Autorité
des marchés
financiers

16 avril 2025

Guide d'application et de mise en œuvre

Règlement sur la gestion et le signalement des incidents de sécurité de l’information de certaines institutions financières et des agents d’évaluation du crédit

Table des matières

1. Introduction

L'encadrement de la gestion des incidents de sécurité de l'information (Incidents) par l'Autorité des marchés financiers (AMF) découle de l'obligation légale s'appliquant aux institutions financières (IF)[1] et aux agents d'évaluation du crédit (AEC) de suivre des pratiques de gestion saine et prudente[2].

Établi sur la base de cette obligation, le *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit*[3] (Règlement) définit ce qu'est un Incident. Il énonce également les obligations des organisations visées par le Règlement en matière de signalement d'Incidents à l'AMF. La définition d'Incident est la base des obligations prévues au Règlement.

Un Incident se définit comme étant « une atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent »[4].

L'AMF a établi des lignes directrices pour informer les IF et les AEC des mesures qui, de son avis, peuvent être prises pour satisfaire aux obligations qui leur incombent en fonction des lois qui leur sont applicables. Ainsi, l'encadrement de la gestion d'un Incident se compose d'obligations réglementaires et d'attentes formulées dans les différentes lignes directrices.

Pour un rappel des attentes de l'AMF en matière de gestion d'Incidents, consultez les lignes directrices suivantes :

Pour les fondements :

- *Ligne directrice sur la gouvernance*;
- *Ligne directrice sur la gestion intégrée des risques*;
- *Ligne directrice sur la conformité*.

Pour les attentes plus spécifiques :

- *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*;
- *Ligne directrice sur la gestion du risque opérationnel*;
- *Ligne directrice sur la gestion de la continuité des activités*;
- *Ligne directrice applicable aux agents d'évaluation du crédit*.

2. Objectif du guide

L'AMF a élaboré ce guide afin d'accompagner les organisations visées par le Règlement dans sa mise en œuvre et son application. Il apporte entre autres des précisions sur la politique de gestion des Incidents à élaborer, incluant les éléments à y intégrer, les procédures et mécanismes à mettre en place permettant de détecter, d'évaluer et de

---

1 Article 485 de la *Loi sur les assureurs*, RLRQ, c. A-32.1, article 601.1 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, paragraphe u de l'article 43 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, article 277 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02.

2 Articles 47 et 66 de la *Loi sur les agents d'évaluation du crédit*, RLRQ, c.A-8. Dans le cas des agents d'évaluation du crédit, il est question de l'obligation de suivre des pratiques de gestion appropriées assurant le respect des droits conférés par la loi.

3 A.M. 2024-13, 2024, G.O. II, 6381, *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit*

4 Article 2 du Règlement.

répondre aux Incidents, le contenu du registre des Incidents ainsi que le processus de signalement des Incidents à l'AMF.

À noter que le guide évoluera en continu en fonction des bonnes pratiques du domaine, de l'expérience acquise et des besoins des parties prenantes.

3. Organisations visées par le Règlement

Les organisations visées par le Règlement sont les assureurs autorisés, les fédérations de sociétés mutuelles, les fédérations de caisses ainsi que les caisses qui ne sont pas membres d'une fédération[5], les institutions de dépôts autorisées, les sociétés de fiducie autorisées et les agents d'évaluation du crédit désignés par l'AMF (collectivement désignées par le terme « Organisations »).

À noter qu'une fédération de caisses est responsable du respect des obligations prévues au Règlement, notamment l'obligation d'établir et de mettre en œuvre une politique de gestion des Incidents à l'égard des caisses qui en sont membres et d'aviser l'AMF en cas d'Incident.

Dans le cas de sociétés mutuelles, chacune d'entre elles est responsable d'établir et de mettre en place une politique de gestion des Incidents et de signaler ceux-ci à l'AMF. Une fédération de sociétés mutuelles est également tenue de respecter les obligations réglementaires au même titre que les sociétés mutuelles.

4. Politique de gestion des Incidents

Le Règlement prévoit l'obligation pour les Organisations d'établir et de mettre en œuvre une politique de gestion des Incidents. Ainsi, à l'instar des autres types de politiques, celle sur la gestion des incidents peut prendre différentes formes, c'est-à-dire qu'elle peut être spécifique ou faire partie intégrante d'une autre politique, telle qu'une politique sur la sécurité de l'information.

La politique devrait être constituée de tous les attributs propres à celle-ci et contenir notamment une description claire des rôles et responsabilités. À cet effet, les bonnes pratiques prévoient qu'une politique devrait être élaborée et révisée périodiquement par la haute direction et être approuvée par le conseil d'administration.

La politique de gestion et de signalement des incidents doit minimalement mentionner les documents officiels décrivant les procédures et les mécanismes de l'Organisation qui lui permettent de détecter, d'évaluer et de répondre aux Incidents. Si les pratiques de détection, d'évaluation et de réponse aux incidents se basent sur des standards, des normes ou autres documents techniques de sources reconnues, ces derniers devraient être mentionnés à la politique.

Le Règlement étant construit sur la base de principes, les Organisations ont la flexibilité de déterminer le contenu de leur politique ainsi que son opérationnalisation.

---

[5] *Loi sur les coopératives de services financiers*, RLRQ, c. 67.2

5. Procédures et mécanismes permettant de détecter, d'évaluer et de répondre aux Incidents

L'AMF encourage les Organisations à s'inspirer des publications d'organismes nationaux et internationaux, comme l'Organisation internationale de normalisation (ISO)[6], l'Information Systems Audit and Control Association (ISACA), le National Institute of Standards and Technology (NIST) ou encore le Control Objectives for Information and Related Technology (COBIT) pour développer leurs mécanismes et procédures. Ces organismes recommandent la mise en place de plusieurs bonnes pratiques qui contribuent à une saine gestion des Incidents.

Afin de s'assurer que la détection, l'évaluation et la réponse aux Incidents sont faites de manière cohérente et objective, les organismes nommés précédemment ont identifié de bonnes pratiques qui pourraient être mises en place par les Organisations. En voici des exemples :

- Catégoriser les Incidents en fonction de critères comme le type d'événement et les causes.
- Classifier les Incidents afin de définir le traitement et le niveau d'escalade requis.
- Utiliser des cotes prédéfinies aux fins d'établissement de la sévérité d'un Incident et de sa classification.
- S'assurer que l'ensemble des processus, procédures et mécanismes mis en place s'insèrent dans un processus global de gestion des Incidents.
- Établir des standards de documentation des Incidents afin de s'assurer d'une évaluation uniforme de ceux-ci.
- Mettre en place des mesures de contrôle et de supervision afin de s'assurer de gérer les Incidents de manière à atteindre les objectifs suivants :
    - Minimiser les préjudices subis;
    - Diminuer le risque de récurrence de l'Incident;
    - Signaler leur survenance.
- Mettre à jour et tester annuellement l'ensemble des mécanismes de détection et de réponse aux Incidents.
- Effectuer la collecte en continu d'informations dans les journaux des systèmes d'information afin d'enregistrer les activités des utilisateurs, les exceptions, les défaillances des systèmes et autres événements liés à la sécurité de l'information.
- Vérifier et tenir à jour les journaux des systèmes d'information.
- Obtenir des informations sur les vulnérabilités techniques des systèmes d'information en temps opportun.

L'exposition de l'Organisation à ces vulnérabilités devrait être évaluée et les mesures appropriées devraient être prises pour traiter tous risques associés.

- Demander aux employés et aux tierces parties qui utilisent les systèmes d'information et les services de technologies de l'information et des communications de l'Organisation de signaler toute faiblesse observée ou suspectée en matière de sécurité de l'information dans les systèmes ou services.
- Obtenir l'assurance raisonnable, avant d'entrer en relation d'affaires avec un tiers, que ce dernier a des procédures et des contrôles en place pour assurer une saine gestion de ses Incidents.

[6] Voir notamment la norme ISO 27035

6. Signalement des Incidents

Signalement aux dirigeants et gestionnaires

L'Organisation doit prévoir à sa politique des critères de signalement (escalade) internes aux différents paliers hiérarchiques, incluant les dirigeants ou les gestionnaires[7].

L'Organisation doit aussi prévoir un signalement à l'AMF de même qu'à toute partie prenante, comme les clients, les tiers, les consommateurs et les autres organismes de réglementation, et ce, en fonction des différentes obligations qui lui sont applicables.

Le délai pour effectuer le signalement et la méthode de signalement devraient être mentionnés à la politique. Dans l'établissement des différents signalements, l'Organisation doit aussi prendre en considération l'Incident qui survient chez un tiers à qui elle a confié l'exercice de toute partie d'une activité, dans la mesure où l'Incident affecte l'activité qui lui a été confiée.

Dans l'établissement des critères de signalement des Incidents, les bonnes pratiques recommandent de prendre en considération :

- la catégorisation;
- la sévérité;
- la classification.

La **catégorisation** permet de regrouper les Incidents dans le but d'en faciliter la gestion. Elle se base sur la nature de l'Incident, notamment :

- le type d'Incident, c'est-à-dire l'événement (vol de données, panne, etc.); ou
- les causes de l'Incident (cyberattaque, erreur humaine, etc.).

La **sévérité** d'un Incident indique l'importance et l'urgence que l'Organisation accorde à la maîtrise et la clôture (résolution) de l'Incident. Les critères utilisés pour déterminer la sévérité devraient notamment tenir compte :

- du temps prévu pour que les opérations reviennent en mode normal;
- de l'impact sur les clients;
- de l'ampleur des impacts confirmés ou prévus de l'Incident sur les opérations de l'Organisation, comme les impacts financiers, de réputation ou réglementaires;

L'ampleur des impacts peut être évaluée en tenant compte notamment des données suivantes : les renseignements personnels, les actifs informationnels ou encore les utilisateurs affectés par l'Incident.

- du moment de la survenance de l'Incident et du délai estimé pour sa clôture (résolution).

[7] L'utilisation des termes « dirigeants » et « gestionnaires » est basée sur la terminologie des lois sur lesquelles le Règlement s'appuie. Ainsi, dans le cas d'une caisse ou d'une fédération de caisses, il est question de « gestionnaires », tandis que pour les autres Organisations, le terme « dirigeants » est utilisé. Dans les deux cas, le terme fait référence à la haute direction de l'Organisation.

La **classification** vise à qualifier l'Incident afin de confirmer son statut et d'en prioriser la gestion. Elle doit prendre en considération l'ensemble des informations obtenues, dont :

- la catégorisation (type, cause);
- la sévérité;
- la gravité des impacts pour l'Organisation, les clients et le système financier;
- tout autre élément pertinent.

Personne responsable de la gestion des Incidents

L'Organisation doit prévoir à sa politique la nomination d'une personne responsable de surveiller la gestion et le signalement des Incidents. Cette personne devrait voir à l'établissement et à la mise en œuvre de la politique dans l'Organisation.

Une case pour désigner la personne responsable de la gestion des Incidents est prévue dans les services en ligne de l'AMF.

La déclaration des Incidents à l'AMF relève du responsable de la gestion et du signalement des Incidents, mais ce dernier peut la déléguer à un autre intervenant.

En cas de doute quant à l'importance relative d'un événement ou d'un Incident, l'Organisation peut consulter son responsable des relations avec les institutions ou encore communiquer directement avec l'AMF.

7. Registre des Incidents

Chaque Organisation doit tenir et mettre à jour un registre des Incidents. Les renseignements consignés au registre doivent être conservés d'une manière sécurisée et confidentielle, pendant une période de cinq ans à compter de la date du rapport de fin d'Incident.

Tous les renseignements relatifs au cycle de vie de la gestion des Incidents devraient être consignés au registre. Ceux-ci doivent être aussi complets que possible et permettre de soutenir les évaluations, les décisions et les mesures à prendre. Le registre devrait permettre de reproduire historiquement et fidèlement l'ensemble des renseignements recueillis et des interventions effectuées tout au long du cycle de vie de la gestion d'un Incident.

En plus d'être utilisés aux fins d'analyse, les renseignements consignés au registre peuvent permettre de faire ressortir des tendances en matière d'Incidents et ainsi contribuer à une saine gestion de l'ensemble des risques d'une organisation.

Les renseignements mentionnés ci-dessous doivent être minimalement consignés au registre.

Renseignements à consigner au registre	Précisions	Case correspondante du formulaire Web, lorsqu'applicable
Date et heure de l'Incident	Vise **la détection et l'occurrence** de l'Incident. La détection est le moment où l'Incident a été rapporté pour la première fois dans l'Organisation, tandis que l'occurrence est le moment où l'Incident s'est produit (s'il est connu).	**Moment où l'Incident a été rapporté** Page 3, question 7 **Moment où l'Incident s'est produit** Page 3, question 8
Localisation de l'Incident	Fait référence à l'origine de l'Incident, c'est-à-dire interne (employé) ou externe (consultant, tierce partie ou organisation malveillante reconnue) Dans le cas où l'origine est externe, le pays devrait être précisé.	Page 3, question 12
Nature de l'Incident	La nature peut être déterminée par le type d'Incident (vol de données) ou encore la ou les causes de l'Incident (cyberattaque).	**Type principal de l'Incident** Page 3, question 5 **Cause(s) de l'Incident** Page 5, question 5
Description détaillée de l'Incident	La description devrait être exhaustive et, entre autres, comprendre les renseignements suivants : • la catégorisation; • la côte de sévérité; • la classification aux fins de traitement et de signalement; • les vulnérabilités identifiées; • les impacts en termes de disponibilité, d'intégrité et de confidentialité; • la nature des données affectée. Les informations suivantes peuvent également être intégrées : • l'appréciation quant à la récurrence potentielle d'un Incident de même nature; • les mesures prises pour la résolution des vulnérabilités identifiées; • les conclusions lors de la clôture de l'Incident.	Page 3, question 4

Renseignements à consigner au registre	Précisions	Case correspondante du formulaire Web, lorsqu'applicable
Préjudices engendrés par l'Incident	Les critères pour établir les préjudices devraient notamment prendre en compte les services et les ressources affectées de même qu'une évaluation des impacts de l'Incident[8].	
Tiers concernés par l'Incident	Tout tiers impliqué dans l'Incident. Inclut les destinataires du signalement d'un Incident conformément à ce qui est prévu à la politique de l'Organisation.  **Une bonne pratique est d'identifier le type de client touché par l'Incident et de donner une estimation de la volumétrie.**	**Intervenants internes ou externes liés** Page 3, question 12 **Clientèle affectée** Page 4, question 3 **Organisation(s) financière(s) ou non-financière(s) informée(s)** Page 3, question 15
Actions prises	Les actions prises comprennent : • les stratégies, procédures ou mesures d'atténuation mises en place afin de contrôler l'Incident et prévenir sa récurrence; • les communications envoyées conformément à la politique de l'Organisation; • la date et l'heure du ou des signalements.	**Parties prenantes informées** Page 3, questions 13 à 15 **Actions prises** Page 5, questions 1 à 5
Appréciation de l'Organisation quant à la récurrence potentielle de l'Incident	Évaluation de la probabilité que l'Incident se produise à nouveau. Cette évaluation peut être revue à la lumière de nouveaux renseignements sur l'Incident. Une bonne pratique est de documenter l'évolution de cette appréciation par l'Organisation.	Page 6, question 2
Actions prévues	Il peut s'agir des mesures prises pour réduire la probabilité que de nouveaux Incidents de même nature se produisent à nouveau (si ces moyens ne sont pas encore mis en place).	Page 6, question 1

[8] Pour obtenir plus d'informations sur l'évaluation des impacts d'un Incident, consulter les pages 59 et suivantes du *Format for Incident Reporting Exchange (FIRE) :* Final report 15 April 2025 du Financial Stability Board .

Renseignements à consigner au registre	Précisions	Case correspondante du formulaire Web, lorsqu'applicable
Date de la maîtrise de l'Incident	Date à laquelle l'Organisation a maîtrisé l'Incident et que les activités ont pu reprendre leur cours normal. À noter que dans le cas d'un Incident impliquant des renseignements personnels, les activités ne sont pas toujours perturbées. Dans ce cas, on considère que l'Incident est maîtrisé lorsque la pratique ou le processus à l'origine de l'Incident a cessé ou a été corrigé.	Page 3, question 9
Date de clôture de l'Incident	Date à laquelle l'Incident est clos, c'est-à-dire que tous les plans d'action ont été réalisés.	Page 3, question 9

En plus des renseignements énoncés ci-dessus, le registre devrait contenir tous les renseignements sur l'Incident permettant à l'Organisation de faire un signalement complet à l'AMF.

8. Processus de signalement à l'Autorité des marchés financiers

Suivant ses critères de signalement internes aux différents paliers hiérarchiques, l'Organisation doit aviser l'AMF lorsqu'un Incident est signalé à ses dirigeants ou à ses gestionnaires. L'Organisation doit signaler les Incidents à l'AMF, par l'entremise des services en ligne, au plus tard 24 heures après que le dirigeant, ou selon le cas, le gestionnaire a été avisé de la situation.

L'Organisation doit communiquer à l'AMF, au meilleur de sa connaissance, tout renseignement spécifié au formulaire de signalement jusqu'à ce l'Incident signalé soit maîtrisé et que le rapport de fin d'Incident ait été transmis.

Un Incident maîtrisé signifie généralement que les affaires ont repris leur cours normal sans nécessairement que la gestion de l'Incident soit totalement terminée.

Suivant le signalement initial à l'AMF d'un Incident, l'Organisation doit transmettre dans les services en ligne toute correction ou tout élément nouveau concernant l'Incident. Les signalements subséquents à l'AMF, pour chaque Incident, doivent être faits dans un délai n'excédant pas trois jours calendaires, et ce, même si aucun développement n'est apparu ou aucune information additionnelle n'a été découverte.

Tout au long du traitement d'un Incident et des signalements par l'entremise des services en ligne, l'AMF pourrait exiger des clarifications sur les renseignements rapportés. À ce titre, il sera possible pour les Organisations de joindre des documents complémentaires en annexe au formulaire de signalement de l'AMF.

L'ensemble des renseignements découlant du rapport doit être transmis à partir des champs prévus à cet effet dans le formulaire. Les renseignements ainsi qu'un rapport confirmant la maîtrise de l'Incident et la reprise normale des activités doivent être transmis dans un délai n'excédant pas 30 jours suivants la maîtrise de l'Incident. Il est aussi possible de transmettre dans les services en ligne, à la section « Documents supplémentaires », un rapport s'il contient des informations supplémentaires pertinentes qui n'ont pas déjà été communiquées.

9. Assistance

Pour obtenir de l'assistance dans l'utilisation des services en ligne, les Organisations peuvent également trouver de l'information à la page Comment s'inscrire aux services en ligne - Représentants et futurs professionnels | AMF ou communiquer avec l'AMF au 1 877 525-0337.

En cas de doute au sujet de l'importance relative d'un Incident à signaler, les Organisations peuvent consulter la personne responsable de leur dossier à l'AMF ou encore communiquer avec l'AMF.