, services, domaines d'activité ou secteurs de marché ou dans leur extension ainsi que dans des transactions importantes ou complexes (Cm 73 Circ.-FINMA 17/1) |  |  |  |
| Évaluer si le contrôle des risques participe activement au processus de définition des limites posées en matière de risques et s'assure qu'elles sont notamment en conformité avec la tolérance au risque et avec les résultats des tests de résistance et qu'elles ont été définies de manière à constituer un instrument de pilotage efficace au plan opérationnel pour la direction (Cm 74 Circ.-FINMA 17/1) |  |  |  |
| Déterminer si la fonction de contrôle des risques remet au moins une fois par semestre à la direction un rapport relatif à l'évolution du profil de risque de l'établissement et son activité (Cm 75 Circ.-FINMA 17/1). | Examiner le rapport semestriel relatif aux risques destiné à la direction ainsi que le rapport annuel sur les risques (et sur l'activité de la fonction de contrôle des risques) remis à l'organe responsable de la haute direction (avec copie à la révision interne ainsi qu'à la société d'audit), et évaluer leur adéquation / exhaustivité. |  |  |
| Évaluer si la fonction de contrôle des risques remet à l'organe responsable de la haute direction, au moins une fois par an, un rapport sur l'évolution du profil de risque de l'établissement et son activité (Cm 75 Circ.-FINMA 17/1). |  |  |  |
| Se procurer et évaluer les éléments probants selon lesquels le contrôle des risques assume effectivement les autres tâches et responsabilités (information en temps utile en cas d'évolution particulière de la situation) (Cm 76 Circ.-FINMA 17/1) |  |  |  |
| Identifier et documenter les contrôles internes réalisés par la fonction de contrôle des risques et évaluer leur efficacité conceptuelle / exhaustivité. | Effectuer des tests de contrôles afin de confirmer l'efficacité de fonctionnement des contrôles internes effectués par la fonction de contrôle des risques. |  |  |
| *„Confirmation that the organizational set-up of the compliance function and the compensation system did not lead to a conflict of interest“.*  *„Bestätigung, dass die organisatorische Anordnung der Funktion Risikokontrolle und das Entschädigungssystem keine Zielkonflikte herbeiführten“.*  *“Confirmation que le positionnement de la fonction de contrôle des risques dans l’organisation et le mode de rémunération n’ont pas généré de conflits d’objectifs.”* | | | | | |
|  | **Positionnement dans la structure organisationnelle et prévention des conflits d'intérêts** | *Déterminer si le positionnement de la fonction de contrôle des risques dans la structure organisationnelle est adéquat compte tenu de la taille de l’établissement ainsi que de la complexité de ses activités et de son organisation, et s'il n'a pas généré de conflits d'intérêts et si elle indépendante des unités d'affaires génératrices de revenus (Cm 62 à 68 Circ.-FINMA 17/1), notamment :* |  |  |  |
| Déterminer si le positionnement de la fonction de contrôle des risques dans la structure organisationnelle est en conformité avec la Circ.-FINMA 17/1 – en particulier sous l'angle de la prévention des conflits d'intérêts et de l'indépendance envers les unités d'affaires génératrices de revenus – et est approprié étant donné les modifications récentes et celles prévues de la situation générale, des contrôles et de l'organisation de l'établissement (Cm 60 à 64 Circ.-FINMA 17/1). |  |  |  |
| Identifier le (ou les) membre(s) de la direction ayant été désigné(s) responsable de la fonction de contrôle des risques et évaluer si cette fonction dispose d'un droit illimité à l'information, à son accès et à sa consultation en sa qualité d'instance de contrôle indépendante (Cm 64 et 65 Circ.-FINMA 17/1). |  |  |  |
| Déterminer si le système de rémunération des collaborateurs de la fonction de contrôle des risques (salaires, bonus, honoraires, par ex.) ne crée par des incitations susceptibles de générer des conflits d'intérêts (Cm 63 Circ.-FINMA 17/1). | Appliquer des contrôles de substance afin de confirmer que la rémunération des collaborateurs de la fonction de contrôle des risques ne dépend pas du résultat de produits ou de transactions spécifiques. |  |  |
|  |  | Évaluer si le contrôle des risques (instance de contrôle indépendante) dispose d'un accès direct à l'organe responsable de la haute direction (Cm 66 Circ.-FINMA 17/1) |  |  |  |
|  |  | **\*** Évaluer si une fonction de contrôle des risques autonome a été instaurée en qualité d'instance de contrôle indépendante et si un *chief risk officer* a été désigné pour cette instance (Cm 67 Circ.-FINMA 17/1) |  |  |  |
|  |  | Pour les établissements d’importance systémique uniquement :  Déterminer si un *chief risk officer* qui est membre de la direction a été désigné (Cm 68 Circ.-FINMA 17/1) |  |  |  |

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

1. Art. 10 al. 2 et 3 de l'ordonnance FINMA du 31 octobre 2024 sur l’audit prudentiel (RS *956.161.1*) [↑](#footnote-ref-2)
2. Les établissements soumis au régime des petites banques doivent effectuer au moins des analyses de scénarios. [↑](#footnote-ref-3)