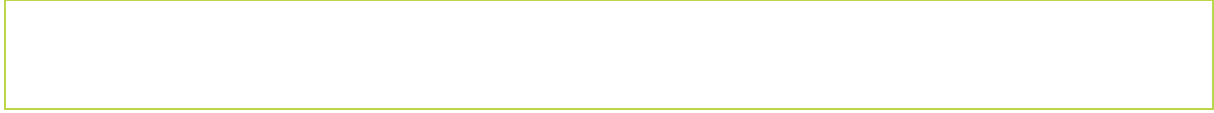


Orientations

Relative aux contrôles internes applicables aux administrateurs d'indices de référence, aux agences de notation de crédit et aux infrastructures de transparence du marché

Table des matières

1	Champ d'application.....	4
2	Références législatives, abréviations et définitions.....	5
2.1	Références législatives	5
2.2	Abréviations	6
2.3	Définitions	7
3	Objet.....	8
4	Obligations en matière de conformité et de déclaration.....	8
4.1	Statut des orientations	8
4.2	Exigences de déclaration.....	8
5	Orientations sur les contrôles internes.....	10
5.1	Cadre de contrôle interne	10
	Composante 1.1 – Environnement de contrôle.....	10
	Composante 1.2 – Gestion des risques	11
	Composante 1.3 – Activités de contrôle	12
	Composante 1.4 – Information et communication.....	14
	Composante 1.5 – Activités de surveillance	15
5.2	Fonctions de contrôle interne.....	16
	Proportionnalité – Fonctions de contrôle interne.....	17
	Composante 2.1 – Fonction de vérification de la conformité.....	18
	Composante 2.2 – Fonction de gestion des risques	19
	Composante 2.3 – Fonction de gestion de la sécurité de l'information (uniquement pour les entités surveillées qui ne sont pas soumises au règlement DORA)	20
	Composante 2.4 – Fonction d'audit interne	21
	Composante 2.5 Fonction de réexamen (pour les ANC uniquement).....	22
	Composante 2.6 – Fonction de supervision (uniquement pour les AIR).....	23



1 Champ d'application

Qui ?

1. Les présentes orientations s'appliquent :

(i) aux administrateurs d'indices de référence agréés, enregistrés ou reconnus auprès de l'ESMA (conjointement dénommés les «AIR») conformément au règlement concernant les indices de référence ;

(ii) les agences de notation de crédit établies dans l'Union et enregistrées auprès de l'ESMA (les «ANC») conformément au règlement sur les agences de notation de crédit (le «règlement ANC») ;

(iii) les prestataires de services de communication de données [à l'exclusion des fournisseurs consolidés de formalités (CTP)] établis dans l'Union et agréés par l'ESMA (PSCD) conformément au MiFIR ;

(iv) les référentiels des titrisations établis dans l'Union et enregistrés auprès de l'ESMA (RT) conformément au règlement sur les titrisations ;

(v) les référentiels centraux établis dans l'Union et enregistrés auprès de l'ESMA conformément au règlement EMIR ;

(vi) les référentiels centraux établis dans l'Union et enregistrés auprès de l'ESMA conformément au règlement SFTR (ci-après dénommés conjointement les «entités surveillées»).

Quoi ?

2. Les présentes orientations concernent les questions relatives à la structure et aux mécanismes de contrôle interne nécessaires pour garantir i) le respect effectif, par un AIR, des articles 4 à 10 du règlement concernant les indices de référence ; ii) le respect effectif, par les ANC, de l'article 6, paragraphe 1, points 2 et 4, de l'article 9 et de l'annexe I, section A, du règlement ANC ; iii) le respect effectif, par un PSCD, des articles 27 *septies*, 27 *octies* et 27 *decies* du MiFIR ; et iv) le respect effectif, par un RC ou un RT, des articles 78 et 79 du règlement EMIR.

Quand ?

3. Les présentes orientations sont applicables à partir du 1^{er} octobre 2026.

4. À compter de la date visée au point 3, les orientations sur le contrôle interne des ANC (ESMA33-9-371) sont abrogées.

2 Références législatives, abréviations et définitions

2.1 Références législatives

MiFIR	Règlement (UE) n° 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) n° 648/2012 ¹
Règlement concernant les indices de référence	Règlement (UE) 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement et modifiant les directives 2008/48/CE et 2014/17/UE et le règlement (UE) n° 596/2014 ²
Règlement sur les titrisations	Règlement (UE) 2017/2402 du Parlement européen et du Conseil du 12 décembre 2017 créant un cadre général pour la titrisation ainsi qu'un cadre spécifique pour les titrisations simples, transparentes et standardisées, et modifiant les directives 2009/65/CE, 2009/138/CE et 2011/61/UE et les règlements (CE) n° 1060/2009 et (UE) n° 648/2012 ³
Règlement ANC	Règlement (CE) n° 1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit ⁴
Règlement DORA	Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 ⁵
Règlement EMIR	Règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux ⁶
SFTR	Règlement (UE) 2015/2365 du Parlement européen et du Conseil du 25 novembre 2015 relatif à la transparence des opérations de

¹ JO L 173 du 12.6.2014, p. 84.

² JO L 171 du 29.6.2016, p. 1.

³ JO L 347 du 28.12.2017, p. 35.

⁴ JO L 302 du 17.11.2009, p. 1.

⁵ JO L 333 du 27.12.2022, p. 1.

⁶ JO L 201 du 27.7.2012, p. 1.

financement sur titres et de la réutilisation et modifiant le règlement (UE) n° 648/2012⁷

2.2 Abréviations

AINE	Administrateur indépendant non exécutif
AIR	Administrateur d'indice de référence
ANC	Agence de notation de crédit
ARM	Mécanisme de déclaration agréé
CCI	Cadre de contrôle interne
DC	Document de consultation
DPA	Dispositif de publication agréé
ESMA	European Securities and Markets Authority (ESMA – Autorité européenne des marchés financiers)
FCI	Fonction de contrôle interne
IA	Intelligence artificielle
IG	Informations relatives à la gestion
NTR	Normes techniques de réglementation
PSCD	Prestataire de services de communication de données
RC	Référentiel central
Règlement DORA	Règlement sur la résilience opérationnelle numérique
RT	Référentiel des titrisations
TIC	Technologies de l'information et des communications
UE	Union européenne

⁷ JO L 337 du 23.12.2015, p. 1.

2.3 Définitions

Direction générale exécutive	<p>Il s'agit des plus hauts dirigeants assurant la direction quotidienne de l'entité surveillée. Il s'agit généralement du président-directeur général (PDG) ou équivalent et de ses rapports directs.</p>
Entités surveillées	<p>Aux fins des présentes orientations, il s'agit des entités relevant de la compétence de surveillance de l'ESMA, à savoir :</p> <ul style="list-style-type: none">▪ AIR▪ ANC▪ PSCD (à l'exclusion des fournisseurs de systèmes consolidés de publication)▪ RT▪ RC
Infrastructures de transparence du marché	<p>Aux fins des présentes orientations, on entend par :</p> <ul style="list-style-type: none">▪ les prestataires de services de communication de données,▪ les référentiels des titrisations et▪ les référentiels centraux
Organe de direction	<p>L'organisme ou les organismes qui sont désignés conformément au droit national, qui sont habilités à définir la stratégie, les objectifs et l'orientation générale de l'entité, qui supervisent et contrôlent la prise de décision en matière de gestion et qui comprennent des personnes qui dirigent effectivement les activités de l'entité.</p> <p>Il s'agit des organes de direction les plus élevés au sein d'une organisation.</p> <p>Le terme est défini à l'article 3, paragraphe 1, point 20, du règlement concernant les indices de référence et à l'article 2, paragraphe 1, point 22, du MiFIR.</p> <p>Il couvre les notions de :</p> <ul style="list-style-type: none">▪ « conseil d'administration ou de surveillance » d'une agence de notation, faisant partie de la « direction générale », au sens de l'article 3, paragraphe 1, point n), du règlement sur les ANC]▪ « conseil d'administration ou de surveillance, ou les deux, conformément au droit national des sociétés », tel que défini à l'article 2, paragraphe 27, du règlement EMIR.
Règlements pertinents	<p>Aux fins des présentes orientations, on entend par :</p> <ul style="list-style-type: none">▪ Règlement concernant les indices de référence▪ Règlement ANC

- Règlement EMIR
- MiFIR
- Règlement sur les titrisations
- SFTR

3 Objet

5. Les présentes orientations exposent les attentes de l'ESMA en ce qui concerne les composantes et les caractéristiques d'un cadre de contrôle interne efficace et les fonctions des différents contrôles internes au sein d'une entité surveillée.

4 Obligations en matière de conformité et de déclaration

4.1 Statut des orientations

6. Le présent document contient des orientations formulées en vertu de l'article 16 du règlement instituant l'ESMA. Conformément à l'article 16, paragraphe 3, du règlement instituant l'ESMA, les entités surveillées mettent tout en œuvre pour respecter les présentes orientations.

4.2 Exigences en matière de déclaration

7. Les acteurs des marchés financiers auxquels les présentes orientations s'appliquent ne sont pas tenus de déclarer s'ils se conforment aux présentes orientations. L'ESMA évaluera l'application des présentes orientations par les entités surveillées dans le cadre de sa surveillance et de son contrôle continu des activités des entités surveillées.
8. Dans le cadre de la mise en œuvre des présentes orientations, l'ESMA appliquera le principe de proportionnalité. Si toutes les entités surveillées sont censées démontrer les composantes et les caractéristiques d'un système de contrôle interne efficace décrites dans les présentes orientations, l'ESMA calibrera ses attentes au titre de la section 4.2 en fonction de la nature, de l'ampleur, de la complexité et du profil de risque global d'une entité surveillée et en fonction de la manière dont ces caractéristiques peuvent affecter la protection des investisseurs, le bon fonctionnement du marché et la stabilité financière.
9. Lorsqu'elle évalue la nature d'une entité surveillée, l'ESMA tient compte de l'activité et du type d'opérations de l'entité surveillée, y compris son rôle/mission sur le marché, le type, la diversité et le caractère critique des produits et services proposés par l'entité surveillée.

10. Lors de l'évaluation de l'échelle des activités d'une entité surveillée, l'ESMA tiendra compte de facteurs pertinents tels que l'effectif, les recettes, le nombre de clients et de produits, la part de marché, les interconnexions avec d'autres secteurs/infrastructures, les services auxiliaires et leur relation avec les services de base, ainsi que d'autres facteurs spécifiques à la taille et à l'incidence sur le marché de l'entité surveillée.
11. Lorsqu'elle évaluera la complexité d'une entité surveillée, l'ESMA tiendra compte, entre autres facteurs, de sa structure et de ses modalités organisationnelles (structure/rerelations du groupe, services partagés, externalisation, etc.), ainsi que de ses caractéristiques opérationnelles en ce qui concerne les personnes, les processus, la technologie, les offres de produits et les interconnexions.
12. Pour calibrer ses attentes, l'ESMA tient compte des conditions d'enregistrement ou de reconnaissance d'une entité surveillée. La nature, l'ampleur et la complexité d'une entité surveillée peuvent changer après son enregistrement ou sa reconnaissance, et il est de sa responsabilité de veiller à ce que ses contrôles internes restent proportionnés à sa nature, à son ampleur et à sa complexité. L'ESMA communiquera, dans le cadre de sa surveillance, si elle a un seuil d'attentes en vertu des sections 5.1 et 5.2 plus élevé que ceux établis lors de l'enregistrement ou de la reconnaissance.

5 Orientations sur les contrôles internes

13. Afin de démontrer que les entités surveillées respectent le point 2 des présentes orientations, les entités surveillées doivent démontrer que leurs politiques, procédures et pratiques de travail atteignent les objectifs des sections **5.1** (Cadre de contrôle interne) et **5.2** (Fonctions de contrôle interne) des présentes orientations.

5.1 Cadre de contrôle interne

14. Afin de garantir un CCI efficace, les entités soumises à la surveillance doivent inclure les composantes et caractéristiques suivantes dans leurs politiques, procédures et pratiques de travail.

Principes généraux

15. L'organe de direction de l'entité surveillée doit être responsable de la supervision et de l'approbation de toutes les composantes du CCI, ainsi que de la supervision du fait que ces composantes font l'objet d'une surveillance et sont régulièrement mises à jour par la direction générale exécutive. La direction générale exécutive de l'entité surveillée doit être chargée d'établir, de mettre en œuvre et de mettre à jour les politiques, procédures et pratiques écrites de contrôle interne qui soutiennent les composantes du CCI.
16. Dans le cadre de la mise en place de ces politiques et procédures, une entité soumise à la surveillance doit disposer d'un processus décisionnel clair, transparent et documenté et d'une répartition claire des rôles et des responsabilités au sein de son CCI, y compris ses lignes d'activité et ses FCI.

Composante 1.1 – Environnement de contrôle

17. L'organe de direction et la direction générale exécutive d'une entité surveillée contribuent tous deux à donner l'exemple au plus haut niveau en ce qui concerne l'importance du contrôle interne. La direction générale exécutive est responsable du développement et de la performance du contrôle interne ainsi que de l'évaluation de l'adéquation et de l'efficacité de l'environnement de contrôle. L'organe de direction doit exercer la supervision de la direction générale exécutive dans ces domaines.

Caractéristiques

- 1.1.1 La direction générale exécutive de l'entité surveillée doit être chargée de mettre en place une solide culture de l'éthique et de la conformité au sein de l'entité surveillée grâce à la mise en œuvre de politiques et de procédures régissant la conduite du personnel de l'entité surveillée.

- 1.1.2** La direction générale exécutive de l'entité surveillée doit veiller à ce que les politiques et procédures de l'entité surveillée :
- i. précisent que les activités de l'entité surveillée doivent être menées conformément à la réglementation applicable et aux valeurs d'entreprise de l'entité surveillée ;
 - ii. précisent que, outre le respect des exigences juridiques et réglementaires et des politiques internes, le personnel est tenu de se comporter avec honnêteté et intégrité et d'exercer ses fonctions en faisant preuve de la compétence, du soin et de la diligence requis ; et
 - iii. veillent à ce que le personnel soit conscient des éventuelles mesures disciplinaires internes et externes, actions en justice et sanctions susceptibles de découler d'une faute.
- 1.1.3** La direction générale de l'entité surveillée doit établir, maintenir et mettre à jour régulièrement des politiques, mécanismes et procédures de contrôle interne écrits adéquats.
- 1.1.4** La direction générale de l'entité surveillée doit rester responsable des activités externalisées à des prestataires de services externes ou déléguées à des partenaires commerciaux.

Composante 1.2 – Gestion des risques

18. Aux fins d'une gestion efficace des risques, les entités surveillées doivent veiller à mettre en place un processus dynamique et en constante évolution permettant d'identifier, d'évaluer et de mesurer tous les risques susceptibles d'avoir une incidence sur la capacité d'une entité surveillée à s'acquitter des obligations qui lui incombent en vertu des règlements pertinents, ou sur la poursuite de ses activités. Cela inclut, par exemple, les risques résultant de l'utilisation de nouvelles technologies par l'entité surveillée et des changements apportés à son paysage des risques externes. Le processus doit permettre à l'entité surveillée de surveiller, de gérer, d'atténuer et de déclarer correctement les risques importants associés à ces objectifs.

Caractéristiques

- 1.2.1 L'entité surveillée doit mener ses évaluations internes des risques conformément à une méthodologie définie et complète d'évaluation des risques.
- 1.2.2 L'entité surveillée doit définir son appétence au risque et déterminer les niveaux de tolérance au risque.
- 1.2.3 La méthodologie d'évaluation des risques de l'entité surveillée doit englober toutes les lignes d'activité et les FCI de l'entité surveillée.
- 1.2.4 Le processus d'évaluation des risques de l'entité surveillée doit identifier et évaluer les changements susceptibles d'avoir une incidence significative sur le système de contrôle interne. Il s'agit notamment d'apporter des modifications à son environnement, à son organisation, à ses activités et à son fonctionnement.
- 1.2.5 La méthodologie d'évaluation des risques de l'entité surveillée doit faire l'objet d'une évolution et d'améliorations continues.

Composante 1.3 – Activités de contrôle

- 19. Les activités de contrôle doivent être, par nature, des mesures de prévention, de détection, de correction ou de dissuasion.

Caractéristiques

- 1.3.1 *Séparation des tâches* – L'entité surveillée doit assurer une séparation appropriée des tâches afin de gérer les risques de conflit d'intérêts, de fraude et d'erreur humaine. La séparation des tâches doit garantir que les membres du personnel chargés de l'exécution d'une tâche ne sont pas les seuls responsables de l'approbation du résultat de son exercice. En particulier, les membres du personnel chargés de l'élaboration, de la mise en œuvre ou de l'approbation d'une tâche/d'un poste de travail ne sont pas seuls responsables de sa validation, de son évaluation et de son examen.⁸ Lorsque cela ne peut être évité, cela doit être atténué par le fait que les membres du personnel ne sont pas exclusivement responsables de l'activité.⁹

⁸ Par exemple, les membres du personnel responsables des activités de développement des systèmes ne doivent pas participer à l'administration des bases de données, aux opérations informatiques, ni à l'administration et à la maintenance des systèmes informatiques et des réseaux. Pour les ANC, i) les personnes qui procèdent à l'analyse d'une notation de crédit ne doivent pas être seules responsables de l'approbation de la notation de crédit; ii) les personnes responsables de l'élaboration des méthodes de notation ne doivent pas être seules responsables de leur approbation; iii) les personnes responsables de la validation, de l'évaluation ou du réexamen d'une méthode de notation de crédit ne doivent pas être seules responsables de l'approbation de la validation, de l'évaluation ou du réexamen de ces méthodes.

⁹ Par exemple, au moyen d'un contrôle à quatre yeux.

- 1.3.2** *Documentation* — L'entité surveillée doit documenter ses politiques et procédures couvrant tous les domaines de ses activités soumis aux dispositions de la réglementation applicable.
- 1.3.3** *Contrôles et tests de contrôle documentés* – L'entité soumise à la surveillance doit documenter les contrôles clés mis en place pour garantir le respect de ses politiques et procédures établies conformément aux règlements pertinents.
- 1.3.4** *Désignation des responsabilités* – L'entité surveillée doit désigner de manière claire et définie les rôles ou fonctions responsables de l'exécution des contrôles relatifs aux obligations au titre des règlements pertinents et préciser leurs rôles et responsabilités respectifs. Ce faisant, l'entité surveillée doit établir une distinction entre les contrôles quotidiens au niveau opérationnel et ceux effectués par des fonctions de contrôle spécifiques.
- 1.3.5** *Autorisations et approbations* – L'entité surveillée doit disposer de processus ou de mécanismes d'autorisation pour garantir que seules les personnes autorisées ont accès aux informations et aux outils sur la base du besoin d'en connaître et du moindre privilège. L'entité surveillée doit également disposer de processus ou de mécanismes dans toutes ses activités afin de garantir que les activités ne sont approuvées et exécutées que par des membres du personnel agissant dans le cadre de leur autorité.¹⁰
- 1.3.6** *Vérifications, validations, rapprochements et réexamens* – L'entité surveillée doit prendre des mesures pour détecter et agir en temps utile en cas d'activités inappropriées, non autorisées, erronées ou frauduleuses.¹¹
- 1.3.7** *Contrôles généraux des technologies de l'information et de la communication (TIC)* (uniquement pour les entités surveillées qui ne sont pas soumises au règlement DORA) – L'entité surveillée doit mettre en œuvre des stratégies, politiques et procédures qui garantissent la résilience opérationnelle numérique des systèmes TIC de l'entité surveillée afin de soutenir les processus opérationnels de l'entité surveillée.

L'entité surveillée doit concevoir ses contrôles et solutions en matière de TIC de manière proportionnée. Par conséquent, les contrôles en matière de TIC varieront d'une organisation à l'autre en fonction de la nature, de l'échelle et de

¹⁰ Par exemple, pour les ANC, seules les personnes désignées comme responsables des tâches respectives doivent procéder au processus de notation de crédit, à la validation des méthodes et à l'examen des résultats de la validation.

¹¹ Il s'agit notamment de la validation des données et des contrôles des données d'entrée, de l'examen des listes pour l'accès autorisé aux informations confidentielles. Pour les ANC, ces contrôles s'appliquent aux activités de notation de crédit et aux processus sous-tendant ces activités, tels que la validation de la méthodologie/du modèle de crédit.

la complexité des processus opérationnels sous-jacents et des fonctions pertinentes prises en charge par ces systèmes.

Les entités surveillées doivent veiller à disposer de contrôles suffisants pour garantir la qualité des données, en termes de disponibilité, de confidentialité et d'intégrité des données, y compris la validation des données, les contrôles du traitement et les procédures de contrôle des fichiers de données.

L'entité surveillée doit mettre en place un système de gestion de la sécurité de l'information pertinent et des activités de contrôle connexes. Dans ce cadre, une entité surveillée doit déterminer les contrôles nécessaires pour garantir l'authenticité, la confidentialité, l'intégrité et la disponibilité des informations telles qu'elles sont traitées, de la source à l'utilisateur final.

L'entité surveillée doit établir et documenter toutes les activités pertinentes de contrôle des processus d'acquisition, de développement et de maintenance des TIC.

Composante 1.4 – Information et communication

20. Les entités surveillées doivent établir des procédures permettant de procéder à une communication descendante d'informations exactes, exhaustives et de qualité à destination du personnel et des parties prenantes externes. Les entités surveillées doivent également établir des procédures pour la communication régulière d'informations sur le système et les activités de contrôle interne à l'organe de direction et à la direction générale exécutive, y compris des informations relatives au comportement et au respect des contrôles internes.

Caractéristiques

- 1.4.1** L'entité surveillée doit assurer une communication interne et externe appropriée, en communiquant en temps utile des informations exactes, complètes et de bonne qualité au marché, aux clients, aux utilisateurs de ses produits et services et aux régulateurs.
- 1.4.2** L'entité surveillée doit mettre en place des canaux de communication à la hausse, y compris une procédure de dénonciation des dysfonctionnements, afin de permettre la remontée des problèmes importants de contrôle interne à l'organe de direction et à la direction générale exécutive. L'organe de direction et la direction générale exécutive doivent également recevoir régulièrement des informations actualisées sur le système et les activités de contrôle interne, y compris sur la sécurité de l'information. L'entité surveillée doit disposer de procédures de remontée de l'information en cas de désaccord important entre les FCI et les unités opérationnelles.

- 1.4.3** L'entité surveillée doit mettre en place des canaux de communication vers le personnel depuis l'organe de direction, la direction générale exécutive et les fonctions de contrôle. Cela doit comprendre des mises à jour régulières sur les objectifs et les responsabilités en matière de contrôle interne, la communication des problèmes recensés en matière de conformité ou de sécurité de l'information, ainsi que des présentations et des formations sur les politiques et les procédures.

Composante 1.5 – Activités de surveillance

21. Les entités surveillées doivent s'assurer qu'elles mènent des activités de surveillance permettant de vérifier si les composantes du système de contrôle interne de l'entité surveillée sont bien présentes et fonctionnent efficacement.

Caractéristiques

- 1.5.1** L'entité surveillée doit veiller à ce que les évaluations du système de contrôle interne soient réalisées à différents niveaux opérationnels de l'entité surveillée, tels que les lignes d'activité, les fonctions de contrôle et les fonctions d'audit interne ou d'évaluation indépendante.
- 1.5.2** Les activités de suivi doivent être conçues et réalisées de manière à permettre à l'entité surveillée de vérifier si l'entité surveillée respecte ses exigences légales et réglementaires, y compris le respect de ses codes de conduite, politiques et procédures internes. Cela inclut les politiques et procédures de l'entité surveillée en matière de sécurité de l'information.
- 1.5.3** Les systèmes de contrôle interne doivent être évalués à intervalles réguliers ou de façon thématique, ou selon une combinaison de ces deux éléments.
- 1.5.4** Les entités surveillées doivent intégrer les évaluations continues dans les processus opérationnels et les adapter à l'évolution des conditions.
- 1.5.5** Les entités surveillées doivent veiller à ce que les manquements constatés lors du suivi des évaluations et les mesures correctives requises soient signalés à l'organe de direction et à la direction générale exécutive, qui doivent ensuite contrôler la mise en œuvre en temps utile de la ou des mesures correctives.
- 1.5.6** En cas d'externalisation, l'entité surveillée doit confier la mission de suivi des processus opérationnels externalisés à un membre du personnel. Les entités surveillées doivent veiller à ce que des informations suffisantes sur les objectifs et les attentes en matière de livraison soient fournies au prestataire de services, et à ce que la diligence requise soit menée avant la nomination du prestataire.

5.2 Fonctions de contrôle interne

22. Afin de garantir l'efficacité des FCI, les entités surveillées doivent inclure les composantes et caractéristiques suivantes dans leurs politiques, procédures et pratiques de travail.

Principes généraux

23. L'ESMA considère que les FCI des entités surveillées doivent disposer de ressources suffisantes et d'un personnel doté d'une expertise suffisante pour s'acquitter de leurs tâches. Le personnel travaillant dans les FCI doit avoir une connaissance technique suffisante des activités de l'entité surveillée et des risques associés. Lorsqu'une entité surveillée a externalisé les tâches opérationnelles d'une FCI au niveau du groupe ou à un prestataire extérieur, l'ESMA considère que l'entité surveillée conserve l'entière responsabilité des activités de la FCI externalisée. Les entités surveillées doivent veiller à ce que le personnel chargé des FCI ait un niveau hiérarchique approprié pour disposer de l'autorité nécessaire à l'exercice de ses responsabilités. Par exemple, les membres du personnel chargés de la conformité, de la gestion des risques, de l'audit interne, de la gestion de la sécurité de l'information, de l'examen (pour les ANC) et de la supervision (pour les AIR) doivent avoir un accès illimité et faire régulièrement rapport à l'organe de direction.
24. Les activités peuvent être menées au niveau du groupe ou par d'autres entités juridiques au sein d'une structure d'entreprise, à condition que la structure du groupe n'entrave pas la capacité de l'organe de direction d'une entité surveillée à assurer la surveillance prudentielle, ni la capacité de la direction générale exécutive à gérer efficacement ses risques, ni la capacité de l'ESMA à surveiller efficacement l'entité surveillée. Dans tous les cas, l'orientation 1.1.4 s'applique.
25. Afin de garantir l'indépendance des FCI d'une entité surveillée, l'ESMA attend des entités surveillées qu'elles tiennent compte des principes suivants lorsqu'elles définissent les rôles et responsabilités de leurs FCI :
- i. les FCI doivent être distinctes, du point de vue organisationnel, des fonctions/activités qu'elles ont pour mission de surveiller, auditer ou contrôler ;
 - ii. les FCI ne doivent pas s'acquitter de tâches opérationnelles relevant du champ d'application des activités professionnelles qu'elles sont censées surveiller, auditer ou contrôler ;
 - iii. le membre du personnel chargé d'une FCI ne doit pas rendre compte à une personne responsable de la gestion des activités que la FCI surveille, audite ou contrôle ;

26. le personnel exerçant des responsabilités liées aux FCI doit avoir accès à une formation interne ou externe pertinente afin de garantir l'adéquation de ses compétences à l'exécution des tâches.

Proportionnalité – Fonctions de contrôle interne

27. Si toutes les entités surveillées sont censées démontrer les caractéristiques des FCI efficaces décrites dans les présentes orientations, l'ESMA calibre ses attentes en fonction de la nature, de l'échelle et de la complexité de l'entité surveillée, comme décrit à la section 3.4 des présentes orientations.
28. La présente section expose plus en détail la manière dont l'ESMA tient compte de la proportionnalité dans sa surveillance des fonctions de contrôle interne.

Séparation des fonctions

29. La séparation des tâches doit être intégrée dans l'élaboration des activités de contrôle. Il peut toutefois arriver que le droit de l'Union n'exige pas une séparation des tâches et qu'une telle séparation ne soit pas pratique compte tenu de la nature, de l'ampleur et de la complexité de l'entité surveillée. Dans ce cas, d'autres témoins peuvent être plus appropriés. Lorsque d'autres contrôles sont utilisés, les entités surveillées doivent documenter la raison d'être de l'accord, identifier les risques éventuels, mettre en œuvre des contrôles compensatoires pour y remédier et démontrer que le dispositif ne nuit pas à l'environnement de contrôle.

Ressources

30. Pour certaines entités surveillées, il peut ne pas être proportionné de disposer de personnel à temps plein dans toutes les fonctions, compte tenu de leur nature, de leur ampleur et de leur complexité. Dans ces cas, une entité surveillée peut choisir d'augmenter le nombre d'heures de ressources afin de faire correspondre les activités de contrôle ou d'externaliser l'activité.

Spécialisation au sein des fonctions

31. À mesure qu'une entité surveillée se développe et que son environnement de contrôle arrive à maturité, elle doit recourir à la spécialisation du personnel pour bénéficier de l'expertise du personnel dans des processus clés ou des domaines à risque. Les entités surveillées d'une certaine nature, ampleur et complexité doivent mettre en place des équipes de surveillance ou d'enquête spécifiques au sein de leur fonction de vérification de la conformité.

Maturité des activités de contrôle

32. La maturité des activités de contrôle (c'est-à-dire manuelles, hybrides, automatisées et, dans certains cas, intégrant des outils d'intelligence artificielle) doit refléter la nature, l'ampleur et la complexité ainsi que le profil de risque global d'une entité surveillée. Pour les entités surveillées d'une certaine nature, ampleur et complexité, il doit y avoir un degré plus élevé de contrôles automatisés ainsi qu'une plus grande intégration entre les systèmes de fonctions de contrôle afin d'optimiser les activités de suivi et la déclaration par une entité surveillée des informations de gestion à la direction générale exécutive et à l'organe de direction.

Composante 2.1 – Fonction de vérification de la conformité

33. La fonction de vérification de la conformité d'une entité surveillée est chargée de surveiller le respect, par l'entité surveillée et son personnel, des obligations qui leur incombent en vertu du règlement applicable, et d'en rendre compte. La fonction de vérification de la conformité est chargée de suivre les évolutions des textes législatifs et réglementaires applicables à ses activités. La fonction de vérification de la conformité est également chargée de conseiller l'organe de direction sur les lois, règles, règlements et normes que l'entité surveillée doit respecter et d'évaluer, conjointement avec d'autres fonctions pertinentes, l'incidence éventuelle de tout changement apporté à l'environnement juridique ou réglementaire sur les activités de l'entité surveillée.

Caractéristiques

- 2.1.1** La fonction de vérification de la conformité doit remplir ses fonctions indépendamment des lignes d'activité et doit présenter des rapports réguliers à l'organe de direction de l'entité surveillée et, le cas échéant, directement aux AINE.
- 2.1.2** La fonction de vérification de la conformité doit conseiller et aider les membres du personnel à respecter les obligations qui leur incombent en vertu du règlement applicable. La fonction de vérification de la conformité doit être proactive dans l'identification des risques et de toute non-conformité potentielle, en surveillant et en évaluant les activités en temps utile, ainsi qu'en assurant le suivi des mesures correctrices.
- 2.1.3** La fonction de vérification de la conformité doit veiller à ce que la conformité soit surveillée au moyen d'un programme de surveillance clairement défini et structuré. Le champ d'application des activités de vérification de la conformité doit couvrir l'ensemble des processus et systèmes opérationnels et informatiques susceptibles d'avoir une incidence sur le respect, par l'entité surveillée, du règlement applicable.
- 2.1.4** La fonction de vérification de la conformité, le cas échéant en conjonction avec d'autres fonctions pertinentes, doit évaluer l'incidence possible de toute

modification de l'environnement juridique ou réglementaire sur les activités de l'entité surveillée et communiquer, le cas échéant, avec la fonction de gestion des risques sur le risque de conformité de l'entité surveillée en temps utile.

- 2.1.5** La fonction de vérification de la conformité doit veiller au respect des politiques de conformité et faire rapport à l'organe de direction et à la direction générale exécutive sur le risque de conformité auquel l'entité surveillée est exposée.
- 2.1.6** La fonction de vérification de la conformité doit coopérer avec la fonction de gestion des risques dans le but d'échanger les informations nécessaires à l'accomplissement de leurs tâches respectives.
- 2.1.7** Les conclusions de la fonction de vérification de la conformité doivent être prises en compte par l'organe de direction et la direction générale exécutive ainsi que par la fonction de gestion des risques dans le cadre de leurs processus d'évaluation des risques.

Composante 2.2 – Fonction de gestion des risques

- 34. La fonction de gestion des risques d'une entité surveillée est responsable de l'élaboration et de la mise en œuvre du cadre de gestion des risques.

Caractéristiques

- 2.2.1** La fonction de gestion des risques doit accomplir ses missions indépendamment des lignes d'activité et des unités dont elle surveille les risques, mais elle ne doit pas être empêchée d'interagir avec celles-ci.
- 2.2.2** La fonction de gestion des risques doit veiller à ce que tous les risques susceptibles d'avoir une incidence sur la capacité d'une entité surveillée à s'acquitter des obligations qui lui incombent en vertu des règlements pertinents, ou sur la poursuite de ses activités, soient identifiés, évalués et mesurés. Les risques importants pesant sur ces objectifs doivent ensuite être surveillés, gérés, atténués et correctement signalés en temps utile par les unités concernées au sein de l'entité surveillée, ainsi qu'aux unités concernées au sein de celle-ci.
- 2.2.3** La fonction de gestion des risques doit surveiller le profil de risque de l'entité surveillée par rapport à l'appétence au risque de l'entité surveillée afin de permettre la prise de décision.
- 2.2.4** La fonction de gestion des risques doit donner des conseils quant aux propositions des lignes d'activité et aux décisions prises par celles-ci en matière de risque, et indiquer à l'organe de direction si ces décisions sont conformes à l'appétence au risque et aux objectifs de l'entité.

- 2.2.5** La fonction de gestion des risques doit recommander des améliorations du cadre de gestion des risques et, le cas échéant, des modifications des politiques et procédures en matière de risques. La fonction de gestion des risques doit revoir les seuils de risque en fonction de toute modification de l'appétence au risque de l'organisation.

Composante 2.3 – Fonction de gestion de la sécurité de l'information (uniquement pour les entités surveillées qui ne sont pas soumises au règlement DORA)

35. La fonction de gestion de la sécurité de l'information d'une entité surveillée est responsable du développement et de la mise en œuvre de la sécurité de l'information au sein de l'entité surveillée. Une entité surveillée doit créer une fonction favorisant une culture de la sécurité de l'information au sein de l'entité surveillée.

Caractéristiques

- 2.3.1** La fonction de gestion de la sécurité de l'information doit être chargée d'examiner et de contrôler le respect par l'entité surveillée des politiques et procédures de l'entité surveillée en matière de sécurité de l'information.
- 2.3.2** La fonction de gestion de la sécurité de l'information doit gérer les activités de l'entité surveillée en matière de sécurité de l'information.
- 2.3.3** La fonction de gestion de la sécurité de l'information doit élaborer et instaurer un programme de sensibilisation à la sécurité de l'information permettant au personnel de renforcer la culture de la sécurité et de développer une compréhension globale du cadre de sécurité de l'information de l'entité surveillée.
- 2.3.4** La fonction de gestion de la sécurité de l'information doit rendre compte à l'organe de direction et à la direction générale exécutive et les conseiller sur l'état d'avancement du système de gestion de la sécurité de l'information et les risques y afférents (par exemple, des informations sur les projets de sécurité de l'information, les incidents liés à la sécurité de l'information et les résultats des examens de la sécurité de l'information).

Composante 2.4 – Fonction d'audit interne

36. Une fonction d'audit interne d'une entité surveillée est chargée de fournir un service d'assurance et de conseil indépendant et objectif dans le but d'améliorer les activités de l'organisation. Elle aide l'organisation à atteindre ses objectifs en instaurant une approche systématique et disciplinée visant à évaluer et à améliorer l'efficacité du système de contrôle interne.

Caractéristiques

- 2.4.1** La fonction d'audit interne doit exercer ses fonctions indépendamment des lignes d'activité et des autres FCI. Elle doit être régie par une charte d'audit interne définissant son rôle et ses responsabilités et être soumise à la supervision de l'organe de direction.
- 2.4.2** La fonction d'audit interne doit suivre une approche fondée sur les risques et respecter les normes internationales en matière d'audit interne.
- 2.4.3** La fonction d'audit interne doit examiner de manière indépendante les activités de l'entité surveillée, y compris les activités externalisées, et fournir une assurance objective que ces activités sont conformes aux politiques et

procédures de l'entité surveillée ainsi qu'aux exigences juridiques et réglementaires applicables.

- 2.4.4** La fonction d'audit interne doit établir, au moins une fois par an, sur la base des objectifs annuels de contrôle de l'audit interne, un plan d'audit soumis à la supervision de l'organe de direction.
- 2.4.5** La fonction d'audit interne doit fournir des rapports réguliers aux membres indépendants de l'organe de direction ou au comité d'audit, le cas échéant.
- 2.4.6** La fonction d'audit interne doit communiquer ses recommandations d'audit d'une manière claire et cohérente qui permette à l'organe de direction et à la direction générale exécutive de comprendre le caractère significatif des recommandations et de hiérarchiser les priorités en conséquence.
- 2.4.7** Les recommandations relatives à l'audit interne doivent être soumises à une procédure de suivi formelle aux niveaux hiérarchiques appropriés, afin de garantir leur mise en œuvre effective et en temps utile et afin de rendre des comptes à ce sujet.

Composante 2.5 Fonction de réexamen (pour les ANC uniquement)

- 37. La fonction de réexamen d'une ANC est chargée de réexaminer les méthodes de notation de crédit au moins une fois par an. La fonction de réexamen de l'ANC est également chargée de valider et de réexaminer les nouvelles méthodes, ainsi que toute modification des méthodes existantes.

Caractéristiques

- 2.5.1** La fonction de réexamen doit accomplir ses missions indépendamment des lignes d'activité responsables des activités de notation de crédit et doit présenter ses rapports aux AINE de l'ANC à intervalles réguliers.
- 2.5.2** Ni les actionnaires de l'ANC ni les membres de son personnel associés au développement économique ne doivent accomplir les missions de la fonction de réexamen.
- 2.5.3** Les membres du personnel responsables des analyses ne doivent participer ni à l'approbation de méthodes, modèles et principales hypothèses de notation nouvellement définis ni à la validation et au réexamen de méthodes, modèles et principales hypothèses de notation existants.
- 2.5.4** Le personnel de la fonction de réexamen doit soit être entièrement responsable de l'approbation des méthodes, modèles et principales hypothèses de notation

soit détenir la majorité des droits de vote au sein des comités qui en sont responsables.

2.5.5 Le personnel chargé de la fonction de réexamen responsable de la validation et/ou de la révision d'une méthode, et qui participe également à sa phase de développement, ne doit pas être seul responsable ou avoir la majorité des droits de vote dans les comités d'approbation de la méthode.

2.5.6 En cas d'externalisation de la fonction de réexamen, l'ANC doit tenir compte de l'orientation 1.5.6. En outre, l'ANC doit disposer de mécanismes de contrôle interne appropriés pour garantir qu'elle respecte systématiquement les exigences réglementaires et maintient des normes de qualité analytiques appropriées.

Composante 2.6 – Fonction de supervision (uniquement pour les AIR)¹²

38. La fonction de supervision surveille les principaux aspects de la fourniture d'indices de référence. Cela inclut, sans s'y limiter, le réexamen de la définition et de la méthodologie de l'indice de référence, la gestion des tiers participant à la fourniture de l'indice de référence, l'évaluation des audits internes et externes ou des examens du cadre de contrôle de l'administrateur, et la notification aux autorités compétentes concernées de toute faute pertinente.

Caractéristiques

2.6.1 La fonction de supervision de l'AIR conserve son indépendance vis-à-vis de tout organe de direction ou de toute fonction de l'AIR et de toute partie externe à l'AIR. L'indépendance suppose que les membres chargés de la fonction de supervision ne sont pas confrontés à des conflits d'intérêts entre leurs activités en tant que membres chargés de la fonction de supervision et leurs autres activités. L'AIR doit mettre en œuvre un cadre opérationnel de contrôle interne afin de prévenir et d'atténuer tout conflit d'intérêts potentiel.

2.6.2 L'AIR doit disposer de politiques et de procédures claires concernant la mise en place et les responsabilités de la fonction de supervision et de ses membres, y compris des politiques et des procédures relatives aux mises à jour de la méthodologie relative aux indices de référence et aux examens de l'intégrité des données.

2.6.3 La fonction de supervision de l'AIR doit régulièrement procéder à une auto-évaluation afin d'évaluer son efficacité et l'adéquation de ses membres aux fins

¹² Les AIR non significatifs qui appliquent l'article 26 du règlement concernant les indices de référence sont censés appliquer les présentes orientations proportionnellement aux exigences de l'article 26.

de la fonction, d'identifier les conflits d'intérêts potentiels et de proposer des domaines d'amélioration, si nécessaire.

- 2.6.4** La fonction de supervision de l'AIR doit maintenir un canal de communication défini et régulier avec l'organe de direction, la direction générale exécutive et d'autres fonctions clés. La fonction de supervision de l'AIR doit également être en mesure d'accéder aux informations de gestion et de les contester, ainsi que de recevoir des mises à jour concernant l'état d'avancement des mesures correctives à la suite d'audits internes et externes, de rapports sur les risques et de rapports de conformité.
- 2.6.5** La fonction de supervision de l'AIR doit maintenir un canal de communication défini avec les autorités compétentes concernées, y compris en signalant toute faute ou violation commise par des administrateurs ou des contributeurs.