5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Projet de règlement

Loi sur les agents d'évaluation du crédit
(chapitre A-8.2, a. 66 et 73)

Loi sur les assureurs
(chapitre A-32.1, a. 485 et 496)

Loi sur les coopératives de services financiers
(chapitre C-67.3, a. 601.1 et 601.9)

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2, a. 43 par. u) et 45.9)

Loi sur les sociétés de fiducie et les sociétés d'épargne
(chapitre S-29.02, a. 277 et 286)

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

Avis est donné par l'Autorité des marchés financiers (l'« Autorité ») que, conformément à l'article 67 de la *Loi sur les agents d'évaluation du crédit*, chapitre A-8.2 (la « LAEC »), à l'article 486 de la *Loi sur les assureurs*, RLRQ, c. A-32.1 (la « LA »), à l'article 601.2 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 (la « LCSF »), à l'article 45 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2 (la « LIDPD ») et à l'article 278 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 (la « LSFSE »), le règlement suivant (le « Projet de règlement »), dont le texte est publié ci-dessous, pourra être pris par l'Autorité et ensuite soumis au ministre des Finances du Québec pour approbation, avec ou sans modification, à l'expiration d'un délai de 75 jours à compter de sa publication au Bulletin de l'Autorité :

- *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*

Le Projet de règlement est également accessible sur la page d'accueil du site Web de l'Autorité au **www.lautorite.qc.ca** à la section « Consultations publiques ».

Contexte

Le Projet de règlement s'inscrit dans la mission de l'Autorité de veiller notamment à ce que les institutions financières disposent de pratiques de gestion saine et prudente lesquelles contribuent notamment à leur résilience. Le Projet de règlement s'inscrit également dans la mission de l'Autorité à l'égard des agents d'évaluation du crédit (« AEC ») en regard de sa charge de surveiller et contrôler leurs pratiques de gestion. Développer et maintenir de saines pratiques de gestion permet aux institutions financières et aux AEC de prévenir et de gérer les incidents pouvant leur porter préjudices, nuire à leur réputation et dans le cas des institutions financières, mettre en péril leur solvabilité.

Objectif du Projet de règlement

Le Projet de règlement s'applique aux institutions financières ainsi qu'aux AEC suivants :

Institutions financières

- Un assureur autorisé en vertu de la LA et une fédération de sociétés mutuelles visée par la LA;
- Une fédération et une caisse qui n'est pas membre d'une fédération visées à la LCSF;
- Une institution de dépôts autorisée en vertu de la LIDPD;
- Une société de fiducie autorisée en vertu de la LSFSE.

Agents d'évaluation du crédit

- Les AEC désignés par l'Autorité en vertu de la LAEC.

1. Application

Le Projet de règlement propose un encadrement pour la gestion et le signalement des incidents de sécurité de l'information (« Incident(s) »), pouvant survenir chez une institution financière, un AEC ou chez un tiers à qui est confié l'exercice de toute partie d'une activité.

Il est proposé qu'en présence d'une fédération et des caisses qui en sont membres, les obligations proposées au Projet de règlement soient applicables à la fédération. Cette dernière aurait notamment la responsabilité de voir à l'élaboration et à la mise en place d'une politique de signalement des Incidents auprès de ses gestionnaires et de l'Autorité incluant les Incidents pouvant survenir auprès d'une caisse membre.

Il est également proposé que le Projet de règlement soit applicable à une fédération de sociétés mutuelles ainsi qu'à chacune des sociétés qui en sont membre.

2. Politique de gestion des incidents de sécurité de l'information

Le Projet de règlement propose entre autres l'obligation pour un AEC ou une institution financière d'établir et de mettre en œuvre une politique de gestion des Incidents. La politique devrait notamment prévoir des procédures et des mécanismes permettant de détecter, d'évaluer et de répondre à un Incident. Également, elle devrait prévoir une procédure de signalement d'un Incident aux dirigeants[1] de l'institution financière ou de l'AEC, de même qu'à toute partie prenante.

3. Signalement à l'Autorité des marchés financiers

L'institution financière ou l'AEC serait tenu de signaler à l'Autorité, l'Incident signalé à ses dirigeants ou, selon le cas, à ses gestionnaires, ayant un risque d'occasionner des répercussions négatives, au plus tard 24 heures suivant l'Incident.

De même, tout incident faisant l'objet d'un signalement à un autre organisme de réglementation, à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, contractuellement, est chargé de dédommager le préjudice qui aurait pu être causé par cet incident devrait être signalé à l'Autorité dans ce même délai. Par exemple, un incident

[1] Dans le cas d'une fédération, le signalement d'un Incident devra plutôt être fait aux gestionnaires au sens de la LCSF.

signalé au Bureau du Surintendant des institutions financières (« BSIF »), aux corps policiers ou à un assureur couvrant le cyberrisque, devrait également être signalé à l'Autorité.

Enfin, tout incident de confidentialité pour lequel un avis a été transmis à la Commission d'accès à l'information devra être signalé au même moment à l'Autorité.

4. Registre des incidents de sécurité de l'information

L'institution financière ou l'AEC aurait à tenir à jour un registre des Incidents comprenant notamment, pour chaque Incident, la description de celui-ci, le préjudice engendré, les tiers concernés, l'acception des risques résiduels et les justificatifs afférents, les actions prises ou prévues et la date de sa clôture. Les renseignements qui y sont consignés devraient être conservés de manière sécurisée et confidentielle, afin d'en maintenir l'intégrité pour une période minimale de 7 ans.

5. Sanctions administratives pécuniaires

Finalement, le Projet de règlement prévoit des sanctions administratives pécuniaires que l'Autorité pourrait imposer à l'institution financière ou à l'AEC qui ne respecte pas les dispositions du Projet de règlement. L'imposition d'une sanction suivra les dispositions législatives applicables à l'institution financière ou l'AEC fautif. Un avis de non-conformité devrait être transmis avant l'imposition d'une sanction.

Les obligations prévues au Projet de règlement s'ajoutent aux attentes énoncées aux lignes directrices de l'Autorité destinées aux institutions financières et des AEC relativement à leurs obligations de suivre des pratiques de gestion. Il ne les remplace pas.

Commentaires

Toute personne intéressée à formuler des commentaires au sujet de ce Projet de règlement est priée de les faire parvenir par écrit au plus tard le **20 février 2024** en s'adressant à :

Me Philippe Lebel
Secrétaire et directeur général du secrétariat et des affaires juridiques
Autorité des marchés financiers
Place de la cité, tour Cominar
2640, boulevard Laurier, 3ième étage
Québec (Québec) G1V 5C1
Télécopieur : 418 525-9512
Courrier électronique : consultation-en-cours@lautorite.qc.ca

À défaut d'avis contraire à cet effet, tous les commentaires seront affichés sur le site Web de l'Autorité, au www.lautorite.qc.ca. Par conséquent, nous invitons les intervenants à ne pas inclure de renseignements personnels directement dans les commentaires à publier et à préciser en quel nom ils présentent leur mémoire.

Renseignements additionnels

Des précisions ou des renseignements additionnels peuvent être obtenus en s'adressant à

Isabelle Déry
Analyste expert en normalisation des institutions financières
Direction de l'encadrement prudentiel et des simulations
Autorité des marchés financiers
Téléphone : (418) 525-0337, poste 4176
Numéro sans frais : 1 877 525-0337
Isabelle.dery@lautorite.qc.ca

Luc Verreault
Analyste expert en normalisation des institutions financières
Direction de l'encadrement prudentiel et des simulations
Autorité des marchés financiers
Téléphone : (514) 395-0337, poste 4644
Numéro sans frais : 1 877 525-0337
Luc.verreault@lautorite.qc.ca

Le 7 décembre 2023

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

Loi sur les agents d'évaluation du crédit
(chapitre A-8.2, a. 66 et 73)

Loi sur les assureurs
(chapitre A-32.1, a. 485 et 496)

Loi sur les coopératives de services financiers
(chapitre C-67.3, a. 601.1 et 601.9)

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2, a. 43, par. u) et a. 45.9)

Loi sur les sociétés de fiducie et les sociétés d'épargne
(chapitre S-29.02, a. 277 et 286)

CHAPITRE I
CHAMP D'APPLICATION ET INTERPRÉTATION

1. Le présent règlement s'applique aux institutions financières suivantes :

1° un assureur autorisé en vertu de la Loi sur les assureurs (chapitre A-32.1) et une fédération de sociétés mutuelles visée par cette loi;

2° une fédération et une caisse qui n'est pas membre d'une fédération, visées par la Loi sur les coopératives de services financiers (chapitre C-67.3);

3° une institution de dépôts autorisée en vertu de la Loi sur les institutions de dépôts et la protection des dépôts (chapitre I-13.2.2);

4° une société de fiducie autorisée en vertu de la Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02).

Il s'applique également à un agent d'évaluation du crédit désigné en vertu de la Loi sur les agents d'évaluation du crédit (chapitre A-8.2).

2. Pour l'application du présent règlement, on entend par « incident de sécurité de l'information » une atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent.

CHAPITRE II
GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

SECTION I
POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

3. Une institution financière ou un agent d'évaluation du crédit doit établir et mettre en œuvre une politique de gestion des incidents de sécurité de l'information qui comporte, notamment, des procédures et des mécanismes permettant de détecter et d'évaluer les incidents de sécurité de l'information ainsi que d'y répondre, lorsque ces incidents surviennent au sein de l'institution, d'une caisse membre d'une fédération, de l'agent ou d'un tiers à qui cette institution, cette caisse ou cet agent a confié l'exercice de toute partie d'une activité.

La politique de gestion des incidents de sécurité de l'information comporte également une procédure de signalement des incidents de sécurité de l'information aux dirigeants ou, selon le cas, au gestionnaire de l'institution financière ou de l'agent d'évaluation du crédit, y compris une procédure de signalement à ceux-ci lorsque cet incident survient au sein d'une caisse membre d'une fédération ou d'un tiers visé au premier alinéa.

En outre, la politique doit prévoir une procédure de signalement à toute autre partie prenante, notamment aux clients, aux tiers à qui cette institution ou cet agent a confié l'exercice de toute partie d'une activité, aux consommateurs, à l'Autorité des marchés financiers de même qu'aux autres organismes de réglementation.

4. Une institution financière ou un agent d'évaluation du crédit doit désigner, par écrit, un de ses dirigeants ou, dans le cas d'une coopérative de services financiers, un de ses gestionnaires, responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information.

SECTION III
SIGNALEMENT À L'AUTORITÉ DES MARCHÉS FINANCIERS

5. Une institution financière ou un agent d'évaluation du crédit doit signaler à l'Autorité tout incident de sécurité de l'information ayant un risque d'occasionner des répercussions négatives qui a été signalé à ses dirigeants ou, selon le cas, à ses gestionnaires au plus tard 24 heures suivant cet incident.

L'institution financière ou l'agent d'évaluation du crédit doit aussi signaler à l'Autorité, dans ce même délai, tout incident de sécurité de l'information qui a été signalé à un organisme de réglementation, à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, ou, contractuellement, est chargé de dédommager le préjudice qui aurait pu être causé par cet incident.

6. Une institution financière ou un agent d'évaluation du crédit doit, lorsqu'il avise la Commission d'accès à l'information, instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), d'un incident de confidentialité visé au deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), le signaler au même moment à l'Autorité.

7. Une institution financière ou un agent d'évaluation du crédit signale à l'Autorité un incident de sécurité de l'information en remplissant le formulaire disponible sur le site Web de l'Autorité.

8. Une institution financière ou un agent d'évaluation du crédit doit aviser l'Autorité de l'évolution de la situation au plus tard 3 jours suivant l'avis visé à l'article 5 et au plus tard tous les 3 jours suivant l'avis précédent jusqu'à la clôture de l'‘incident.

9. Dans les 3 jours suivants la clôture de l'incident, une institution financière ou un agent d'évaluation du crédit transmet à l'Autorité un avis confirmant que l'incident est maîtrisé et que les activités ont repris leur cours normal.

10. Une institution financière ou un agent d'évaluation du crédit transmet à l'Autorité un rapport dans un délai de 30 jours suivant la clôture de l'incident de sécurité de l'information. Le rapport contient, notamment, les éléments suivants :

1° l'identification de la source et du type d'incident;

2° l'appréciation de l'institution financière ou de l'agent d'évaluation du crédit quant à la récurrence potentielle de l'incident;

3° les moyens pris pour réduire la probabilité que de nouveaux incidents de même nature ne se produisent.

SECTION IV
REGISTRE DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

11. Une institution financière ou un agent d'évaluation du crédit doit tenir à jour un registre des incidents de sécurité de l'information qui comprend, pour chaque incident :

1° la date et l'heure de celui-ci;

2° sa localisation;

3° sa nature;

4° une description détaillée de celui-ci, incluant les renseignements contenus au paragraphe 2° de l'article 10;

5° les préjudices engendrés par celui-ci;

6° les tiers concernés par l'incident;

7° les actions prises;

8° l'acceptation ou non du risque résiduel et les justificatifs afférents;

9° les actions prévues;

10° la date de sa clôture.

12. Une institution financière ou un agent d'évaluation du crédit doit conserver les renseignements consignés au registre de manière sécurisée et confidentielle, afin d'en maintenir l'intégrité pour une période minimale de 7 ans à compter de la date du rapport visé à l'article 10.

CHAPITRE III
SANCTIONS ADMINISTRATIVES PÉCUNIAIRES

13. Une sanction administrative pécuniaire d'un montant de 250 $ dans le cas d'une personne physique ou de 1 000 $ dans les autres cas peut être imposée à une institution financière ou à un agent d'évaluation du crédit visé à l'article 1 :

1° qui, en contravention à l'article 4, n'a pas désigné, par écrit, un de ses dirigeants ou, selon le cas, un de ses gestionnaires, responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information;

2° qui, en contravention de l'article 5, ne signale pas à l'Autorité un incident au plus tard 24 heures suivant cet incident;

3° qui, en contravention à l'article 6, ne transmet pas à l'Autorité le signalement prévu à cet article au moment où un avis est transmis à la Commission d'accès à l'information;

4° qui, en contravention à l'article 8, n'avise pas l'Autorité de l'évolution de la situation, au plus tard 3 jours suivant l'avis visé à l'article 7 et au plus tard tous les 3 jours suivant l'avis précédent, jusqu'à la clôture de l'incident;

5° qui, en contravention à l'article 9, ne transmet pas à l'Autorité un avis conforme à cet article, dans les 3 jours suivant la clôture d'un incident de sécurité de l'information.

14. Une sanction administrative pécuniaire d'un montant de 500 $ dans le cas d'une personne physique ou de 2 500 $ dans les autres cas peut être imposée à une institution financière ou à un agent d'évaluation du crédit l'entité visée à l'article 1 :

1° qui, en contravention à l'article 3, n'établit pas ou ne met pas en œuvre une politique de gestion des incidents de sécurité de l'information;

2° qui, en contravention à l'article 11, ne tient pas à jour un registre des incidents de sécurité de l'information;

3° qui, en contravention à l'article 12, ne conserve pas les renseignements au registre des incidents de sécurité de l'information pour une période minimale de 7 ans à compter de la date du rapport visé à l'article 10.

CHAPITRE IV
DISPOSITION FINALE

15. Le présent règlement entre en vigueur le (*indiquer ici la date d'entrée en vigueur du présent règlement*).

Draft Regulation

Credit Assessment Agents Act
(chapter A-8.2, ss. 66 and 73)

Insurers Act
(chapter A-32.1, ss. 485 and 496)

Act respecting financial services cooperatives
(chapter C-67.3, ss. 601.1 and 601.9)

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2, s. 43, par. *u*, and s. 45.9)

Trust Companies and Savings Companies Act
(chapter S-29.02, ss. 277 and 286)

Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents

Notice is hereby given by the Autorité des marchés financiers (the "Authority") that, in accordance with section 67 of the Credit Assessment Agents Act, CQLR, c. A-8.2 (the "CAAA"), section 486 of the Insurers Act, CQLR, c. A-32.1, section 601.2 of the Act respecting financial services cooperatives, CQLR, c. C-67.3 (the "AFSC"), section 45 of the Deposit Institutions and Deposit Protection Act, CQLR, c. I-13.2.2 (the "DIDPA"), and section 278 of the Trust Companies and Savings Companies Act, CQLR, c. S-29.02 (the "TCSCA"), the following regulation (the "Draft Regulation"), the text of which is published hereunder, may be made by the Authority and subsequently submitted to the Québec Minister of Finance for approval, with or without amendment, after 75 days have elapsed since its publication in the Bulletin of the Authority:

- *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents*

The Draft Regulation is also available under "Public consultations" on the Authority's website at **www.lautorite.qc.ca**.

Background

The Draft Regulation fits within the Authority's mission to ensure that financial institutions have sound and prudent management practices that support their resilience. The Draft Regulation also fits within the Authority's mission in relation to credit assessment agents ("CAAs") and its mandate to supervise and control their management practices. Developing and maintaining sound management practices helps financial institutions and CAAs prevent and manage incidents that could cause them injury, harm their reputation or, in the case of financial institutions, jeopardize their solvency.

Purpose of the Draft Regulation

The Draft Regulation applies to the following financial institutions and CAAs:

Financial institutions

- Insurers authorized under the Insurers Act and federations of mutual companies governed by the Insurers Act;
- Federations and credit unions not members of a federation that are subject to the AFSC;
- Deposit institutions authorized under the DIDPA;
- Trust companies authorized under the TCSCA.

Credit assessment agents

- CAAs designated by the Authority under the CAAA.

1. Application

The Draft Regulation proposes a framework for the management and reporting of information security incidents ("incident(s)") that may occur within a financial institution, a CAA or a third party entrusted with the performance of any part of an activity.

It is proposed that, where there is a federation and its member credit unions, the proposed obligations in the Draft Regulation would apply to the federation. The federation would be responsible for, among other things, developing and implementing a policy for the reporting of incidents to its managers and the Authority, including incidents that may occur within a member credit union.

It is also proposed that the Draft Regulation would apply to a federation of mutual companies and to each company that is a member of the federation.

2. Information security incident management policy

The Draft Regulation proposes requiring, among other things, that CAAs and financial institutions develop and implement an incident management policy. The policy would have to include procedures and mechanisms for detecting, assessing and responding to incidents. It would also have to include a procedure for the reporting of incidents to the officers[1] of the financial institution or the CAA and to any stakeholders.

3. Reporting to the Autorité des marchés financiers

Any incident with potentially adverse impacts that a CAA or a financial institution reports to its officers or, as the case may be, to its managers would have to be reported to the Authority no later than 24 hours after it occurs.

Also, the Authority must be notified, within that same period, of any incident that is reported to another regulatory authority, a person or a body responsible under law for the prevention, detection or repression of crime or statutory offences or contractually responsible for providing compensation for injury that may have been caused by the incident. Accordingly, any incident reported to the Office of the Superintendent of Financial Institutions ("OSFI"), the police or an insurer covering cyber risk would have to be reported to the Authority.

Any confidentiality incident for which notification is sent to the Commission d'accès à l'information must be reported to the Authority at the same time.

4. Information security incident register

The financial institution or the CAA would be required to maintain a current incident register that includes, for each incident, a description of the incident, any injury caused by it, the third parties involved in it, acceptance of the residual risk, actions taken, planned actions and the incident close date. The information recorded in the incident register would have to be kept in a secure and confidential manner so as to maintain the integrity of the information for a minimum period of seven years.

[1] In the case of a federation, the incident would have to be reported to the managers within the meaning of the AFSC.

5. Monetary administrative penalties

Lastly, the Draft Regulation sets out monetary administrative penalties that the Authority may impose on a financial institution or a CAA that contravenes the provisions of the Draft Regulation. Penalties will be imposed according to the statutory provisions applicable to the contravening financial institution or CAA. A notice of non-compliance would have to be sent before a penalty is imposed.

The obligations set out in the Draft Regulation adds to the Authority's guideline expectations for financial institutions and CAAs relating to their obligation to adhere to management practices but does not replace them.

Comments

Comments regarding this Draft Regulation may be made in writing before **February 20, 2024** to:

Me Philippe Lebel
Corporate Secretary and Executive Director, Legal Affairs
Autorité des marchés financiers
Place de la cité, tour Cominar
2640, boulevard Laurier, 3ème étage
Québec (Québec) G1V 5C1
Fax: 418-525-9512
E-mail: consultation-en-cours@lautorite.qc.ca

Unless otherwise noted, comments will be posted on the Authority's website at www.lautorite.qc.ca. Please do not include personal information directly in comments to be published and state on whose behalf you are making the submission.

Additional Information

Additional information may be obtained from:

Isabelle Déry
Financial Institution Standardization Analyst
Prudential Policy and Simulations
Autorité des marchés financiers
Telephone: 418-525-0337, ext. 4176
Toll-free: 1-877-525-0337
Isabelle.dery@lautorite.qc.ca

Luc Verreault
Financial Institution Standardization Analyst
Prudential Policy and Simulations
Autorité des marchés financiers
Telephone: 514-395-0337, ext. 4644
Toll-free: 1-877-525-0337
Luc.verreault@lautorite.qc.ca

December 7, 2023

REGULATION RESPECTING THE MANAGEMENT AND REPORTING OF INFORMATION SECURITY INCIDENTS BY CERTAIN FINANCIAL INSTITUTIONS AND BY CREDIT ASSESSMENT AGENTS

Credit Assessment Agents Act
(chapter A-8.2, ss. 66 and 73)

Insurers Act
(chapter A-32.1, ss. 485 and 496)

Act respecting financial services cooperatives
(chapter C-67.3, ss. 601.1 and 601.9)

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2, s. 43, par. *u* and s. 45.9)

Trust Companies and Savings Companies Act
(chapter S-29.02, ss. 277 and 286)

CHAPTER I
SCOPE AND INTERPRETATION

1. This Regulation applies to the following financial institutions:

(1) insurers authorized under the Insurers Act (chapter A-32.1) and federations of mutual companies that are subject thereto;

(2) federations and credit unions not members of a federation that are subject to the Act respecting financial services cooperatives (chapter C-67.3);

(3) deposit institutions authorized under the Deposit Institutions and Deposit Protection Act (chapter I-13.2.2); and

(4) trust companies authorized under the Trust Companies and Savings Companies Act (chapter S-29.02).

This Regulation also applies to credit assessment agents designated under the Credit Assessment Agents Act (chapter A-8.2).

2. For purposes of this Regulation, "information security incident" means an attack on the availability, integrity or confidentiality of information systems or the information they contain.

CHAPTER II
MANAGEMENT OF INFORMATION SECURITY INCIDENTS

DIVISION I
INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

3. A financial institution or a credit assessment agent must develop and implement an information security incident management policy that includes, without limitation, procedures and mechanisms for detecting, assessing and responding to information security incidents where such incidents occur within the institution, a credit union that is a member of a federation, the agent or a third party to which the institution, the credit union or the agent has entrusted the performance of any part of an activity.

The information security incident management policy must also contain a procedure for the reporting of information security incidents to the officers or, as the case may be, to the managers of the financial institution or the credit assessment agent, including a procedure

for the reporting of such incidents thereto when they occur within a credit union that is a member of a federation or a third party contemplated in paragraph 1.

Furthermore, the policy must include a procedure for the reporting of incidents to any other stakeholders, including clients, third parties to which the institution or agent has entrusted the performance of any part of an activity, consumers, the Autorité des marchés financiers and any other regulatory bodies.

4. A financial institution or a credit assessment must assign, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, in the case of a financial services cooperative, to one of its managers.

DIVISION II
REPORTING TO THE AUTORITÉ DES MARCHÉS FINANCIERS

5. A financial institution or a credit assessment agent must, if an incident with potentially adverse impacts is reported to its officers or, as the case may be, to its managers, report the incident to the Authority no later than 24 hours after the incident.

The financial institution or the credit assessment agent must, within that same period, also report to the Authority any information security incident that has been reported to a regulatory body, a person or a body responsible under law for the prevention, detection or repression of crime or statutory offences or contractually responsible for providing compensation for injury that may have been caused by the incident.

6. When a financial institution or a credit assessment agent notifies the Commission d'accès à l'information, established under section 103 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1), of a confidentiality incident referred to in paragraph 2 of section 3.5 of the Act respecting the protection of personal information in the private sector (chapter P-39.1), it must report the incident to the Authority at the same time.

7. A financial institution or a credit assessment agent must report an information security incident to the Authority by completing the form available on the Authority's website.

8. A financial institution or a credit assessment agent must notify the Authority of developments in the situation no later than three days following the notice referred to in section 5 and no later than every three days thereafter, until the close of the incident.

9. Within three days from the close of the incident, a financial institution or a credit assessment agent must send to the Authority a notice confirming that the incident is under control and that operations have returned to normal.

10. A financial institution or a credit assessment agent must send the Authority a report within 30 days from the close of the information security incident. The report must, among other things:

(1) identify the source and type of the incident;

(2) provide an assessment by the financial institution or the credit assessment agent regarding a potential recurrence of the incident; and

(3) describe the actions taken to reduce the possibility of new incidents of the same nature occurring.

DIVISION III
INFORMATION SECURITY INCIDENT REGISTER

11. A financial institution or a credit assessment agent must maintain a current information security incident register that includes, for each incident:

(1) the date and time of the incident;

(2) the location of the incident;

(3) the nature of the incident;

(4) a detailed description of the incident, including the information specified in subparagraph 2 of section 10;

(5) any injury caused by the incident;

(6) the third parties involved in the incident;

(7) the actions taken;

(8) acceptance or non-acceptance of the residual risk and the reasons for such acceptance or non-acceptance;

(9) planned actions; and

(10) the incident close date.

12. A financial institution or a credit assessment agent must keep the information recorded in the register in a secure and confidential manner so as to maintain the information's integrity for a minimum period of seven years from the date of the report referred to in section 10.

CHAPTER III
MONETARY ADMINISTRATIVE PENALTIES

13. A monetary administrative penalty of $250, in the case of a natural person, and $1,000, in any other case, may be imposed on a financial institution or a credit assessment agent contemplated in section 1 that:

(1) in contravention of section 4, has not assigned, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, as the case may be, to one of its managers;

(2) in contravention of section 5, fails to report an incident to the Authority no later than 24 hours after the incident;

(3) in contravention of section 6, fails, when notifying the Commission d'accès à l'information of an incident, to report the incident to the Authority at the same time;

(4) in contravention of section 8, fails to notify the Authority of developments in the situation no later than three days following the notice referred to in section 7 and no later than every three days thereafter, until the close of the incident; or

(5) in contravention of section 9, fails to send to the Authority, within three days from the close of an information security incident, a notice consistent with this section;

14. A monetary administrative penalty of $500, in the case of a natural person, and $2,500, in any other case, may be imposed on a financial institution or a credit assessment agent referred to in section 1 that:

(1) in contravention of section 3, fails to develop or implement an information security incident management policy;

(2) in contravention of section 11, fails to maintain a current information security incident register; or

(3) in contravention of section 12, fails to keep the information in the information security incident register for a minimum period of seven years from the date of the report contemplated in section 10.

CHAPTER IV
FINAL PROVISION

15. This Regulation comes into force on (*indiquer ici la date d'entrée en vigueur du présent règlement*).

5.2.2 Publication

Aucune information.