**Points d’audit concernant la gestion des cyberrisques**

**Vue d’ensemble**

|  |  |
| --- | --- |
| **Domaine d’audit :** | **Gestion des cyberrisques** |
| **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 et 68 de l’ordonnance sur les établissements financiers (OEFin)  Cm 13, 50, 52, 53, 58 et 59 de la Circ.-FINMA 17/1 « Gouvernance d’entreprise – banques »  Cm 23 à 26, 40, 61 à 70 et 104 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.**

**Conclusion globale**

| **Thème :** | **Information / Description :** |
| --- | --- |
| Évaluation globale récapitulative | |  |  | | --- | --- | | **Confirmation dans le rapport d’audit :** | **Résumé :** | | Confirmation de la structure adéquate du domaine « gestion des cyberrisques ».  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 cyberrisques**

| **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 cyberrisques 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 cyberrisques 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 cyberrisques. | Examen de la cohérence du contenu de la stratégie relative à la gestion des cyberrisques 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). |  |  |
| *Intégration dans la gestion globale des risques opérationnels ainsi que dans la stratégie, la gouvernance et la sensibilisation (Cm 23 à 26, 30, 40 et 61 de la Circ.-FINMA 23/1)* | | | | |
| 3 | Évaluation si les cyberrisques 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. | Examen sur la base d’un échantillon approprié d’applications des instruments de gestion des risques (par ex. tolérance aux risques, résultats d’audit ainsi qu’évaluations des risques et des contrôles selon Cm 30) pour le domaine des cyberrisques. |  |  |
| 4 | Évaluation si l’organe responsable de la haute direction évalue et approuve au moins une fois par an la tolérance aux cyberrisques conformément à la politique de risque et compte tenu des objectifs stratégiques et financiers de l’établissement. |  |  |  |
| 5 | Évaluation si l’organe responsable de la haute direction approuve régulièrement une stratégie de gestion des cyberrisques et s’assure de son respect. |  |  |  |
| 6 | Évaluation du caractère approprié de l’identification des risques inhérents importants en matière de cyberrisques. Si les cyberrisques 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 cyberrisques importants et évaluation, si les risques potentiels liés aux cyberrisques sont identifiés et pris en compte, et si l’évaluation du caractère important des risques inhérents correspond à la tolérance au risque. |  |  |
| 7 | Évaluation des mesures organisationnelles et techniques relatives à la sensibilisation du personnel concernant les tâches, compétences et responsabilités en matière de réduction des cyberrisques. |  |  |  |
| 8 | Évaluation du caractère approprié des formations sur la cybersécurité relatives aux menaces spécifiques aux cyberrisques et/ou à l’établissement et de l’orientation adéquate de la formation en fonction du groupe cible (par ex. des cadres, des collaborateurs disposant de droits privilégiés ou accrus, des collaborateurs ayant accès à des données critiques, des intervenants externes [y compris des prestataires], etc.). | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des contrôles relatifs à la formation (régulière) du personnel, des collaborateurs clés comme des tiers dans le domaine de la cybersécurité. |  |  |
| 9 | Évaluation du caractère approprié du rapport à la direction (par ex. contenu, régularité, etc.) sur l’évolution des cyberrisques, l’efficacité des contrôles clés et les incidents internes et externes importants. |  |  |  |
| 10 | 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 sécurité informatique et examen des procès-verbaux des séances des comités/fonctions correspondant(e)s. |  |  |  |
| *Tâches, compétences et responsabilités (Cm 62 de la Circ.-FINMA 23/1) :* | | | | |
| 11 | Évaluation du caractère approprié des tâches, compétences et responsabilités au sein de la cyberorganisation (par ex. en ce qui concerne la description des rôles, l’organisation, la délimitation des fonctions, les lignes de rapport et les voies de communication). |  |  |  |
| 12 | Évaluation si les cyberrisques sont pris en compte de manière adéquate dans la planification et l’exécution d'audits par le contrôle des risques indépendant ainsi que par la révision interne. Il convient en particulier de tenir compte des points suivants :   * analyse et évaluation des risques, * planification pluriannuelle, * normes internationales utilisées. |  |  |  |
| 13 | **\*** Évaluation de l’indépendance (Cm 62 de la Circ.-FINMA 17/1) des fonctions internes en relation avec l’évaluation de la situation en matière de risques liés à la cybersécurité. |  |  |  |
| *Procédures, processus et contrôles (y compris développement et amélioration continus) (Cm 62 de la Circ.-FINMA 23/1) :* | | | | |
| 14 | Évaluation si le concept relatif à la gestion des cyberrisques a été établi selon une norme ou des pratiques internationalement reconnues et s’il couvre la situation de risque et les besoins spécifiques de l’établissement. | Sur la base d’un échantillon approprié, examiner si le concept relatif à la gestion des cyberrisques est continuellement développé et amélioré sur la base des enseignements tirés des contrôles et de l’expérience acquise. |  |  |
| *Cm 63 de la Circ.-FINMA 23/1.* | | | | |
| 15 | Évaluation si les composantes TIC (cf. Cm 53 et 54) et les interfaces avec les tiers ont été identifiées, répertoriées et évaluées. | Examen sur la base d’un échantillon approprié des contrôles clés destinés à s’assurer de l’exhaustivité et de l’exactitude des inventaires. Tenir compte notamment des points suivants :   * composantes matérielles ; * composantes logicielles : applications (y compris les dépendances) ; * composantes logicielles : logiciels pour utilisateurs finaux (y compris versionnage) ; * évaluation de la criticité ; * lieu de stockage des données critiques ; * interfaces avec les prestataires externes importants. |  |  |
| 16 | Évaluation s’il existe une définition des données critiques et si ces données ont été répertoriées en conséquence (cf. Cm 7, 53 et 54). |  |  |
| 17 | Évaluation si les composantes TIC (cf. Cm 7, 53 et 54) sont représentées de manière adéquate dans l’infrastructure du réseau, en fonction de leur criticité et de leur besoin de protection. |  |  |
| 18 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à l’identification des menaces potentielles de cyberattaques spécifiques à l’établissement et à l’évaluation des conséquences possibles de l’exploitation de vulnérabilités concernant les composantes TIC répertoriées, les interfaces avec des tiers ainsi que les données critiques (cf. Cm 7, 53 et 54). | **\*** Examen sur la base d’un échantillon approprié des composantes existantes relatives à l’identification et l’évaluation de la situation en matière de cybermenace. L’échantillon servant à évaluer la situation en matière de cybermenace tient au minimum compte des aspects suivants : • les effets de cyberattaques sur l’établissement ; • la probabilité d’occurrence ; • l’évaluation du risque. |  |  |
| 19 | Évaluation si les menaces potentielles spécifiques à l’établissement ainsi que les vulnérabilités, et donc les conséquences des cyberattaques sur les composantes TIC répertoriées, les interfaces avec des tiers et les données critiques (cf. Cm 7, 53 et 54), sont connues et prises en compte de manière adéquate dans le cadre de l’évaluation des risques. |  |  |
| *Dispositif de protection (Cm 64 de la Circ.-FINMA 23/1) :* | | | | |
| 20 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à l’octroi de l’accès logique et/ou physique (standard ou privilégié) aux composantes TIC répertoriées, ainsi qu’aux interfaces avec des tiers (cf. Cm 53 et 54). | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des contrôles relatifs à l’octroi de l’accès logique et/ou physique aux composantes TIC répertoriées, ainsi qu’aux interfaces critiques avec des tiers (cf. Cm 53 et 54). |  |  |
| 21 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à la confirmation (régulière) de l’accès logique et/ou physique (standard ou privilégié) aux composantes TIC répertoriées, ainsi qu’aux interfaces avec des tiers (cf. Cm 53 et 54). | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des contrôles relatifs à la confirmation (régulière) de l’accès logique et/ou physique aux composantes TIC critiques répertoriées, ainsi qu’aux interfaces critiques avec des tiers (voir Cm 7, 53 et 54). |  |  |
| 22 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à l’identification, la gestion et la surveillance de l’accès logique et/ou physique (standard ou privilégié) aux composantes TIC répertoriées, ainsi qu’aux interfaces avec des tiers (cf. Cm 53 et 54). | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des contrôles relatifs à l’identification, la gestion et la surveillance de l’accès logique et/ou physique aux composantes TIC répertoriées, ainsi qu’aux interfaces critiques avec des tiers (cf. Cm 53 et 54). |  |  |
| 23 | Évaluation du caractère approprié des mesures organisationnelles et techniques contre la fuite de données critiques *(data loss prevention)*. | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des mesures organisationnelles et techniques contre la fuite de données critiques *(data loss prevention)*. |  |  |
| 24 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à la gestion de la sécurité du réseau (par ex. zonage, contrôle d’accès au réseau [NAC], pare-feu, *web application firewall* [WAF], protection contre les DDoS, serveurs *proxy*). | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des mesures relatives à la gestion de la sécurité du réseau. |  |  |
| 25 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à la gestion de la sécurité de l’infrastructure (par ex. *endpoint detection and response* [XDR], anti-virus, etc.). | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des mesures relatives à la gestion de l’infrastructure critique. |  |  |
| 26 | Évaluation du caractère approprié des procédures, processus et contrôles relatifs à la garantie de la configuration standard et du renforcement du système (configuration de base et renforcement) des composantes TIC répertoriées, ainsi que leur respect permanent. | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des mesures relatives à la configuration de base et aux renforcements du système pour les système critiques. |  |  |
| 27 | Évaluation de l’approche fondée sur les risques destinée à combler en temps utile les failles de sécurité *(patching)* ou traiter les erreurs de configuration (changement de configuration) dans les systèmes, les applications ou l’infrastructure sous-jacente. | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des mesures destinées à combler des failles de sécurité importantes ou critiques dans des systèmes critiques. |  |  |
| 28 | Évaluation du caractère approprié des prescriptions pour la protection de la confidentialité, de l’intégrité et de la disponibilité des données critiques stockées et transmises. | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle des mesures relatives à la protection de la confidentialité, de l’intégrité et de la disponibilité des données critiques stockées et transmises, par ex. au moyen d’un cryptage. |  |  |
| *Enregistrement et détection (Cm 65 de la Circ.-FINMA 23/1)* | | | | |
| 29 | Évaluation si des irrégularités (par ex. comportement anormal) et des événements touchant à la sécurité sont identifiés rapidement au moyen d’une surveillance continue des TIC et si les conséquences potentielles de ces événements sont évaluées de manière adéquate. |  |  |  |
| 30 | Évaluation si les valeurs par défaut pour les opérations de réseau autorisées et les flux de données attendus (par ex. en ce qui concerne les flux de données entre les différentes zones du réseau et les interfaces entre les systèmes TIC) sont techniquement définies au moyen de cas d’utilisation SIEM pour les utilisateurs et les systèmes et évaluation du processus de mise à jour de ces cas d’utilisation. |  |  |  |
| 31 | Évaluation si les composantes TIC répertoriées et leur utilisation par les collaborateurs et les tiers font l’objet d’une surveillance systématique et continue. | Examen sur la base d’un échantillon approprié si toutes les composantes TIC critiques répertoriées ainsi que toutes les applications commerciales fournissent l’historique des événements à un système central et si cet historique est analysé afin d’identifier les cyberincidents. |  |  |
| 32 | Évaluation du caractère approprié des mesures techniques relatives à la détection des cyberincidents sur la base de scénarios de cyberrisques définis (appelés cas d’utilisation). |  |  |
| 33 | Évaluation de la mise à jour et des tests réguliers des processus et des instructions relatifs à la détection des incidents de cybersécurité. |  |  |  |
| *Réaction (Cm 66 et 68 de la Circ.-FINMA 23/1) :* | | | | |
| 34 | Évaluation du caractère approprié du plan de réaction relatif au traitement des incidents de cybersécurité reconnus, en particulier la manière dont il est coordonné avec les groupes d’intérêts internes et externes, et quel soutien est nécessaire de la part de parties prenantes externes en cas d’incident. | Sur la base d’un échantillon approprié d’éléments, examiner si le plan de réaction est efficace et réalisé à temps en cas d’incident ou lors d’un test. |  |  |
| 35 | Évaluation du caractère approprié des processus relatifs à l’analyse, la documentation et la classification rapides des messages issus des systèmes de détection (appelés événements). | Examen de l’efficacité opérationnelle des processus relatifs à l’analyse et la classification des messages issus des systèmes de détection (appelés événements). |  |  |
| 36 | Évaluation du caractère approprié des processus et des mesures (par ex. les *playbooks*) destinés à délimiter et atténuer les dommages en cas de cyberattaques. |  |  |  |
| 37 | Évaluation si les exigences découlant de la communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l’art. 29 al. 2 LFINMA » sont prises en compte dans le plan de réaction. | Sur la base d’un échantillon approprié de cyberattaques partiellement réussies ou réussies, examen de l’efficacité opérationnelle et du respect du processus de déclaration conformément aux exigences de la communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l’art. 29 al. 2 LFINMA ». |  |  |
| *Rétablissement (Cm 67 de la Circ.-FINMA 23/1) :* | | | | |
| 38 | Évaluation du caractère approprié de l’appréciation et des améliorations périodiques relatives aux processus de réaction et de rétablissement. | Examen sur la base d’un échantillon approprié de l’efficacité opérationnelle de la documentation et de la mise en œuvre des enseignements tirés d’incidents passés. |  |  |
| 39 | Évaluation du caractère approprié des processus de rétablissement destinés à garantir un rétablissement rapide des systèmes après une cyberattaque. | Sur la base d’un échantillon approprié d’éléments, examiner si les processus de rétablissement après une cyberattaque ont été vérifiés au moyen de tests appropriés (appelés *walk throughs*, exercices *table top*). |  |  |
| *Analyses de vulnérabilité, tests d’intrusion et cyberexercices fondés sur des scénarios de risque (Cm 69 et 70 de la Circ.-FINMA 23/1) :* | | | | |
| 40 | Évaluation du caractère approprié des processus relatifs à la réalisation régulière d’analyses de vulnérabilité, de tests d’intrusion et de cyberexercices fondés sur des scénarios reposant sur les menaces potentielles spécifiques à l’établissement. |  |  |  |
| 41 | Évaluation si des analyses de vulnérabilité et des tests d’intrusion sont régulièrement effectués sur toutes les composantes TIC accessibles par Internet et au moins sur les systèmes nécessaires à l’exécution de processus critiques ou contenant des données critiques. |  |  |  |
| 42 | Évaluation du caractère approprié des prescriptions et processus spécifiques à l’établissement relatifs au traitement des vulnérabilités identifiées et à leur correction fondée sur les risques. | Sur la base d’un échantillon approprié, examiner si les vulnérabilités importantes ou critiques détectées par les analyses de vulnérabilité et les tests d’intrusion ont été corrigées conformément aux prescriptions définies. |  |  |
| 43 | Évaluation du caractère approprié des ressources techniques et personnelles destinées à assurer la mise en place, la réalisation et l’exécution fondée sur les risques des analyses de vulnérabilité, des tests d’intrusion ainsi que des cyberexercices fondés sur des scénarios. |  |  |  |
| 44 | Évaluation si les résultats des cyberexercices sont documentés et rapportés sous une forme appropriée. |  |  |  |

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

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