5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Publication de projets de règlements à la Gazette officielle du Québec pour consultation – Règlements sur les renseignements relatifs à la surveillance pour différents secteurs[i]

Vous trouverez, ci-dessous, les projets de règlements suivants, en versions française et anglaise :

- *Règlement sur les renseignements relatifs à la surveillance des assureurs autorisés;*

- *Règlement sur les renseignements relatifs à la surveillance des institutions de dépôts autorisées*;

- *Règlement sur les renseignements relatifs à la surveillance des coopératives de services financiers*;

- *Règlement sur les renseignements relatifs à la surveillance des sociétés de fiducie autorisées*.

Ces projets de règlements ont été publié dans la Partie 2 de la *Gazette officielle du Québec* du 26 février 2020 (152e année, n° 9). Les règlements pourront être édicté par le ministre des Finances à l'expiration du délai de 45 jours à compter de leur publication dans la *Gazette officielle du Québec*.

Toute personne intéressée ayant des commentaires à formuler à ce sujet est priée de les faire parvenir par écrit à l'adresse mentionnée dans l'avis, avant l'expiration du délai de 45 jours à compter de la publication à la *Gazette officielle du Québec*.

Le 27 février 2020

---

[i] Diffusion autorisée par Les Publications du Québec

Projets de règlement

Projet de règlement

Loi sur les assureurs
(chapitre A-32.1)

Renseignements relatifs à la surveillance des assureurs autorisés

Avis est donné par les présentes, conformément aux articles 10 et 11 de la Loi sur les règlements (chapitre R-18.1), que le projet de Règlement sur les renseignements relatifs à la surveillance des assureurs autorisés, dont le texte apparaît ci-dessous, pourra être édicté par le ministre des Finances à l'expiration d'un délai de 45 jours à compter de la présente publication.

Ce projet de règlement vise à préciser, pour l'application des articles 178 et 179 de la Loi sur les assureurs (chapitre A-32.1), lesquels des renseignements détenus par un assureur autorisé relatifs à la surveillance exercée à son égard par l'Autorité des marchés financiers sont confidentiels.

Il vise également à prévoir à quelles conditions ces renseignements confidentiels peuvent être utilisés par l'assureur autorisé comme preuve dans le cadre d'une procédure intentée par lui, le ministre, l'Autorité ou le Procureur général.

Des renseignements additionnels concernant ce projet de règlement peuvent être obtenus en s'adressant à Monsieur Jean-Hubert Smith-Lacroix, coordonnateur à la Direction générale du droit corporatif et des politiques relatives au secteur financier, ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4, par téléphone au numéro (418) 646-7466, par télécopieur au numéro (418) 646-5744 ou par courrier électronique à l'adresse suivante : jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Toute personne intéressée ayant des commentaires à formuler au sujet de ce projet de règlement est priée de les faire parvenir par écrit avant l'expiration du délai de 45 jours mentionné ci-dessus au ministre des Finances, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Le ministre des Finances,
Eric Girard

Règlement sur les renseignements relatifs à la surveillance des assureurs autorisés

Loi sur les assureurs
(chapitre A-32.1, art. 178 et 179)

1. Pour l'application de l'article 178 de la Loi sur les assureurs, les renseignements détenus par un assureur autorisé relatifs à la surveillance exercée par l'Autorité à l'égard de cet assureur et qui sont confidentiels sont les suivants :

a) toute cote attribuée par l'Autorité des marchés financiers à l'assureur autorisé pour évaluer son profil de risque ainsi que toute autre cote d'évaluation de son profil de risque fondée en grande partie sur des renseignements obtenus de l'Autorité;

b) tout stade d'intervention attribué à l'assureur autorisé aux termes d'un cadre de surveillance des institutions financières de l'Autorité;

c) toute instruction écrite prise à l'égard de l'assureur autorisé;

d) tout rapport établi par l'Autorité ou à sa demande ou toute recommandation formulée par celle-ci dans le cadre de ses fonctions de surveillance, y compris la correspondance échangée à cet égard avec ses administrateurs ou ses dirigeants.

2. Pour l'application du paragraphe 2° de l'article 179 de la Loi sur les assureurs, l'assureur autorisé concerné par ces renseignements peut les utiliser comme preuve dans toute procédure concernant l'application de la Loi sur les assureurs ou la Loi sur les sociétés par actions (chapitre S-31.1) intentée par lui, par le ministre responsable de l'application de ces lois, par l'Autorité des marchés financiers ou par le procureur général du Québec, à condition que soit rendue une ordonnance interdisant ou restreignant la publication, la divulgation ou la diffusion d'un renseignement ou d'un document, ou une ordonnance de huis clos.

3. Le présent règlement entre en vigueur (*inscrire ici la date d'entrée en vigueur*).

71980

Draft Regulation

An Act respecting financial services cooperatives
(chapter C-67.3)

Supervisory information of financial services cooperatives

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of financial services cooperatives, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

The draft Regulation specifies, for the purposes of sections 564.1 and 564.2 of the Act respecting financial services cooperatives (chapter C-67.3), which information held by a financial services cooperative in relation to the supervision of the insurer by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the financial services cooperative as evidence in any proceedings brought by the financial services cooperative, the Minister, the Authority or the Attorney General.

Further information on the draft Regulation may be obtained by contacting Jean-Hubert Smith-Lacroix, coordinator, Direction générale du droit corporatif et des politiques relatives au secteur financier, Ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4; telephone: 418 646-7466; fax: 418 646-5744; email: jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Finance, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Eric Girard,
Minister of Finance

Regulation respecting the supervisory information of financial services cooperatives

An Act respecting financial services cooperatives
(chapter C-67.3, ss. 564.1 and 564.2)

1. For the purposes of section 564.1 of the Act respecting financial services cooperatives, the following information held by a financial services cooperative in relation to the supervision of the financial services cooperative by the Autorité des marchés financiers (the Authority) is confidential information:

(a) any risk profile assessment rating assigned to the financial services cooperative by the Authority and any other risk profile assessment rating based in large part on information obtained from the Authority;

(b) any intervention stage rating assigned to the financial services cooperative under a framework of the Authority for the supervision of financial institutions;

(c) any instruction in writing with regard to the financial services cooperative;

(d) any report drafted by or at the request of the Authority, or any recommendation made by the Authority as part of its supervisory functions, including any correspondence exchanged in that regard with its directors or officers.

2. For the purposes of paragraph 2 of section 564.2 of the Act respecting financial services cooperatives, the financial services cooperative concerned by the information may use that information as evidence in any proceedings concerning the administration or enforcement of the Act respecting financial services cooperatives that are brought by the financial services cooperative, the Minister responsible for the administration of that Act, the Autorité des marchés financiers or the Attorney General of Québec, providing an order is made to prohibit or restrict the publication, disclosure or dissemination of the information or document, or an order is made for a hearing in camera.

3. This Regulation comes into force on (*insert the date of coming into force*).

104265

Draft Regulation

Insurers Act
(chapter A-32.1)

Supervisory information of authorized insurers

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of authorized insurers, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

The draft Regulation specifies, for the purposes of sections 178 and 179 of the Insurers Act (chapter A-32.1), which information held by an authorized insurer in relation to the supervision of the authorized insurer by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the authorized insurer as evidence in any proceedings brought by the authorized insurer, the Minister, the Authority or the Attorney General.

Further information on the draft Regulation may be obtained by contacting Jean-Hubert Smith-Lacroix, coordinator, Direction générale du droit corporatif et des politiques relatives au secteur financier, Ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4; telephone: 418 646-7466; fax: 418 646-5744; email: jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Finance, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Eric Girard,
Minister of Finance

Regulation respecting the supervisory information of authorized insurers

Insurers Act
(chapter A-32.1, ss. 178 and 179)

1. For the purposes of section 178 of the Insurers Act, the following information held by an authorized insurer in relation to the supervision of the authorized insurer by the Autorité des marchés financiers (the Authority) is confidential information:

(a) any risk profile assessment rating assigned to the authorized insurer by the Authority and any other risk profile assessment rating based in large part on information obtained from the Authority;

(b) any intervention stage rating assigned to the authorized insurer under a framework of the Authority for the supervision of financial institutions;

(c) any instruction in writing with regard to the authorized insurer;

(d) any report drafted by or at the request of the Authority, or any recommendation made by the Authority as part of its supervisory functions, including any correspondence exchanged in that regard with its directors or officers.

2. For the purposes of paragraph 2 of section 179 of the Insurers Act, the authorized insurer concerned by the information may use that information as evidence in any proceedings concerning the administration or enforcement of the Insurers Act or the Business Corporations Act (chapter S-31.1) that are brought by the authorized insurer, the Minister responsible for the carrying out or administration of those Acts, the Autorité des marchés financiers or the Attorney General of Québec, providing an order is made to prohibit or restrict the publication, disclosure or dissemination of the information or document, or an order is made for a hearing in camera.

3. This Regulation comes into force on (*insert the date of coming into force*).

104264

Draft Regulation

Trust Companies and Savings Companies Act
(chapter S-29.02)

Supervisory information of authorized trust companies

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of authorized trust companies, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

The draft Regulation specifies, for the purposes of sections 156 and 157 of the Trust Companies and Savings Companies Act (chapter S-29.02), which information held by an authorized trust company in relation to the supervision of the authorized trust company by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the authorized trust company as evidence in any proceedings brought by the authorized trust company, the Minister, the Authority or the Attorney General.

Projet de règlement

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2)

Renseignements relatifs à la surveillance des institutions de dépôts autorisées

Avis est donné par les présentes, conformément aux articles 10 et 11 de la Loi sur les règlements (chapitre R-18.1), que le projet de Règlement sur les renseignements relatifs à la surveillance des institutions de dépôts autorisées, dont le texte apparaît ci-dessous, pourra être édicté par le ministre des Finances à l'expiration d'un délai de 45 jours à compter de la présente publication.

Ce projet de règlement vise à préciser, pour l'application des articles 32.11 et 32.12 de la Loi sur les institutions de dépôts et la protection des dépôts (chapitre I-13.2.2), lesquels des renseignements détenus par une institution de dépôts autorisée relatifs à la surveillance exercée à son égard par l'Autorité des marchés financiers sont confidentiels.

Il vise également à prévoir à quelles conditions ces renseignements confidentiels peuvent être utilisés par l'institution de dépôts autorisée comme preuve dans le cadre d'une procédure intentée par elle, le ministre, l'Autorité ou le Procureur général.

Des renseignements additionnels concernant ce projet de règlement peuvent être obtenus en s'adressant à Monsieur Jean-Hubert Smith-Lacroix, coordonnateur à la Direction générale du droit corporatif et des politiques relatives au secteur financier, ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4, par téléphone au numéro (418) 646-7466, par télécopieur au numéro (418) 646-5744 ou par courrier électronique à l'adresse suivante : jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Toute personne intéressée ayant des commentaires à formuler au sujet de ce projet de règlement est priée de les faire parvenir par écrit avant l'expiration du délai de 45 jours mentionné ci-dessus au ministre des Finances, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Le ministre des Finances,
Eric Girard

Règlement sur les renseignements relatifs à la surveillance des institutions de dépôts autorisées

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2, art. 32.11 et 32.12)

1. Pour l'application de l'article 32.11 de la Loi sur les institutions de dépôts et la protection des dépôts, les renseignements détenus par une institution de dépôts autorisée relatifs à la surveillance exercée par l'Autorité à l'égard de cette institution et qui sont confidentiels sont les suivants :

a) toute cote attribuée par l'Autorité des marchés financiers à l'institution de dépôts autorisée pour évaluer son profil de risque ainsi que toute autre cote d'évaluation de son profil de risque fondée en grande partie sur des renseignements obtenus de l'Autorité;

b) tout stade d'intervention attribué à l'institution de dépôts autorisée aux termes d'un cadre de surveillance des institutions financières de l'Autorité;

c) toute instruction écrite prise à l'égard de l'institution de dépôts autorisée;

d) tout rapport établi par l'Autorité ou à sa demande ou toute recommandation formulée par celle-ci dans le cadre de ses fonctions de surveillance, y compris la correspondance échangée à cet égard avec ses administrateurs ou ses dirigeants.

2. Pour l'application du paragraphe 2° de l'article 32.12 de la Loi sur les institutions de dépôts et la protection des dépôts, l'institution de dépôts autorisée concernée par ces renseignements peut les utiliser comme preuve dans toute procédure concernant l'application de la Loi sur les institutions de dépôts et la protection des dépôts ou, dans le cas d'une société d'épargne du Québec, de la Loi sur les sociétés par action (chapitre S-31.1) intentée par elle, par le ministre responsable de l'application de ces lois, par l'Autorité des marchés financiers ou par le procureur général du Québec, à condition que soit rendue une ordonnance interdisant ou restreignant la publication, la divulgation ou la diffusion d'un renseignement ou d'un document, ou une ordonnance de huis clos.

3. Le présent règlement entre en vigueur (*inscrire ici la date d'entrée en vigueur*).

71982

Draft Regulations

Draft Regulation

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2)

Supervisory information of authorized deposit institutions

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of authorized deposit institutions, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

The draft Regulation specifies, for the purposes of sections 32.11 and 32.12 of the Deposit Institutions and Deposit Protection Act (chapter I-13.2.2), which information held by an authorized deposit institution in relation to the supervision of the authorized deposit institution by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the authorized deposit institution as evidence in any proceedings brought by the authorized deposit institution, the Minister, the Authority or the Attorney General.

Further information on the draft Regulation may be obtained by contacting Jean-Hubert Smith-Lacroix, coordinator, Direction générale du droit corporatif et des politiques relatives au secteur financier, Ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4; telephone: 418 646-7466; fax: 418 646-5744; email: jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Finance, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Eric Girard,
Minister of Finance

Regulation respecting the supervisory information of authorized deposit institutions

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2, ss. 32.11 and 32.12)

1. For the purposes of section 32.11 of the Deposit Institutions and Deposit Protection Act, the following information held by an authorized deposit institution in relation to the supervision of the authorized deposit institution by the Autorité des marchés financiers (the Authority) is confidential information:

(a) any risk profile assessment rating assigned to the authorized deposit institution by the Authority and any other risk profile assessment rating based in large part on information obtained from the Authority;

(b) any intervention stage rating assigned to the authorized deposit institution under a framework of the Authority for the supervision of financial institutions;

(c) any instruction in writing with regard to the authorized deposit institution;

(d) any report drafted by or at the request of the Authority, or any recommendation made by the Authority as part of its supervisory functions, including any correspondence exchanged in that regard with its directors or officers.

2. For the purposes of paragraph 2 of section 32.12 of the Deposit Institutions and Deposit Protection Act, the authorized deposit institution concerned by the information may use that information as evidence in any proceedings concerning the administration or enforcement of the Deposit Institutions and Deposit Protection Act or, in the case of a Québec savings company, the Business Corporations Act (chapter S-31.1) that are brought by the authorized deposit institution or Québec savings company, the Minister responsible for the carrying out or administration of those Acts, the Autorité des marchés financiers or the Attorney General of Québec, providing an order is made to prohibit or restrict the publication, disclosure or dissemination of the information or document, or an order is made for a hearing in camera.

3. This Regulation comes into force on (*insert the date of coming into force*).

104266

Projet de règlement

Loi sur les coopératives de services financiers
(chapitre C-67.3)

Renseignements relatifs à la surveillance des coopératives de services financiers

Avis est donné par les présentes, conformément aux articles 10 et 11 de la Loi sur les règlements (chapitre R-18.1), que le projet de Règlement sur les renseignements relatifs à la surveillance des coopératives de services financiers, dont le texte apparaît ci-dessous, pourra être édicté par le ministre des Finances à l'expiration d'un délai de 45 jours à compter de la présente publication.

Ce projet de règlement vise à préciser, pour l'application des articles 564.1 et 564.2 de la Loi sur les coopératives de services financiers (chapitre C-67.3), lesquels des renseignements détenus par une coopérative de services financiers relatifs à la surveillance exercée à son égard par l'Autorité des marchés financiers sont confidentiels.

Il vise également à prévoir à quelles conditions ces renseignements confidentiels peuvent être utilisés par la coopérative de services financiers comme preuve dans le cadre d'une procédure intentée par elle, le ministre, l'Autorité ou le Procureur général.

Des renseignements additionnels concernant ce projet de règlement peuvent être obtenus en s'adressant à Monsieur Jean-Hubert Smith-Lacroix, coordonnateur à la Direction générale du droit corporatif et des politiques relatives au secteur financier, ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4, par téléphone au numéro (418) 646-7466, par télécopieur au numéro (418) 646-5744 ou par courrier électronique à l'adresse suivante : jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Toute personne intéressée ayant des commentaires à formuler au sujet de ce projet de règlement est priée de les faire parvenir par écrit avant l'expiration du délai de 45 jours mentionné ci-dessus au ministre des Finances, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Le ministre des Finances,
Eric Girard

Règlement sur les renseignements relatifs à la surveillance des coopératives de services financiers

Loi sur les coopératives de services financiers
(chapitre C-67.3, art. 564.1 et 564.2)

1. Pour l'application de l'article 564.1 de la Loi sur les coopératives de services financiers, les renseignements détenus par une coopérative de services financiers relatifs à la surveillance exercée par l'Autorité à l'égard de cette coopérative et qui sont confidentiels sont les suivants :

a) toute cote attribuée par l'Autorité des marchés financiers à la coopérative de services financiers pour évaluer son profil de risque ainsi que toute autre cote d'évaluation de son profil de risque fondée en grande partie sur des renseignements obtenus de l'Autorité;

b) tout stade d'intervention attribué à la coopérative de services financiers aux termes d'un cadre de surveillance des institutions financières de l'Autorité;

c) toute instruction écrite prise à l'égard de la coopérative de services financiers;

d) tout rapport établi par l'Autorité ou à sa demande ou toute recommandation formulée par celle-ci dans le cadre de ses fonctions de surveillance, y compris la correspondance échangée à cet égard avec ses administrateurs ou ses dirigeants.

2. Pour l'application du paragraphe 2° de l'article 564.2 de la Loi sur les coopératives de services financiers, la coopérative de services financiers concernée par ces renseignements peut les utiliser comme preuve dans toute procédure concernant l'application de la Loi sur les coopératives de services financiers intentée par elle, par le ministre responsable de l'application de cette loi, par l'Autorité des marchés financiers ou par le procureur général du Québec, à condition que soit rendue une ordonnance interdisant ou restreignant la publication, la divulgation ou la diffusion d'un renseignement ou d'un document, ou une ordonnance de huis clos.

3. Le présent règlement entre en vigueur (*inscrire ici la date d'entrée en vigueur*).

71981

Draft Regulation

An Act respecting financial services cooperatives
(chapter C-67.3)

Supervisory information of financial services cooperatives

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of financial services cooperatives, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

The draft Regulation specifies, for the purposes of sections 564.1 and 564.2 of the Act respecting financial services cooperatives (chapter C-67.3), which information held by a financial services cooperative in relation to the supervision of the insurer by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the financial services cooperative as evidence in any proceedings brought by the financial services cooperative, the Minister, the Authority or the Attorney General.

Further information on the draft Regulation may be obtained by contacting Jean-Hubert Smith-Lacroix, coordinator, Direction générale du droit corporatif et des politiques relatives au secteur financier, Ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4; telephone: 418 646-7466; fax: 418 646-5744; email: jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Finance, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Eric Girard,
Minister of Finance

Regulation respecting the supervisory information of financial services cooperatives

An Act respecting financial services cooperatives
(chapter C-67.3, ss. 564.1 and 564.2)

1. For the purposes of section 564.1 of the Act respecting financial services cooperatives, the following information held by a financial services cooperative in relation to the supervision of the financial services cooperative by the Autorité des marchés financiers (the Authority) is confidential information:

(a) any risk profile assessment rating assigned to the financial services cooperative by the Authority and any other risk profile assessment rating based in large part on information obtained from the Authority;

(b) any intervention stage rating assigned to the financial services cooperative under a framework of the Authority for the supervision of financial institutions;

(c) any instruction in writing with regard to the financial services cooperative;

(d) any report drafted by or at the request of the Authority, or any recommendation made by the Authority as part of its supervisory functions, including any correspondence exchanged in that regard with its directors or officers.

2. For the purposes of paragraph 2 of section 564.2 of the Act respecting financial services cooperatives, the financial services cooperative concerned by the information may use that information as evidence in any proceedings concerning the administration or enforcement of the Act respecting financial services cooperatives that are brought by the financial services cooperative, the Minister responsible for the administration of that Act, the Autorité des marchés financiers or the Attorney General of Québec, providing an order is made to prohibit or restrict the publication, disclosure or dissemination of the information or document, or an order is made for a hearing in camera.

3. This Regulation comes into force on (*insert the date of coming into force*).

104265

Draft Regulation

Insurers Act
(chapter A-32.1)

Supervisory information of authorized insurers

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of authorized insurers, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

Projet de règlement

Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02)

Renseignements relatifs à la surveillance des sociétés de fiducie autorisées

Avis est donné par les présentes, conformément aux articles 10 et 11 de la Loi sur les règlements (chapitre R-18.1), que le projet de Règlement sur les renseignements relatifs à la surveillance des sociétés de fiducie autorisées, dont le texte apparaît ci-dessous, pourra être édicté par le ministre des Finances à l'expiration d'un délai de 45 jours à compter de la présente publication.

Ce projet de règlement vise à prévoir, pour l'application des articles 156 et 157 de la Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02), lesquels des renseignements détenus par une société de fiducie autorisée relatifs à la surveillance exercée à son égard par l'Autorité des marchés financiers sont confidentiels.

Il vise également à prévoir à quelles conditions ces renseignements confidentiels peuvent être utilisés par la société de fiducie autorisée comme preuve dans le cadre d'une procédure intentée par elle, le ministre, l'Autorité ou le Procureur général.

Des renseignements additionnels concernant ce projet de règlement peuvent être obtenus en s'adressant à Monsieur Jean-Hubert Smith-Lacroix, coordonnateur à la Direction générale du droit corporatif et des politiques relatives au secteur financier, ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4, par téléphone au numéro (418) 646-7466, par télécopieur au numéro (418) 646-5744 ou par courrier électronique à l'adresse suivante : jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Toute personne intéressée ayant des commentaires à formuler au sujet de ce projet de règlement est priée de les faire parvenir par écrit avant l'expiration du délai de 45 jours mentionné ci-dessus au ministre des Finances, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Le ministre des Finances,
Eric Girard

Règlement sur les renseignements relatifs à la surveillance des sociétés de fiducie autorisées

Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02, art. 156 et 157)

1. Pour l'application de l'article 156 de la Loi sur les sociétés de fiducie et les sociétés d'épargne, les renseignements détenus par une société de fiducie autorisée relatifs à la surveillance exercée par l'Autorité à l'égard de cette société de fiducie et qui sont confidentiels sont les suivants :

a) toute cote attribuée par l'Autorité des marchés financiers à la société de fiducie pour évaluer son profil de risque ainsi que toute autre cote d'évaluation de son profil de risque fondée en grande partie sur des renseignements obtenus de l'Autorité;

b) tout stade d'intervention attribué à la société de fiducie aux termes d'un cadre de surveillance des institutions financières de l'Autorité;

c) toute instruction écrite prise à l'égard de la société de fiducie;

d) tout rapport établi par l'Autorité ou à sa demande ou toute recommandation formulée par celle-ci dans le cadre de ses fonctions de surveillance, y compris la correspondance échangée à cet égard avec ses administrateurs ou ses dirigeants.

2. Pour l'application du paragraphe 2° de l'article 157 de la Loi sur les sociétés de fiducie et les sociétés d'épargne, la société de fiducie peut utiliser ces renseignements comme preuve dans toute procédure concernant l'application de la Loi sur les sociétés de fiducie et les sociétés d'épargne ou la Loi sur les sociétés par actions (chapitre S-31.1) intentée par elle, par le ministre responsable de l'application de ces lois, par l'Autorité des marchés financiers ou par le procureur général du Québec, à condition que soit rendue une ordonnance interdisant ou restreignant la publication, la divulgation ou la diffusion d'un renseignement ou d'un document, ou une ordonnance de huis clos.

3. Le présent règlement entre en vigueur (*inscrire ici la date d'entrée en vigueur*).

71983

The draft Regulation specifies, for the purposes of sections 178 and 179 of the Insurers Act (chapter A-32.1), which information held by an authorized insurer in relation to the supervision of the authorized insurer by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the authorized insurer as evidence in any proceedings brought by the authorized insurer, the Minister, the Authority or the Attorney General.

Further information on the draft Regulation may be obtained by contacting Jean-Hubert Smith-Lacroix, coordinator, Direction générale du droit corporatif et des politiques relatives au secteur financier, Ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4; telephone: 418 646-7466; fax: 418 646-5744; email: jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Finance, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Eric Girard,
Minister of Finance

Regulation respecting the supervisory information of authorized insurers

Insurers Act
(chapter A-32.1, ss. 178 and 179)

1. For the purposes of section 178 of the Insurers Act, the following information held by an authorized insurer in relation to the supervision of the authorized insurer by the Autorité des marchés financiers (the Authority) is confidential information:

(a) any risk profile assessment rating assigned to the authorized insurer by the Authority and any other risk profile assessment rating based in large part on information obtained from the Authority;

(b) any intervention stage rating assigned to the authorized insurer under a framework of the Authority for the supervision of financial institutions;

(c) any instruction in writing with regard to the authorized insurer;

(d) any report drafted by or at the request of the Authority, or any recommendation made by the Authority as part of its supervisory functions, including any correspondence exchanged in that regard with its directors or officers.

2. For the purposes of paragraph 2 of section 179 of the Insurers Act, the authorized insurer concerned by the information may use that information as evidence in any proceedings concerning the administration or enforcement of the Insurers Act or the Business Corporations Act (chapter S-31.1) that are brought by the authorized insurer, the Minister responsible for the carrying out or administration of those Acts, the Autorité des marchés financiers or the Attorney General of Québec, providing an order is made to prohibit or restrict the publication, disclosure or dissemination of the information or document, or an order is made for a hearing in camera.

3. This Regulation comes into force on (*insert the date of coming into force*).

104264

Draft Regulation

Trust Companies and Savings Companies Act
(chapter S-29.02)

Supervisory information of authorized trust companies

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the supervisory information of authorized trust companies, appearing below, may be made by the Minister of Finance on the expiry of 45 days following this publication.

The draft Regulation specifies, for the purposes of sections 156 and 157 of the Trust Companies and Savings Companies Act (chapter S-29.02), which information held by an authorized trust company in relation to the supervision of the authorized trust company by the Autorité des marchés financiers (the Authority) is confidential information.

It also prescribes the conditions on which such confidential information may be used by the authorized trust company as evidence in any proceedings brought by the authorized trust company, the Minister, the Authority or the Attorney General.

Further information on the draft Regulation may be obtained by contacting Jean-Hubert Smith-Lacroix, coordinator, Direction générale du droit corporatif et des politiques relatives au secteur financier, Ministère des Finances, 8, rue Cook, 4e étage, Québec (Québec) G1R 0A4; telephone: 418 646-7466; fax: 418 646-5744; email: jean-hubert.smith-lacroix@finances.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Finance, 390, boulevard Charest Est, 8e étage, Québec (Québec) G1K 3H4.

Eric Girard,
Minister of Finance

Regulation respecting the supervisory information of authorized trust companies

Trust Companies and Savings Companies Act
(chapter S-29.02, ss. 156 and 157)

1. For the purposes of section 156 of the Trust Companies and Savings Companies Act, the following information held by an authorized trust company in relation to the supervision of the authorized trust company by the Autorité des marchés financiers (the Authority) is confidential information:

(a) any risk profile assessment rating assigned to the authorized trust company by the Authority and any other risk profile assessment rating based in large part on information obtained from the Authority;

(b) any intervention stage rating assigned to the authorized trust company under a framework of the Authority for the supervision of financial institutions;

(c) any instruction in writing with regard to the authorized trust company;

(d) any report drafted by or at the request of the Authority, or any recommendation made by the Authority as part of its supervisory functions, including any correspondence exchanged in that regard with its directors or officers.

2. For the purposes of paragraph 2 of section 157 of the Trust Companies and Savings Companies Act, the authorized trust company concerned by the information may use that information as evidence in any proceedings concerning the administration or enforcement of the Trust Companies and Savings Companies Act or the Business Corporations Act (chapter S-31.1) that are brought by the authorized trust company, the Minister responsible for the carrying out or administration of those Acts, the Autorité des marchés financiers or the Attorney General of Québec, providing an order is made to prohibit or restrict the publication, disclosure or dissemination of the information or document, or an order is made for a hearing in camera.

3. This Regulation comes into force on (*insert the date of coming into force*).

104267

5.2.2 Publication

DÉCISION N° 2020-PDG-0006

Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications

Vu le pouvoir de l'Autorité des marchés financiers (l'« Autorité ») d'établir des lignes directrices destinées à tous les assureurs autorisés, à une catégorie seulement d'entre eux ou à une fédération dont de tels assureurs sont membres, conformément à l'article 463 de la *Loi sur les assureurs*, RLRQ, c. A-32.1 (la « LASS »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les coopératives de services financiers, à une catégorie seulement d'entre elles, à des caisses, à une fédération dont de telles caisses sont membres ou à toutes les personnes morales faisant partie d'un groupe coopératif, conformément à l'article 565.1 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 (la « LCSF »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les sociétés de fiducie autorisées ou à une catégorie d'entre elles seulement, conformément à l'article 254 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 (la « LSFSE »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les institutions de dépôts autorisées, à une catégorie d'entre elles seulement ou aux fédérations dont de telles institutions sont membres, conformément à l'article 42.2 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2 (la « LIDPD »);

Vu les pouvoirs de l'Autorité d'établir une ligne directrice prévus par les articles 463 de la LASS, 565.1 de la LCSF, 254 de la LSFSE et 42.2 de la LIDPD, qui appartiennent exclusivement à son président-directeur général, conformément à l'article 24 de la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1;

Vu la publication pour consultation au Bulletin de l'Autorité le 10 janvier 2019 [(2019) vol. 16, n° 1, B.A.M.F., section 5.2.1] du projet de *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications* (la « ligne directrice »);

Vu la publication pour une seconde consultation au Bulletin de l'Autorité le 28 novembre 2019 [(2019) vol. 16, n° 47, B.A.M.F., section 5.2.1] du projet de ligne directrice;

Vu les modifications apportées au projet de ligne directrice à la suite de chacune de ces consultations;

Vu le deuxième alinéa des articles 463 de la LASS, 254 de la LSFSE , 42.2 de la LIDPD et du troisième alinéa de l'article 565.1 de la LCSF, selon lequel l'Autorité publie à son Bulletin les lignes directrices qu'elle établit après en avoir transmis une copie au ministre des Finances (le « Ministre »);

Vu le projet de ligne directrice proposé par la Direction principale de l'encadrement des institutions financières, de la résolution et de l'assurance-dépôts et la recommandation du surintendant de l'encadrement de la solvabilité d'établir celle-ci;

En conséquence :

L'Autorité établit la *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, dont le texte est annexé à la présente décision, et en autorise la publication au Bulletin après en avoir transmis une copie au Ministre.

La *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications* prend effet le 27 février 2020.

Fait le 25 février 2020.

Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications
(Loi sur les assureurs, RLRQ, c. A-32.1, art. 463 et 464)
(Loi sur les coopératives de services financiers, RLRQ, c. C-67.3, art. 565.1 et 566)
(Loi sur les sociétés de fiducie et les sociétés d'épargne, RLRQ, c. S-29.02, art. 254 et 255)
(Loi sur les institutions de dépôts et la protection des dépôts, RLRQ, c. I-13.2.2, art. 42.2 et 42.3)

L'Autorité des marchés financiers publie, en versions française et anglaise, la ligne directrice suivante :

- *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*

Avis de publication

La ligne directrice s'applique aux assureurs autorisés, aux fédérations de sociétés mutuelles, aux coopératives de services financiers et personnes morales faisant partie d'un groupe coopératif, aux sociétés de fiducie autorisées, aux sociétés d'épargne et aux autres institutions de dépôts autorisées.

Elle a été établie par l'Autorité le 25 février 2020 et est effective à compter du **27 février 2020**. L'Autorité s'attend à ce que l'institution financière s'approprie les attentes de la présente ligne directrice et qu'elle les mette en œuvre d'ici le 27 février 2021.

Elle est publiée ci-après et est disponible sur le site Web de l'Autorité, à l'onglet « Professionnels » aux sections « Institutions de dépôt et sociétés de fiducie » et « Assureurs », sous l'onglet « Lignes directrices ».

Renseignements additionnels

Des renseignements additionnels peuvent être obtenus en s'adressant à :

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

Le 27 février 2020

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE SUR LA GESTION DES RISQUES LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS

Février 2020

TABLE DES MATIÈRES

Préambule

La présente ligne directrice est une indication des attentes de l'Autorité des marchés financiers (l'« Autorité ») à l'égard de l'obligation légale des institutions financières de suivre des pratiques de gestion saine et prudente. Elle porte donc sur l'interprétation, l'exécution et l'application de cette obligation imposée aux institutions financières.

Dans cette optique, l'Autorité privilégie une approche basée sur des principes plutôt que d'édicter des règles précises. Ainsi, du fondement même d'une ligne directrice, l'Autorité confère aux institutions financières la latitude nécessaire leur permettant de déterminer elles-mêmes les stratégies, politiques et procédures pour la mise en œuvre de ces principes de saine gestion et de voir à leur application en regard de la nature, de la taille, de la complexité de leurs activités et de leur profil de risque. À cet égard, la ligne directrice illustre des façons de se conformer aux principes énoncés.

Note de l'Autorité

L'Autorité considère la gouvernance, la gestion intégrée des risques et la conformité (GRC) comme les assises sur lesquelles doivent reposer la gestion saine et prudente et les saines pratiques commerciales d'une institution financière et conséquemment, les bases sur lesquelles l'encadrement prudentiel donné par l'Autorité s'appuie.

La présente ligne directrice s'inscrit dans cette perspective et énonce les attentes de l'Autorité à l'égard des pratiques en matière de gestion saine et prudente des risques liés aux technologies de l'information et des communications (« TIC »).

Champ d'application

La présente ligne directrice s'applique aux assureurs autorisés, à une fédération de sociétés mutuelles, aux coopératives de services financiers et personnes morales faisant partie d'un groupe coopératif, aux sociétés de fiducie autorisées, aux sociétés d'épargne et aux autres institutions de dépôts autorisées régis par les lois suivantes :

- *Loi sur les assureurs*, RLRQ, c. A-32.1[1];
- *Loi sur les coopératives de services financiers*, RLRQ, c. 67.3[2];
- *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02[3];
- *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2[4].

Aux seules fins de cette ligne directrice, les expressions « institution » ou « institution financière » sont utilisées indistinctement pour référer aux entités visées par celle-ci.

Enfin, cette ligne directrice s'applique tant à l'institution financière qui opère de façon autonome qu'à celle qui est membre d'un groupe financier.

Dans le cas des coopératives de services financiers et des sociétés mutuelles d'assurance membres d'une fédération, les normes ou politiques adoptées à leur intention par la fédération doivent être cohérentes, voire convergentes, avec les principes de gestion saine et prudente tel qu'il est précisé dans la présente ligne directrice.

1 Art. 463 et 464 de la Loi sur les assureurs.

2 Art. 565.1 et 566 de la Loi sur les coopératives de services financiers.

3 Art. 254 et 255 de la Loi sur les sociétés de fiducie et les sociétés d'épargne.

4 Art. 42.2 et 42.3 de la Loi sur les institutions de dépôts et protection des dépôts.

Prise d’effet et processus de mise à jour

La *Ligne directrice sur la gestion des risques liés aux technologies de l’information et des communications* est effective à compter du 27 février 2020.

En regard de l’obligation légale des institutions de suivre des pratiques de gestion saine et prudente, l’Autorité s’attend à ce que chaque institution se soit approprié les principes de cette ligne directrice en élaborant des stratégies, politiques et procédures adaptées à sa nature, sa taille, la complexité de ses activités et son profil de risque.

L’Autorité s’attend à ce que l’institution financière s'approprie les attentes de la présente ligne directrice et qu’elle les mette en œuvre d’ici le 27 février 2021.

Cette ligne directrice sera actualisée en fonction des développements en matière de gestion du risque des technologies de l’information et des communications et à la lumière des constats effectués dans le cadre des travaux de surveillance menés auprès des institutions financières visées.

Introduction

La progression rapide des innovations technologiques contribue à transformer les processus et les modèles d'affaires des institutions financières. Ces innovations introduisent par contre des risques significatifs alors qu'en parallèle, ces mêmes institutions sont de plus en plus interconnectées ou dépendantes de systèmes hérités[5] et de fournisseurs externes pour mener à bien leurs activités.

L'adoption des innovations technologiques accentue les risques de perte, de fuite, de vol, de corruption et d'accès non autorisé aux données. Elle expose davantage les institutions aux risques de cyberattaques qui sont de plus en plus sophistiquées, fréquentes, ciblées et difficiles à détecter.

Les risques liés aux technologies de l'information et des communications (« TIC »)[6] peuvent avoir des conséquences défavorables tant au niveau financier et légal que sur les clients et la réputation d'une institution.

Cette ligne directrice énonce les attentes de l'Autorité à l'égard de la gestion du risque TIC, lesquelles visent ultimement le renforcement de la résilience du secteur financier face à ce risque. Ces attentes visent notamment l'établissement d'une hygiène adéquate de sécurité par la mise en place de mesures[7] contribuant à prévenir la matérialisation d'un incident majeur et à limiter ses impacts.

Il est de la responsabilité de l'institution de bien comprendre l'ensemble des risques TIC auxquels elle est confrontée et de s'assurer qu'ils soient pris en compte adéquatement en fonction de sa nature, de sa taille, de la complexité de ses activités et de son profil de risque. Il est également de la responsabilité de l'institution de connaître les meilleures pratiques en matière de gestion des risques TIC et de se les approprier dans la mesure où celles-ci répondent à ses besoins.

---

5 Un système hérité, patrimonial ou *legacy system* en anglais, est un matériel et/ou logiciel continuant d'être utilisé dans une organisation, alors qu'il est supplanté par des systèmes plus modernes. Il fait partie d'un ensemble organisé de ressources qui permet de collecter, emmagasiner, traiter et distribuer de l'information.

6 L'Autorité définit le risque TIC comme étant le risque d'affaires lié à l'utilisation, la propriété, l'opération et l'adoption des TIC. Ce risque comprend notamment les risques de disponibilité et de continuité, de sécurité (incluant la cybersécurité), de changement, d'intégrité des données et d'infogérance.

7 Ces mesures portent tant sur des pratiques fondamentales de gouvernance des TIC que sur des mesures opérationnelles telles que le déploiement, en temps opportun, des mises à jour de sécurité des logiciels, la détection du trafic non autorisé sur les infrastructures réseau, la gestion des privilèges d'accès à l'information, le renforcement des mécanismes d'authentification pour l'accès aux systèmes critiques ou le contrôle des logiciels malveillants.

1. Les types de risques liés aux technologies de l'information et des communications (TIC)

L'Autorité s'attend à ce que l'institution financière mette en place une taxonomie qui lui est propre afin de s'assurer que tous les types de risques liés aux TIC soient répertoriés.

La taxonomie devrait avoir un caractère prospectif et prendre en considération les risques technologiques omniprésents dans l'ensemble des processus des institutions financières. Cette taxonomie devrait être développée afin d'en faciliter l'agrégation et de contribuer à l'établissement d'un portrait complet. Ainsi, elle devrait présenter un caractère exhaustif des risques liés aux TIC, permettant aux responsables de l'identification des risques d'envisager tous les types de risques susceptibles d'avoir des répercussions sur les objectifs de l'institution.

Le risque technologique devrait être évalué de manière holistique, en considérant tant les risques courants que les risques de ne pas répondre adéquatement aux changements ou à l'arrivée de technologies nouvelles ou émergentes, et ce, afin d'accroître l'agilité et la capacité de l'institution à répondre aux changements à travers le temps.

Au-delà des risques opérationnels dérivés des risques liés aux technologies, les risques stratégiques suivants[8] peuvent entraver l'atteinte des stratégies de l'institution et devraient être pris en considération :

- Le risque de gouvernance technologique[9];
- Le risque de positionnement technologique[10];
- Le risque d'exécution technologique[11].

Afin de prévenir un faux sentiment de sécurité ou d'urgence, il importe notamment que l'institution :

- utilise une terminologie TIC et une taxonomie claires et constantes pour la description des risques;
- agrège[12] les risques TIC au niveau de l'institution pour que ceux-ci soient considérés en combinaison avec tous les autres risques qui doivent être gérés.

8 Ces trois regroupements de risques stratégiques peuvent être décrits sous d'autres libellés selon la taxonomie établie par l'institution financière.

9 Le risque que le conseil d'administration ne parvienne pas à s'assurer de la mise en place des éléments nécessaires pour gouverner le développement et l'exécution de la stratégie TIC.

10 Le risque qu'au moment de la définition de la stratégie, la position technologique visée au sein de l'industrie ne soit pas enchâssée adéquatement dans la stratégie d'affaires, ne soit pas viable ou ne soit pas réalisable.

11 Le risque que, dans l'exécution de sa stratégie et de son plan stratégique, la haute direction n'atteigne pas les objectifs TIC stratégiques désirés ainsi que les objectifs d'affaires associés.

12 Les risques liés aux TIC peuvent être agrégés selon de multiples dimensions (par unités organisationnelles, par types de risques liés aux TIC, par processus, etc.).

Dans l'élaboration de sa taxonomie des risques, l'institution financière devrait établir un nombre raisonnable de catégories qui permettent de regrouper adéquatement les risques sans pour autant affaiblir le caractère particulier de chaque catégorie.

La sécurité de l'information, la gestion de crise, l'infogérance et l'infonuagique, la continuité des activités, la gestion de programmes et de projets[13], la gestion des changements, les opérations liées aux TIC, l'éthique, les ressources humaines et la propriété intellectuelle sont quelques-unes des catégories de risques liées aux TIC qui devraient être considérées dans l'élaboration de la taxonomie.

Dans l'éventualité où une institution financière dispose déjà d'une taxonomie des risques dans un secteur fonctionnel donné, par exemple l'audit interne, celle-ci pourrait être considérée dans l'élaboration d'une taxonomie des risques organisationnels, car elle pourrait contenir des catégories dont l'application à l'échelle de l'institution est éprouvée. Une fois développée, cette taxonomie devrait être communiquée à ceux qui participent directement aux activités d'évaluation des risques et aux contrôles, afin d'en assurer une utilisation cohérente dans l'identification et l'agrégation des risques TIC.

[13] Par exemple, des risques peuvent résulter de l'interdépendance entre différents projets ou de la dépendance de plusieurs projets sur les mêmes ressources et expertises.

2. La gouvernance des TIC

L'Autorité s'attend à ce que l'institution financière mette en place une gouvernance des TIC développée à partir de sources, de recommandations et de normes reconnues[14].

La gouvernance des TIC devrait refléter les changements qui s'opèrent au fil du temps. La qualité des pratiques de gouvernance est un facteur important au maintien de la confiance des marchés. Ainsi, la gouvernance des TIC devrait tenir compte en continu des bonnes pratiques reconnues par les organismes professionnels et internationaux existants et s'aligner avec les objectifs d'affaires de l'institution.

Le développement de la gouvernance des TIC devrait notamment considérer :

- la compréhension et l'acceptation des responsabilités liées à l'utilisation des TIC et des données par les individus et les groupes au sein de l'institution;
- l'évaluation des TIC et leurs activités, lors de l'étude des plans et politiques, afin qu'ils soient alignés aux objectifs de l'institution, qu'ils considèrent les bonnes pratiques et répondent aux besoins des parties intéressées;
- l'évaluation des plans de l'institution pour que les TIC supportent les processus d'affaires avec la capacité requise;
- la prise en considération du cycle de vie des données dans la définition des responsabilités;
- la mesure dans laquelle les TIC répondent aux obligations règlementaires, légales, contractuelles ainsi qu'aux standards et normes professionnelles et internationales;
- la façon dont les individus se comportent envers les autres (pour l'ensemble des parties prenantes) dans les pratiques et la prise de décisions liés aux TIC.

Les divers éléments de l'encadrement établi par l'institution financière (stratégies, politiques, etc.) devraient considérer et arrimer entre eux les dispositions déjà existantes[15], inhérentes et utiles à la gestion des risques technologiques.

[14] Exemples : OCDE, G7, NIST, ISACA-Cobit et ISO.

[15] Ces dispositions sont susceptibles d'avoir été définies et documentées distinctement à travers les années et pourraient comporter des contradictions.

2.1 Rôles et responsabilités

Le conseil d'administration

En sus des attentes[16] déjà émises par l'Autorité, le conseil d'administration devrait notamment s'assurer :

- que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement éthique et sécuritaire dans l'exploitation des technologies;
- d'échanger à l'égard des TIC avec les parties intéressées (internes et externes) afin d'appuyer par une documentation sa compréhension des besoins et porter un jugement sur la conception actuelle et future de la gouvernance des TIC;
- que les rôles et responsabilités de la fonction TIC et des fonctions de gestion de la sécurité de l'information et de la continuité des activités soient clairement définis dans l'établissement et le maintien de la gouvernance des TIC;
- que les structures, rôles et fonctions de support soient évalués régulièrement afin de permettre le développement et l'amélioration continue de la gouvernance des TIC.

De plus, le conseil d'administration devrait, conformément à la section 2.2, veiller à l'attribution des responsabilités liées au développement de l'encadrement des risques TI, notamment par l'appréciation des compétences nécessaires à l'exercice de ces responsabilités. Il devrait par ailleurs veiller à l'assignation :

- d'un responsable[17] pour les systèmes informatiques et les technologies de l'information qui supportent les objectifs de l'entreprise[18];
- d'un responsable à la seconde ligne de défense, tel un chef de la sécurité de l'information[19] (ou une autre personne de la haute direction et de la seconde ligne de défense), pour la surveillance du déploiement de l'encadrement relatif à la sécurité de l'information et à la sécurité physique des infrastructures technologiques de l'institution;
- d'un responsable à la seconde ligne de défense, tel un chef des données[20] (ou une autre personne de la haute direction et de la seconde ligne de défense[21]), lequel

16 AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance,* Septembre 2016.

17 Tel un directeur des technologies ou un chef des technologies ou de l'information. Ces derniers portent parfois aussi le nom de *Chief Technology Officer* (CTO) ou *Chief Information Officer* (CIO).

18 Cette personne est notamment responsable de l'exécution des plans stratégiques TIC, des processus reliés aux technologies (opérations, architecture, gestion de risque…), du développement des infrastructures technologiques de l'institution et de la présentation au conseil d'administration des propositions technologiques ainsi que des statuts de la mise en œuvre des stratégies et encadrements liés aux TIC.

19 Ce poste porte parfois aussi le nom de *Chief Information Security Officer* (CISO).

20 Ce poste porte parfois aussi le nom de *Chief Data Officer* (CDO).

21 AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*, Septembre 2016.

surveille l'encadrement approuvé à l'égard de la collecte, l'emmagasinage et l'utilisation des données à travers l'institution;

- de responsables, au sein de la haute direction, pour l'ensemble des différents actifs informationnels et risques TIC présents dans l'institution.

Le conseil d'administration devrait s'assurer d'obtenir des mises à jour sur les scénarios considérés dans le développement et la mise à l'essai (tests) des plans de recouvrement en cas de désastre et de continuité des activités afin de comprendre les objectifs de maintien de la disponibilité des opérations et systèmes TIC critiques. De plus, il devrait avoir une compréhension globale des processus d'escalade lors de brèches ou d'incidents de sécurité, incluant le moment où il devrait être notifié.

La haute direction

En sus des rôles et responsabilités qui lui sont généralement dévolus[22], la haute direction devrait notamment :

- mettre en place une fonction TIC opérant sous la surveillance d'une fonction de contrôle de la deuxième ligne de défense;
- délimiter clairement les responsabilités de la fonction de la sécurité de l'information, pour favoriser son indépendance et objectivité, notamment en la séparant des processus opérationnels TIC et par la mise en place de contrôles compensatoires au besoin. Cette fonction devrait n'être responsable d'aucun audit interne;
- définir les rôles et responsabilités pour le maintien et la diffusion, au sein de l'institution, d'une documentation et de l'information permettant la prise de décision éclairée à l'égard des TIC;
- gérer la relation entre les services offerts par la fonction TIC et les unités d'affaires de manière formelle et transparente et en utilisant un langage commun pour assurer l'atteinte des objectifs stratégiques;
- établir et maintenir une architecture d'entreprise comprenant les processus, informations, données et couches d'architectures d'applications, de technologies et de sécurité;
- distinguer les personnes responsables ou imputables dans la gestion du risque TIC de celles qui doivent être consultées ou informées;
- évaluer régulièrement, en collaboration avec les fonctions de conformité et d'audit interne, l'environnement de contrôle (les autoévaluations, les revues d'assurance, l'identification des déficiences dans les contrôles, la conformité des processus supportés par les TIC aux lois[23], règlements et obligations contractuelles, etc.);

22 AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*, Septembre 2016.

23 Notamment à la *Loi sur la protection des renseignements personnels* dans le secteur privé et à la Loi concernant le cadre juridique des technologies de l'information.

- revoir périodiquement les écarts de conformité (dont les dérogations approuvées par le conseil d'administration) aux encadrements établis pour le risque TIC[24].

Dans l'établissement de la stratégie TIC, la haute direction devrait notamment :

- établir une vue holistique des environnements d'affaires et des environnements TIC (actuels et à venir) afin d'identifier les initiatives de transformation requises;
- définir et documenter la façon dont elle fera évoluer ses TIC, son architecture technologique, sa structure organisationnelle et ses dépendances clés avec les partenaires et fournisseurs, pour supporter sa stratégie d'affaires;
- arrimer adéquatement et en continu les plans stratégiques TIC et les stratégies d'affaires tout en considérant la capacité des TIC, actuelle et requise dans le futur;
- considérer l'utilisation des innovations technologiques dans la planification stratégique et les décisions d'architecture d'entreprise;
- définir des objectifs prévoyant le maintien de la capacité de l'institution à anticiper les incidents TIC, à les détecter et à en assurer le recouvrement[25] pour assurer la résilience des systèmes TIC.

De plus, en matière de sécurité de l'information, le responsable désigné de la haute direction devrait notamment :

- développer, documenter et diffuser une politique de sécurité de l'information qui définit les principes et les règles à suivre pour la protection de la confidentialité, l'intégrité et la disponibilité des informations de l'institution et de ses clients;
- définir des objectifs de sécurité de l'information clairs pour les systèmes, les services TIC, les processus et les personnes;
- appliquer la politique de sécurité de l'information à toutes les activités de l'institution et inclure l'information traitée chez les intervenants externes[26] au périmètre de l'institution;
- déployer des contrôles pour les actifs[27] informationnels qui soient proportionnels à la criticité et la sensibilité desdits actifs;

[24] Les dérogations devraient être revues périodiquement, en fonction de la nature évolutive des TIC et des menaces inhérentes, pour assurer qu'elles demeurent à un niveau acceptable et qu'elles seront corrigées en temps opportun.

[25] Un incident TIC, un cyberincident ou un incident de sécurité de l'information se produit notamment lorsqu'une interruption inattendue dans la livraison des services TIC ou une brèche de sécurité d'un système vient compromettre la disponibilité, l'intégrité ou la confidentialité des données ou des systèmes TIC.

[26] Dans le cas d'intervenants externes, il convient ici d'établir des ententes appropriées sur le traitement sécuritaire de l'information.

[27] Les actifs informationnels (données, matériels et logiciels) ne sont pas limités uniquement à ceux détenus par l'institution. Ils englobent aussi les actifs informationnels confiés ou livrés par les clients ou des tiers.

- conduire des régimes d'essais systématiques adéquats pour valider l'efficacité des contrôles mis en place;
- déployer des programmes de formation et de sensibilisation en sécurité de l'information;
- produire des indicateurs de performance de la sécurité couvrant notamment les impacts d'affaires (pour le bénéfice du personnel non technique) et l'efficacité des contrôles de sécurité.

À l'égard de la reddition, la haute direction devrait notamment rendre compte :

- des objectifs et des indicateurs recueillis liés aux TIC et à ses processus en temps opportun et de manière systématique;
- des résultats découlant de la vigie conduite sur les bonnes pratiques et les normes en développement, au niveau national et international, liées aux TIC et leurs impacts potentiels sur les activités de l'institution;
- des enjeux clés liés aux TIC incluant les projets, les priorités et les incidents TIC significatifs de même que des rapports réguliers sur le risque TIC.

Autres rôles

La fonction de gestion des risques[28] de l'institution financière devrait surveiller la fonction TIC de l'institution et prendre en charge la surveillance de l'ensemble des risques TIC, tant les risques opérationnels et stratégiques que ceux qui découlent des innovations[29] liées aux TIC. Cette fonction devrait aussi assurer un suivi rigoureux des risques importants ainsi qu'une veille des risques émergents liés aux TIC.

L'assurance objective attendue de la fonction d'audit interne, sur la suffisance et l'efficacité de la gouvernance des TIC, devrait notamment couvrir l'efficience et l'efficacité des opérations TIC, la protection des actifs informationnels et la fiabilité et l'intégrité de leurs processus de divulgation.

Les activités d'audit interne de l'institution devraient comprendre la revue de la conception et de l'efficacité des contrôles de sécurité de l'information, incluant les contrôles maintenus par les parties externes. L'audit interne devrait aussi revoir les assurances fournies par une partie externe et qui ont le potentiel de nuire à l'institution, à sa clientèle ou à d'autres parties intéressées.

D'autres rôles définis à travers l'institution ont un effet sur la gouvernance et la gestion des risques TIC. Bien qu'ils n'y soient pas directement liés, ils se présentent tout de même comme des parties intéressées et devraient être considérés dans la définition des rôles et responsabilités. Il pourrait s'agir, par exemple, des responsables de la continuité des affaires ou des ressources humaines.

---

[28] Le chef de la gestion des risques ou un membre désigné de la haute direction en mesure de synthétiser, vulgariser et communiquer efficacement l'information liée aux TIC auprès de divers auditoires.

[29] Par exemple, les risques de biais ou d'utilisation non éthique des technologies de données massives et d'intelligence artificielle.

2.2 Probité et compétences

En concordance avec les attentes[30] déjà émises par l'Autorité, une gouvernance efficace et efficiente, qui inclut les technologies de l'information et des communications, requiert un niveau adéquat d'expertise, de qualifications professionnelles, de connaissances et d'expériences de la part des instances décisionnelles.

Les membres des instances décisionnelles et les mécanismes de gouvernance établis (par exemple : comités d'audit, gestion de risques et gestion des TIC) devraient avoir la connaissance et la compréhension de l'utilisation des TIC, des tendances et orientations futures des TIC de même que l'autorité nécessaire pour mener à bien leurs responsabilités respectives.

Dans l'évaluation de la compétence des personnes membres des instances décisionnelles, une grille d'aptitudes et de connaissances dont les critères portent sur les TIC, devrait être établie, actualisée et appliquée périodiquement auprès des personnes occupant des postes stratégiques liés à la gouvernance et la gestion des risques liés aux TIC ou plus fréquemment si requis.

Dans cette perspective, il devrait y avoir un recensement périodique de l'ensemble des compétences courantes à l'égard des TIC présentes au sein de l'institution, ainsi que celles requises à la réalisation des stratégies et à l'atteinte des objectifs.

Afin de minimiser le risque qu'il n'y ait pas suffisamment d'expertise TIC aux postes clés, un processus formel d'acquisition de compétences qui traite des enjeux stratégiques liés aux TIC devrait être développé.

De même, un programme de formation complet sur la sensibilisation à la sécurité des TIC devrait être déployé à l'ensemble du personnel et tenir compte minimalement du paysage courant des menaces (dont les cybermenaces) et de leurs conséquences, des lois, des règlements, des encadrements établis par l'institution et des responsabilités du personnel dans la protection des actifs informationnels.

Ce programme de formation devrait être mis à jour et reconduit régulièrement pour l'ensemble du personnel de l'institution et pour tout fournisseur de service qui accède aux actifs informationnels.

De même, avant l'emploi, tout au long de celui-ci et à sa terminaison, l'institution devrait mener régulièrement des vérifications de sécurité pour les ressources humaines (incluant les consultants, les partenaires et les fournisseurs) ayant accès aux données et aux systèmes TIC et qui peuvent exposer l'institution à des vols de données, du sabotage, de la fraude et d'autres risques liés aux TIC.

[30] AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur les critères de probité et de compétence, Juin 2012.

2.3 Documentation à l'égard des TIC

Les encadrements de l'institution devraient préciser les rôles et les responsabilités des instances décisionnelles et des unités opérationnelles à l'égard de l'établissement, du maintien et de la consultation sécuritaire de la documentation et l'information permettant la prise de décision éclairée à l'égard des TIC.

Cette documentation ne devrait pas être statique, mais plutôt évoluer dans le temps. Tout comme les affaires, les TIC d'une institution sont en perpétuel changement au rythme des acquisitions, des mises à jour et des changements externes. Cette documentation devrait contenir suffisamment d'informations agrégées pour faciliter la prise de décision concernant la stratégie TIC.

La documentation devrait notamment regrouper des informations qui reflètent l'état de la stratégie TIC, l'architecture actuelle et ciblée, les objectifs et risques TIC stratégiques, les plans et leurs états courants, les énoncés d'impact des risques liés aux TIC et les processus et structures existantes pour leur gestion, la méthodologie de développement et les processus d'opérations.

De plus, parmi les documents stratégiques qui sont issus des meilleures pratiques, l'institution financière devrait considérer :

- la description des contextes auxquels fait face l'institution, les lignes d'affaires et les fonctions de support;
- la description de l'impact des risques TIC sur les stratégies d'affaires;
- le registre des risques TIC et la matrice des risques et contrôles TIC;
- les modèles et processus d'opérations des TIC.

Bien que la documentation puisse être préparée et maintenue par diverses composantes de l'institution, elle devrait toutefois être revue par la haute direction et les éléments clés[31] devraient être approuvés par le conseil d'administration.

[31] Les éléments clés présentés au conseil d'administration devraient être formulés de manière que ses membres puissent facilement en faire l'appréciation afin de prendre une décision informée.

3. La gestion des risques liés aux TIC

L'Autorité s'attend à ce que l'institution financière considère l'ensemble des activités nécessaires à la préparation, au traitement et au suivi requis dans la gestion des risques liés aux TIC.

L'élaboration des stratégies, des politiques et des procédures permettant d'identifier, d'évaluer, de quantifier, de contrôler, d'atténuer et de suivre les risques TIC, devrait considérer les activités nécessaires de préparation, de traitement et de suivi requises pour que les premières heures d'une crise réelle soient moins dommageables. Par exemple, l'ensemble des mesures prévues par l'institution, notamment les mesures de réponse et de recouvrement, devraient faire l'objet de simulations de crise. De plus, les intervenants et spécialistes externes requis par ces mesures devraient être préqualifiés et les termes et conditions contractuels préétablis.

Dans la mise en place de pratiques robustes de gestion des risques TIC à travers l'institution, cette dernière devrait aussi tenir compte de la participation des parties intéressées externes afin de s'assurer que l'information juste et pertinente à la gestion des risques est distribuée et utilisée par tous.

Le cadre de gestion des risques TIC devrait permettre l'établissement et le maintien d'une vue holistique des risques TIC incluant les liens et les dépendances entre les gens, les processus d'affaires de bout en bout, les fonctions de l'institution, les systèmes TIC et les actifs qui supportent ces processus et ces personnes. Le recensement des rôles, processus et fonctions d'affaires devrait permettre d'identifier leurs importances relatives et leurs interdépendances aux risques TIC.

3.1 Préparation

La sélection des mesures préparatoires pour la gestion des risques TIC devrait notamment contribuer à la protection des données sensibles (telles que les informations des clients) contre la divulgation, la fuite ou les accès non autorisés. Elle devrait aussi contribuer à la résilience de l'environnement TIC. Ces mesures devraient couvrir, entre autres, les contrôles d'accès, l'authentification, l'intégrité et la confidentialité des données, l'enregistrement des activités et le suivi des événements de sécurité[32].

Dans sa préparation, l'institution financière devrait être en mesure de saisir l'impact du risque technologique sur les opérations, incluant la mission, les fonctions ou la réputation, ainsi que sur les actifs et individus. En conséquence, l'approche intégrée pour gérer le risque TIC devrait être appliquée à l'échelle de l'institution. Elle devrait permettre notamment :

- d'assurer un alignement de l'ensemble des outils et des échelles d'évaluation des risques utilisés et une utilisation constante, convenue et transparente;

[32] L'annexe aborde plusieurs mesures complémentaires à considérer et qui ont fait leurs preuves dans la gestion des risques liés à la sécurité de l'information., aux opérations TIC, à l'infogérance et aux projets de transformation TIC.

- d'utiliser un processus rigoureux pour le recensement périodique des actifs informationnels et leurs vulnérabilités, afin d'associer adéquatement les risques aux actifs de manière holistique. Il en va de même des menaces internes et externes et des probabilités et impacts d'affaires potentiels, afin de déterminer le niveau de risque et établir les plans d'action adéquats. Cette gestion des actifs devrait aussi couvrir les données, le personnel, les systèmes TIC (incluant ses diverses composantes matérielles et logicielles) et les locaux les abritant;
- d'exploiter un cadre de classification[33] permettant de définir la criticité des données et des actifs informationnels (incluant ceux qui sont gérés par des parties intéressées externes) minimalement selon leurs exigences de disponibilité, d'intégrité et de confidentialité;
- d'utiliser des processus de gestion d'incidents TIC, dotés d'objectifs de reprise et recouvrement adéquats et permettant la proactivité dans la gestion des risques;
- d'assurer un suivi adéquat et en temps opportun des activités de mitigation des risques présents au registre des risques TIC;
- de suivre l'efficacité des mesures de mitigation, de même que le nombre d'incidents signalés afin de les corriger lorsque nécessaire;
- de considérer des facteurs financiers, légaux, règlementaires, opérationnels ainsi que des facteurs liés à la clientèle et à la réputation dans l'évaluation du risque TIC.

Outre l'évaluation du risque TIC inhérent à ses activités, ses produits ou ses services (incluant particulièrement le cyberrisque), l'institution financière devrait considérer l'impact que ce risque représente pour ses partenaires, fournisseurs, clients ainsi que pour les autres participants du secteur financier, lorsque pertinent.

L'institution financière devrait réaliser des évaluations des risques liés aux TIC à intervalles planifiés, lorsque des changements significatifs sont prévus ou ont lieu et lorsque des incidents opérationnels ou de sécurité significatifs se matérialisent, en tenant compte de critères établis. L'évaluation des risques liés aux TIC devrait s'inscrire dans un processus systématique et cyclique permanent.

Par ailleurs, l'institution financière devrait utiliser des méthodes permettant de faire le lien entre les scénarios de risques liés aux TIC et leurs impacts potentiels sur les actifs informationnels et sur les processus d'affaires afin que l'ensemble des parties intéressées comprennent[34] les effets des évènements indésirables liés aux technologies de l'information et des communications.

---

33 Cette classification devrait refléter la mesure dans laquelle un incident de sécurité de l'information affectant un actif informationnel a le potentiel de nuire, à l'institution, à sa clientèle ou à d'autres parties intéressées.

34 Les évaluations des risques liés aux TIC requièrent que les résultats soient exprimés en des termes d'affaires clairs et non ambigus. Une gestion efficace des risques liés aux TIC requiert une compréhension commune, entre les secteurs d'affaires et technologiques, des risques qui devraient être gérés et leurs raisons sous-jacentes. Les parties intéressées à la gestion des risques liés aux TIC devraient avoir la capacité de comprendre et d'exprimer la manière dont des événements ou incidents défavorables interagissent sur les objectifs d'affaires de l'institution.

De plus, l'institution financière devrait :

- identifier tous les points individuels de défaillance potentielle dans les systèmes TIC et les architectures de réseaux afin que des mesures appropriées soient déployées pour mitiger les risques d'interruption;
- conduire les analyses d'impact d'affaires de bout en bout pour les processus d'affaires critiques afin que les plans de recouvrement (en cas de désastre) et de continuité des activités priorisent adéquatement les opérations critiques de l'institution dans le recouvrement des systèmes TIC;
- considérer un ensemble plausible[35] d'événements et de scénarios de désastre, incluant des événements de cybersécurité, dans la planification des plans de recouvrement et de continuité;
- inclure les dispositions régissant le recouvrement dans les délais requis et la conduite de tests périodiques dans la stratégie de sauvegarde des données pour assurer l'efficacité des procédures.

Les processus et les procédures assurant la résilience des systèmes TIC devraient tenir compte continuellement de l'évolution rapide des menaces. Ils devraient permettre de contenir les impacts des incidents de sécurité potentiels et accélérer le retour aux opérations normales. Parmi ces processus et procédures, il y a notamment la planification des plans de réponse et de recouvrement, les communications, l'analyse, la mitigation et l'amélioration continue.

Afin d'éviter d'accroître son exposition à des risques de sécurité et de stabilité, l'institution financière devrait établir des plans de remplacement en temps opportun de son matériel et logiciel TIC avant qu'ils n'atteignent la date de fin de support annoncée par leurs fournisseurs.

3.2 Traitement

Dans le traitement des risques TIC, l'institution financière devrait notamment :

- déterminer les mesures nécessaires à la mise en œuvre des options de traitement des risques identifiés;
- comparer les mesures déterminées avec les meilleures pratiques existantes et vérifier qu'aucune mesure nécessaire n'a été omise;
- produire une déclaration des contrôles répertoriant les mesures et la justification de leur inclusion ou exclusion;
- maintenir et utiliser des encadrements de sécurité, et les processus et les procédures qui en découlent, pour gérer les systèmes d'information et les actifs;

[35] L'institution devrait notamment considérer des scénarios à faible probabilité qui entraînent des impacts élevés de nature financière et non-financière (réputation, conformité, etc.).

- effectuer la maintenance et la réparation des éléments composant les systèmes TIC conformément aux encadrements établis par l'institution.

De plus, l'institution financière devrait:

- détecter en continu les activités anormales sur les infrastructures réseau, les systèmes TIC et les actifs informationnels afin de comprendre l'évolution d'événements non désirés et leurs impacts potentiels et de vérifier l'efficacité des mesures de protection;
- mettre à l'essai et maintenir les processus de détection précités afin d'assurer une connaissance adéquate et opportune des événements anormaux;
- exécuter et maintenir les processus et procédures de réponse et de récupération afin d'assurer la réponse aux incidents de cybersécurité détectés et la restauration des systèmes ou des actifs;
- recevoir, analyser et répondre aux vulnérabilités dévoilées par des sources internes ou externes (tests conduits à l'interne, bulletins ou recherches spécialisées en sécurité);
- exécuter et réviser les activités planifiées pour empêcher l'expansion d'un évènement auprès d'autres systèmes TIC, en atténuer les effets et résoudre l'incident.

L'accès aux dispositifs[36] de retrait ou d'extraction des données devrait aussi faire l'objet d'une évaluation de risque et devrait être autorisé uniquement lorsqu'un besoin d'affaires réel existe, afin de prévenir les risques de fuite de données.

L'institution financière devrait démontrer qu'elle évalue les risques associés à l'entretien continu de ses systèmes hérités et que des contrôles adéquats sont déployés pour gérer efficacement les risques de ces technologies. Si les systèmes hérités supportent des opérations critiques, l'institution financière devrait avoir en place une stratégie pour gérer l'infrastructure vieillissante.

Les applications développées ou acquises par les utilisateurs finaux pour l'automatisation de leurs opérations, incluant les applications accessibles par l'Internet, devraient être approuvées par les secteurs d'affaires pertinents et la fonction TIC de l'institution. Ces applications devraient être prises en considération dans les processus de gestion des actifs informationnels et de gestion des risques TIC. L'institution financière devrait s'assurer de la mise en place de mesures de sécurité adéquates contre la perte ou la fuite de données et l'exposition à des virus malicieux liées à ces applications. De plus, l'institution financière devrait déployer des contrôles permettant de surveiller et détecter l'utilisation non autorisée de ces applications[37].

[36] Par exemple, l'utilisation d'appareils informatiques portatifs (tablette, cellulaire, etc.), de dispositifs d'emmagasinage (clé USB, disque dur portable, etc.), de courriels, de messagerie instantanée et de copies imprimées.

[37] **Shadow IT** (parfois **Rogue IT**) est aussi un terme utilisé pour désigner des systèmes TIC mis en œuvre au sein d'organisations sans approbation.

Dans l'évaluation des risques et des contrôles, les mécanismes de protection peuvent inclure l'évitement ou l'élimination du risque en ne s'engageant pas dans une activité d'affaires particulière. Ils peuvent aussi inclure l'atténuation du risque à travers les contrôles ou le partage ou transfert du risque.

L'institution financière devrait évaluer régulièrement l'adéquation de ses ressources avec l'appétit pour le risque par des exercices de simulation de crise pour l'ensemble des risques matériels et potentiels, classifiés selon leur probabilité et leur impact (p. ex. : les risques TIC, dont le cyberrisque).

Dans le maintien régulier de son registre des risques TIC, connus et potentiels, l'institution devrait décrire notamment leurs attributs et activités de contrôles de façon claire et suffisamment détaillée. Le registre des risques TIC devrait être mis à jour de manière prospective et l'adéquation des contrôles devrait être évaluée régulièrement.

3.3 Suivi

En concordance avec les attentes[38] déjà émises, les bonnes pratiques généralement reconnues de même que la législation applicable, l'Autorité s'attend notamment, en matière de divulgation et de transparence, à ce que l'institution financière mette en place les mécanismes nécessaires pour notifier promptement les parties intéressées internes et externes, incluant l'Autorité, lors d'un incident opérationnel.

Les processus et les procédures mis en place dans le cadre de la gestion des incidents de l'institution financière devraient permettre d'intervenir et de rétablir les services le plus rapidement possible lors d'incidents liés aux TIC. Ils devraient notamment :

- coordonner les réponses et les activités de recouvrement requises suite à la notification aux parties prenantes internes et externes;
- contribuer à minimiser les impacts sur la clientèle;
- rendre compte des incidents selon des critères préétablis;
- partager l'information utile contribuant au rehaussement de la sécurité de l'information;
- gérer les relations publiques et l'impact sur la réputation de l'institution.

De plus, l'institution financière devrait conduire des analyses spécifiques suite à un incident majeur pour améliorer ses plans de réponse et de recouvrement. Elle devrait notamment :

- explorer les données recueillies dans ses infrastructures par ses systèmes de détection;
- identifier et mesurer les impacts de l'incident;

[38] AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur la gestion de risque opérationnel, Décembre 2016.

- mitiger ou accepter et documenter le risque des nouvelles vulnérabilités identifiées;
- formuler et communiquer aux parties prenantes internes les leçons apprises dans la résolution de l'incident;
- recevoir, analyser et répondre aux vulnérabilités dévoilées par des sources internes ou externes (tests conduits à l'interne, bulletins ou recherches spécialisées en sécurité).

À partir des leçons apprises, des constats et des décisions prises lors de la gestion des risques TIC, l'institution financière devrait procéder à la révision de ses stratégies, notamment celles établies à partir de ses activités préparatoires (Section 3.1). Cette révision devrait être conduite à l'aide d'objectifs d'évaluation clairs, d'attentes et de méthodologies établies et diffusées aux parties intéressées et de comptes rendus comportant des conclusions claires et des actions correctives concrètes.

ANNEXE - Normes complémentaires aux lignes directrices de l'Autorité

L'Autorité s'attend à ce que la mise en œuvre des pratiques de gestion saine et prudente, énoncées dans l'ensemble de ses lignes directrices, considèrent les pratiques spécifiques liées aux TIC qui ont fait leurs preuves et sont généralement reconnues.

La gestion du risque TIC repose sur l'appropriation par l'institution financière des attentes émises dans plusieurs lignes directrices de l'Autorité dont celles portant notamment sur la gouvernance, la gestion intégrée des risques et la conformité. Toutefois, elle repose aussi sur les attentes émises dans les sections précédentes de la présente ligne directrice et sur la mise en œuvre de plusieurs pratiques spécifiques aux TIC.

Dans cette perspective, les pratiques[39] qui suivent concourent à l'établissement d'une approche holistique. Leur utilisation contribue à prévenir et à atténuer les risques TIC, comme par exemple, ceux liés à son utilisation et à son opération.

Sécurité des TIC

L'institution financière devrait mettre en place des mécanismes robustes de sécurité permettant d'assurer la livraison de ses services critiques et l'identification des incidents liés aux TIC.

Parmi les mécanismes à considérer, il y a notamment la gestion des identités et des accès, la formation et sensibilisation, la ségrégation des réseaux et la protection de leur intégrité, la sécurité des données, la protection des appareils de types « *endpoints* », la vérification de l'intégrité des logiciels et du microcode, les processus de protection de l'information et les solutions[40] technologiques de protection contribuant à la résilience des systèmes et des actifs informationnels. De même, la détection d'événements et d'anomalies, la surveillance en continu des systèmes d'information et la mise à l'essai des processus de détection devraient être considérées.

L'institution financière devrait définir un processus pour recueillir, sécuriser, entreposer, consolider, traiter et revoir les journaux d'événements TIC pour faciliter les opérations de surveillance de sécurité. Cela devrait comprendre notamment les journaux d'événements des coupe-feu, des applications, des systèmes d'exploitation et des événements d'authentification.

L'institution financière devrait s'assurer que l'accès[41] logique et physique aux actifs informationnels et aux ressources associées est limité aux utilisateurs, processus ou

---

39 Les thèmes abordés dans cette annexe sont tirés des meilleures pratiques recommandées par différents organismes nationaux ou internationaux dont notamment le NIST, Cobit, G7 et ISO.

40 Par exemple : coupe-feu, contrôle d'accès réseau, dispositif de détection et prévention d'intrusion, antivirus, chiffrement, outil de suivi et analyse des journaux.

41 Cela comprend tout autant les accès des usagers réguliers ou à hauts privilèges que les accès à distance.

appareils autorisés ainsi qu'aux activités autorisées selon un processus rigoureux et prédéfini.

Les privilèges d'accès octroyés devraient être établis sur la base des principes « besoin de savoir », « moindre privilège » et « ségrégation des tâches », uniquement au personnel autorisé et de façon à prévenir les accès injustifiés à de larges ensembles de données et prévenir le contournement des contrôles de sécurité.

L'institution financière devrait limiter l'usage de compte d'accès génériques ou partagés et s'assurer que les usagers puissent être identifiés dans l'utilisation des systèmes TIC. Les exceptions devraient être justifiées, recensées et approuvées.

L'institution financière devrait soumettre ses contrôles à l'égard de la sécurité de l'information à différents types d'évaluation, de tests et des revues indépendantes périodiques et à des tests d'intrusions[42] et des exercices de type « Red Team [43]».

Dans l'évaluation des risques de la sécurité de l'information, l'institution financière devrait notamment :

- identifier les risques de sécurité de l'information liés à la perte de confidentialité, d'intégrité et de disponibilité des informations et identifier les responsables des risques;
- établir et tenir à jour les critères de risque de sécurité de l'information incluant les critères d'acceptation des risques et les critères de réalisation des évaluations des risques de sécurité de l'information.

L'institution financière devrait maintenir activement la sécurité de son information en considérant les changements aux menaces et vulnérabilités, incluant celles résultant des changements à ses actifs informationnels, le stade auquel ils sont dans leur cycle de vie[44] et son environnement d'affaires.

Dans le développement d'une sécurité de l'information adéquate pour les systèmes TIC, l'institution devraient s'assurer d'une ségrégation adéquate entre la sécurité opérationnelle et la gestion des risques.

---

42 Les tests d'intrusion et les évaluations de vulnérabilités produisent une image d'un système informatique dans un état et à un moment spécifique. Cette image est limitée aux portions du système qui est testé durant les tentatives d'intrusion. Dans cette perspective, les tests d'intrusion et les évaluations de vulnérabilités ne sont pas des substituts pour l'évaluation des risques TIC.

43 Les exercices de type Red Team consistent à effectuer une simulation permettant à l'institution de détecter et répondre à des attaques ciblées. Les processus de contrôle des personnes et de la technologie en place dans l'institution sont revus tout au long de l'exercice en simulant les objectifs et les actions d'un attaquant.

44 Ceci fait référence au processus traitant de la planification et de la conception des actifs informationnels jusqu'à leur déclassement et élimination.

Opérations liées aux TIC

Les innovations technologiques, telles que l'infonuagique, l'Internet des objets et les mégadonnées, ont un impact significatif sur la fonction TIC (notamment au niveau des processus qui doivent être adaptés) dont la gestion des capacités et la gestion de la sécurité, et des connaissances qui devraient être bonifiées pour opérer dans de nouveaux systèmes TIC.

Dans ce contexte, il importe que le personnel des opérations TIC ait l'information, les ressources et les outils requis pour détecter tout problème qui s'introduit dans les opérations des centres de traitement, des réseaux, des infrastructures de sécurité de l'information et dans le support aux utilisateurs. Ces éléments devraient contribuer notamment :

- à l'établissement d'un inventaire exhaustif du matériel de traitement de l'information, des ressources, des emplacements, etc.;
- à la priorisation des efforts de mitigation des risques TIC;
- à l'identification de contrôles de mitigation comme des politiques et des procédures pour la sécurité physique et logique, la gestion des données, du personnel et des changements, la distribution et transmission d'informations, les sauvegardes et le support utilisateurs, etc.;
- au suivi et à la reddition de la performance, de la planification de la capacité et de l'autoévaluation des contrôles.

L'institution financière devrait déployer un processus de gestion des configurations du matériel et du logiciel constituant ses systèmes d'information permettant d'avoir une visibilité et un contrôle efficace et sécuritaire de ses systèmes.

L'institution financière devrait s'assurer de minimiser les risques d'interruptions aux opérations par la mise en place de processus adéquats pour la gestion des changements touchant les équipements TIC (matériels et logiciels) et les procédures liées au développement, l'exécution, le support et l'entretien des systèmes TIC de production. Ces processus devraient prévoir notamment :

- des évaluations de risques de sécurité et d'impacts (notamment en relation avec les autres actifs informationnels) avant l'implantation des changements proposés;
- des tests suffisants pour les nouvelles TIC, les rehaussements et les correctifs envisagés aux systèmes existants avant leur déploiement;
- les exigences et les niveaux d'approbation requis pour le déploiement des changements;
- des procédures clairement définies pour l'évaluation, l'approbation et le déploiement des changements d'urgence, incluant les approbateurs, afin de réduire les risques de sécurité et de stabilité des environnements de production;
- une ségrégation stricte des tâches dans le processus de mise à jour des logiciels afin de restreindre la possibilité qu'un seul individu développe, compile et déploie

du code logiciel d'un environnement de développement à un environnement de production;

- l'activation de l'enregistrement des activités dans les journaux d'audit et de sécurité.

Dans l'optique de réduire les risques d'interruptions des opérations provenant de l'exploitation mal intentionnée de bogues ou vulnérabilités des logiciels, l'institution financière devrait établir des pratiques et des standards sécurisés pour encadrer la programmation, la revue des codes sources et la mise à l'essai de la sécurité applicative de ses systèmes TIC. Lorsque l'application de ces pratiques soulève des enjeux de disponibilité, d'intégrité et de confidentialité de l'information et des systèmes TIC, ces derniers devraient être compilés, suivis et corrigés.

L'institution financière devrait s'assurer du déploiement de processus pour que soit évalué et géré l'ensemble des risques opérationnels associés à l'utilisation, la propriété, l'opération et l'adoption des TIC au sein de l'institution. Elle devrait notamment :

- implanter une structure opérationnelle TIC adéquate pour supporter les activités d'affaires de l'institution;
- revoir et comprendre comment les systèmes en place supportent les processus d'affaires associés;
- supporter un environnement de contrôle approprié à travers l'identification, l'évaluation, la gestion et le suivi des risques opérationnels liés aux TIC selon des préceptes semblables à ceux de la *Ligne directrice sur la gestion du risque opérationnel*;
- créer un environnement opérationnel physique et logique sécuritaire;
- prévoir une continuité et résilience opérationnelle;
- prévoir une sélection, dotation, succession et formation adéquate du personnel lié aux TIC.

Infogérance et infonuagique

L'infogérance ne réduit pas nécessairement les risques liés aux TIC. Elle peut exposer l'institution financière à des risques accrus de sécurité, de performance opérationnelle et de continuité des activités en cas de mauvaise gestion. La gestion adéquate de ces risques demeure toujours sous la responsabilité de l'institution. Ainsi, l'institution financière devrait identifier les risques stratégiques liés aux TIC inhérents aux initiatives d'infogérance, mettre en place un programme efficace de gestion de ces risques et suivre les risques émanant de toute entente d'infogérance.

En concordance avec les attentes[45] émises par l'Autorité, l'institution financière demeure responsable du recouvrement de ses activités lorsqu'un désastre affecte ses fournisseurs lors de l'impartition de sa stratégie TIC avec l'infonuagique. Aussi, elle devrait considérer

[45] AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur la gestion des risques liés à l'impartition, 2010.

le risque TIC, et notamment le cyberrisque, dans l'évaluation du niveau d'expérience et d'expertise requis pour l'activité impartie et la gestion des relations d'impartition.

L'institution financière devrait s'assurer de l'efficacité de son cadre de gestion des risques TIC lorsque des ententes d'infogérance sont conclues avec des fournisseurs de services externes ou des membres de son groupe.

L'adoption croissante par les institutions financières de services infonuagiques a de nombreux avantages (économies d'échelle, accès aux bonnes pratiques, agilité, etc.). La nature distribuée de ces services peut aussi améliorer la résilience lors de désastres ou d'interruptions de services. L'Autorité considère ces services infonuagiques comme une forme d'infogérance et dans cette optique, les institutions financières devraient se référer aux attentes de la *Ligne directrice sur la gestion des risques liés à l'impartition.*

L'institution financière devrait bien comprendre les caractéristiques typiques des services infonuagiques, notamment la colocation, l'amalgamation des données et la forte propension du traitement informatique dans des sites multiples ou distribués. Des actions devraient être envisagées pour identifier et gérer les risques associés à l'accès, la confidentialité, l'intégrité, la souveraineté, la conformité règlementaire et l'audit des données. Notamment, l'institution financière devrait s'assurer que le fournisseur de services possède l'habilité d'identifier et de faire la ségrégation des données client en utilisant des contrôles physiques et logiques robustes. De plus, l'institution financière devrait maintenir, dans sa liste centralisée d'ententes d'impartition importantes, toute information utile à la gestion des risques de ses données (nature, sensibilité, emplacement(s) du traitement, de l'emmagasinage et de la circulation des données, etc.).

Dans le contexte de l'infogérance et l'infonuagique, l'institution financière devrait notamment :

- assurer contractuellement son droit d'auditer (ainsi que celui des autres autorités compétentes, le cas échéant) de même que leur accès physique aux locaux des fournisseurs de service d'infonuagique;
- assurer la sécurité des données et l'emplacement du traitement informatique par des contrôles[46] adéquats (établis par une approche basée sur les risques) comme les technologies de chiffrement des données en transit, en mémoire et au repos;
- mitiger les risques d'impartition en chaîne lorsque les fournisseurs impartissent eux-mêmes certaines activités à d'autres fournisseurs;
- développer des plans de contingence et des stratégies de sortie appropriés afin de pouvoir quitter toute entente contractuelle sans interruption dans la livraison de ses services, sans effets indésirables sur la conformité règlementaire et sans impact sur la continuité et la qualité des services TIC fournis aux clients;

[46] L'institution devrait considérer notamment, dans l'établissement des ententes contractuelles et de niveaux de services, l'utilisation d'objectifs et de mesures de sécurité de l'information, l'utilisation de sa propre définition du cycle de vie des données, et l'établissement de ses besoins de surveillance de la sécurité et chiffrement de ses données.

- suivre le développement du risque potentiel de concentration lorsque la livraison de ses services critiques repose sur un nombre restreint de fournisseurs de services;
- suivre et obtenir l'assurance de la conformité des fournisseurs aux objectifs et mesures de sécurité et aux attentes de performance.

Considérant le nombre de fournisseurs et la variété des impacts potentiels de l'infogérance et l'infonuagique chez les institutions financières, un niveau de contrôle serré devrait être mis en place. La cybersécurité ne devrait pas être considérée uniquement au niveau des fournisseurs majeurs ou des fournisseurs de services critiques. De fait, certains autres fournisseurs pourraient constituer un maillon faible dans les processus de sécurité.

L'utilisation des services de certaines tierces parties peut ne pas constituer une forme d'impartition. Par contre, plusieurs de leurs services sont fournis à l'aide des TIC ou mettent en jeu des informations potentiellement confidentielles. Ces tierces parties peuvent aussi être exposées à des bris de sécurité. L'institution financière devrait évaluer les risques de bris de confidentialité, d'intégrité et de disponibilité des informations traitées par ces services et les gérer adéquatement.

Projets et programmages de transformation

La mise en place de toute stratégie TIC requiert le démarrage formel de programmes de gestion du changement technologique. De tels programmes nécessitent des ressources, une gestion et un suivi approprié et ils introduisent aussi de nouveaux risques qui doivent être mitigés. Parmi ces risques, il y a notamment la perturbation des services fournis aux clients, la perte d'avantages concurrentiels, l'impact négatif sur la réputation et le retard dans la mise en œuvre de produits ou de processus critiques et stratégiques.

L'institution financière devrait établir un cadre de gestion des projets assurant l'utilisation constante de pratiques de gestion pour la livraison de résultats répondant aux besoins et aux objectifs d'affaires et de sécurité. La gestion des risques prévue dans ce cadre devrait permettre d'identifier, d'évaluer, de gérer et de suivre les risques associés tout au long du cycle de vie des projets.

Ce cadre de gestion devrait couvrir les pratiques nécessaires pour gérer tout le cycle de vie des projets. Il devrait aussi permettre d'établir les plans de projets TIC complets requis pour la mise en place des stratégies. Ces plans de projet devraient définir clairement la portée du projet, les analyses coûts-bénéfices et de faisabilité, les activités, les livrables et les jalons importants et les rôles et responsabilités des ressources requises pour chaque phase du projet.

Lorsque les projets portent spécifiquement sur l'acquisition, le développement ou la modification de systèmes TIC nouveaux ou existants, l'institution financière devrait s'assurer que les processus, les procédures et les contrôles de son cadre respectent le principe de prise en compte de la sécurité dès la conception *(« security by design »)* afin de permettre la mise en place de système TIC fiable et résilient aux attaques.

L'institution financière devrait normaliser et outiller sa méthodologie de gestion du projet. Elle devrait définir clairement le cycle de vie du développement des systèmes TIC qui

comprend différentes étapes, dont notamment l'identification des besoins en sécurité de l'information, et dont l'ordre devrait être respecté afin que les besoins métiers puissent être transformés en systèmes ou en applications et que leur entretien puisse être maîtrisé;

De plus, l'institution devrait gérer les changements engendrés par les projets au niveau des structures et des processus, notamment les aspects informels ou intangibles (perceptions de l'impact, modifications d'habitudes de travail, etc.), la communication, l'état de préparation organisationnelle (p. ex., résistance aux changements), la formation et le support postérieur au lancement.

AUTORITÉ DES MARCHÉS FINANCIERS

GUIDELINE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY RISK MANAGEMENT

February 2020

TABLE OF CONTENTS

Preamble

This guideline is an indication of what the *Autorité des marchés financiers* (the "AMF") expects of financial institutions in terms of their legal obligation to follow sound and prudent management practices. As such, it covers the interpretation, performance and application of this obligation.

In light of this, the AMF prefers a principles-based approach to a rules-based one. Its guidelines are therefore designed to be sufficiently flexible to enable financial institutions to establish their own strategies, policies and procedures for the implementation of sound management principles and to put in place sound practices commensurate with their nature, scale, complexity and risk profile. In this regard, the guideline demonstrates ways to meet the principles it contains.

AMF Note

The AMF believes that sound and prudent management and sound commercial practices of financial institutions, and thus the AMF's prudential framework, should rest on three pillars: governance, integrated risk management and compliance (GRC).

This guideline reflects this perspective and sets out the AMF's expectations for sound and prudent information and communications technology ("ICT") risk management practices.

Scope

This guideline is intended for authorized insurers, federations of mutual companies, financial services cooperatives and legal persons belonging to a cooperative group, authorized trust companies, savings companies and other deposit institutions governed by the following statutes:

- *Insurers Act*, CQLR, c. A-32.1;[1]
- *Act respecting financial services cooperatives*, CQLR, c. 67.3;[2]
- *Trust Companies and Savings Companies Act*, CQLR, c. S-29.02;[3]
- *Deposit Institutions and Deposit Protection Act*, CQLR, c. I-13.2.2.[4]

Solely for the purposes of this guideline, the generic terms “institution” and “financial institution” are used without distinction in referring to the entities covered by the guideline.

Lastly, this guideline applies to financial institutions operating independently as well as to financial institutions operating as members of a financial group.

The standards or policies adopted by a federation with respect to financial services cooperatives and mutual insurance associations that are members of the federation should be consistent, if not convergent, with the principles of sound and prudent management set down in legislation and clarified in this guideline.

1 Sections 463 and 464.

2 Sections 565.1 and 566.

3 Sections 254 and 255.

4 Sections 42.2 and 42.3.

Effective date and updating

The effective date of this *Guideline on Information and Communications Technology Risk Management* is February 27, 2020.

With respect to legal obligation imposed on the institutions to follow sound and prudent management practices, the AMF expects each institution to adopt the principles of this guideline by developing strategies, policies and procedures commensurate with its nature, scale, complexity and risk profile.

The AMF expects financial institutions to adopt and implement the expectations in this guideline by February 27, 2021.

This guideline will be updated to take into account developments in ICT risk management and reflect observations made by the AMF in the course of its supervisory activities in relation to the financial institutions concerned.

Introduction

While the rapid pace of technological innovations has helped to transform financial institution processes and business models, such innovations are introducing significant risks at a time when institutions are becoming more and more interconnected or dependent on legacy systems[5] and external suppliers to carry out their activities.

The adoption of technological innovations is also increasing the risk of data being lost, leaked, stolen, corrupted, or accessed without authorization. Institutions are exposed to an ever-greater risk of increasingly sophisticated, frequent and difficult-to-detect cyber attacks.

Information and communications technology (ICT) risks[6] can have adverse consequences, both financial and legal, for an institution's clients and reputation.

This guideline describes the AMF's expectations with respect to ICT risk. The ultimate goal of these expectations is to strengthen the financial sector's resilience in response to this risk. In particular, these expectations are intended to ensure the development of appropriate security hygiene through the implementation of measures[7] that will help prevent a major incident and limit its impact.

Each institution is responsible for clearly understanding all its ICT risks and ensuring that they are appropriately considered in light of the institution's nature, size, complexity and risk profile. The institution is also responsible for staying current on ICT risk management best practices and adopting them to the extent that they meet its needs.

---

5 A legacy system is a piece of hardware and/or software that continues to be used in an organization despite being superseded by more modern systems. It forms part of an organized assembly of resources enabling the collection, storage, processing and distribution of information.

6 The AMF defines ICT risk as the business risk associated with the use, ownership, operation and adoption of ICT. This risk includes availability, continuity, security (including cybersecurity), change, data integrity and outsourcing risk.

7 Such measures include both basic ICT governance practices and operational measures such as the timely deployment of software security updates, the detection of unauthorized traffic on network infrastructures, the management of information access rights, the strengthening of authentication mechanisms for access to critical systems and the monitoring of malware.

1. Types of ICT risks

The AMF expects financial institutions to put in place a taxonomy that catalogues all types of ICT risks.

The taxonomy should be forward-looking and capture the technology risks that are ever-present in all financial institution processes. The taxonomy should be developed in order to facilitate the aggregation and obtain a comprehensive picture of its ICT risks. It should therefore provide a comprehensive set of ICT risks so that those involved in risk identification may consider all types of risks that could affect the institution's objectives.

Technology risk should be assessed holistically, taking into consideration both common risks and the risks of not responding appropriately to technological changes or the arrival of new or emerging technologies in order to enhance the institution's agility and ability to respond to changes over time.

In addition to operational risks derived from technology-related risks, the following strategic risks[8] can impede the achievement of the institution's objectives and should be considered:

- Technology governance risk;[9]
- Technology positioning risk;[10]
- Technology implementation risk.[11]

To guard against a false sense of security or urgency and optimally define ICT risk tolerance, the institution should, among other things:

- use clear ICT terminology and a consistent taxonomy to describe risks;
- aggregate ICT risks[12] at the level of the institution so that they are considered in combination with all the other risks that must be managed.

In developing its risk taxonomy, the financial institution should aim for a reasonable number of categories so that risks may be properly aggregated without the discrete nature of the categories becoming eroded.

---

8 These three groups of strategic risks can be described using other wording, according to the taxonomy established by the financial institution.

9 The risk that the board of directors fails to put in place the requisite elements to govern the development and implementation of its IT strategy.

10 The risk that, at the time the strategy is defined, the technology position aimed for in the industry is not adequately embedded in the business strategy, not viable or not feasible.

11 The risk that, when implementing its strategy and strategic plan, senior management fails to achieve the sought-after strategic IT objectives and related business goals.

12 ICT risks can be aggregated according to multiple dimensions (organizational units, types of ICT risks, processes, etc.).

Some of the ICT risk categories that should be considered when developing the taxonomy are information security, crisis management, outsourcing, cloud computing, business continuity, program and project management,[13] change management, ICT operations, ethics, human resources and intellectual property.

If a financial institution has an existing risk taxonomy that is used within a particular functional area, such as internal audit, it could be considered in the development of an organization-wide risk taxonomy, as it may include categories that have been proven to be applicable to the organization. Once developed, this taxonomy should be communicated to those directly involved in risk assessment and control activities so that it may be used consistently in the identification and aggregation of ICT risks.

[13] For example, risks may result from the interdependence between various projects or from the dependence of several projects on the same resources and expertise.

2. ICT governance

The AMF expects financial institutions to implement ICT governance developed using accepted sources, recommendations and standards.[14]

ICT governance should reflect changes made over time. The quality of governance practices is an important factor in maintaining market confidence. ICT governance should therefore continuously take into account good practices recognized by existing professional and international bodies and should align with the institution's business goals.

The following, in particular, should be considered in establishing ICT governance:

- understanding and acceptance by individuals and groups within the institution of responsibilities related to ICT and data use;
- assessment of ICT and ICT activities, when plans and policies are reviewed, to ensure that they align with the institution's goals, reflect good practices and meet stakeholders' needs;
- evaluation of the institution's plans to ensure that ICT will support business processes with the required capacity;
- consideration of the data life cycle in defining responsibilities;
- the extent to which ICT satisfies regulatory, legal and contractual obligations and professional and international standards;
- the way individuals behave towards others (for all stakeholders) in ICT-related practices and decisions.

The various elements of the framework established by the financial institution (strategies, policies, etc.) should consider and align already existing provisions[15] that are inherent in and relevant to the management of technology risks.

[14] E.g., OECD, G7, NIST, ISACA-Cobit and ISO.

[15] These provisions may have been defined or documented separately over the years and could contain contradictions.

2.1 Roles and responsibilities

Board of directors

In accordance with certain expectations[16] already issued by the AMF, the board should ensure, in particular, that:

- senior management promotes a corporate culture based on ethical and secure behaviour in the use of technology;
- ICT-related information is exchanged with internal and external stakeholders in order to support through documentation its understanding of needs and make judgments about the current and future design of ICT governance;
- the roles and responsibilities of the ICT function and the information security and business continuity management functions are clearly defined in establishing and maintaining ICT governance;
- support structures, roles and functions are regularly assessed to enable the development and continuous improvement of ICT governance.

In addition, the board of directors should, in accordance with section 2.2, ensure that responsibilities related to developing the IT risk framework are assigned, including through an assessment of the competencies required to fulfill those responsibilities. Moreover, it should ensure that the following individuals are assigned:

- an individual responsible[17] for the computer systems and information technology supporting the business's objectives;[18]
- a member of senior management in the second line of defence, such as a chief information security officer (CISO), or another member of senior management and in the second line of defence, to oversee the deployment of the framework ensuring information security and the physical security of the institution's technology infrastructures;
- a member of senior management in the second line of defence, such as a chief data officer (CDO), or another member of senior management in the second line of defence,[19] to oversee the approved framework for the collection, storage and use of data across the institution;
- members of senior management to be responsible for all of the various information assets and ICT risks present in the institution.

---

16 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*. September 2016.

17 Such as a chief technology officer (CTO) or chief information officer (CIO).

18 This person is responsible for, among other things, execution of the ICT strategic plans, application of technology-related processes (operations, architecture, risk management, etc.) and development of the institution's technology infrastructures and also presents technology proposals and status reports on the implementation of ICT-related strategies and frameworks to the board.

19 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*. September 2016.

The board of directors should obtain updates on the scenarios considered in developing and testing disaster recovery and business continuity plans so that it understands the objectives in maintaining the availability of critical ICT operations and systems. In addition, it should have a thorough understanding of the escalation processes for security breaches or incidents, including when it should be notified.

Senior management

In addition to the roles and responsibilities that normally devolve to it,[20] senior management should, in particular:

- establish an ICT function that operates under the oversight of a second-line-of-defence control function;
- clearly delineate the responsibilities of the information security function to ensure its independence and objectivity by, in particular, segregating it from ICT operational processes and implementing compensating controls where needed. This function should not be responsible for any internal audits;
- define roles and responsibilities for maintenance and dissemination, within the institution, of the documentation and information required for informed stakeholder decision-making regarding ICT;
- manage the relationship between the services provided by the ICT function and the business units in a formal and transparent manner while using a common language to ensure the achievement of strategic objectives;
- establish and maintain an enterprise architecture consisting of the processes, information, data and layers of application, technology and security architectures;
- identify the individuals responsible or accountable for ICT risk management and those who must be consulted or informed;
- working with the compliance and internal audit functions, regularly evaluate the control environment (self-evaluations, assurance reviews, identification of control deficiencies, compliance of ICT-backed processes with laws,[21] regulations and contractual obligations, etc.);
- periodically review non-compliance (including exceptions approved by the board of directors) with the frameworks established for ICT risk.[22]

In establishing the ICT strategy, senior management should, in particular:

---

[20] AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*. September 2016.

[21] Particularly the Act respecting the protection of personal information in the private sector and the Act to establish a legal framework for information technology.

[22] Exceptions should be reviewed periodically in light of the changing nature of ICT and inherent threats to ensure that they remain at an acceptable level and will be corrected in a timely manner.

- develop a holistic view of the business environments and the ICT environments (current and future) in order to identify the required transformation initiatives;
- define and document how the ICT, technology architecture, organizational structure and key dependencies with partners and suppliers will evolve in order to support its business strategy;
- properly align ICT strategic plans and business strategies on an ongoing basis while taking into account current and future ICT capacity;
- consider using technological innovations in strategic planning and enterprise architecture decisions;
- define objectives to maintain the institution's capacity to anticipate, detect and recover from ICT incidents[23] in order to ensure ICT system resilience.

Moreover, in terms of the institution's information security, the designated member of senior management should, in particular:

- develop, document and disseminate an information security policy that defines the principles and rules for safeguarding the confidentiality, integrity and availability of the information of the institution and its clients;
- define clear information security objectives for systems, ICT services, processes and people;
- apply the information security policy to all the institution's activities and include information handled by external stakeholders within the institution's scope;[24]
- deploy controls for information assets[25] that are proportional to the criticality and sensitivity of those assets;
- do systematic testing to ensure that the controls in place are effective;
- deploy information security training and awareness programs;
- produce security performance indicators covering areas such as the business impacts (for the benefit of non-technical personnel) and effectiveness of security controls.

Senior management should report on the following, in particular:

---

[23] An ICT, cyber or information security incident normally occurs when an unplanned disruption in the delivery of ICT services or a security breach in a system compromises the availability, integrity or confidentiality of ICT data or systems.

[24] For external stakeholders, it is acceptable here to establish appropriate agreements regarding the secure treatment of information.

[25] Information assets (data, hardware and software) are not limited to those held by the institution. They also include information assets entrusted or delivered by clients or third parties.

- the objectives and indicators gathered in relation to ICT and its processes on a systematic and timely basis;
- the results of monitoring done with respect to ICT-related best practices and standards in development, at the national and international levels, and the potential impacts of such best practices and standards on the institution's activities;
- key ICT issues, including significant ICT projects, priorities and incidents, as well as regular reports on ICT risk.

Other roles

The institution's risk management function[26] should oversee its ICT function and assume responsibility for monitoring all ICT risks (i.e., both operational and strategic risks and risks arising from ICT-related innovations[27]). This function should also rigorously monitor material and emerging ICT risks.

The objective assurance expected from the internal audit function regarding the sufficiency and efficacy of ICT governance should cover, among other things, the efficiency and effectiveness of ICT operations, the safeguarding of information assets, and the reliability and integrity of their reporting processes.

The institution's internal audit activities should include a review of the design and effectiveness of the information security controls, including the controls maintained by external parties. Internal audit should also review the assurances provided by an external party when they have the potential to adversely affect the institution, its clients or other stakeholders.

Other roles defined across the institution—such as the person in charge of business management and the person in charge of human resources—have an effect on ICT risk governance and management. Although not directly involved in ICT risk governance and management, they are nonetheless stakeholders and should be considered in defining roles and responsibilities.

[26] The chief risk officer (CRO) or a designated member of senior management must be able to synthesize, explain in plain language and communicate ICT-related information effectively to various audiences.

[27] For example, risks of bias or unethical use of big data technologies and artificial intelligence.

2.2 Integrity and competency

In accordance with the expectations[28] already issued by the AMF, effective and efficient governance, which includes information and communications technology, requires decision-making bodies to have an appropriate level of expertise, professional qualifications, knowledge or experience.

The members of the decision-making bodies and the established governance mechanisms (e.g., audit, risk management and ICT management committees) should have a knowledge and understanding of ICT use, future trends and directions and have sufficient authority to fulfil their respective responsibilities.

When evaluating the competency of members of decision-making bodies, an aptitude and knowledge grid with ICT-related criteria should be developed, kept up to date and applied on a regular basis—or more frequently, if necessary—for individuals in strategic positions related to ICT governance and risk management.

The institution should therefore periodically take stock of all current ICT competencies within the institution and those needed to carry out strategies and achieve objectives.

To minimize the risk of having insufficient ICT expertise in key positions, a formal process for acquiring competencies pertaining to ICT-related strategic issues should be developed.

Similarly, a comprehensive ICT security awareness training program should be implemented for all personnel and should, at a minimum, take into account the current threat landscape (including cyber threats) and threat impacts, laws, regulations, the frameworks established by the institution and the responsibilities of personnel in safeguarding information assets.

The training program should be updated and renewed regularly for all of the institution's personnel and for any service provider with access to information assets.

Moreover, the institution should conduct regular security screening of human resources (including consultants, partners and suppliers) before they are hired, over the course of their employment and after their employment ends, where those human resources have access to ICT systems and data and may expose the institution to data theft, sabotage, fraud and other ICT risks.

2.3 ICT documentation

The institution's frameworks should clarify the roles and responsibilities of decision-making bodies and operating units in establishing, maintaining and securely consulting documentation and information enabling stakeholders to make informed decisions about ICT.

---

[28] *Guideline Governing Integrity and Competency Criteria*, June 2012.

This documentation should not be static but should, instead, evolve over time. As with the business, an institution's ICT constantly changes based on acquisitions, updates and external influences. The documentation should contain sufficient aggregated information to facilitate decision-making concerning the ICT strategy.

In particular, the documentation should consolidate information that reflects the status of its ICT strategy, current and target architecture, strategic ICT risks and objectives, ICT plans and current plan status, ICT risk impact statements and existing processes and structures for ICT risk management, development methodology and operation processes.

In addition, the strategic documents derived from best practices that should be considered by the financial institution include:

- a description of the situations faced by the institution and its business lines and support functions;
- a description of the impact of ICT risks on business strategies;
- the ICT risk register and ICT risk and control matrix;
- ICT operating models and processes.

While the documentation may be prepared and maintained by various components of the institution, it should be reviewed by senior management and the key elements[29] should be approved by the board of directors.

[29] The key elements presented to the board of directors should be worded so the board members can easily assess them in order to make an informed decision.

3. ICT risk management

The AMF expects the financial institution to consider all activities necessary to the preparation, treatment and monitoring required in managing ICT risks.

The development of strategies, policies and procedures enabling ICT risk identification, assessment, quantification, control and monitoring should take into account the preparation, treatment and monitoring activities that need to be carried out to lessen any harm that might occur in the first hours of an actual crisis. For example, all measures planned by the institution, including response and recovery measures, should be subjected to stress testing. In addition, the external stakeholders and specialists required by those measures should be prequalified and contractual terms and conditions should be pre-established.

In implementing robust ICT risk management practices across the institution, the latter should also take into account the participation of external stakeholders to ensure that accurate information relevant to risk management is distributed and used by everyone.

The ICT risk management framework should make it possible to establish and maintain a holistic view of ICT risks, including relationships and dependencies between people, end-to-end business processes, the institution's functions, ICT systems and assets supporting such processes and people. By taking stock of roles, processes and business functions, it should be possible to identify their relative importance and their interdependencies with the ICT risks.

3.1 Preparation

The selection of preparatory measures to manage ICT risks should, in particular, help to safeguard sensitive data (such as client information) against disclosure, leaks or unauthorized access. They should also contribute to ICT environment resilience. These measures should cover, among other things, access controls, authentication, data integrity and confidentiality, activity recording and security event monitoring.[30]

During preparations, the financial institution should understand the impact of technology risk on operations, including mission, functions or reputation, as well as on assets and individuals. Consequently, the integrated approach to managing ICT risk should be applied institution-wide and should enable the institution to, among other things:

- align all risk assessment tools and scales used and ensure consistent, agreed-upon and transparent use;
- use a rigorous process to periodically identify information assets and their vulnerabilities in order to appropriately relate risks to assets in a holistic manner.

[30] The appendix covers various additional measures to be considered and that have proven useful in managing the risks related to information security, ICT operations, outsourcing and ICT transformation projects.

The same applies to internal and external threats and potential likelihoods and business impacts in order to determine the level of risk and establish appropriate action plans. This asset management process should also cover data, personnel and the ICT systems (including the various hardware and software components of those systems) and the premises housing them;

- use a classification framework[31] enabling the criticality of data and information assets (including those managed by external stakeholders) to be defined, minimally, according to their availability, integrity and confidentiality requirements;
- use ICT incident management processes with appropriate resumption and recovery objectives to ensure proactive risk management;
- ensure proper and timely monitoring of activities to mitigate the risks recorded in the ICT risk register;
- monitor the effectiveness of mitigation measures, along with the number of reported incidents in order to correct them when necessary;
- consider financial, legal, regulatory, operational, client-related and reputational factors in assessing ICT risk.

In addition to assessing the ICT risk inherent in its activities, products or services (including, in particular, cyber risk), the financial institution should consider what this risk represents for its partners, suppliers and clients and also for other financial sector participants, when relevant.

The financial institution should assess ICT risks at planned intervals, when significant changes are expected or occur and when significant operational and security risks materialize, taking into account the established criteria. ICT risk assessment should be part of an ongoing systematic and cyclical process.

Furthermore, financial institutions should use methods enabling them to make the link between ICT risk scenarios and their potential impact on information assets and business processes so that all stakeholders[32] understand the effects of adverse events related to information and communications technology.

The financial institution should:

- identify all potential individual points of failure in the ICT systems and network architectures to ensure that appropriate measures are taken to mitigate disruption risks;

---

[31] This classification should reflect the degree to which an information security incident affecting an information asset has the potential to adversely affect the institution and its clients or other stakeholders.

[32] ICT risk assessments require the outcomes to be expressed in clear and unambiguous business terms. Effective ICT risk management also requires the business and technology areas to share a common understanding of the risks that should be managed and the underlying reasons for them. ICT risk management stakeholders should have the ability to understand and express how adverse events or incidents may affect the institution's business objectives.

- carry out end-to-end business impact analyses for critical business processes to ensure that disaster recovery and business continuity plans appropriately prioritize the institution's critical operations during ICT systems recovery;
- consider a plausible[33] set of disaster events and scenarios, including cybersecurity events, in recovery and continuity plan planning;
- include provisions for recovery within specified time frames and periodic testing in the data backup strategy to ensure procedure effectiveness.

Processes and procedures ensuring ICT system resilience should continually take into account rapidly evolving threats. Such processes and procedures should enable containment of the impacts of potential security incidents and help accelerate a return to normal operations. They include response and recovery plan planning, communications, analysis, mitigation and continuous improvement.

To avoid increased exposure to security and stability risks, the financial institution should establish plans for the timely replacement of its ICT hardware and software before the end-of-support dates indicated by their suppliers.

3.2 Treatment

In treating ICT risks, the financial institution should, in particular:

- determine all controls that are necessary to implement the treatment options for the identified risks;
- compare the controls so determined against existing best practices and verify that no required controls have been omitted;
- produce a statement containing the necessary controls and the justification for inclusions or exclusions of controls;
- maintain and use security frameworks and the processes and procedures arising from it to manage information systems and assets;
- maintain and repair ICT system components in accordance with the institution's established frameworks.

In addition, the financial institution should:

- continuously detect abnormal network infrastructure, ICT system and information asset activity in order to understand the evolution and potential impacts of undesirable events and verify the effectiveness of protection measures;

[33] The institution should consider, in particular, low-likelihood scenarios that have high financial or non-financial (reputation, compliance, etc.) impacts.

- test and maintain the aforementioned detection processes to ensure appropriate and timely knowledge of abnormal events;

- execute and maintain response and recovery processes and procedures in order to ensure a response to detected cybersecurity incidents and the restoration of systems or assets;

- receive, analyze and address the vulnerabilities identified by internal or external sources (in-house testing, bulletins or specialized security research);

- perform and review planned activities to prevent the expansion of an event to other ICT systems, mitigate its effects and resolve the incident.

Access to data retrieval and extraction tools[34] should also undergo a risk assessment and should, in order to protect against potential data leaks, be authorized only if there is an actual business.

The financial institution should demonstrate that it assesses the risks related to ongoing maintenance of its legacy systems and that adequate controls are in place to effectively manage the risks of these technologies. If the legacy systems support critical operations, the financial institution should have a strategy in place for managing ageing infrastructure.

Applications developed or acquired by end-users to automate their operations, including applications accessible via the Internet, should be approved by the relevant business areas and the institution's ICT function. Such applications should be taken into account in the information asset management and ICT risk management processes. The financial institution should ensure that appropriate safeguards against data loss or leaks and the exposure to malicious viruses linked to such applications are put in place. In addition, the financial institution should implement controls to monitor and detect the unauthorized use of such applications.[35]

In risk and control assessment, protection mechanisms may include risk avoidance or elimination where the institution does not engage in a specific business activity. They may also include risk mitigation through controls or risk sharing or transfer.

The financial institution should regularly assess the adequacy of its resources in light of its risk appetite by means of stress tests for all material and potential risks, categorized by likelihood and impact (e.g., ICT risks, including cyber risks).

As part of the regular maintenance of its register of known and potential ICT risks, the institution should clearly describe, in particular, their attributes and related control

[34] For example, the use of portable computer devices (tablets, cellphones, etc.), storage devices (USB keys, portable hard drives, etc.), e-mail, instant messaging and printed copies.

[35] The term **Shadow IT** (or sometimes **Rogue IT**) is also used to describe unapproved ICT systems implemented within organizations.

activities in sufficient detail. The ICT risk register should be updated on a forward-looking basis and the adequacy of controls should be regularly assessed.

3.3 Follow-up

The AMF expects the financial institution to align its disclosure and transparency practices with previously issued expectations,[36] generally accepted good practices and applicable legislation by, among other things, implementing the mechanisms needed to promptly notify internal and external stakeholders, including the AMF, when there is an operational incident.

The processes and procedures put in place by the financial institution for incident management should allow action to be taken and services to be resumed as quickly as possible when ICT-related incidents occur. In particular, they should:

- coordinate required responses and recovery activities after internal and external stakeholders have been notified;
- help minimize the impacts on clients;
- report incidents according to pre-determined criteria;
- share useful information contributing to enhanced information security;
- manage public relations and the impact on the institution's reputation.

In addition, the financial institution should conduct specific analyses following a major incident to improve its response and recovery plans. The institution should, in particular:

- explore the data gathered in its infrastructures by its detection systems;
- identify and measure the incident's impacts;
- mitigate or accept and document the risk for newly identified vulnerabilities;
- identify lessons learned when resolving the incident and communicate them to internal stakeholders;
- receive, analyze and respond to the vulnerabilities identified by internal or external sources (in-house testing, bulletins or specialized security research).

Based on lessons learned, observations and decisions made when managing ICT risks, the financial institution should review its strategies—particularly those developed during its preparatory activities (Section 3.1). The review should be guided by clear assessment

[36] AUTORITÉ DES MARCHÉS FINANCIERS. *Operational Risk Management Guideline,* December 2016.

objectives, established expectations and methodologies disseminated to stakeholders, and reports containing clear conclusions and tangible corrective actions.

APPENDIX - Complementary standards to the AMF's guidelines

The AMF expects the implementation of sound and prudent management practices, set out in all its guidelines, to take into account specific proven and generally accepted practices related to ICT.

ICT risk management depends on the financial institution adopting the expectations described in various AMF guidelines, including those on governance, integrated risk management and compliance. However, ICT risk management also depends on the expectations described in the previous sections of this guideline and the implementation of a number of ICT-specific practices.

In this perspective, the following practices[37] contribute to the establishment of a holistic approach. Applying them helps to prevent and mitigate ICT risks such as those related to the use and operation of ICT.

ICT security

The financial institution must implement robust security mechanisms enabling it to ensure the delivery of critical services and the identification of ICT incidents.

Mechanisms to consider include identity and access management, training and awareness, network segregation and protection of network integrity, data security, protection of endpoint devices, verification of software and microcode integrity, information protection processes and technological protection solutions contributing to system and information asset resilience.[38] Similarly, event and anomaly detection, continuous information system monitoring and detection process monitoring should be considered.

The financial institution should define a process to gather, secure, store, consolidate, treat and review ICT event logs to facilitate security monitoring operations. The latter should include firewall, application, operating system and authentication event logs.

The financial institution should ensure that physical and logical access[39] to information assets and associated resources is limited to authorized users, processes and devices and to activities authorized in accordance with a rigorous and predefined process.

Access rights should be granted on a "need to know," "least privilege" or "segregation of duties" basis, only to authorized personnel and in such a manner as to prevent large data sets from being improperly accessed and security controls from being bypassed.

---

[37] The topics discussed in this appendix are drawn from best practices recommended by national or international organizations, including the NIST, Cobit, the G7 and the ISO.

[38] E.g., firewalls, network access controls, intrusion detection and prevention tools, anti-virus software, encryption and log monitoring and analysis tools.

[39] This includes both regular or high-privilege user access and remote access.

The financial institution should limit the use of generic or shared access accounts and ensure that ICT system users can be identified. Exceptions should be justified, compiled and documented.

The financial institution should subject its information security controls to various types of periodic independent assessments, tests and reviews as well as penetration testing[40] and red team exercises.[41]

In assessing information security risks, the financial institution should, among other things:

- identify information security risks related to the loss of confidentiality, integrity and availability of information, and name the persons responsible for the risks;
- establish and maintain information security risk criteria, including risk acceptance criteria and criteria for assessing information security risks.

The financial institution should actively maintain the security of its information while taking into account threats and vulnerabilities, including those resulting from changes to its information assets, the stage they are at in their life cycle[42] and its business environment.

There should be adequate segregation between operational security and risk management duties in developing appropriate ICT information security for the financial institution's ICT systems.

ICT operations

Technological innovations, such as cloud computing, the Internet of things and metadata, have a significant impact on the ICT function (particularly at the level of the processes that must be adapted, including capacity management and security management, and knowledge that should be enhanced to fit new ICT systems).
In this context, it is important for ICT operations personnel to have the information and tools they need to detect any potential problems in processing centre operations, networks, IT security infrastructures and user support. Such tools and information should, among other things, assist in:

[40] Penetration testing and vulnerability assessments produce an image of a computer system in a specific state and at a specific time. This image is limited to the portions of the system that are tested during penetration attempts. In this perspective, penetration testing and vulnerability assessments are not substitutes for an ICT risk assessment.

[41] Red team exercises simulate targeted attacks to test the institution's detection and response capabilities. The institution's control processes for people and technology are reviewed throughout the exercise by simulating the objectives and actions of an attacker.

[42] This refers to the process from information asset planning and design through to decommissioning and disposal.

- preparing an exhaustive inventory of information processing hardware, resources, locations, etc.;
- prioritizing ICT risk mitigation efforts;
- identifying mitigation controls such as policies and procedures for physical and logical security; data, personnel and change management; information distribution and transmission; backups; and user support;
- performance, capacity planning and control self-assessment monitoring and reporting.

The financial institution should implement a process for managing the configurations of the hardware and software components of its information systems so as to have visibility and effective and secure control of its systems.

The financial institution should minimize business disruption risk by establishing appropriate processes to manage changes affecting ICT equipment (hardware and software) and procedures involved in the development, delivery, support and maintenance of ICT production systems. These processes should provide for, among other things:

- pre-implementation security risk and impact assessments (particularly in relation to other information assets);
- sufficient testing for the new ICT and planned upgrades and patches to the existing systems prior to rollout;
- requirements and approval levels needed for the change rollout;
- clearly defined procedures for evaluating, approving and implementing urgent changes, including approvers, in order to reduce production environment security and stability risks;
- strict segregation of duties in the software updating process in order to restrict the ability of a single person to develop and compile software code and deploy it from a development environment to a production environment;
- activation of activity recording in the audit and security logs.

To reduce business interruption risk from the exploitation of software bugs or vulnerabilities, the institution should establish a framework of secure practices and standards for programming, source code reviews and application security testing for its ICT systems. Any information and ICT system availability, integrity and confidentiality issues identified in applying such practices should be compiled, monitored and corrected.

The financial institution should ensure that processes are deployed to assess and manage all operational risks associated with the use, ownership, operation and adoption of ICT. The institution should, in particular:

- implement an appropriate ICT operational structure to support the institution's business activities;
- review and understand how the existing systems support the related business processes;
- support an appropriate control environment through the identification, assessment, management and monitoring of ICT operational risks based on precepts similar to those set out in the Operational Risk Management Guideline;
- create a secure physical and logical operational environment;
- provide for operational continuity and resilience;
- provide for appropriate selection, staffing, replacement and training of ICT personnel.

Outsourcing and cloud computing

Outsourcing does not necessarily reduce ITC-related risks. It can expose the institution to increased security, operational performance and business continuity risks if poorly managed. Responsibility for properly managing those risks continues to rest with the institution. The institution should therefore identify the ICT strategic risks involved in outsourcing initiatives, implement an effective risk program for managing such risks, and monitor the risks stemming from any outsourcing arrangement.

In accordance with the expectations[43] issued by the AMF, the financial institution remains responsible for recovering its operations after a disaster affecting its suppliers when its ICT strategy is outsourced with cloud computing. It should also consider ICT risk, particularly cyber risk, when assessing the level of experience and expertise required to perform the outsourced activity and manage the outsourcing relationship.

The financial institution should ensure the effectiveness of its ICT risk management framework when outsourcing agreements are entered into with external service providers or members of its group.

The increasing use by financial institutions of cloud computing services carries many advantages (economies of scale, access to good practices, agility, etc.). The distributed nature of such services may also enhance resilience to disasters or service disruptions. The AMF considers cloud computing services to be a form of outsourcing. Financial institutions should therefore refer to the AMF's expectations in its *Outsourcing Risk Management Guideline*.

The financial institution should have a clear understanding of the typical characteristics of cloud computing services, including colocation, data amalgamation and a strong propensity for computer processing to be performed at multiple or distributed sites. The

43 *Outsourcing Risk Management Guideline,* 2010.

institution should consider taking actions to identify and manage the risks associated with data access, confidentiality, integrity, sovereignty, regulatory compliance and auditing. In particular, the financial institution should satisfy itself that the service provider has the ability to identify and segregate client data through robust physical and logical controls. The financial institution should also keep all information relevant to the management of its data-related risks (e.g., nature, sensitivity and location(s) of data processing, storage and traffic) in its centralized list of material outsourcing arrangements.

In the specific context of outsourcing and cloud computing, the financial institution should, in particular:

- contractually secure its right to audit (and the right to audit of the relevant authorities, if applicable) and its right to access the premises of the cloud computing supplier;
- ensure that data and the location of computer processing are secure through the use of appropriate controls[44] (established using a risk-based approach) such as encryption technologies for data in transit, in memory and at rest;
- mitigate supply chain outsourcing risks when suppliers outsource certain activities to other suppliers;
- develop appropriate contingency plans and exit strategies enabling the institution to terminate any contractual agreement without any disruption in service delivery or any impact on regulatory compliance or the continuity and quality of ICT services provided to clients;
- monitor the development of potential concentration risk if the delivery of critical services depends on a small number of service providers;
- monitor and obtain assurance of supplier compliance with security objectives and measures and performance expectations.

Given the number of suppliers and the variety of potential impacts that outsourcing and cloud computing can have on financial institutions, strict controls should be put into place. Cybersecurity should not be considered only at the level of major suppliers or critical service providers. Certain other suppliers could, in fact, be a weak link in the security processes.

While using the services of certain third parties may not constitute a form of outsourcing, many of those services are delivered using ICT or involve information that is potentially confidential. Such third parties may also be exposed to security breaches. The financial institution should assess and appropriately manage the confidentiality breach, integrity

[44] When establishing contractual and service level agreements, the institution should, among other things, consider using information security objectives and measures, applying its own definition of the data life cycle and determining its security monitoring and data encryption needs.

breach and availability breach risks associated with the information processed by such third parties.

Change projects and programs

The implementation of any ICT strategy requires a formal start-up of technology change management programs. Such programs require resources and need to be properly managed and monitored. They also introduce new risks that have to be mitigated. These risks include, among other things, client service disruptions, loss of competitive advantages, negative reputational impact and delays in implementing critical and strategic products or processes.

The financial institutions should establish a project management framework that will ensure the ongoing use of management practices to deliver results that meet business and security needs and objectives. Risk management under the framework should allow the related risks to be identified, assessed, managed and monitored throughout a project's life cycle.

This management framework should cover the practices needed to manage a project's entire life cycle. It should also enable the development of the comprehensive ICT project plans required to implement the strategies. These project plans should clearly define the project scope, cost-benefit and feasibility analyses, activities, deliverables and key milestones, and the roles and responsibilities of the resources needed for each project phase.

When projects relate specifically to the acquisition, development or modification of new or existing ICT systems, the financial institution should ensure that the processes, procedures and controls in its framework adhere to the security-by-design principle to ensure that a reliable, attack-resilient ICT system is implemented.

The financial institution should standardize its project management methodology and support it with tools. It should clearly define the ICT system development life cycle, which consists of various steps—including the identification of information security needs—that must be completed in sequence so that business needs can be translated into systems or applications and those systems and applications can be properly maintained.

In addition, the institution should manage project-generated structure- and process-level changes, including informal and intangible aspects (e.g., perceived impact and changes to work habits), communications, organizational readiness (e.g., resistance to change), training and post-launch support.

DÉCISION N° 2020-PDG-0018

Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale

Vu le pouvoir de l'Autorité des marchés financiers (l'« Autorité ») d'établir des lignes directrices destinées à tous les assureurs autorisés, à une catégorie seulement d'entre eux ou à une fédération dont de tels assureurs sont membres, conformément à l'article 463 de la *Loi sur les assureurs*, RLRQ, c. A-32.1 (la « LA »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les coopératives de services financiers, à une catégorie seulement d'entre elles, à des caisses, à une fédération dont de telles caisses sont membres ou à toutes les personnes morales faisant partie d'un groupe coopératif, conformément à l'article 565.1 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 (la « LCSF »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les institutions de dépôts autorisées, à une catégorie d'entre elles seulement ou aux fédérations dont de telles institutions sont membres, conformément à l'article 42.2 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2 (la « LIDPD »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les sociétés de fiducie autorisées ou à une catégorie d'entre elles seulement, conformément à l'article 254 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 (la « LSFSE »);

Vu le pouvoir de l'Autorité d'établir une ligne directrice prévu aux articles 463 de la LA, 565.1 de la LCSF, 42.2 de la LIDPD et 254 de la LSFSE, qui appartient exclusivement à son président-directeur général, conformément à l'article 24 de la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1;

Vu la publication pour consultation au Bulletin de l'Autorité le 12 décembre 2019 [(2019) vol. 16, n° 49, B.A.M.F., section 5.2.1] du projet de *Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale* (la « ligne directrice »);

Vu les modifications apportées au projet de ligne directrice à la suite de cette consultation;

Vu le deuxième alinéa des articles 463 de la LA, 254 de la LSFSE et 42.2 de la LIDPD et du troisième alinéa de l'article 565.1 de la LCSF, selon lesquels l'Autorité publie à son Bulletin les lignes directrices qu'elle établit après en avoir transmis une copie au ministre des Finances (le « Ministre »);

Vu le projet de ligne directrice proposé par la Direction principale de l'encadrement des institutions financières, de la résolution et de l'assurance-dépôts et la recommandation du surintendant de l'encadrement de la solvabilité d'établir celle-ci;

En conséquence :

L'Autorité établit la *Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale*, dans les versions française et anglaise, dont le texte est annexé à la présente décision, et en autorise la publication au Bulletin après en avoir transmis une copie au Ministre.

La *Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale* prend effet le 1er mars 2020.

Fait le 26 février 2020.

Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale
(Loi sur les assureurs, RLRQ, c. A-32.1, articles 463 et 464)
(Loi sur les coopératives de services financiers, RLRQ, c. C-67.3, articles 565.1 et 566)
(Loi sur les institutions de dépôts et protection des dépôts, RLRQ, c. I-13.2.2, articles 42.2 et 42.3)
(Loi sur les sociétés de fiducie et les sociétés d'épargne, RLRQ, c. S-29.02, articles 254 et 255*)*

L'Autorité des marchés financiers publie la *Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale* (la « Ligne directrice »), s'appliquant aux assureurs, aux coopératives de services financiers, aux institutions de dépôts, aux sociétés de fiducie, et aux sociétés d'épargne du Québec, qui font partie d'un groupe dont le montant notionnel brut moyen de l'ensemble des dérivés en cours non compensés par une contrepartie centrale pour les mois de mars, avril et mai d'une année donnée est supérieur à 12 milliards de dollars. La date de prise d'effet de la Ligne directrice est le 1er mars 2020.

La Ligne directrice est publiée ci-après et est disponible sur le site Web de l'Autorité, à l'onglet « Professionnels » sous « Assureurs » ou « Institutions de dépôt » sous la rubrique « Lignes directrices ».

Renseignements additionnels

Des renseignements additionnels peuvent être obtenus en s'adressant à :

Karim Trad
Direction de l'encadrement prudentiel des institutions financières
Autorité des marchés financiers
Téléphone : (418) 525-0337, poste 4604
Numéro sans frais : 1 877 525-0337
karim.trad@lautorite.qc.ca

Le 27 février 2020

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE EN MATIÈRE DE MARGES RELATIVES AUX DÉRIVÉS DE GRÉ À GRÉ NON COMPENSÉS PAR UNE CONTREPARTIE CENTRALE

Mars 2020

TABLE DES MATIÈRES

Introduction

Le G20 a établi des orientations en matière de marges relatives aux dérivés de gré à gré[1] non compensés par une contrepartie centrale[2] dans le cadre de la réforme déjà entamée des marchés financiers. Il avait été convenu qu'une plus grande transparence des marchés ainsi qu'un meilleur encadrement des produits et des intervenants seraient nécessaires afin d'atténuer le risque systémique induit par ces transactions.

C'est ainsi qu'un cadre mondial visant à réduire le risque généré par un éventuel défaut d'une contrepartie dans le cadre d'un dérivé de gré à gré a été publié conjointement par le Comité de Bâle sur le contrôle bancaire (le « CBCB ») et l'Organisation internationale des commissions de valeurs (l'« OICV ») en mars 2015[3].

La présente ligne directrice s'inscrit donc dans le cadre de l'invitation conjointe du CBCB et de l'OICV lancée aux différentes juridictions de communiquer des attentes concernant les meilleures pratiques en matière d'échange de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale. Les ajustements apportés aux phases d'instauration progressive effectués par le CBCB et l'OICV en juillet 2019 sont également intégrés à la présente.

---

1 Les notions de *dérivé* et de *dérivé de gré à gré* font référence à celles définies à l'article 3 de la *Loi sur les instruments dérivés*, RLRQ, c. I-14.01.

2 La notion de *contrepartie centrale* fait référence à celle de *chambre de compensation* définie à l'article 3 de la *Loi sur les instruments dérivés.*

3 Exigences de marges pour les dérivés non compensés centralement, Comité de Bâle sur le contrôle bancaire et Organisation internationale des commissions de valeurs, Mars 2015.

1. Champ d'application

La *Ligne directrice en matière de marges relatives aux dérivés de gré à gré non compensés par une contrepartie centrale* (la « ligne directrice ») énonce les attentes de l'Autorité des marchés financiers (l' « Autorité ») en matière d'échange de marge à l'égard des dérivés de gré à gré non compensés par une contrepartie centrale. Cette ligne directrice s'applique à une **institution visée** qui transige un dérivé de gré à gré non compensé par une contrepartie centrale (« dérivé visé ») avec une **contrepartie visée**.

Au sens de la présente ligne directrice, est une **institution visée** pour la période allant du 1er septembre 2021 au 31 août 2022, et pour chaque même période de douze mois subséquente, l'institution financière qui remplit les deux conditions suivantes :

1. Elle est un assureur, une coopérative de services financiers, une institution de dépôts, une société de fiducie, ou une société d'épargne du Québec, régie par une des lois suivantes (« **institution locale** »):

   - *Loi sur les assureurs,* RLRQ, c. A-32.1 ;
   - *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 ;
   - *Loi sur les institutions de dépôts et la protection des dépôts,* RLRQ, c. I-13.2.2 ;
   - *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 ;

2. Elle fait partie d'un même **groupe financier** dont le montant notionnel brut moyen de l'ensemble de ses dérivés visés en cours à la fin des mois de mars, avril et mai de cette année, est supérieur à 12 milliards de dollars.

Aux fins de la présente ligne directrice, une entité est considérée comme une entité du même **groupe financier** qu'une autre entité dans les cas suivants :

a. ses états financiers et ceux de l'autre entité sont consolidés dans des états financiers consolidés établis conformément à l'un des référentiels comptables suivants :

   i) les IFRS;

   ii) les principes comptables généralement reconnus des États-Unis d'Amérique;

b. les conditions suivantes sont réunies :

   i) ni elle, ni l'autre entité, ni aucune tierce entité n'a établi ses états financiers conformément aux normes ou aux principes visés au sous-paragraphe *i* ou *ii* ci-dessus;

   ii) si ses états financiers et ceux de l'autre entité étaient établis par elle, l'autre entité ou la tierce entité conformément aux normes ou aux principes visés au sous-paragraphe *i* ou *ii* ci-dessus, ils auraient été, au moment pertinent, obligatoirement établis de façon consolidée;

c. les deux entités sont soumises à une réglementation prudentielle faisant ensemble l'objet d'une supervision consolidée.

Le montant notionnel brut moyen d'un **groupe financier** sur une base consolidée est établi en faisant la somme du montant notionnel brut de tous les dérivés visés transigés par les différentes entités du **groupe financier** duquel est soustrait la somme du montant notionnel brut de tous les dérivés transigés entre les entités de ce même **groupe financier**.

De plus, les dérivés visés transigés entre une **institution visée** et une entité du même **groupe financier** ne sont pas couverts par la présente dans la mesure où les conditions suivantes sont réunies :

a. les deux contreparties aux dérivés visés conviennent de soustraire ceux-ci de l'application de la présente ligne directrice;

b. les deux contreparties sont encadrées par un programme de gestion centralisée du risque raisonnablement conçu pour surveiller et gérer les risques associés à tous les dérivés transigés entre elles au moyen de procédures d'évaluation, de mesure et de contrôle;

c. les modalités des dérivés visés conclus entre les deux contreparties sont documentées dans un format approprié.

Au sens de la présente ligne directrice, une **contrepartie visée** est une entité financière qui remplit la deuxième condition mentionnée à la page 4 pour être considérée comme une **institution visée**. Cependant, les entités suivantes ne sont pas considérées comme une **contrepartie visée** :

a. le gouvernement du Canada, le gouvernement d'un territoire du Canada ou le gouvernement d'un territoire étranger;

b. une société d'État dont la totalité ou la quasi-totalité de ses passifs est la responsabilité du gouvernement de son territoire de constitution;

c. une personne qui est la propriété exclusive d'un gouvernement visé au paragraphe *a* et dont la totalité ou la quasi-totalité des passifs est la responsabilité de celui-ci;

d. une municipalité, une commission scolaire, une université, un programme de services sociaux qui bénéficie du soutien financier régulier d'un gouvernement;

e. une entité *ad hoc* servant uniquement de véhicule de transfert de flux par l'émission de titres et dont la totalité ou la quasi-totalité des passifs est la responsabilité d'un gouvernement visé au paragraphe *a*;

f. la Banque du Canada ou la banque centrale d'un territoire étranger;

g. la Banque des règlements internationaux;

h. une banque multilatérale de développement[4].

De plus, ne sont pas considérées comme une **institution visée** ou une **contrepartie visée**, toutes les entités, communément appelées entités *ad hoc*, appartenant au même **groupe financier** qu'une **institution visée** ou une **contrepartie visée** lorsque les deux conditions suivantes s'appliquent :

a. leur objectif principal est l'un des suivants :

   i) financer un ou plusieurs portefeuilles d'actifs;

   ii) procurer aux investisseurs une exposition à un ensemble particulier de risques;

   iii) acquérir des actifs immobiliers ou physiques, ou y investir;

b. si leur objectif principal est celui visé au sous-paragraphe i ou ii du paragraphe a, tous leurs emprunts, y compris leurs obligations envers leur contrepartie à un dérivé, sont uniquement garantis par leurs actifs.

Aux fins de la présente ligne directrice, est considérée comme une **convention de compensation bilatérale** une entente qui prévoit les obligations pour **l'institution visée** et sa **contrepartie visée** de faire ce qui suit :

a. compenser les montants calculés de marges de variation pour les dérivés visés par ladite convention;

b. échanger la marge de variation par le dépôt de sûretés, nonobstant le fait que l'**institution visée** ou sa **contrepartie visée** puisse avoir fait défaut d'une obligation née d'un autre dérivé visé par ladite convention.

Dans le cadre d'une telle convention, l'Autorité s'attend à ce que l'**institution visée** ait un motif raisonnable de croire qu'en cas de contestation judiciaire, les tribunaux compétents ou les autorités administratives compétentes concluront que l'exposition découlant de la **convention de compensation bilatérale** correspond au montant net en vertu des lois des territoires concernés.

[4] Voir l'Annexe 2.

2. Pratiques adéquates en matière d'échange de marges

L'Autorité s'attend à ce que toute **institution visée** ait en place des pratiques adéquates en matière d'échange de marges pour tous les dérivés visés transigés avec une **contrepartie visée**, à l'exception des suivants:

- contrats à terme sur devises réglés par livraison physique;
- swaps de devises;
- transactions de change à paiement fixe, réglées par livraison physique et associées à l'échange de capital de swaps de devises.

Une **institution locale** faisant partie d'un **groupe financier** dont le montant notionnel brut moyen de l'ensemble de ses dérivés visés en cours à la fin des mois de mars, avril et mai d'une année donnée **franchit le cap des 12 milliards de dollars** acquiert le statut d'**institution visée** en date du 1er septembre de cette même année. À partir de cette date, et ce, jusqu'au 31 août de l'année suivante, la ligne directrice s'appliquera à tous les nouveaux dérivés visés transigés avec une **contrepartie visée**. Toutefois, l'Autorité ne s'attend pas à ce que les attentes en matière de marge initiale pour les dérivés visés existants soient rencontrées[5].

À l'inverse, une **institution visée** faisant partie d'un **groupe financier** dont le montant notionnel brut moyen de l'ensemble de ses dérivés visés en cours à la fin des mois de mars, avril et mai d'une année donnée **devient inférieur à 12 milliards de dollars**, perd son statut d'**institution visée**. Dès lors, la ligne directrice ne s'appliquera plus à tous les dérivés visés impliquant cette institution, peu importe la date à laquelle le dérivé visé a été transigé, et ce, tant et aussi longtemps qu'elle ne récupérera pas le statut d'**institution visée**.

Il en va de même quant au statut de **contrepartie visée**.

L'Autorité s'attend à ce qu'une **institution visée** ait signalé de manière adéquate son statut, ou tout changement par rapport à celui-ci, à sa contrepartie et qu'elle ait obtenu le statut de cette dernière avant de transiger un dérivé visé afin d'évaluer si la ligne directrice devrait s'appliquer.

Les attentes en matière de marge initiale et de marge de variation pour un dérivé visé n'ont pas à être rencontrées si les conditions suivantes sont réunies :

a. le dérivé est transigé par suite de la modification ou de la fin et du remplacement, par les contreparties à ce dérivé, de dérivés soumis à l'un des exercices suivants :

   i) un exercice multilatéral de compression de portefeuille effectué par un tiers indépendant;

[5] À cet égard, il est opportun de noter que toute modification importante apportée à un dérivé visé existant en crée un nouveau. Par exemple, une modification visant à prolonger la durée d'un dérivé visé existant sera considérée comme créatrice d'un nouveau dérivé.

ii) un exercice bilatéral de compression de portefeuille;

b. l'exercice de compression de portefeuille prévu au sous-paragraphe *i* ou *ii* du paragraphe a fait intervenir les deux contreparties qui sont les contreparties au dérivé visé;

c. les dérivés soumis à l'exercice de compression de portefeuille prévu au sous-paragraphe *i* ou *ii* du paragraphe a n'incluent pas de dérivés visés.

L'Autorité permet à une **institution visée** de se conformer aux exigences d'échange de marges applicables à sa **contrepartie visée** plutôt qu'aux attentes énoncées à la présente, dans la mesure où l'**institution visée** juge ces exigences équivalentes. Bien que l'Autorité n'entende pas valider au préalable l'équivalence, elle se réserve le droit d'en faire un examen approfondi dans le cadre d'un exercice de surveillance. L'Autorité s'attend donc à ce que l'**institution visée** documente les exigences applicables à sa contrepartie dans le cas où elle choisit de s'y conformer.

L'Autorité s'attend à ce qu'une **institution visée**, qui transige des dérivés visés, échange une marge initiale, qui est fonction de l'exposition future potentielle, et une marge de variation, qui est fonction de l'exposition courante.

L'Autorité s'attend à ce que tout montant quotidien d'échange de marge bilatérale (somme de la marge initiale due et de la marge de variation due) supérieur au montant minimal de transfert (le « MMT ») préalablement déterminé par les deux contreparties soit transféré. Le MMT déterminé ne peut excéder 750 000 dollars. Dans le cas où une **institution visée** transige un dérivé visé avec une **contrepartie visée** qui est étrangère, l'**institution visée** peut utiliser le MMT en vigueur dans le régime de la **contrepartie visée**.

2.1 Marge de variation

L'Autorité s'attend à ce que la marge de variation soit échangée, sous réserve du MMT, sur une base bilatérale et à ce qu'elle couvre intégralement l'exposition au prix du marché. Elle s'attend également à ce que la marge de variation soit calculée et réclamée dans les deux jours ouvrables qui suivent la date à laquelle le dérivé visé a été transigé, puis tous les jours par la suite.

L'Autorité s'attend à ce que la marge de variation pour les dérivés visés qui font l'objet d'une même **convention de compensation bilatérale** juridiquement exécutoire soit échangée sur une base nette. En l'absence d'une telle convention, la marge de variation devrait être échangée sur une base brute.

2.2 Marge initiale

Une **institution visée** devrait échanger avec sa **contrepartie visée** une marge initiale, sous réserve du dépassement d'un seuil de marge initiale (le « SMI ») préalablement établi par elles et n'excédant pas 75 millions de dollars. Le SMI, qui est appliqué au niveau du groupe financier de l'**institution visée**, s'applique à l'ensemble des dérivés visés avec le **groupe financier** auquel appartient la **contrepartie visée**.

L'Autorité s'attend à ce que la marge initiale soit échangée, sous réserve du MMT et du SMI, sur une base brute. Elle s'attend également à ce que la marge initiale soit calculée et réclamée dans les deux jours ouvrables qui suivent la date à laquelle le dérivé visé a été transigé, puis quotidiennement par la suite, et ce, jusqu'à la date d'échéance, d'expiration ou de fin du dérivé visé. L'**institution visée** dispose alors de deux jours ouvrables pour recevoir une ou des sûreté(s) correspondant à la marge initiale réclamée.

La marge initiale échangée peut être calculée en ayant recours à l'une des méthodes suivantes :

- le barème standardisé de marge initiale prévu à l'Annexe 1;
- un modèle quantitatif de marge initiale.

La méthode retenue devrait rester la même pour tous les dérivés visés d'une même catégorie d'actifs transigés avec une même **contrepartie visée**.

Une **institution visée** peut s'en remettre à sa **contrepartie visée** en ce qui a trait au calcul de la marge initiale à réclamer si une convention écrite juridiquement exécutoire a été conclue entre les deux contreparties selon laquelle la **contrepartie visée** doit calculer la marge initiale pour tous les dérivés visés de la même catégorie transigés entre elles.

2.2.1 Utilisation du barème standardisé de marge initiale

La marge initiale réclamée est calculée en deux étapes :

1. pour chaque dérivé visé compris dans un portefeuille soumis à une **convention de compensation bilatérale** juridiquement exécutoire, le taux de marge correspondant à sa catégorie d'actifs indiquée au barème prévu à l'Annexe 1 est multiplié par son montant notionnel brut. La somme des résultats obtenus est appelée « marge initiale brute » du portefeuille;
2. le montant de marge initiale brute est ajusté selon la formule suivante :

*Marge initiale standardisée nette = 0,4 * Marge initiale brute + 0,6 * RNB * Marge initiale brute*

Dans cette formule, le RNB correspond au coût de remplacement net divisé par le coût de remplacement brut pour les dérivés visés compris dans un portefeuille soumis à une **convention de compensation bilatérale** juridiquement exécutoire.

La marge initiale réclamée sur un portefeuille selon le barème standardisé de marge est donc le montant de la marge initiale standardisée nette.

Une **institution visée** n'est pas tenue de calculer et de réclamer la marge initiale relative à un dérivé visé pour lequel elle n'encourt aucun risque de contrepartie.

2.2.2 Utilisation d'un modèle quantitatif de marge initiale

L'utilisation d'un modèle quantitatif de marge initiale requiert le respect de plusieurs conditions préalables. Bien que l'Autorité n'entende pas préapprouver (avant utilisation) ou approuver (pendant l'utilisation) de manière systématique les modèles utilisés afin d'établir les montants de marge initiale, elle se réserve le droit d'en faire un examen approfondi dans le cadre d'un exercice de surveillance.

Toutefois, l'Autorité s'attend à ce que l'**institution visée** fasse examiner par une personne raisonnablement qualifiée et indépendante de celle ayant élaboré le modèle quantitatif de marge initiale interne afin de s'assurer qu'il respecte les attentes ayant trait à son développement qui sont énoncées ci-dessous.

De plus, l'Autorité s'attend à ce qu'un modèle quantitatif de marge initiale soit soumis à un processus de gouvernance interne qui teste régulièrement les extrants du modèle par rapport aux données de marché récentes selon le type et la complexité des dérivés considérés.

L'Autorité s'attend également à ce qu'un modèle quantitatif de marge initiale ne permette pas la compensation du montant de marge initiale à réclamer par l'**institution visée** avec le montant de marge initiale à fournir à la **contrepartie visée**, ou qu'il prenne en compte ce montant de quelque autre manière.

Une **institution visée** devrait disposer d'un processus rigoureux et bien défini pour réestimer, réévaluer et mettre à jour tout modèle quantitatif de marge initiale qu'elle développe afin qu'il demeure applicable et pertinent pour les différents types de dérivés visés. Si elle se fie au modèle d'un tiers fournisseur, y compris sa **contrepartie visée**, l'**institution visée** devrait avoir l'assurance raisonnable que les processus en place chez le tiers fournisseur font en sorte que le modèle demeure applicable et pertinent.

L'Autorité s'attend à ce que l'**institution visée** examine et révise les données ayant servi à calibrer tout modèle quantitatif de marge initiale interne au moins annuellement, et plus fréquemment si les conditions de marché le justifient.

Une **institution visée** devrait documenter adéquatement les aspects importants de tout modèle quantitatif de marge initiale interne, y compris la gestion et l'évaluation des dérivés visés auxquels il s'applique, le contrôle, la supervision et la validation du modèle de marge initiale, tout processus d'examen, ainsi que les résultats de ces derniers.

2.2.3 Attentes relatives au développement d'un modèle quantitatif de marge initiale interne

L'**institution visée** souhaitant utiliser un modèle quantitatif de marge initiale interne devrait respecter les conditions suivantes :

a. les exigences de marge initiale reposent sur une estimation de l'exposition future potentielle des dérivés visés;

b. l'exposition future potentielle d'un dérivé visé reflète une estimation de l'intervalle de confiance unilatéral de 99 % pour une variation de la valeur d'un dérivé déterminé ou d'un portefeuille de dérivés déterminés durant une période de liquidation d'au moins 10 jours;

c. toutes les données servant à calibrer le modèle reposent sur une période de données historiques pondérées également, avec une période d'observation d'au moins 1 an et d'au plus 5 ans qui comprend une période de tensions financières pour chaque grande catégorie d'actifs à laquelle le modèle est appliqué;

d. le modèle doit tenir compte des principaux risques inhérents aux dérivés visés pour lesquels la marge initiale est calculée. Les catégories de risque devraient comprendre, sans s'y limiter, le risque de change, le risque de taux d'intérêt, le risque de crédit, le risque lié aux actions et celui lié aux marchandises, le cas échéant;

e. le modèle peut s'appliquer à un portefeuille de dérivés visés, et dans ce cas, il devrait couvrir que les dérivés visés pour lesquels il s'applique et qui font l'objet d'une même **convention de compensation bilatérale** juridiquement exécutoire;

f. le modèle peut tenir compte de la diversification, de la couverture et de la compensation des risques du portefeuille de dérivés visés auquel il est appliqué si ceux-ci portent sur la même catégorie d'actifs et qu'ils font l'objet de la même **convention de compensation bilatérale** juridiquement exécutoire.

3. Sûretés

Une sûreté déposée par une **institution visée** à titre de marge initiale ne devrait pas être réutilisée par sa **contrepartie visée**.

Les sûretés suivantes sont admissibles en vue de l'échange de marge, qu'il s'agisse de la marge initiale ou de la marge de variation:

a. les espèces;

b. l'or;

c. les titres de créance notés par une agence de notation reconnue et ayant une notation de :

- au moins BB- s'ils sont émis ou garantis par le gouvernement du Canada, la Banque du Canada ou le gouvernement d'une province ou d'un territoire du Canada;
- au moins BB- s'ils sont émis par un gouvernement étranger ayant une notation d'au moins BB-;
- au moins BBB- s'ils sont émis par une personne morale;
- au moins A-3/P-3 s'ils sont à court terme;

d. les titres de capitaux propres inscrits à la cote d'une bourse reconnue;

e. les titres d'un fonds d'investissement si les conditions suivantes sont réunies:

i) le cours des titres est publié quotidiennement;

ii) le fonds d'investissement n'investit que dans les sûretés énumérées ci-dessus.

Les titres émis par la **contrepartie visée** ou une entité du même **groupe financier** ne sont pas considérés comme des sûretés admissibles.

L'Autorité s'attend à ce que les sûretés reçues à titre de marge soient conservées de manière à ce qu'en cas de défaut de la **contrepartie visée**, elles soient disponibles en temps opportun pour l'**institution visée**.

Toutes les sûretés déposées à titre de marge initiale par une **institution visée** doivent être détenues dans un ou plusieurs comptes ouverts auprès d'un dépositaire autorisé, qui sont clairement identifiés comme tels et qui sont séparés des sûretés et des biens de la **contrepartie visée** les recevant.

L'**institution visée** peut exiger un niveau de séparation plus important, soit une séparation des sûretés déposées à titre de marge initiale par d'autres **contreparties visées**.

4. Décotes

Toute sûreté reçue à titre de marge devrait faire l'objet d'une décote afin de tenir compte de la fluctuation possible de sa valeur.

En plus de cette décote, l'Autorité s'attend à ce que l'**institution visée** applique une décote supplémentaire lorsque la sûreté reçue est libellée dans une monnaie autre que la monnaie de règlement du dérivé visé à l'égard duquel elle est reçue.

L'Autorité ne s'attend pas à ce que l'**institution visée** applique une décote supplémentaire lorsque la sûreté reçue consiste en l'un des actifs suivants :

a. des espèces déposées à titre de marge de variation;

b. tout actif autre que des espèces qui remplit les conditions suivantes :

   i) il est déposé à titre de marge de variation;

   ii) il est libellé dans une monnaie prévue dans la **convention de compensation bilatérale** juridiquement exécutoire s'appliquant au dérivé visé à l'égard duquel la sûreté est reçue;

c. tout actif qui remplit les conditions suivantes :

   i) il est déposé à titre de marge initiale;

   ii) il est libellé dans la monnaie dans laquelle l'**institution visée** et sa **contrepartie visée** ont convenu par écrit d'effectuer les paiements à la fin du dérivé visé à l'égard duquel la sûreté est reçue.

L'Autorité s'attend à ce qu'une **institution visée** qui souhaite calculer la décote et, s'il y a lieu, la décote supplémentaire à appliquer à une sûreté procède selon l'une des méthodes suivantes :

a. un modèle de décote qui remplit les conditions suivantes :

   i) il est raisonnablement conçu pour couvrir une estimation de l'intervalle de confiance unilatéral de 99 % pour une variation de la valeur de la sûreté durant une période de détention de 10 jours;

   ii) il est calibré au moyen de données historiques datant d'au moins 1 an et obtenues d'une source indépendante et fiable;

b. le barème standardisé de décotes figurant à l'Annexe 3.

L'Autorité s'attend à ce que dans le cas où une **institution visée** se sert du modèle de décote d'un tiers fournisseur, y compris sa **contrepartie visée**, elle ait l'assurance raisonnable que les processus en place chez le tiers fournisseur font en sorte que le modèle de décote demeure pertinent et performant.

Toutefois, si l'**institution visée** utilise un modèle de décote interne, l'Autorité s'attend à ce qu'elle prenne les mesures suivantes :

a. elle établit, met en œuvre et maintient des politiques et des procédures raisonnablement conçues pour veiller à ce que le modèle soit vérifié régulièrement par rapport à des données historiques qui comprennent des périodes de tensions sur les marchés;

b. elle examine, au moins annuellement et plus fréquemment si les conditions de marché le justifient, les données d'essai utilisées pour calibrer le modèle et, au besoin, le recalibre;

c. elle procède de manière raisonnablement fréquente à un examen indépendant du modèle;

d. elle effectue au moins annuellement et plus fréquemment si les conditions de marché le justifient, une évaluation de l'intégrité et de la fiabilité des données utilisées dans le modèle, notamment l'exactitude et l'adéquation des données d'essai;

e. elle corrige dès que possible toute lacune importante relevée dans le modèle;

f. elle actualise les données et recalcule la décote applicable, au moins une fois tous les 3 mois, pour chaque actif détenu à titre de sûreté à l'égard d'un dérivé visé en cours et pour lequel une décote a été calculée au moyen du modèle;

g. si les conditions de marché le justifient, pour chaque sûreté reçue à titre de marge relativement à un dérivé visé en cours et pour lequel une décote a été calculée au moyen du modèle, elle actualise les données selon une période d'observation plus courte et recalcule la décote applicable.

5. Règlement des différends

L'Autorité s'attend à ce que l'**institution visée** conclue avec chaque **contrepartie visée** une convention écrite établissant des procédures rigoureuses et solides qui permettent de déterminer, de traiter et, dès que possible après détermination, de régler leurs différends portant sur la marge initiale, la marge de variation ou la décote appliquée.

L'Autorité s'attend à ce que les procédures de règlement des différends établissent ce qui suit :

a. la façon de déterminer ce qui constitue un différend;

b. la façon de régler un désaccord sur le montant de la marge initiale ou de la marge de variation à fournir;

c. la façon de régler un désaccord sur la valorisation des dérivés visés;

d. la façon de régler un désaccord sur la valorisation des sûretés;

e. la façon de régler un désaccord au sujet des décotes sur les sûretés reçues à titre de marge.

L'Autorité s'attend également à ce que l'**institution visée** avise ses instances décisionnelles de tout différend survenant avec une **contrepartie visée** au sujet d'une marge initiale, d'une marge de variation ou d'une décote appliquée qui n'est pas réglé dans un délai raisonnable, et ce, dans les cas suivants :

a. le différend est important;

b. l'**institution visée** a, avec sa **contrepartie visée**, plusieurs différends qui, pris ensemble, sont importants;

c. le différend s'inscrit dans une tendance récurrente de différends avec une ou plusieurs **contreparties visées**.

L'Autorité s'attend également à ce qu'une **institution visée** lui signale tout différend qui n'est pas réglé dans un délai raisonnable après avoir été soumis à ses instances décisionnelles.

6. Introduction des attentes pour l'échange de marges de variation et de marges initiales

Les attentes de l'Autorité relativement à l'échange de marges de variation sont effectives à compter du 1er mars 2020 et celles relatives à l'échange de marges initiales à compter du 1er septembre 2021.

Annexe 1

Barème standardisé de marge initiale

Catégorie d'actifs	**Taux de marge initiale (en % de l'exposition notionnelle)**
Crédit : échéance résiduelle de 0 à 2 ans	2
Crédit : échéance résiduelle de 2 à 5 ans	5
Crédit : échéance résiduelle de 5 ans et plus	10
Marchandises	15
Titres de capitaux propres	15
Change	6
Taux d'intérêt : échéance résiduelle de 0 à 2 ans	1
Taux d'intérêt : échéance résiduelle de 2 à 5 ans	2
Taux d'intérêt : échéance résiduelle de 5 ans et plus	4
Autres	15

Annexe 2

Liste de banques multilatérales de développement :

- Banque internationale pour la reconstruction et le développement (BIRD)
- Société financière internationale (SFI)
- Banque asiatique de développement (BAsD)
- Banque africaine de développement (BAfD)
- Banque européenne pour la reconstruction et les développements (BERD)
- Banque interaméricaine de développement (BID)
- Banque européenne d'investissement (BEI)
- Fonds européen d'investissement (FEI)
- Banque nordique d'investissement (BNI)
- Banque de développement des Caraïbes (BDC)
- Banque de développement islamique (BDI)
- Banque de développement du Conseil d'Europe (BDCE)

Annexe 3

Barème standardisé de décote

Catégorie d'actifs	Décote (en % de la valeur de marché)
Espèces dans la même monnaie	0
Titres de créance émis ou garantis par le gouvernement du Canada, la Banque du Canada ou le gouvernement d'une province ou d'un territoire du Canada, un gouvernement étranger ou une banque centrale étrangère: échéance résiduelle <1 an	0,5
Titres de créance émis ou garantis par le gouvernement du Canada, la Banque du Canada ou le gouvernement d'une province ou d'un territoire du Canada, un gouvernement étranger ou une banque centrale étrangère: échéance résiduelle entre 1 et 5 ans	2
Titres de créance émis ou garantis par le gouvernement du Canada, la Banque du Canada ou le gouvernement d'une province ou d'un territoire du Canada, un gouvernement étranger ou une banque centrale étrangère : échéance résiduelle >5 ans	4
Obligations d'entreprise/obligations sécurisées de qualité : échéance résiduelle <1 an	1
Obligations d'entreprise/obligations sécurisées de qualité : échéance résiduelle entre 1 et 5 ans	4
Obligations d'entreprise/obligations sécurisées de qualité : échéance résiduelle >5 ans	8
Actions cotées sur une bourse reconnue	15
Or	15
Décote supplémentaire sur les actifs à l'égard desquels les obligations en vertu des dérivés visés sont dans une monnaie différente de celle de la sûreté	8

AUTORITÉ DES MARCHÉS FINANCIERS

GUIDELINE ON MARGINS FOR OVER-THE-COUNTER DERIVATIVES NOT CLEARED BY A CENTRAL COUNTERPARTY

March 2020

TABLE OF CONTENTS

Introduction

The G20 provided guidance on margining for over-the-counter (OTC) derivatives[1] not cleared by a central counterparty[2] (“non-centrally cleared OTC derivatives”) as part of its ongoing financial markets reform program. It had been agreed that improved transparency in the OTC derivatives markets and further regulation of OTC derivatives and market participants would be necessary to mitigate the systemic risk posed by OTC derivatives transactions.

A global framework aimed at reducing risk caused by the potential default of an OTC derivatives counterparty was therefore published jointly by the Basel Committee on Banking Supervision (the “BCBS”) and the International Organization of Securities Commissions (”IOSCO”) in March 2015.[3]

This guideline is in response to the invitation by the BCBS and IOSCO for jurisdictions to communicate their expectations regarding best practices in respect of the exchange of margin for non-centrally cleared OTC derivatives. It incorporates the adjustments made to the implementation phases by the BCBS and IOSCO in July 2019.

1 The terms “derivative” and “over-the-counter derivative” are as defined in section 3 of the *Derivatives Act*, CQLR, c. I-14.01.

2 The term “central counterparty” refers to the definition of “clearing house” in section 3 of the *Derivatives Act*.

3 *Margin requirements for non-centrally cleared derivatives,* Basel Committee on Banking Supervision and the Board of the International Organization of Securities Commissions, March 2015.

1. Scope

The *Guideline on margins for over-the-counter derivatives not cleared by a central counterparty* (the "guideline") sets out the expectations of the Autorité des marchés financiers (the "AMF") regarding the exchange of margin for non-centrally cleared OTC derivatives ("covered derivatives"). This guideline applies to a **covered institution** that trades covered derivatives with a **covered counterparty**.

Within the meaning of this guideline, a financial institution is a **covered institution** for the period of September 1, 2021 to August 31, 2022, and for each subsequent 12-month period, if both of the following apply:

1. It is an insurer, a financial services cooperative, a deposit institution, a trust company or a Québec savings company governed by one of the following laws ("**local institution**"):

   - *Insurers Act*, CQLR, c. A-32.1;
   - *Act respecting financial services cooperatives*, CQLR, c. C-67.3;
   - *Deposit Institutions and Deposit Protection Act*, CQLR, c. I-13.2.2;
   - *Trust Companies and Savings Companies Act*, CQLR, c. S-29.02;

2. It belongs to a **financial group** whose aggregate month-end average gross notional amount of outstanding covered derivatives for the months of March, April and May of that year exceeds $12 billion.

For the purposes of this guideline, an entity (the "first entity") is an affiliated entity of another entity (the "second entity") within the same **financial group** if any of the following apply:

a. the first entity and the second entity are consolidated in consolidated financial statements prepared in accordance with:

   (i) IFRS; or

   (ii) generally accepted accounting principles in the United States of America;

b. all of the following apply:

   (i) neither the first entity's nor the second entity's financial statements, nor the financial statements of another entity, were prepared in accordance with the principles or standards specified in the above subparagraphs a*(i)* or *(ii)*;

   (ii) the first entity and the second entity would have been, at the relevant time, required to be consolidated in consolidated financial statements prepared by the first entity, the second entity or the other entity, if the consolidated financial statements were prepared in accordance with the principles or standards specified in the above subparagraphs a*(i)* or *(ii)*;

c. both entities are prudentially regulated entities supervised together on a consolidated basis.

The average gross notional amount of a **financial group** on a consolidated basis is the sum of the gross notional amount of all covered derivatives traded by the various entities of the **financial group** less the aggregate gross notional amount of derivatives traded between the entities of that **financial group**.

Covered derivatives traded between a **covered institution** and an entity of the same **financial group** are not covered by this guideline if all of the following apply:

a. both counterparties to the covered derivatives agree to exempt them from the application of this guideline;

b. both counterparties are subject to a centralized risk management program reasonably designed to assist in monitoring and managing the risks associated with all derivatives between the counterparties through evaluation, measurement and control procedures;

c. the terms of the covered derivatives between the two counterparties are documented in an appropriate format.

Within the meaning of this guideline, a **covered counterparty** is a financial entity that meets the second condition on page 4 for consideration as a **covered institution**. However, an entity is not a **covered counterparty** if the entity is any of the following:

a. the Government of Canada, the government of a jurisdiction of Canada or the government of a foreign jurisdiction;

b. a crown corporation for which the government of the jurisdiction where the crown corporation was constituted is liable for all or substantially all the liabilities of the crown corporation;

c. a person or company wholly owned by a government referred to in paragraph *a* if the government is liable for all or substantially all the liabilities of the person or company;

d. a municipality, school board, university or social service program that receives regular government financial support;

e. a special purpose entity that operates solely as a pass-through funding vehicle through the issuance of securities for which a government referred to in paragraph *a* is responsible for all or substantially all the liabilities;

f. the Bank of Canada or a central bank of a foreign jurisdiction;

g. the Bank for International Settlements;

h. a multilateral development bank.[4]

[4] See Annex 2.

Any entity, commonly known as a special purpose entity, belonging to the same **financial group** as a **covered institution** or a **covered counterparty** is not considered a **covered institution** or a **covered counterparty** if both of the following apply:

a. its primary objective is one of the following:

   (i) finance one or more asset pools;

   (ii) provide investors with exposure to a specific set of risks;

   (iii) acquire or invest in real estate or physical assets;

b. if its primary objective is the one referred to in subparagraph a(i) or (ii), all of its indebtedness, including obligations owing to its derivative counterparty, is secured solely by its assets.

For the purposes of this guideline, a **bilateral netting agreement** is an agreement that requires the **covered institution** and its **covered counterparty** to:

a. net the calculated amounts of variation margin for the covered derivatives that are subject to the **bilateral netting agreement**, and

b. exchange variation margin by delivering collateral, even if the **covered institution** or the **covered counterparty** is in default of an obligation under another derivative that is subject to the **bilateral netting agreement**.

In respect of a **bilateral netting agreement**, the AMF expects a **covered institution** to have a reasonable basis to believe that, in the event of a legal challenge, the relevant courts or administrative authorities would find the exposure under the netting agreement to be the net amount under the laws of the relevant jurisdictions.

2. Appropriate margining practices

The AMF expects all **covered institutions** to have appropriate margining practices in place for all covered derivatives traded with a **covered counterparty**, with the exception of:

- physically settled foreign exchange forwards;
- cross-currency swaps; and
- fixed physically settled foreign exchange transactions associated with the exchange of principal of cross-currency swaps.

A **local institution** belonging to a **financial group** whose aggregate month-end average gross notional amount of outstanding covered derivatives for March, April and May of a given year **exceeds $12 billion** becomes a **covered institution** as of September 1 of that year. From that date until August 31 of the following year, the guideline will apply to all new covered derivatives traded with a **covered counterparty**. However, the AMF does not expect initial margin expectations to be met for existing covered derivatives.[5]

Conversely, a **covered institution** belonging to a **financial group** whose aggregate month-end average gross notional amount of outstanding covered derivatives for March, April and May of a given year **falls below $12 billion** ceases to be a **covered institution**. From that time on, the guideline will not apply to any covered derivative involving the institution, regardless of the date on which the derivative was traded, until such time as the institution has recovered its status as a **covered institution**.

The same holds true for a **covered counterparty**.

The AMF expects a **covered institution** to adequately declare its status, or any change thereto, to its counterparty and obtain the counterparty's status before trading a covered derivative in order to determine whether the guideline should apply.

The expectations with respect to initial margin and variation margin for a covered derivative do not have to be met if all of the following apply:

a. the derivative is traded as a result of counterparties changing or terminating and replacing derivatives submitted to either of the following:

   (i) a multilateral portfolio compression exercise conducted by an independent third party; or

   (ii) a bilateral portfolio compression exercise;

b. the portfolio compression exercise referred to in subparagraph a*(i)* or *(ii)* involves both counterparties to the covered derivative;

[5] In this regard, it should be noted that any material amendment to an existing covered derivative qualifies as a new derivative. For example, any amendment that is intended to extend an existing covered derivative will be considered a new derivative.

c. the derivatives submitted to the portfolio compression exercise referred to in subparagraph a*(i)* or *(ii)* do not include a covered derivative.

The AMF permits **covered institutions** to comply with the margin exchange requirements applicable to their **covered counterparties** rather than the expectations set out in this guideline, insofar as the **covered institutions** deem those requirements to be equivalent. Although the AMF does not intend to validate the equivalence beforehand, it reserves the right to conduct an in-depth equivalence review as part of its supervisory actions. Therefore, the AMF expects **covered institutions** to document the requirements applicable to their counterparties where the **covered institutions** choose to comply with them.

The AMF expects a **covered institution** that trades covered derivatives to exchange initial margin, which is based on potential future exposure, and variation margin, which is based on current exposure.

The AMF expects any daily amount of two-way margin exchanged (sum of initial and variation margin owing) exceeding the minimum transfer amount ("MTA") previously set by both counterparties to be transferred. The applicable MTA may not exceed $750,000. If a **covered institution** trades a covered derivative with a foreign **covered counterparty**, the **covered institution** may use the MTA applicable in the jurisdiction of the **covered counterparty**.

2.1 Variation margin

The AMF expects variation margin to be exchanged, subject to the MTA, on a bilateral basis and to fully collateralize the mark-to-market exposure. It also expects variation margin to be calculated and called within two business days of the date the covered derivative was traded. Thereafter, variation margin must be calculated and called on a daily basis.

The AMF expects variation margin for covered derivatives subject to a single legally enforceable **bilateral netting agreement** to be exchanged on a net basis. Where such an agreement is not in place, variation margin must be exchanged on a gross basis.

2.2 Initial margin

A **covered institution** should exchange initial margin with its **covered counterparty**, subject to an amount in excess of an initial margin threshold ("IMT") previously set by both parties and not exceeding $75 million. The IMT, which is applied at the level of the **covered institution's** financial group, applies to all covered derivatives with the **financial group** to which the **covered counterparty** belongs.

The AMF expects initial margin to be exchanged, subject to the MTA and IMT, on a gross basis. It also expects initial margin to be calculated and called within two business days of the date the covered derivative was traded. Thereafter, initial margin must be calculated and called on a daily basis until the maturity, expiration or termination date of the covered

derivative. The **covered institution** therefore has two business days to receive the collateral corresponding to the amount of initial margin called.

The exchanged amount of initial margin may be calculated using one of the following methods:

- the standardized initial margin schedule in Annex 1;
- a quantitative initial margin model.

The choice between the two methods should be made consistently for all covered derivatives within the same asset class traded with the same **covered counterparty**.

A **covered institution** may rely on its **covered counterparty** to calculate the amount of initial margin to be called if the **covered institution** is a party to a legally enforceable written agreement with its **covered counterparty** under which the latter must calculate initial margin for all covered derivatives within the same asset class traded between them.

2.2.1 Use of the standardized initial margin schedule

The initial margin amount to be called is calculated in two steps:

1. for each covered derivative in a portfolio subject to a legally enforceable **bilateral netting agreement**, the margin rate corresponding to its asset class indicated in the schedule in Annex 1 is multiplied by its gross notional amount. The aggregate results obtained are referred to as the portfolio's "gross initial margin".
2. the gross initial margin amount is adjusted using the following formula:

*Net standardized initial margin = 0.4 * Gross initial margin + 0.6 * NGR * Gross initial margin*

Where NGR (or "net-to-gross ratio") is defined as the net replacement cost over the gross replacement cost for covered derivatives in a portfolio subject to a legally enforceable **bilateral netting agreement**.

Therefore, the amount of initial margin to be called on a portfolio according to the standardized margin schedule is the net standardized initial margin amount.

A **covered institution** is not required to calculate and call initial margin for a covered derivative for which the institution faces no counterparty risk.

2.2.2 Use of a quantitative initial margin model

Using a quantitative initial margin model requires meeting several prerequisite conditions. Although the AMF does not intend to systematically pre-approve (prior to use) or approve (during use) the models used to determine the amounts of initial margin, it reserves the right to conduct an in-depth review of the models as part of its supervisory actions.

However, the AMF expects the **covered institution** to have its internal quantitative initial margin model reviewed by a reasonably qualified person who is independent of the person who developed the model to ensure that it meets the expectations relating to model development outlined below.

The AMF also expects a quantitative initial margin model to be subject to an internal governance process that regularly tests the model's output against recent market data based on the type and complexity of the derivatives for which the model is being used.

Furthermore, the AMF expects a quantitative initial margin model to not permit any initial margin amount that may be collected by the **covered institution** to be offset by, or otherwise take into account, any initial margin that may be provided to the **covered counterparty**.

A **covered institution** should have a rigorous and well-defined process for re-estimating, re-evaluating and updating any quantitative initial margin model it develops to ensure continued applicability and relevance for the various types of covered derivatives. If it is using a model developed by a third party vendor, including its **covered counterparty**, the **covered institution** should have reasonable assurance that the vendor's processes ensure the model's continued applicability and relevance.

The AMF expects **covered institutions** to review and revise the data used to calibrate any internal quantitative initial margin model at least annually, and more frequently as market conditions warrant.

A **covered institution** should adequately document material aspects of any internal quantitative initial margin model, including the management and valuation of the covered derivatives to which it applies, the control, oversight, and validation of the initial margin model, any review processes and the results of such processes.

2.2.3 Expectations relating to the development of an internal quantitative initial margin model

Covered institutions wishing to use an internal quantitative initial margin model should meet the following conditions:

a. Initial margin requirements are based on an estimate of potential future exposure of covered derivatives;

b. The potential future exposure of a covered derivative reflects an estimate of the one-tailed 99% confidence interval for a change in value of a covered derivative or a portfolio of covered derivatives over a minimum close-out period of 10 days;

c. All data used to calibrate the model are based on an equally weighted historical observation period of at least one year and not more than five years that incorporates a period of financial stress for each broad asset class to which the model is applied;

d. The model must account for the material risks inherent in the covered derivatives for which initial margin is being calculated. The risk categories should include, but should not be limited to, foreign exchange risk, interest rate risk, credit risk, equity risk and commodity risk, as appropriate;

e. The model may apply to a portfolio of covered derivatives, in which case it should only consider the covered derivatives to which it applies and that are subject to a single legally enforceable **bilateral netting agreement**;

f. The model may account for diversification, hedging and risk offsets of the portfolio of covered derivatives to which it applies provided the derivatives are within the same asset class and are subject to the same legally enforceable **bilateral netting agreement**.

3. Collateral

Any collateral delivered by a **covered institution** as initial margin should not be re-used by its **covered counterparty**.

The following collateral instruments are eligible for the exchange of margin (both variation and initial margin):

a. cash;

b. gold;

c. debt securities rated by a recognized rating agency where these are either:

- at least BB- when issued by or guaranteed by the Government of Canada, the Bank of Canada or the government of a province or territory of Canada;
- at least BB- when issued by a foreign government with a credit rating of at least BB-;
- at least BBB- when issued by a corporate entity;
- at least A-3/P-3 for short-term debt instruments.

d. equities listed on a recognized exchange; and

e. securities of an investment fund if:

(i) a price for the securities is publicly quoted daily, and

(ii) the investment fund is limited to investing in the above listed instruments.

Securities issued by the **covered counterparty** or by any entity within the same **financial group** are not considered eligible collateral.

The AMF expects collateral received as margin to be held in such a way as to ensure that it is available in a timely manner to the **covered institution** in the event of the **covered counterparty**'s default.

All collateral deposited as initial margin by a **covered institution** must be held in one or more accounts at a permitted depository that are clearly identified as holding collateral and that are segregated from the **covered counterparty**'s collateral and property.

The **covered institution** may require a further level of segregation, i.e., segregation from the collateral deposited as initial margin by other **covered counterparties**.

4. Haircuts

Any collateral received as margin should be haircutted to account for potential changes in its value.

In addition to this haircut, the AMF expects a **covered institution** to apply an additional haircut where the collateral received is denominated in a currency other than the currency of settlement for the covered derivative for which the collateral is received.

The AMF does not expect a **covered institution** to apply an additional haircut where the collateral received is any of the following:

a. cash posted for variation margin;

b. an asset other than cash that is:

   (i) posted for variation margin, and

   (ii) denominated in the currency agreed upon in the legally enforceable **bilateral netting agreement** that applies to the covered derivative for which the collateral is received;

c. any asset that is:

   (i) posted for initial margin, and

   (ii) denominated in the currency for which payments will be made upon the termination of the covered derivative for which the collateral is received as agreed upon in writing between the **covered institution** and its **covered counterparty**.

The AMF expects a **covered institution** that wants to calculate the haircut and, if applicable, the additional haircut on the collateral, to use either of the following:

a. a haircut model that is:

   (i) reasonably designed to cover an estimate of the one-tailed 99% confidence interval for a change in value of the collateral over a 10-day holding period, and

   (ii) calibrated using historical data of not less than one year obtained from an independent and reliable source;

b. the standardized haircut schedule in Annex 3.

Where a **covered institution** uses the haircut model of a third party vendor, including its **covered counterparty**, the AMF expects the **covered institution** to have reasonable assurance that the third party vendor's processes ensure the haircut model's continued relevance and efficiency.

However, if the **covered institution** uses an internal haircut model, the AMF expects it to:

a. establish, implement and maintain policies and procedures reasonably designed to ensure that the haircut model is tested regularly against historical data that includes stressed market conditions;

b. at least annually and more frequently as market conditions warrant, revise the test data used to calibrate the haircut model and, if appropriate, recalibrate the model;

c. on a reasonably frequent basis, conduct an independent review of the haircut model;

d. at least annually and more frequently as market conditions warrant, conduct an assessment on the integrity and reliability of the data used in the model, including the accuracy and appropriateness of the test data used;

e. as soon as practicable, rectify any material deficiencies identified in the haircut model;

f. at least once every three months, update the data and recalculate the applicable haircut for each asset that is held as collateral in respect of an outstanding covered derivative and for which a haircut was calculated using the haircut model;

g. as market conditions warrant, for collateral received as margin in respect of an outstanding covered derivative for which a haircut was calculated using the haircut model, update the data using a shorter observation period and recalculate the applicable haircut.

5. Dispute resolution

The AMF expects a **covered institution** to have a written agreement with each **covered counterparty** that sets out sound and rigorous procedures for identifying, processing and, as soon as practicable after identifying, resolving a dispute between the **covered institution** and the **covered counterparty** relating to initial margin, variation margin or the applied haircut.

The AMF expects the dispute resolution procedures to establish all of the following:

a. how to determine what is considered a dispute;

b. how to settle a disagreement on the amount of initial margin or variation margin to be provided;

c. how to settle a disagreement on the valuation of a covered derivative;

d. how to settle a disagreement on the valuation of the collateral;

e. how to settle a disagreement in relation to a haircut on collateral received as margin.

The AMF also expects a **covered institution** to notify its decision-making bodies of a dispute with a **covered counterparty** relating to initial margin, variation margin or an applied haircut that has not been resolved within a reasonable period of time, if any of the following apply:

a. the dispute is material;

b. the **covered institution** has more than one dispute with its **covered counterparty** and, together, those disputes are material;

c. the dispute is part of a pattern of disputes involving one or more **covered counterparties**.

The AMF further expects a **covered institution** to notify it of any dispute that has not been resolved within a reasonable period of time after the **covered institution** escalated the dispute to its decision-making bodies.

6. Implementation of expectations for the exchange of variation margin and initial margin

The effective dates of the AMF's expectations in respect of the exchange of variation margin and initial margin are March 1, 2020 and September 1, 2021, respectively.

Annex 1

Standardized initial margin schedule

Asset class	**Initial margin (% of notional exposure)**
Credit: residual maturity of 0–2 years	2
Credit: residual maturity of 2–5 years	5
Credit: residual maturity of 5+ years	10
Commodity	15
Equity	15
Foreign exchange	6
Interest rate: residual maturity of 0–2 years	1
Interest rate: residual maturity of 2–5 years	2
Interest rate: residual maturity of 5+ years	4
Other	15

Annex 2

List of multilateral development banks

- International Bank for Reconstruction and Development (IBRD)
- International Finance Corporation (IFC)
- Asian Development Bank (ADB)
- African Development Bank (AfDB)
- European Bank for Reconstruction and Development (EBRD)
- Inter-American Development Bank (IADB)
- European Investment Bank (EIB)
- European Investment Fund (EIF)
- Nordic Investment Bank (NIB)
- Caribbean Development Bank (CDB)
- Islamic Development Bank (IDB)
- Council of Europe Development Bank (CEDB)

Annex 3

Standardized haircut schedule

Asset class	**Haircut (% of market value)**
Cash in the same currency	0
Debt securities issued by or guaranteed by the Government of Canada or the Bank of Canada or the government of a province or territory of Canada or a foreign government or a foreign central bank: residual maturity less than one year	0.5
Debt securities issued by or guaranteed by the Government of Canada or the Bank of Canada or the government of a province or territory of Canada or a foreign government or a foreign central bank: residual maturity between one and five years	2
Debt securities issued by or guaranteed by the Government of Canada or the Bank of Canada or the government of a province or territory of Canada or a foreign government or a foreign central bank: residual maturity greater than five years	4
High-quality corporate/covered bonds: residual maturity less than one year	1
High-quality corporate/covered bonds: residual maturity between one and five years	4
High-quality corporate/covered bonds: residual maturity greater than five years	8
Equities listed on a recognized exchange	15
Gold	15
Additional haircut on assets in which the currency of the covered derivatives differs from the currency of the collateral	8