PENTA

FINMA - FEUILLE DE ROUTE 2025 : CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ

Votre roadmap pour rester conforme aux normes de la FINMA en matière de cyberrisques

2025

Les risques cybernétiques présentent un danger important pour la réputation et les opérations des institutions financières suisses. Face au problème, la FINMA a renforcé la surveillance de tous les établissements financiers, peu importe leur taille et leur spécialité.

Contenu

Les avancées numériques telles que le cloud sont inévitables.

Elles offrent de nombreux avantages et de nouvelles possibilités et fonctionnalités.

Mais elles engendrent aussi des risques.

Le cloud est un paysage complexe qui, pour les secteurs fortement réglementés (tels que la finance et le droit, pour ne citer que deux exemples), **nécessite beaucoup de prudence,** non seulement du point de vue de la conformité, mais aussi en termes de sécurité.

Les fournisseurs de services cloud doivent offrir de solides garanties, et les institutions financières, à leur tour, doivent pouvoir faire preuve d'une cybersécurité infaillible auprès de leurs clients.
Êtes-vous prêt et équipé à cet effet ?

Si la réponse est non, ou si vous n'êtes pas sûr, Penta a élaboré ce guide de conformité aux normes imposées par la FINMA en matière de cyber risques en 2025. Il a été conçu dans le but d'aider les institutions financières suisses à exercer leurs activités en toute confiance, en sachant qu'elles respectent toutes les exigences réglementaires applicables en garantissant un niveau adéquat de **sécurité et de conformité.**

Aperçu

Aperçu

La FINMA vise à garantir la stabilité des institutions financières suisses en évaluant les risques auxquels chaque entreprise est exposée.

Son objectif premier est de superviser et de protéger le secteur financier suisse et sa réputation.

Les risques informatiques sont une menace croissante et le principal danger à même de compromettre cette réputation. Mais la mise en place de mesures d'atténuation ne consiste pas simplement à cocher des cases et à respecter les règles.

À une échelle plus réduite, si votre entreprise ne fait pas le nécessaire pour atténuer les risques informatiques, elle s'expose à des conséquences catastrophiques. C'est pourquoi la conformité ne doit pas être considérée comme la référence absolue, mais comme une **base de départ.**

Cependant, sur un plan plus général, le professionnalisme croissant et l'agilité des criminels obligent le secteur financier à rester vigilant. Après tout, une attaque réussie peut entraîner des pannes, interrompre le partage d'informations et la communication et compromettre la disponibilité, la confidentialité et l'intégrité, sans parler du risque de vol pur et simple.

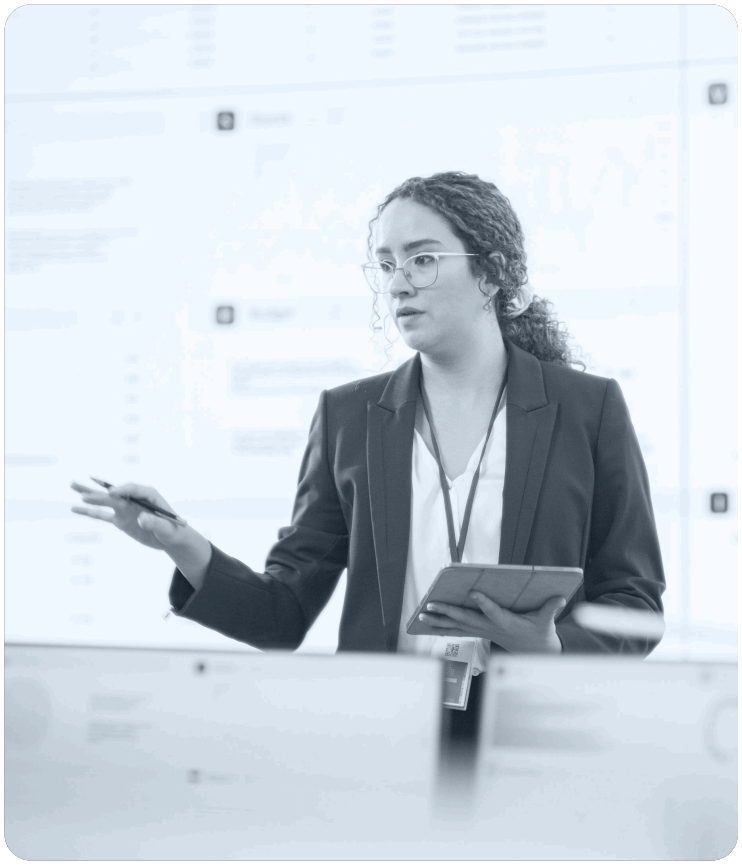
Pourtant, **selon la FINMA,** les entreprises soumises à ses réglementations ne sont toujours pas suffisamment **sensibilisées aux risques** et les processus cybernétiques sont souvent trop fragmentés pour permettre une analyse précise et globale de la situation en termes de risques.

De plus, de nouvelles **failles de sécurité** apparaissent constamment et doivent être identifiées et corrigées le plus rapidement possible, ce qui ne fait qu'exacerber la situation.

Les neuf principaux risques en 2025 / Les principaux facteurs de risque

Les neuf principaux risques en 2025

- Risque associé aux taux d'intérêt
- Risque de crédit lié aux hypothèques
- Risque de crédit associé à d'autres prêts
- Risque de **cyberattaques**
- Risque relatif à la lutte contre le blanchiment d'argent
- Risque lié aux difficultés croissantes concernant l'accès aux marchés étrangers
- Risque d'élargissement des écarts de rendement
- Risque lié à l'externalisation
- Risque de liquidité et de financement



Comme vous pouvez le constater, les cyberattaques et l'externalisation font partie des neuf risques explicitement identifiés, et ce sont précisément ces deux domaines – au cœur de notre expertise – que nous allons explorer dans ce rapport.

Les principaux facteurs de risque

- Des plans de réponse incomplets (ou inexistants) sont en place en cas d'incidents cybernétiques, ou l'efficacité de ces plans n'est pas vérifiée.
- Les établissements supervisés n'intègrent pas explicitement les cyberrisques dans les exigences qualitatives imposées pour la gestion des risques opérationnels. Ils ne sont donc pas en mesure de garantir une gestion systématique et complète des risques cybernétiques.
- Les cyberrisques et les tolérances associées ne sont pas définis de manière adéquate, ou aucune mesure de cyberprotection n'est mise en place.
- Les assujettis n'ont défini aucune exigence claire en matière de cybersécurité à l'égard des prestataires de services, ou le respect de ces exigences n'est pas régulièrement contrôlé.

Externalisation et ses dangers associés

Externalisation et ses dangers associés

L'externalisation n'est pas un concept nouveau. Toutefois, portée par la numérisation et la volonté des entreprises de se recentrer sur leurs activités principales, elle ne cesse de croître. Le nombre de services externalisés par institution augmente, tout comme celui des sous-traitants impliqués.

Cela complexifie la chaîne d'approvisionnement et accroît les risques associés.

L'externalisation présente de nombreux avantages – loin d'être négligeables – **comme une flexibilité accrue, un potentiel d'innovation renforcé et une meilleure résilience opérationnelle.**

Cependant, FINMA identifie aujourd'hui l'externalisation de fonctions critiques à des tiers comme un risque opérationnel majeur.

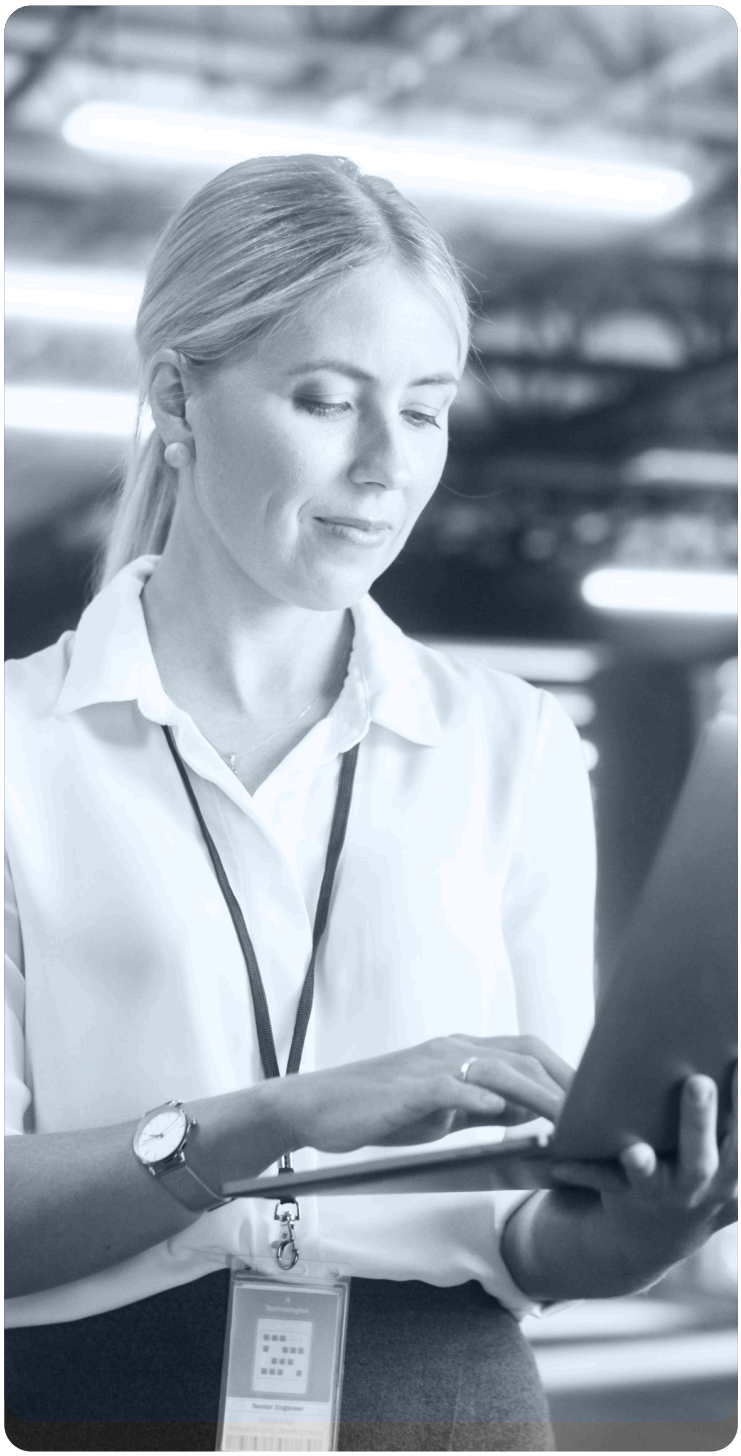
L'autorité souligne **qu'un tiers des cyberattaques** visant des institutions financières proviennent de prestataires tiers.

Elle ajoute que les perturbations ou défaillances dans les fonctions critiques gérées par ces tiers pourraient, **dans les cas extrêmes, menacer la stabilité du marché financier dans son ensemble.**

Pourquoi ? Parce que de nombreuses institutions dépendent d'un nombre restreint de fournisseurs pour des fonctions critiques telles que les services cloud.

Cette concentration renforce la dépendance du secteur à ces prestataires.

Une interruption de service ou un accès non autorisé pourrait ainsi impacter gravement la stabilité du marché financier suisse.



FINMA souligne que de nombreuses institutions **doivent encore améliorer leur compréhension** de la chaîne d'approvisionnement et des risques qui y sont liés.

L'autorité s'inquiète particulièrement du fait que, dans certains cas, ces risques **ne soient ni correctement identifiés,** ni surveillés, encore moins maîtrisés.

Les processus fréquemment externalisés incluent les paiements (externalisés par deux tiers des banques) ainsi que l'infrastructure et les opérations IT (externalisées par 80 % des banques et 60 % des assureurs).

Par conséquent, ces institutions sont fortement dépendantes de leurs prestataires pour assurer leurs services.

Cependant, elles demeurent entièrement responsables du suivi de ces prestataires et de la mise en œuvre des mesures nécessaires en cas de problème.

Gérer et surveiller efficacement les prestataires et les risques associés est donc **crucial pour garantir l'intégrité opérationnelle.**

Les organisations ne peuvent pas déléguer la responsabilité de leur bonne conduite commerciale, y compris lorsqu'il s'agit d'externalisation.

Elles **doivent développer les compétences nécessaires** pour superviser efficacement les fonctions externalisées et intervenir rapidement lorsque cela s'impose.

Cyberattaques selon la FINMA : les dernières tendances (2023–2024)

Cyberattaques selon la FINMA : les dernières tendances (2023–2024)

Les menaces cybernétiques demeurent l'un des principaux risques opérationnels pour le secteur financier suisse.

La FINMA signale une hausse de 30 % des cyberattaques réussies ou partiellement réussies sur un an.

Environ un tiers de ces incidents sont liés à des prestataires de services externes, soulignant les vulnérabilités continues liées à l'externalisation et aux services IT tiers.

Les programmes malveillants et les accès non autorisés sont les méthodes d'attaque les plus fréquentes, avec une hausse notable des attaques ciblant les petites structures, notamment les gérants de fortune indépendants et les intermédiaires d'assurance non liés.

L'e-mail reste la principale porte d'entrée, en particulier pour les attaques de type BEC (Business Email Compromise) et les fraudes aux dirigeants (CEO fraud).

Les attaques de type DDoS ont également connu une recrudescence, motivées à la fois par des considérations financières et idéologiques.

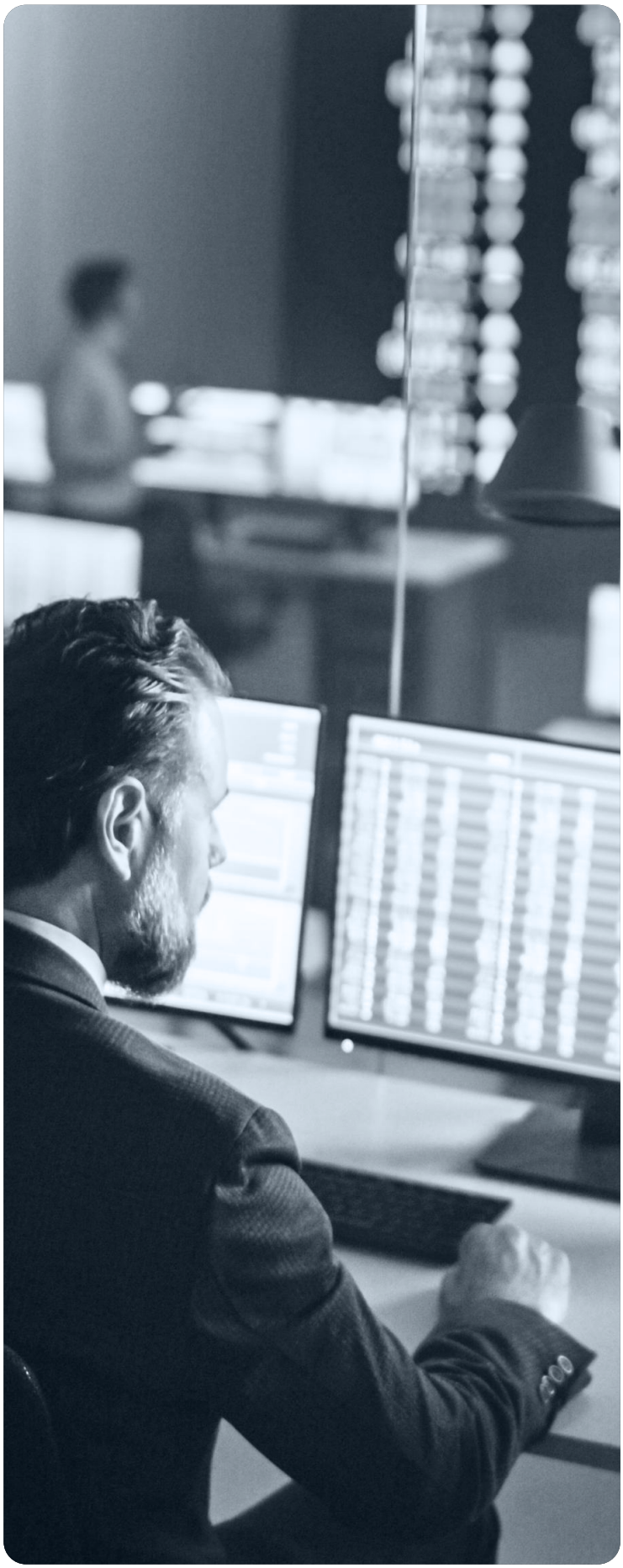
Les attaques de la chaîne d'approvisionnement, y compris celles ciblant les fournisseurs de services cloud, continuent de progresser et représentent près de 30 % des incidents signalés.

La FINMA insiste sur la nécessité d'améliorer la gestion du cycle de vie des infrastructures IT, de renforcer les politiques de sécurité avec les tiers et d'accélérer la détection et la réponse aux incidents.

Ces éléments sont essentiels pour protéger les opérations critiques et les données sensibles.

À qui les directives de la FINMA en matière de cybersécurité s’appliquent-elles ?

À qui les directives de la FINMA en matière de cybersécurité s'appliquent-elles ?



La grande majorité des fournisseurs de services financiers et des sociétés exerçant sur le marché financier suisse nécessitent une autorisation.

Dans la plupart des cas, elle est accordée par la FINMA.

Toute personne ou entreprise qui souhaite gérer l'argent de ses clients, utiliser des fonds provenant d'investisseurs, souscrire des polices d'assurance ou créer et gérer des placements collectifs doit recevoir une autorisation de la FINMA.

Les sociétés qui reçoivent cette autorisation seront dès lors supervisées.

Les activités de contrôle effectuées par la FINMA varient : cela peut aller d'une surveillance intensive et continue à la simple inscription au registre, après quoi la FINMA n'interviendra que si elle reçoit des allégations de mauvaise conduite.

Dans certaines circonstances, les prestataires de services doivent adhérer à un organisme privé d'autorégulation.

Pour vérifier si un individu, une entreprise ou un produit financier a obtenu les autorisations nécessaires, recherchez son nom sur le site de la FINMA.

Comment atténuer les cybermenaces internes et celles liées aux tiers / Signalements auprès de la FINMA : vos obligations légales

Comment atténuer les cybermenaces internes et celles liées aux tiers

Les banques suisses doivent protéger leurs infrastructures contre diverses formes d'attaque, y compris, mais sans s'y limiter, le phishing, les maliciels ou l'indisponibilité des systèmes informatiques.

Toutes les banques et négociants en valeurs mobilières qui relèvent de la juridiction de la FINMA doivent appliquer un concept « systématique et global » pour repousser les menaces provenant du monde virtuel.

Ils doivent notamment définir des mesures concrètes en termes de gouvernance, d'identification, de protection, de détection, de réponse et de récupération des systèmes et services menacés par des cyberrisques ou des cyberattaques.

Signalements auprès de la FINMA : vos obligations légales

Si votre entreprise, qui est réglementée par L'Autorité fédérale de surveillance des marchés financiers, subit une cyberattaque, vous devez en informer la FINMA par l'intermédiaire de votre gestionnaire de compte dans les 24 heures suivant la détection et procéder à une évaluation initiale de sa gravité.

Si la FINMA découvre que vous exercez vos activités (sciemment ou non) sans autorisation (cela inclut le fait de ne pas lui transmettre de rapport dans le délai imparti en cas de cyberattaque) elle ouvrira une enquête. Si elle découvre des preuves en ce sens, elle peut lancer **des procédures exécutoires** et imposer des mesures plus ou moins sévères qui peuvent aller jusqu'à la liquidation de l'entreprise.

Un rapport (comme décrit à la page suivante) doit ensuite être soumis à la FINMA via la **plateforme Web de saisie et de demande, dans un délai de 72 heures.**

Éléments à inclure dans un rapport de cyberattaque adressé à la FINMA

- Nom de l'entreprise
- Personne à contacter, y compris ses coordonnées (numéro de téléphone et adresse e-mail)
- Date et heure de soumission du rapport à la FINMA
- Date et heure de détection de l'attaque
- Date et heure de l'attaque, si ces éléments sont déjà connus
- Description de la cyberattaque et statut actuel
- Évaluation initiale du degré de gravité de la cyberattaque (voir la section *« Déterminer le degré de gravité d'une cyberattaque »* ci-dessous)
- Évolution du degré de gravité
  - décroissant
  - stable
  - croissant
- Entités affectées (unités organisationnelles touchées au sein de l'établissement ou du fournisseur de services)
- Objectifs de protection
  - confidentialité
  - intégrité
  - disponibilité
- Fonctions d'importance critique, processus ou actifs touchés
  - informations
  - infrastructure technologique
  - bâtiments ou personnel

- Nombre de clients concernés (statut actuel)
- Vecteurs de l’attaque
  - e-mail
  - attaque via Internet
  - attaque par force brute
  - usurpation d’identité
  - support amovible
  - perte/vol de périphériques
  - exploitation de vulnérabilités logicielles
  - exploitation de vulnérabilités matérielles
  - autre (veuillez préciser)
- Type d’attaque (par exemple)
  - DDoS
  - accès non autorisé
  - maliciel
  - mauvaise utilisation/utilisation abusive de l’infrastructure technologique
- Contre-mesures administratives, opérationnelles et/ou techniques et les échéances attendues
- Mesures de communication (contenu, destinataire, date)

Il est important de noter que si, suite à la soumission du rapport, de nouveaux **développements ou de nouvelles évaluations** surviennent concernant la même attaque, un nouveau rapport doit être soumis dans les 72 heures.

La FINMA souhaite être informée le plus rapidement possible des cyber incidents critiques dont sont victimes les assujettis.

Cela lui permet non seulement d'apporter son soutien en cas de crise, mais aussi de prendre les mesures nécessaires pour avertir les autres établissements d'attaques identiques ou similaires.

Concernant les cyberattaques évaluées comme ayant un degré de gravité **« Élevé »** ou **« Grave »** (voir la section « Déterminer le degré de gravité d'une cyberattaque » ci-dessous), une fois le dossier traité, la FINMA s'attend à recevoir un rapport conclusif sur les causes associées.

Celui-ci doit inclure :

- une analyse
- les raisons pour lesquelles l'attaque a réussi
- les effets de celle-ci sur le respect des prescriptions réglementaires, sur les opérations et sur les clients
- les mesures visant à atténuer les conséquences de l'attaque

Pour les cyberattaques dont le degré de sévérité est « Grave », il faut également transmettre les preuves et les analyses du bon fonctionnement de l'organisation de crise.

Pour les cyberattaques dont le degré de gravité est « Moyen », un rapport conclusif sur les causes est suffisant.

Déterminer le degré de gravité d’une cyberattaque

Déterminer le degré de gravité d'une cyberattaque

Critères utilisés par la FINMA pour procéder à une évaluation du degré de gravité d'une cyberattaque :

Grave

Dommages (effectifs ou prévus) durables et de grande ampleur affectant les objectifs de protection (disponibilité, intégrité, confidentialité) des actifs critiques.

- Disponibilité : les actifs critiques ne sont pas disponibles à moyen ou long terme (panne > 200 % du RTO9).
- Confidentialité/intégrité : les informations sensibles sont affectées dans leur intégralité (ou presque).
- Implications financières ou atteinte à la réputation de l'établissement menaçant son existence.
- Pour surmonter la cyberattaque, il est nécessaire d'activer l'organisation de crise (plan de gestion de la continuité des activités).

Élevé

Les objectifs de protection (disponibilité, intégrité, confidentialité) des actifs critiques sont considérablement atteints ou menacés.

- Disponibilité : les actifs critiques ne sont pas disponibles à moyen terme (panne ≥ RTO).
- Confidentialité/intégrité : les informations sensibles et/ou essentielles au processus opérationnel sont affectées de manière significative.
- Répercussions financières considérables ou atteinte à la réputation de l'établissement.
- Pour surmonter la cyberattaque, il est nécessaire de faire appel à des ressources externes.

Moyen

Menace ou préjudice direct affectant les objectifs de protection (disponibilité, intégrité, confidentialité) des actifs critiques.

- Disponibilité : les actifs critiques ne sont pas disponibles à court terme (panne > 50 % du RTO).
- Confidentialité/intégrité : les informations sensibles sont considérablement affectées.
- Répercussions financières notables ou atteinte à la réputation de l'établissement.
- Les cyberattaques peuvent être surmontées avec les ressources disponibles en interne.

Identifier les actifs critiques et les cyberattaques potentielles associées

Informations sensibles/confidentielles telles que les identifiants des clients, les contrats d'assurance, les données relatives au règlement des sinistres ou au traitement des prestations, les procès-verbaux des réunions du conseil d'administration ou du comité de direction, les informations stratégiques, les données RH.

- Attaques visant les objectifs de protection à travers un accès non autorisé aux données, que ce soit au sein de l'entreprise ou depuis l'extérieur, fuite de données, vol de données, modification des données.

Infrastructure technologique nécessaire à l'exécution d'une fonction critique (matériel, logiciel, infrastructure réseau).

- Attaques DDoS visant les objectifs de protection, perte ou vol de supports de stockage contenant des informations confidentielles, rançongiciel.

Bâtiments essentiels pour l'exécution de fonctions critiques (centre de données, succursales, back-office).

- Attaques visant les objectifs de protection en entravant ou en bloquant l'exécution des mesures de protection en place pour réglementer l'accès aux zones sensibles.

Le personnel exerçant des fonctions critiques ou y contribuant de manière significative, tels que le comité de direction, les négociants, les conseillers clients, ainsi que les collaborateurs clés (les employés disposant de droits avancés, les administrateurs système, le personnel de sécurité, la comptabilité).

- Attaques visant les objectifs de protection à travers des techniques d'ingénierie sociale telles que le spear phishing, les menaces internes, l'usurpation d'identité et le chantage.

Points d’audit de la FINMA dans le cadre de la gestion des cyberrisques

Points d'audit de la FINMA dans le cadre de la gestion des cyberrisques

Ces points d'audit doivent être mis en œuvre par votre équipe pour garantir la conformité de votre entreprise aux normes de la FINMA. Si l'un de ces points n'est pas respecté, vous devrez en expliquer la raison à la FINMA.

1 ☐

Évaluer la manière dont l'établissement gère les cyberrisques, y compris l'importance qu'il leur accorde et comment il procède aux audits correspondants.

2 ☐

Évaluer la pertinence de la stratégie de gestion des cyberrisques mise en place par l'assujetti, y compris les règlements, politiques, procédures, normes, recommandations et directives.

3 ☐

S'assurer que les cyberrisques sont bien pris en compte dans le cadre de la gestion plus globale des risques opérationnels, c'est-à-dire lors de l'identification, de l'évaluation, de l'atténuation et du monitorage des risques opérationnels.

4 ☐

Le conseil d'administration examine-t-il régulièrement (au moins une fois par an) la tolérance de l'établissement à l'égard des cyberrisques ? À la fois pour garantir son adéquation avec la politique de risque globale, et compte tenu des objectifs stratégiques et financiers de l'établissement ?

5 ☐

Le conseil d'administration approuve-t-il régulièrement les stratégies de gestion des cyberrisques et s'assure-t-il qu'elles sont respectées ?

6 ☐

Si les cyberrisques ne sont pas considérés comme des risques inhérents importants, il convient de vérifier que l'explication fournie est satisfaisante et claire.

7 ☐

Évaluer la formation en cybersécurité suivie par les employés, y compris les séances officielles et non officielles concernant leurs capacités et leurs responsabilités lorsqu'il s'agit de réduire les cyberrisques.

8 ☐

S'assurer que la formation en cybersécurité est adaptée aux différents rôles occupés au sein de l'établissement, y compris pour les cadres supérieurs, les employés disposant d'un accès privilégié aux données, les intervenants externes et les prestataires.

9 ☐

S’assurer que le comité de direction reçoit des comptes rendus détaillés sur les cyberrisques, notamment la fréquence des signalements et les informations relatives à l’évolution des cyberrisques, à l’efficacité des contrôles clés et aux incidents majeurs internes et externes.

10 ☐

Évaluer les résultats des procédures d’audit et de contrôle effectuées par l’équipe d’audit interne et/ou d’autres autorités de contrôle (p. ex., le contrôle indépendant des risques) concernant la cybersécurité, et examiner les procès-verbaux des séances des comités/fonctions correspondant(e)s.

11 ☐

Les tâches, compétences et responsabilités spécifiques liées aux cyber risques sont-elles clairement définies pour chaque rôle au sein de l’établissement, par exemple en ce qui concerne la description des rôles, l’organisation, la délimitation des fonctions, la structure hiérarchique et les canaux de communication.

12 ☐

Les cyberrisques sont-ils pris en compte de manière adéquate dans le cadre des audits effectués par les autorités de contrôle indépendant des risques et d’audit interne ? Il convient en particulier de tenir compte des points suivants : l’analyse et l’évaluation des risques, la planification pluriannuelle et l’application des normes internationales.

13 ☐

Vérifier que le concept de cyber risque défini par l’établissement est conforme aux normes ou pratiques reconnues au niveau international, et qu’il est suffisamment explicite pour répondre aux besoins et aux risques encourus par l’assujetti.

14 ☐

Vérifier que les interfaces avec les tiers et les actifs TIC sont identifiés, répertoriés et évalués.

15 ☐

Existe-t-il une définition des données critiques et ces dernières sont-elles répertoriées ?

16 ☐

Vérifier que les actifs TIC sont représentés de manière adéquate dans l’infrastructure réseau, en fonction de leur importance et du degré de protection qu’ils requièrent.

17

Existe-t-il des procédures, des processus et des contrôles adéquats visant à détecter les cyber menaces potentielles types auxquelles est exposé l'établissement ? Permettent-ils d'évaluer les conséquences d'une cyberattaque, par exemple un vol de données critiques, sur la communication avec des tiers et les actifs TIC ?

18

Dans quelle mesure les évaluations de risques permettent-elles d'identifier les menaces potentielles, les vulnérabilités et les répercussions des cyberattaques, telles que le vol de données critiques, sur la communication avec des tiers et l'accès aux TIC, et en tiennent-elles dûment compte ?

19

Les TIC sont-elles accompagnées de procédures, de processus et de contrôles adéquats dans les situations où il est nécessaire d'accorder des droits d'accès aux actifs TIC répertoriés et aux interfaces avec des tiers ?

20

Existe-t-il des procédures, des processus et des contrôles adéquats pour vérifier régulièrement à nouveau l'accès aux actifs TIC répertoriés et aux interfaces avec des tiers ?

21

Évaluer les procédures, processus et contrôles relatifs à la gestion et au monitorage des accès aux actifs TIC répertoriés et aux interfaces avec des tiers.

22

Existe-t-il des mesures organisationnelles et techniques adéquates pour prévenir le vol de données critiques ?

23

Les procédures, les processus et les contrôles relatifs à la gestion de la sécurité des réseaux sont-ils adéquats ? Par exemple : le zoning, le contrôle des accès au réseau, un pare-feu, un pare-feu d'applications Web, une protection contre les attaques DDoS et des serveurs proxy.

24

Vérifier l'efficacité des procédures, des processus et des contrôles relatifs à la gestion de la sécurité de l'infrastructure, comme la technologie de détection et de réponse sur les points de terminaison et les logiciels antivirus.

25

Les procédures, processus et contrôles garantissent-ils une configuration standard et un renforcement des systèmes des actifs TIC ? Garantissent-ils également une conformité continue après leur configuration ?

26

Évaluer l'approche axée sur les risques destinée à réparer rapidement les failles de sécurité (application de correctifs) et à corriger les erreurs de configuration (changement de configuration) dans les systèmes, les applications et l'infrastructure sous-jacente.

27

En ce qui concerne les systèmes, les applications et l'infrastructure sous-jacente, les failles de sécurité sont-elles réparées rapidement (application de correctifs) ? De même, les erreurs de configuration sont-elles également traitées en temps voulu ?

28

Vérifier l'efficacité des dispositions visant à protéger la confidentialité, l'intégrité et la disponibilité des données critiques stockées et transférées.

29

Les irrégularités et les événements de sécurité sont-ils identifiés rapidement grâce à un monitorage continu des TIC, et les conséquences potentielles de ces événements sont-elles évaluées de manière adéquate ?

30

Les valeurs par défaut définies pour les opérations réseau autorisées et les flux de données attendus pour les utilisateurs et les systèmes (par exemple les flux de données entre différentes zones de réseau et les interfaces entre les systèmes TIC) sont-elles définies techniquement à travers un SIEM (Security and Information and Event Management) ? Évaluer le processus de mise à jour de ces valeurs.

31

Les actifs TIC critiques répertoriés et l'utilisation qu'en font les employés et les tierces parties sont-ils systématiquement et continuellement surveillés ?

32

Vérifier l'efficacité des mesures techniques utilisées pour identifier les cyber incidents à l'aide de scénarios de cyberrisques, également connus sous le nom de « cas d'utilisation ».

33

Vérifier que les procédures et les directives de détection des cyber incidents sont régulièrement mises à jour et testées.

34

Vérifier l'efficacité du plan de réponse mis en place pour gérer les incidents cybernétiques identifiés, et en particulier la façon dont il est coordonné entre les intervenants internes et externes. Évaluer le soutien nécessaire de la part d'organismes externes en cas d'incident.

35

Les signalements provenant des systèmes de détection, également appelés « événements », sont-ils analysés, consignés et classés en temps opportun ?

36

Les mesures et les processus appropriés (tels que des playbooks) ont-ils été mis en place pour contenir et atténuer les cyberattaques ?

37

Vérifier que les exigences énoncées dans le document « 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 réponse.

38

Les processus de réponse et de récupération sont-ils évalués et améliorés régulièrement et efficacement ?

39

Vérifier qu'un processus adéquat est en place pour rétablir rapidement les systèmes après une cyberattaque.

40

L'établissement effectue-t-il une évaluation régulière et suffisante des vulnérabilités, des tests d'intrusion et des exercices cybernétiques de simulation basés sur les menaces potentielles types auxquelles il est exposé ?

41 ☐

S’assurer que des analyses de vulnérabilité et des tests d’intrusion sont régulièrement effectués sur tous les actifs TIC accessibles par Internet. Ces analyses et ces tests sont-ils bien effectués sur les systèmes nécessaires à l’exécution de processus critiques et ceux qui contiennent des données critiques ?

42 ☐

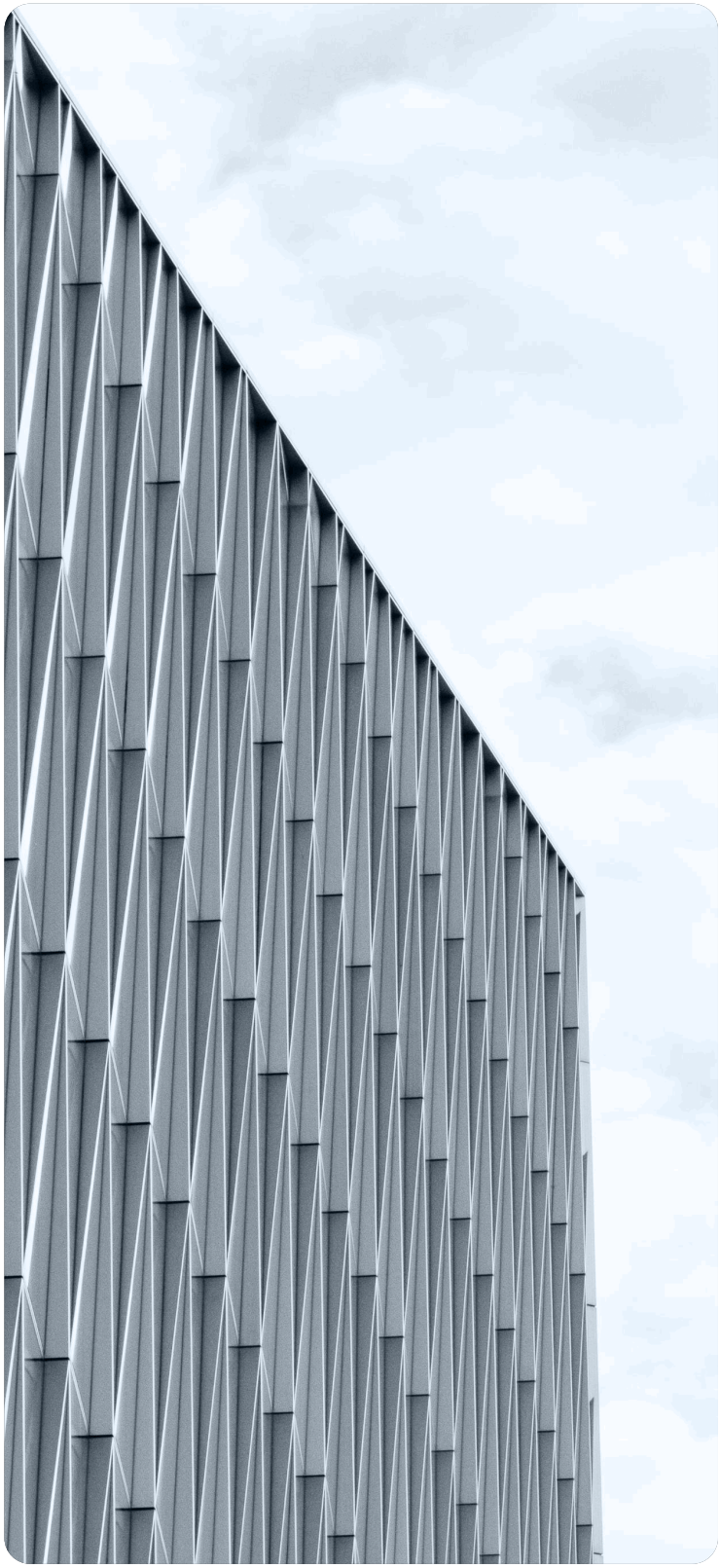
Une fois identifiés, les risques et les failles sont-ils traités et éliminés de façon appropriée ?

43 ☐

Les ressources techniques et humaines sont-elles suffisantes pour la mise en place, le déploiement et l’exécution d’une approche fondée sur les risques lorsqu’il s’agit d’effectuer des analyses de vulnérabilité, des tests d’intrusion et des exercices cybernétiques de simulation ?

44 ☐

Vérifier que les résultats des exercices cybernétiques sont consignés et communiqués de manière appropriée.



Points d’audit de la FINMA dans le cadre de la gestion des cyberrisques

La prochaine étape

En exécutant des analyses de vulnérabilité et des tests d'intrusion, votre entreprise sera en mesure d'identifier et d'atténuer les risques de sécurité de manière proactive avant même qu'ils ne puissent être exploités par des agresseurs.

- Travaillez en collaboration avec des professionnels réputés pour effectuer des analyses et des tests réguliers afin d'identifier les failles potentielles de vos systèmes et de vos réseaux.

- Utilisez les résultats obtenus pour évaluer l'efficacité de vos contrôles existants. Élaborez et mettez en œuvre un plan de remédiation pour corriger les vulnérabilités et les failles identifiées.

- Élaborez et mettez en œuvre un plan de remédiation pour corriger les vulnérabilités et les failles identifiées.

> **Les cyberattaques représentent un danger bien réel pour les entreprises de toutes tailles, et ce danger ne fait qu'augmenter.**
>
> **Afin de garantir votre sécurité et votre conformité, il est important de suivre les conseils de la FINMA à la lettre.**