**Points d’audit concernant la gestion des risques des données critiques**

**Vue d’ensemble**

|  |  |
| --- | --- |
| **Domaine d’audit :** | **Gestion des risques des données critiques** |
| **Étendue de l’audit :** | [Audit / Revue critique][[1]](#footnote-2) |
| **Bases :**  (liste non exhaustive) | Art. 3 al. 2 let. a de la loi sur les banques (LB)  Art. 9 de la loi sur les établissements financiers (LEFin)  Art. 12 de l’ordonnance sur les banques (OB)  Art. 12, 67, 68 et 73 de l’ordonnance sur les établissements financiers (OEFin)  Art. 11 al. 4 et 15 de l’ordonnance sur l’infrastructure des marchés financiers (OIMF)  Cm 13, 50, 52, 53, 58 et 59 de la Circ.-FINMA 17/1 « Gouvernance d’entreprise – banques »  Cm 71 à 82 de la Circ.-FINMA 23/1 « Risques et résilience opérationnels – banques » |
| **Visas :** | |  |  |  |  | | --- | --- | --- | --- | | **Visas :** | **Nom :** | **Fonction :** | **Date :** | | Auditeur : | [Nom] | [Assistant / *Senior* / *Manager* / *Senior manager* / Directeur / Partenaire] | [JJ MM AAAA] | | *Reviewer* : | [Nom] | [*Senior* / *Manager* / *Senior manager* / Directeur / Partenaire] | [JJ MM AAAA] | |

**Le présent document est un programme d’audit standard qui doit être appliqué à toute intervention conformément à la stratégie d’audit (Cm 28 ss de la Circ.-FINMA 13/3 « Activités d’audit »). Il est de la responsabilité de l’équipe d’audit d’adapter le programme d’audit standard à la situation de chaque établissement audité (taille, modèle d’affaires, organisation, processus, exposition aux risques, etc.). Si le contrôle d’audit effectué ne prend pas en compte toutes les procédures prescrites, une justification probante 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. Les points d’audit marqués de deux astérisques (\*\*) ne s’appliquent pas aux établissements selon l’art. 47*a* à 47*e* OFR, ni aux personnes selon l’art. 1*b* LB, ni aux maisons de titres qui ne gèrent pas de comptes.**

**Conclusion globale**

| **Thème :** | **Information / Description :** |
| --- | --- |
| Évaluation globale récapitulative | |  |  | | --- | --- | | **Confirmation dans le rapport d’audit :** | **Résumé :** | | Confirmation du respect des prescriptions prudentielles dans le domaine « Gestion des risques des données critiques ».  Confirmation que l’assujetti a respecté les renforcements ordonnés par la FINMA. | ***Oui*** *(Audit / Revue critique) /* ***Non***  ***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 d’audit – Gestion des risques des données critiques**

| **N°** | **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** |
| --- | --- | --- | --- | --- |
| *Gestion des risques des données critiques dans le respect du principe de proportionnalité, c’est-à-dire en tenant compte de la taille, de la complexité (notamment en ce qui concerne les TIC et l’externalisation), de la structure et du profil de risque :* | | | | |
| 1 | Acquisition des connaissances de base sur la gestion globale des risques des données critiques par l’établissement, dans le respect du principe de proportionnalité et des procédures d’audit suivantes. |  |  |  |
| 2 | Évaluation du caractère approprié des prescriptions internes (par ex. règlements, directives, instructions) relatives à la gestion des risques des données critiques. | Examen de la cohérence du contenu de la stratégie relative à la gestion des risques des données critiques avec d’autres prescriptions internes (par ex. politique de risque, grandes lignes de la gestion des risques à l’échelle de l’établissement, gestion des risques opérationnels, stratégie commerciale, stratégie en matière de TIC ou de données, etc.). |  |  |
| *Intégration dans la gestion globale des risques opérationnels ainsi que dans la stratégie, la gouvernance et la sensibilisation (Cm 23 à 26, 30, 31, 40 et 71 de la Circ.-FINMA 23/1) :* | | | | |
| 3 | Évaluation si les risques des données critiques (par ex. gouvernance des données insuffisante, qualité des données insuffisante, disponibilité insuffisante, manipulation des données non autorisée, perte de données, vol de données, corruption de données) sont intégrés en tant que taxonomie autonome dans la gestion globale des risques opérationnels et s’ils sont ainsi pris en compte de manière globale, c’est-à-dire de manière adéquate dans le cadre de l’identification, l’évaluation, l'atténuation et le contrôle des risques opérationnels. |  |  |  |
| 4 | Évaluation si les résultats d’audit ainsi que les évaluations des risques et des contrôles sont pris en compte lors de l’évaluation des risques conformément au Cm 30. |  |  |  |
| 5 | Évaluation si l’organe responsable de la haute direction approuve régulièrement une stratégie de gestion des risques des données critiques et s’assure de son respect. | Examen si les aspects suivants sont correctement pris en compte dans la stratégie relative au traitement des données critiques et aux mesures de protection :   * définition spécifique à l’établissement des données critiques ; * identification et catégorisation systématiques des données ; * gestion complète des risques des données critiques, * tâches, compétences et responsabilités en matière de gestion des données critiques, * dispositif relatif aux objectifs de protection de la confidentialité, de l’intégrité et de la disponibilité des données critiques. |  |  |
| 6 | Évaluation si l’organe responsable de la haute direction évalue et approuve au moins une fois par an la tolérance aux risques des données critiques conformément à la politique de risque et en tenant compte des objectifs stratégiques et financiers de l’établissement. |  |  |  |
| 7 | Évaluation du caractère approprié de l’identification des risques inhérents importants en matière de risques des données critiques. Si les risques des données critiques ne sont pas identifiés comme des risques inhérents importants, il convient d’évaluer le caractère compréhensible de la justification de cette décision. | Examen sur la base d’un échantillon approprié d’éléments relatifs à l’identification de risques importants et évaluation, si les risques potentiels liés aux risques des données critiques sont identifiés et pris en compte, et si l’évaluation du caractère important des risques inhérents correspond à la tolérance au risque. |  |  |
| 8 | Évaluation des mesures organisationnelles visant à renforcer la sensibilisation du personnel et des principaux intervenants externes (y compris des prestataires) concernant leurs tâches, compétences et responsabilités en matière de réduction générale des risques relatifs au traitement des données critiques. | Examen sur la base d’un échantillon approprié de collaborateurs clés et des principaux intervenants externes (y compris des prestataires) si des mesures suffisantes de sensibilisation à la gestion des données critiques sont prises. Il convient qu'une ou plusieurs des mesures suivantes soient prises :   * confirmation de la prise de connaissance et du respect du code de conduite *(code of conduct)*, * formations de sensibilisation à la gestion des données critiques, * annonces internes et communication régulière sur la gestion des données critiques, la sécurité des données et la protection des données, * formations spécifiques aux groupes cibles pour les personnes internes et externes ayant des droits d’accès (élargis) aux données critiques. |  |  |
| 9 | Évaluation du caractère approprié des formations sur la gestion des données critiques relatives aux risques effectifs et de l’orientation adéquate de la formation en fonction du groupe cible (par ex. des collaborateurs ayant accès à des données critiques, des collaborateurs disposant de droits privilégiés ou élargis, des cadres, des intervenants externes [y compris des prestataires]). |  |  |
| 10 | Évaluation du caractère approprié du rapport à la direction (contenu, régularité, etc.) sur l’évolution des risques TIC pertinents (y compris les risques des données critiques), l’efficacité des contrôles clés et les incidents internes et externes importants. |  |  |  |
| 11 | Évaluation des résultats d’audit et des contrôles de la révision interne et/ou d’autres fonctions de contrôle (par ex. contrôle des risques indépendant) relatifs à la gestion des risques des données critiques et examen des procès-verbaux des séances des comités/fonctions correspondant(e)s. |  |  |  |
| *Tâches, compétences et responsabilités (Cm 72 et 75 de la Circ.-FINMA 23/1) :* | | | | |
| 12 | **\*\*** Évaluation du caractère approprié, de la qualification et de l’indépendance de l’entité qui assure la fonction de contrôle (indépendant) du respect de la confidentialité, de l’intégrité et de la disponibilité des données critiques par des processus, procédures et contrôles appropriés. |  |  |  |
| 13 | **\*\*** Évaluation du caractère approprié des tâches, compétences et responsabilités dans la gestion des données critiques identifiées par l’établissement tout au long du cycle de vie de ces données, afin d’en assurer la confidentialité, l’intégrité et la disponibilité. | **\*\*** Sur la base d’un échantillon approprié de documents adéquats destinés aux collaborateurs clés, examiner si les tâches, compétences et responsabilités sont définies et attribuées de manière adéquate dans la gestion des données critiques. Les aspects suivants doivent être pris en compte :   * description claire des rôles (par ex. *data producer*, *data consumer*, *data administrator*, *data quality analyst*, *data owner / steward / custodian*, etc.) ; * description claire des tâches, compétences et responsabilités des rôles ; * description claire de l’organisation, la délimitation des fonctions, les lignes de rapport et les voies de communication. |  |  |
| 14 | **\*\*** Évaluation du caractère approprié de l’attribution des tâches, compétences et responsabilités dans la gestion des données critiques identifiées par l’établissement tout au long du cycle de vie de ces données, afin d’en assurer la confidentialité, l’intégrité et la disponibilité. | **\*\*** Sur la base d’un échantillon approprié de documents adéquats destinés aux collaborateurs clés, examiner si les aspects suivants ont été pris en compte de manière adéquate :   * qualification et expérience ; * fonction ; * proportionnalité de l’attribution d’éléments de données par responsable des données. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Procédures, processus et contrôles (Cm 74 à 78 de la Circ.-FINMA 23/1) :* | | | | |
| 15 | Évaluation du caractère approprié des contrôles clés dans la gestion des données critiques garantissant la confidentialité, l’intégrité et la disponibilité. Des contrôles clés adéquats sont effectués régulièrement et protègent les données critiques tout au long de leur cycle de vie. Celui-ci inclut : la collecte, l’enregistrement, la conservation, l’utilisation, la modification, la communication, le transfert, l’archivage, l’effacement et la destruction des données. | **\*** Examen de l’efficacité opérationnelle des contrôles clés garantissant :   * la confidentialité, par ex. en ce qui concerne les contrôles en matière de sécurité de l’information et de protection de la vie privée, de contrôles de *compliance*, d’*access management*, de code de conduite, de sensibilisation, etc. ; * l’intégrité, par ex. en ce qui concerne les contrôles de qualité des données, les contrôles de plausibilité, les contrôles de rapprochement automatiques et/ou manuels, l’approbation technique, le principe du double contrôle, la séparation des fonctions, etc. ; * la disponibilité, par ex. en ce qui concerne la surveillance de la transmission et du traitement des données, la traçabilité des données, la sauvegarde et la restauration des données, etc. ; * l’exhaustivité concernant la destruction des données. |  |  |
| 16 | **\*** Évaluation des processus, procédures et contrôles mis en place par l’établissement pour garantir un niveau adéquat de confidentialité ou des exigences de sécurité appropriées relatives à la gestion des données critiques pendant l’exploitation *(run)* ainsi que lors du développement, de la modification et de la migration *(change)* des données critiques. | **\*** Examen de l’efficacité opérationnelle des contrôles clés mis en place par l’établissement pour garantir un niveau adéquat de confidentialité ou des exigences de sécurité appropriées relatives à la gestion des données critiques pendant l’exploitation *(run)* ainsi que lors du développement, de la modification et de la migration *(change)* des données critiques. |  |  |
| *Inventaire (Cm 53, 63 et 73 de la Circ.-FINMA 23/1) :* | | | | |
| 17 | Évaluation si les données critiques de l’organisation sont systématiquement identifiées, répertoriées et catégorisées. Un inventaire des données contient par ex. les informations suivantes (attributs) :   * lieu de stockage ou environnement *cloud* ; * logiciels (y compris gestion des versions) ; * catégorisation (criticité) ; * dépendances au sein de l’établissement ; * sources internes et externes ; * interfaces avec les prestataires externes ; * responsabilité en matière des données. | Examen sur la base d’un échantillon approprié de contrôles de plausibilité ou de qualité des données effectués par l’établissement qui contribuent à garantir l’exhaustivité et l’exactitude de l’inventaire des données. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Gestion des accès (Cm 76 à 78 et 80 de la Circ.-FINMA 23/1) :* | | | | |
| 18 | \* Évaluation du caractère approprié des processus, procédures et contrôles relatifs à l’octroi des accès aux données critiques et aux fonctionnalités de traitement au personnel et à des tiers (définition des rôles, processus d’autorisation, etc.). | **\*** Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des contrôles relatifs à l’octroi de l’accès aux données critiques et aux fonctionnalités de traitement au personnel et à des tiers. Il convient en particulier de tenir compte des points suivants :   * principe du *need-to-know* et du *least privilege* ; * existence d’un système d’authentification et d’autorisation ; * portée et intégration des systèmes contenant des données critiques dans le processus d’autorisation et d’identification ; * portée et intégration de différents comptes d’utilisateurs (par ex. comptes techniques, comptes système, comptes privilégiés, comptes invités, comptes de service à distance, etc.). |  |  |
| 19 | **\*** Évaluation du caractère approprié des processus et contrôles liés à l’identification, la gestion et la surveillance de l’accès (standard et privilégié) aux données critiques. | **\*** Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des contrôles clés relatifs à l’identification, la gestion et la surveillance de l’accès (aussi bien standard que privilégié) aux données critiques. |  |  |
| 20 | **\*** Évaluation si les TIC physiques et logiques qui stockent ou traitent les données critiques sont protégées de manière adéquate. | **\*** Sur la base d’un échantillon approprié de ressources critiques[[2]](#footnote-3), examiner si les données critiques sont protégées de manière adéquate, par ex. au moyen d’un cryptage, d’une transmission sécurisée ou d’autres mesures techniques. |  |  |
| 21 | | **\*** Évaluation du caractère approprié des contrôles et des exigences de sécurité pour les profils d’utilisateurs disposant de privilèges accrus. | **\*** Examen du caractère approprié des contrôles (par ex. évaluation des fichiers journaux, octroi d’autorisations d’accès uniquement temporaires, fréquence accrue des contrôles de révision, principe du double contrôle / de la révision par les pairs) et des exigences de sécurité pour les personnes disposant de privilèges accrus et examen si une liste de ces personnes est tenue et mise à jour continuellement. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Gestion des autorisations hors de Suisse (Cm 79 de la Circ.-FINMA 23/1) :* | | | | |
| 22 | **\*\*** Lorsque les données critiques sont stockées hors de Suisse ou qu’elles sont accessibles depuis l’étranger, évaluation si les risques accrus qui en résultent sont atténués et les données protégées de manière appropriée. | **\*\*** Examen sur la base d’un échantillon approprié si des mesures organisationnelles et techniques sont prises pour contrôler de manière appropriée les risques accrus et protéger de manière appropriée les données critiques lorsqu’elles sont stockées hors de Suisse ou qu’elles sont accessibles depuis l’étranger. |  |  |
| *Incidents (Cm 81 de la Circ.-FINMA 23/1) :* | | | | |
| 23 | Évaluation du caractère approprié des processus, procédures et contrôles relatifs à la gestion des incidents qui entravent de manière importante la confidentialité, l’intégrité ou la disponibilité des données critiques. | Examen de l’efficacité opérationnelle du processus d’annonce à la FINMA sur la base d’un échantillon approprié d’incidents ayant entravé la confidentialité, l’intégrité ou la disponibilité des données critiques. |  |  |
| *Examen de diligence (Cm 82 de la Circ.-FINMA 23/1) :* | | | | |
| 24 | Évaluation du caractère approprié de l’examen de diligence *(due diligence)* lors du choix des prestataires qui peuvent accéder aux données critiques ou les traiter. | Sur la base d’un échantillon approprié de prestataires de services ayant accès à des données critiques, évaluer si un examen de diligence *(due diligence)* adéquat a été ou est effectué lors du choix des prestataires. |  |  |
| 25 | | Évaluation si des critères adéquats relatifs au traitement des prestataires ayant accès à des données critiques sont définis et réglés contractuellement. | Sur la base d’un échantillon approprié de prestataires ayant accès à des données critiques, examiner si la gestion des données critiques a été vérifiée et réglée avant la signature du contrat. |  |  |
| 26 | | Évaluation si les prestataires ayant accès à des données critiques sont périodiquement soumis à une surveillance et à un contrôle dans le cadre du système de contrôle interne de l’établissement. | Sur la base d’un échantillon approprié de prestataires ayant accès à des données critiques, examiner si leur utilisation des données est périodiquement soumise à une surveillance et à un contrôle fondés sur les risques. |  |  |

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

1. Cm 33 et 34 de la Circ.-FINMA 13/3 [↑](#footnote-ref-2)
2. Circ.-FINMA 23/1 annexe 1 [↑](#footnote-ref-3)