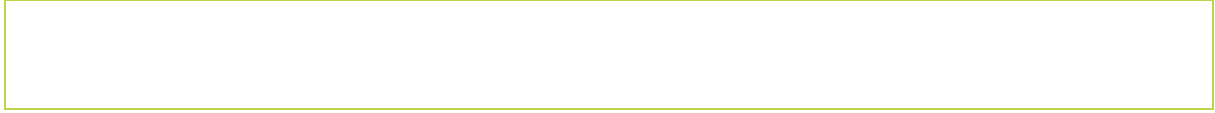


# Orientações

sobre os controlos internos aplicáveis aos administradores de índices de referência, às agências de notação de risco e às infraestruturas de transparência do mercado

## Índice

1	Âmbito de aplicação.....	4
2	Referências legislativas, abreviaturas e definições .....	5
2.1	Referências legislativas .....	5
2.2	Abreviaturas .....	6
2.3	Definições .....	7
3	Finalidade.....	8
4	Obrigações em matéria de cumprimento e de comunicação de informações .....	8
4.1	Natureza das presentes Orientações .....	8
4.2	Obrigações de comunicação de informação .....	8
5	Orientações sobre o controlo interno .....	10
5.1	Quadro de Controlo Interno .....	10
	<b>Componente 1.1 Ambiente de controlo .....</b>	<b>10</b>
	<b>Componente 1.2 Gestão de risco .....</b>	<b>11</b>
	<b>Componente 1.3 Atividades de controlo .....</b>	<b>12</b>
	<b>Componente 1.4 Informação e comunicação .....</b>	<b>14</b>
	<b>Componente 1.5 Atividades de acompanhamento .....</b>	<b>15</b>
5.2	Funções de Controlo Interno .....	16
	<b>Proporcionalidade — Funções de Controlo Interno .....</b>	<b>17</b>
	<b>Componente 2.1 Função de verificação do cumprimento .....</b>	<b>18</b>
	<b>Componente 2.2 Função de Gestão de Risco .....</b>	<b>19</b>
	<b>Componente 2.3 Função de Gestão da Segurança da Informação (apenas para entidades supervisionadas não sujeitas ao Regulamento DORA) .....</b>	<b>20</b>
	<b>Componente 2.4 Função de Auditoria Interna .....</b>	<b>21</b>
	<b>Componente 2.5 Função de Revisão (apenas para as ANR) .....</b>	<b>22</b>
	<b>Componente 2.6 Função de supervisão (apenas para AIR).....</b>	<b>22</b>



## 1 Âmbito de aplicação

### Quem?

1. As presentes Orientações aplicam-se:

(i) aos administradores de índices de referência autorizados, registados ou reconhecidos pela ESMA (coletivamente designados «AIR») em conformidade com o Regulamento IR;

(ii) às agências de notação de risco estabelecidas na União e registadas junto da ESMA (ANR) nos termos do Regulamento ANR;

(iii) aos prestadores de serviços de comunicação de dados (excluindo os prestadores de informações consolidadas (CTP)) estabelecidos na União e autorizados pela ESMA (DRSP) em conformidade com o MiFIR;

(iv) aos repositórios de titularizações estabelecidos na União e registados na ESMA (SR), em conformidade com o SECR;

(v) aos repositórios de transações estabelecidos na União e registados junto da ESMA (RT) em conformidade com o EMIR;

(vi) aos repositórios de transações estabelecidos na União e registados na ESMA em conformidade com o SFTR (a seguir conjuntamente designados por «entidades supervisionadas»).

### O quê?

2. As presentes Orientações dizem respeito a questões relacionadas com a estrutura e os mecanismos de controlo interno necessários para assegurar i) o cumprimento efetivo pelos AIR dos artigos 4.º a 10.º do Regulamento IR; ii) o cumprimento efetivo, por parte das ANR, do artigo 6.º, n.ºs 1, 2 e 4, do artigo 9.º e do anexo I, secção A, do Regulamento ANR; iii) o cumprimento efetivo, por parte do DRSP, dos artigos 27.º-F, 27.º-G e 27.º-I do MiFIR; e iv) o cumprimento efetivo, por parte do RT ou do SR, dos artigos 78.º e 79.º do EMIR.

### Quando?

3. As presentes Orientações aplicam-se a partir de 1 de outubro de 2026.

4. A partir da data referida no n.º 3, as Orientações sobre o controlo interno das ANR (ESMA33-9-371) serão revogadas.

## 2 Referências legislativas, abreviaturas e definições

### 2.1 Referências legislativas

EMIR	Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações <sup>1</sup>
MiFIR	Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativo aos mercados de instrumentos financeiros e que altera o Regulamento (UE) n.º 648/2012 <sup>2</sup>
Regulamento ANR	Regulamento (CE) n.º 1060/2009 do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativo às agências de notação de risco <sup>3</sup>
Regulamento DORA	Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 <sup>4</sup>
Regulamento IR	Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativo aos índices utilizados como índices de referência no quadro de instrumentos e contratos financeiros ou para aferir o desempenho de fundos de investimento e que altera as Diretivas 2008/48/CE e 2014/17/UE e o Regulamento (UE) n.º 596/2014 <sup>5</sup>
SECR	Regulamento (UE) 2017/2402 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2017, que estabelece um regime geral para a titularização e cria um regime específico para a titularização simples, transparente e padronizada, e que altera as Diretivas 2009/65/CE, 2009/138/CE e 2011/61/UE e os Regulamentos (CE) n.º 1060/2009 e (UE) n.º 648/2012 <sup>6</sup>
SFTR	Regulamento (UE) 2015/2365 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativo à transparência

---

<sup>1</sup> JO L 201 de 27.7.2012, p. 1.

<sup>2</sup> JO L 173 de 12.6.2014, p. 84.

<sup>3</sup> JO L 302 de 17.11.2009, p. 1.

<sup>4</sup> JO L 333 de 27.12.2022, p. 1.

<sup>5</sup> JO L 171 de 29.6.2016, p. 1.

<sup>6</sup> JO L 347 de 28.12.2017, p. 35.

das operações de financiamento através de valores mobiliários e de reutilização e que altera o Regulamento (UE) n.º 648/2012<sup>7</sup>

## 2.2 Abreviaturas

AIR	Administrador de índices de referência
ANEI	Administrador não executivo independente
ANR	Agência de notação de risco
APA	Sistema de publicação autorizado
ARM	Mecanismo de comunicação aprovado
DC	Documento de consulta
DRSP	Prestador de serviços de comunicação de dados
ESMA	Autoridade Europeia dos Valores Mobiliários e dos Mercados
Função CI	Função de Controlo Interno
IA	Inteligência artificial
IG	Informação destinada aos órgãos de gestão
NTR	Normas técnicas regulamentares
Quadro CI	Quadro de Controlo Interno
Regulamento DORA	Regulamento Resiliência Operacional Digital
RT	Repositório de transações
SR	Repositório de titularizações
TIC	Tecnologias da informação e comunicação
UE	União Europeia

---

<sup>7</sup> JO L 337 de 23.12.2015, p. 1.

## 2.3 Definições

Direção	<p>As pessoas que ocupam os cargos hierárquicos mais elevados e que garantem a gestão diária da entidade supervisionada. Normalmente, trata-se do diretor executivo (CEO) ou equivalente e seus subordinados diretos.</p>
Entidades supervisionadas	<p>Para efeitos das presentes Orientações, entende-se as entidades sob a supervisão da ESMA, nomeadamente:</p> <ul style="list-style-type: none"><li>▪ AIR</li><li>▪ ANR</li><li>▪ DRSP (excluindo prestadores de informações consolidadas)</li><li>▪ SR</li><li>▪ RT</li></ul>
Infraestruturas de transparência do mercado	<p>Para efeitos das presentes Orientações, tais infraestruturas abrangem:</p> <ul style="list-style-type: none"><li>▪ Prestadores de serviços de comunicação de dados</li><li>▪ Repositórios de titularizações e</li><li>▪ Repositórios de transações</li></ul>
Órgão de Gestão	<p>O órgão ou os órgãos nomeados de acordo com o direito nacional, com poderes para estabelecer a estratégia, os objetivos e a orientação geral da entidade, e que supervisionam e acompanham as decisões de gestão e incluem as pessoas que dirigem efetivamente as atividades da entidade.</p> <p>Refere-se aos órgãos de administração mais elevados de uma organização.</p> <p>O termo é definido no artigo 3.º, n.º 1, ponto (20), do Regulamento IR e no artigo 2.º, n.º 1, ponto (22), do MIFIR.</p> <p>Abrange os conceitos de:</p> <ul style="list-style-type: none"><li>▪ «Conselho de administração ou de supervisão» de uma agência de notação de risco, fazendo parte dos «quadros superiores», na aceção do artigo 3.º, n.º 1, alínea n), do Regulamento ANR</li><li>▪ «o órgão de administração ou de supervisão, ou ambos, nos termos da lei nacional das sociedades», na aceção do artigo 2.º, n.º 27, do EMIR</li></ul>
Regulamentação aplicável	<p>Para efeitos das presentes Orientações, tal regulamentação abrange:</p> <ul style="list-style-type: none"><li>▪ Regulamento IR</li></ul>

- Regulamento ANR
- EMIR
- MiFIR
- SECR
- SFTR

### **3 Finalidade**

5. As presentes Orientações estabelecem as expectativas da ESMA no que diz respeito às componentes e características de um quadro de controlo interno eficaz e às funções dos diferentes controlos internos no âmbito de uma entidade supervisionada.

## **4 Obrigações em matéria de cumprimento e de comunicação de informações**

### **4.1 Natureza das presentes Orientações**

6. O presente documento contém Orientações emitidas ao abrigo do artigo 16.º do Regulamento ESMA. Em conformidade com o disposto no artigo 16.º, n.º 3, do Regulamento ESMA, as entidades supervisionadas desenvolvem todos os esforços para dar cumprimento a estas Orientações.

### **4.2 Obrigação de comunicação de informação**

7. Os participantes no mercado financeiro às quais as presentes Orientações se destinam não estão obrigados a informar se as cumprem. A ESMA avaliará a aplicação destas Orientações pelas entidades supervisionadas, supervisionando e monitorizando continuamente as atividades das mesmas.
8. No quadro da aplicação destas Orientações, a ESMA respeitará o princípio da proporcionalidade. Embora se espere que todas as entidades supervisionadas demonstrem que os seus sistemas de controlo interno apresentam as características de eficácia descritas nestas Orientações, a ESMA calibrará as suas expectativas nos termos da secção 4.2 de acordo com a natureza, a dimensão, a complexidade e o perfil de risco global da entidade supervisionada e com base na forma como essas características podem afetar a proteção dos investidores, o funcionamento ordenado do mercado e a estabilidade financeira.

9. Na avaliação da natureza de uma entidade supervisionada, a ESMA terá em conta a atividade e o tipo de operações da entidade supervisionada, incluindo o seu papel/missão no mercado, o tipo, a diversidade e a importância crítica dos produtos e serviços oferecidos pela mesma.
10. Na avaliação da escala da atividade de uma entidade supervisionada, a ESMA terá em conta fatores relevantes, incluindo o número de efetivos, as receitas, o número de clientes e produtos, a quota de mercado, as interligações com outras indústrias/infraestruturas, os serviços auxiliares e a sua relação com os serviços principais e outros fatores específicos da dimensão e do impacto de mercado da entidade supervisionada.
11. Na avaliação da complexidade de uma entidade supervisionada, a ESMA terá em conta, entre outros fatores, a sua estrutura organizativa e as suas disposições (estrutura e relações de grupo, serviços partilhados, externalização, etc.), bem como as suas características operacionais no que respeita a pessoas, processos, tecnologia, ofertas de produtos e interligações.
12. Ao calibrar as suas expectativas, a ESMA tem em conta as condições do registo ou reconhecimento de uma entidade supervisionada. A natureza, a dimensão e a complexidade de uma entidade supervisionada podem mudar após o seu registo ou reconhecimento, cabendo-lhe a responsabilidade de garantir que os seus controlos internos permaneçam adequados à sua natureza, dimensão e complexidade. Através da sua supervisão, a ESMA informará caso possua um limiar de expectativas mais elevado ao abrigo das secções 5.1 e 5.2 do que aquele definido no momento do registo ou reconhecimento.

## 5 Orientações sobre o controlo interno

13. A fim de demonstrar que as entidades supervisionadas cumprem o disposto no n.º 2 das presentes Orientações, as entidades supervisionadas devem demonstrar que as suas políticas, procedimentos e práticas de trabalho atingem os objetivos enunciados nas secções **5.1** (Quadro de Controlo Interno) e **5.2** (Funções de Controlo Interno) das presentes Orientações.

### 5.1 Quadro de Controlo Interno

14. Para assegurar um quadro de CI eficaz, as entidades supervisionadas devem integrar as seguintes componentes e características nas suas políticas, procedimentos e práticas de trabalho.

#### *Princípios gerais*

15. O órgão de gestão da entidade supervisionada é responsável pela supervisão e aprovação de todas as componentes do quadro de CI, bem como por supervisionar que as suas componentes são sujeitas a acompanhamento e a atualização regular por parte da direção. A direção da entidade supervisionada é responsável pela definição, aplicação e atualização das políticas, procedimentos e práticas de controlo interno escritos subjacentes às componentes do quadro de CI.
16. No âmbito da implementação destas políticas e procedimentos, uma entidade supervisionada deve dispor de um processo de tomada de decisão claro, transparente e documentado, bem como de uma clara atribuição de funções e responsabilidades, no âmbito do seu quadro de CI, incluindo os seus segmentos de atividade e funções de CI.

#### **Componente 1.1 Ambiente de controlo**

17. O órgão de gestão e a direção de uma entidade supervisionada contribuem para a mensagem que é comunicada do topo para a base quanto à importância do controlo interno. A direção é responsável pelo desenvolvimento e a execução do controlo interno e pela avaliação da adequação e eficácia do ambiente de controlo. O órgão de gestão exerce a supervisão da direção executiva nestes domínios.

#### **Características**

- 1.1.1** A direção da entidade supervisionada é responsável por estabelecer uma forte cultura ética e de conformidade no seio da entidade supervisionada através da aplicação de políticas e procedimentos que regulem a conduta do respetivo pessoal.

- 1.1.2** A direção da entidade supervisionada é responsável por assegurar que as políticas e procedimentos da entidade supervisionada:
- i. especificam que a atividade da entidade supervisionada deve ser conduzida em conformidade com os regulamentos aplicáveis e com os valores empresariais da entidade supervisionada;
  - ii. clarificam que, além da conformidade com os requisitos legais e regulamentares e as políticas internas, os membros do pessoal devem assumir uma conduta honesta e íntegra e exercer as suas funções com os devidos profissionalismo, zelo e diligência; e
  - iii. asseguram que os membros do pessoal estão cientes das potenciais medidas disciplinares, ações legais e sanções decorrentes de comportamentos incorretos e inaceitáveis.
- 1.1.3** A direção da entidade supervisionada deve estabelecer, manter e atualizar regularmente, por escrito, procedimentos, mecanismos e políticas de controlo interno adequados.
- 1.1.4** A direção da entidade supervisionada é responsável pelas atividades que subcontrata a prestadores de serviços externos ou que delega noutros parceiros comerciais.

## **Componente 1.2 Gestão de risco**

18. Para efeitos de uma gestão eficaz do risco, as entidades supervisionadas devem assegurar que dispõem de um processo dinâmico e em constante evolução que permita identificar, avaliar e medir todos os riscos passíveis de afetar a capacidade da entidade supervisionada de cumprir as suas obrigações previstas nos regulamentos aplicáveis ou de assegurar a continuidade do seu funcionamento. Tal inclui, por exemplo, os riscos decorrentes da utilização de novas tecnologias pela entidade supervisionada e as alterações no seu panorama de riscos externos. O processo deve permitir à entidade supervisionada acompanhar, gerir, atenuar e comunicar de forma adequada os riscos significativos para a concretização dos objetivos.

### **Características**

- 1.2.1** A entidade supervisionada deve realizar as respetivas avaliações internas dos riscos de acordo com uma metodologia global definida de avaliação de risco.
- 1.2.2** A mesma deve definir a sua apetência pelo risco e identificar os níveis de tolerância ao risco.

- 1.2.3** A metodologia de avaliação do risco da entidade supervisionada deve abranger todos os segmentos de atividade e as funções de CI da entidade supervisionada.
- 1.2.4** O processo de avaliação dos riscos da entidade supervisionada deve identificar e avaliar as alterações passíveis de ter um impacto significativo no sistema de controlo interno. Isso inclui mudanças no seu ambiente, organização, atividades e operações.
- 1.2.5** A metodologia de avaliação do risco da entidade supervisionada deve ser objeto de evolução e melhoria contínuas.

### **Componente 1.3 Atividades de controlo**

19. As atividades de controlo devem ter um carácter de prevenção, deteção, correção ou dissuasão.

#### **Características**

- 1.3.1** *Separação de funções* — A entidade supervisionada deve assegurar uma separação adequada de funções, de forma a gerir os riscos de conflitos de interesses, fraude e erro humano. A separação de funções deve assegurar que as pessoas responsáveis pela execução de uma tarefa não sejam simultaneamente as únicas responsáveis pela aprovação dos respetivos resultados. Em especial, as pessoas responsáveis pelo desenvolvimento, execução ou aprovação de uma tarefa ou elemento de trabalho não devem ser as únicas responsáveis pela sua validação, avaliação e revisão.<sup>8</sup> Quando tal não puder ser evitado, essa situação deve ser mitigada assegurando que os colaboradores em causa não sejam responsáveis exclusivos pela atividade.<sup>9</sup>
- 1.3.2** *Documentação* — A entidade supervisionada deve documentar as políticas e os procedimentos que abrangem todas as atividades empresariais sujeitas às disposições dos regulamentos aplicáveis.
- 1.3.3** *Controlos e testes de controlo documentados* — A entidade supervisionada deve documentar os principais controlos implementados para garantir o

---

<sup>8</sup> Por exemplo, os colaboradores responsáveis pelas atividades de desenvolvimento de sistemas não devem estar envolvidos na gestão de bases de dados, operações de TI e gestão e manutenção de sistemas e redes de TI. No caso das ANR, i) as pessoas que realizam a análise de uma notação de risco não devem ser as únicas responsáveis pela aprovação da notação de risco, ii) as pessoas responsáveis pelo desenvolvimento de metodologias de notação de risco não devem ser as únicas responsáveis pela sua aprovação; iii) as pessoas responsáveis pela validação, avaliação ou revisão de uma metodologia de notação de risco não devem ser as únicas responsáveis pela aprovação da validação, avaliação ou revisão.

<sup>9</sup> Por exemplo, através de uma verificação «de quatro olhos».

cumprimento das políticas e dos procedimentos relevantes para o Regulamento ANR.

- 1.3.4** *Designação de responsabilidades* — A entidade supervisionada deve designar de forma clara e definida os cargos ou funções responsáveis pela realização dos controlos relacionados com as obrigações previstas nos regulamentos aplicáveis e especificar as respetivas tarefas e responsabilidades. Ao fazê-lo, a entidade supervisionada deve distinguir entre os controlos-chave diários a nível da empresa e os realizados por funções de controlo específicas.
- 1.3.5** *Autorizações e aprovações* — A entidade supervisionada deve dispor de processos ou mecanismos de autorização que garantam que apenas as pessoas autorizadas têm acesso a informações e ferramentas com base no princípio da necessidade de conhecer e dos privilégios mínimos. A entidade supervisionada deve também dispor de processos ou mecanismos em todas as atividades empresariais, a fim de assegurar que as atividades são aprovadas e executadas apenas por membros do pessoal que atuem no âmbito da sua autoridade.<sup>10</sup>
- 1.3.6** *Verificações, validações, reconciliações e revisões* — A entidade supervisionada deve tomar medidas para detetar e agir em caso de atividades inadequadas, não autorizadas, erróneas ou fraudulentas.<sup>11</sup>
- 1.3.7** *Controlos gerais das tecnologias da informação e da comunicação (TIC)* (apenas para entidades supervisionadas não sujeitas ao Regulamento DORA) — A entidade supervisionada deve implementar estratégias, políticas e procedimentos que assegurem a resiliência operacional digital dos seus sistemas de TIC no apoio aos respetivos processos empresariais.

A entidade supervisionada deve conceber os seus controlos e soluções de TIC de forma proporcionada. Por conseguinte, os controlos em matéria de TIC variarão entre as organizações em função da natureza, escala e complexidade dos processos empresariais subjacentes, bem como das funções relevantes apoiadas por esses sistemas.

As entidades supervisionadas devem garantir que dispõem de controlos adequados para garantir a qualidade dos dados, em termos de disponibilidade, confidencialidade e integridade, incluindo a validação dos dados, os controlos

---

<sup>10</sup> Por exemplo, no caso das ANR, apenas as pessoas designadas como responsáveis pelas respetivas tarefas devem realizar o processo de notação de risco, a validação das metodologias e a revisão dos resultados da validação.

<sup>11</sup> Tal inclui a validação dos dados e controlos de introdução de dados, bem como a revisão das listas de acesso autorizado a informações confidenciais. Para as ANR, esses controlos aplicam-se às atividades de notação de risco e aos processos subjacentes a essas atividades, tais como a validação da metodologia de crédito/validação de modelo.

sobre o seu tratamento e os procedimentos de verificação dos ficheiros de dados.

A entidade supervisionada deve estabelecer um sistema de gestão de segurança da informação relevante e atividades de controlo conexas. Como parte deste processo, a entidade supervisionada deve determinar os controlos necessários para garantir a autenticidade, confidencialidade, integridade e disponibilidade da informação, uma vez que esta é tratada desde a fonte até ao utilizador final.

A entidade supervisionada deve estabelecer e documentar todas as atividades relevantes de controlo dos processos de aquisição, desenvolvimento e manutenção de TIC.

## **Componente 1.4 Informação e comunicação**

20. As entidades supervisionadas devem estabelecer procedimentos para a partilha descendente de informações exatas, completas e de boa qualidade com o pessoal e as partes interessadas externas. As entidades supervisionadas devem igualmente estabelecer procedimentos para a comunicação regular de informações sobre o sistema de controlo interno e as respetivas atividades ao órgão de gestão e à direção, incluindo dados relativos ao cumprimento e à eficácia dos controlos internos.

### **Características**

- 1.4.1** A entidade supervisionada deve assegurar uma comunicação adequada, tanto interna como externa, garantindo que as informações partilhadas sejam precisas, completas e de elevada qualidade, e que cheguem atempadamente ao mercado, aos clientes, aos utilizadores dos seus produtos e serviços, bem como às entidades reguladoras.
- 1.4.2** A entidade supervisionada deve estabelecer canais de comunicação ascendente, incluindo um procedimento de denúncia de irregularidades, que permitam reportar questões materiais de controlo interno ao órgão de gestão e à direção. O órgão de gestão e a direção também devem receber atualizações regulares sobre o sistema e as atividades de controlo interno, incluindo sobre segurança da informação. A entidade supervisionada deve possuir procedimentos de escalonamento para resolver qualquer desacordo material entre as funções de controlo interno e as unidades operacionais.
- 1.4.3** A entidade supervisionada deve estabelecer canais de comunicação descendente do órgão de gestão, da direção e das funções de controlo para os colaboradores. Tais canais deverão incluir atualizações regulares sobre os objetivos e as responsabilidades em matéria de controlo interno, a

comunicação das questões de verificação do cumprimento identificadas, bem como sessões de apresentação e formação sobre políticas e procedimentos.

## **Componente 1.5 Atividades de acompanhamento**

21. As entidades supervisionadas devem assegurar-se de que realizam atividades de acompanhamento que ajudem a determinar se os componentes do sistema de controlo interno de uma entidade supervisionada estão presentes e funcionam eficazmente.

### **Características**

- 1.5.1** A entidade supervisionada deve assegurar que as avaliações do sistema de controlo interno sejam realizadas a diferentes níveis da entidade supervisionada, tais como segmentos de atividade, funções de controlo e auditoria interna ou funções de avaliação independente.
- 1.5.2** As atividades de acompanhamento devem ser concebidas e realizadas de forma a permitir à entidade supervisionada verificar se cumpre os próprios requisitos legais e regulamentares, incluindo a adesão aos próprios códigos de conduta, políticas e procedimentos internos. Isso inclui as políticas e procedimentos de segurança da informação da entidade supervisionada.
- 1.5.3** As avaliações dos sistemas de controlo interno devem ser realizadas numa base regular ou temática, ou através de uma combinação de ambas.
- 1.5.4** As entidades supervisionadas devem integrar avaliações contínuas nos processos empresariais e ajustá-las às condições em evolução.
- 1.5.5** As entidades supervisionadas devem assegurar que as irregularidades identificadas nas avaliações de acompanhamento e as medidas de reparação necessárias são comunicadas ao órgão de gestão e à direção, os quais devem, em seguida, acompanhar a aplicação oportuna das medidas corretivas.
- 1.5.6** No caso da subcontratação, a entidade supervisionada deve atribuir a um membro do pessoal a tarefa de acompanhamento dos processos operacionais subcontratados. As entidades supervisionadas devem assegurar que os prestadores de serviços recebam informações suficientes sobre os objetivos e as expectativas de prestação, e que a devida diligência seja efetuada antes da designação do prestador.

## 5.2 Funções de Controlo Interno

22. Para garantir o funcionamento eficaz das funções de CI, as entidades supervisionadas devem incluir os seguintes componentes e características nas suas políticas, procedimentos e práticas de trabalho.

### *Princípios gerais*

23. A ESMA considera que as funções de CI das entidades supervisionadas devem dispor de recursos suficientes e ser dotadas de pessoal com conhecimentos especializados suficientes para o desempenho das suas funções. O pessoal que trabalha em Funções de CI deve possuir conhecimentos técnicos suficientes sobre as atividades da entidade supervisionada e os riscos associados. Nos casos em que as entidades supervisionadas tenham subcontratado tarefas operacionais importantes de uma Função de CI ao nível do grupo ou a uma entidade externa, a ESMA considera que a entidade supervisionada mantém a plena responsabilidade pelas atividades subcontratadas dessa Função de CI. A ESMA considera que as entidades supervisionadas devem assegurar que os colaboradores responsáveis pelas funções de CI têm um nível hierárquico adequado, que lhes confira a autoridade necessária para cumprir as suas responsabilidades. Por exemplo, os membros do pessoal responsáveis pelas funções de verificação do cumprimento, gestão de riscos, auditoria interna, gestão da segurança da informação, análise (para as ANR) e supervisão (no caso dos AIR) devem dispor de acesso ilimitado e apresentar relatórios ao órgão de gestão com caráter regular.
24. As atividades podem ser desempenhadas ao nível do grupo ou por outras entidades jurídicas no âmbito de uma estrutura empresarial, desde que essa estrutura não prejudique a capacidade do órgão de gestão da entidade supervisionada de assegurar a supervisão, nem a capacidade da direção de gerir eficazmente os seus riscos, nem a capacidade da ESMA de supervisionar eficazmente a entidade supervisionada. Em todos os casos, aplica-se a Orientação n.º 1.1.4.
25. A fim de assegurar a independência das funções de CI de uma entidade supervisionada, a ESMA espera que a entidade supervisionada tenha em conta os seguintes princípios ao definir as funções e responsabilidades dessas funções de CI:
- i. as funções de CI devem ser funcionalmente independentes das funções ou atividades que constituem o objeto do seu acompanhamento, auditoria ou controlo;
  - ii. as funções de CI não devem desempenhar quaisquer tarefas operacionais que se enquadrem no âmbito das atividades que se destinam a acompanhar, auditar ou controlar;

- iii. o responsável por uma função de CI não deve reportar a uma pessoa diretamente responsável pela gestão das atividades que essa função acompanha, audita ou controla;
26. o pessoal que desempenha responsabilidades relacionadas com funções de CI deve ter acesso a formação interna ou externa relevante, a fim de assegurar a adequação das suas competências ao desempenho das tarefas.

### **Proporcionalidade — Funções de Controlo Interno**

27. Embora se espere que todas as entidades supervisionadas apresentem funções de CI eficazes conforme descrito nas presentes orientações, a ESMA ajusta as suas expectativas de acordo com a natureza, a dimensão e a complexidade de cada entidade supervisionada, conforme indicado na secção 3.4 destas Orientações.
28. Esta secção descreve mais pormenorizadamente a forma como a ESMA tem em conta a proporcionalidade na sua supervisão das funções de CI.

### **Separação de funções**

29. A separação de funções deve ser integrada no desenvolvimento das atividades de controlo. No entanto, podem existir alguns casos em que o direito da União não exija a separação de funções e que essa separação não seja prática, tendo em conta a natureza, a dimensão e a complexidade da entidade supervisionada. Neste caso, os controlos alternativos podem ser mais adequados. Quando são utilizados outros controlos, as entidades supervisionadas devem documentar os fundamentos subjacentes à alternativa, identificar os possíveis riscos, aplicar controlos compensatórios para os resolver e demonstrar que a alternativa não prejudica o ambiente de controlo.

### **Recursos**

30. Para algumas entidades supervisionadas, pode não ser proporcional dispor de colaboradores a tempo inteiro em todas as funções, tendo em conta a sua natureza, dimensão e complexidade. Nestes casos, uma entidade supervisionada pode optar ajustar o número de horas dos recursos às atividades de controlo ou subcontratar a atividade.

### **Especialização no âmbito das funções**

31. À medida que uma entidade supervisionada cresce e o seu ambiente de controlo se consolida, deve recorrer à especialização do pessoal para aproveitar a experiência dos colaboradores em processos-chave ou áreas de risco. As entidades supervisionadas de determinada natureza, escala e complexidade devem dispor de equipas de

acompanhamento ou de investigação específicas no âmbito da respetiva função de verificação do cumprimento.

### **Maturidade das atividades de controlo**

32. A maturidade das atividades de controlo (ou seja, manual, híbrida, automatizada e, em alguns casos, com ferramentas de inteligência artificial) deve refletir a natureza, a escala e a complexidade, bem como o perfil de risco global da entidade supervisionada. No que respeita às entidades supervisionadas de determinada natureza, escala e complexidade, deve existir um grau mais elevado de controlos automáticos, bem como uma maior integração entre os sistemas das funções de controlo, a fim de otimizar as atividades de acompanhamento e o reporte da informação de gestão à direção e ao órgão de gestão por parte da entidade supervisionada.

### **Componente 2.1 Função de verificação do cumprimento**

33. A Função de Verificação do Cumprimento de uma entidade supervisionada é responsável por controlar e comunicar o cumprimento, pela entidade supervisionada e respetivos colaboradores, das obrigações a que está sujeita por força do regulamento aplicável. A Função de Verificação do Cumprimento é responsável por cumprir as alterações legislativas e regulamentares aplicáveis às suas atividades. A Função de Verificação do Cumprimento é também responsável por aconselhar o órgão de gestão sobre as leis, regras, regulamentos e normas que a entidade supervisionada deve cumprir, bem como por avaliar, em conjugação com outras funções relevantes, o possível impacto de quaisquer alterações do quadro jurídico ou regulamentar nas atividades da entidade supervisionada.

#### **Características**

- 2.1.1** A Função de Verificação do Cumprimento deve desempenhar as suas funções de forma independente dos segmentos de atividade e apresentar relatórios periódicos ao órgão de gestão da entidade supervisionada e, se for caso disso, diretamente aos ANEI.
- 2.1.2** A Função de Verificação do Cumprimento deve aconselhar e ajudar os membros do pessoal a cumprir as obrigações previstas no regulamento aplicável. A Função de Verificação do Cumprimento deve ser proativa na identificação de riscos e de eventuais incumprimentos através do acompanhamento e avaliação atempados das atividades, bem como do acompanhamento das medidas corretivas.
- 2.1.3** A Função de Verificação do Cumprimento assegura que a verificação é efetuada através de um programa de acompanhamento da verificação do cumprimento estruturado e bem definido. O âmbito das atividades de verificação do

cumprimento deve abranger todos os processos e sistemas empresariais e informáticos que possam afetar a conformidade da entidade supervisionada com o regulamento aplicável.

- 2.1.4** A Função de Verificação do Cumprimento deve, quando aplicável e em colaboração com outras funções relevantes, avaliar o possível impacto de quaisquer alterações do quadro jurídico ou regulamentar nas atividades da entidade supervisionada e, se for caso disso, comunicar com a Função de Gestão de Risco relativamente ao risco de incumprimento da entidade supervisionada.
- 2.1.5** A Função de Verificação do Cumprimento deve assegurar a observância das políticas de conformidade e reportar ao órgão de gestão e à direção qualquer risco de conformidade da entidade supervisionada.
- 2.1.6** A Função de Verificação do Cumprimento deve colaborar com a Função de Gestão de Risco, trocando as informações necessárias ao desempenho das respetivas tarefas.
- 2.1.7** As conclusões da Função de Verificação do Cumprimento devem ser tidas em conta pelo órgão de Gestão e pela direção, bem como pela Função de Gestão de Risco, no âmbito dos respetivos processos de avaliação de risco.

## **Componente 2.2 Função de Gestão de Risco**

- 34. A ESMA considera que a Função de Gestão de Risco da entidade supervisionada é responsável pelo desenvolvimento e pela implementação do quadro de gestão de risco.

### **Características**

- 2.2.1** A Função de Gestão de Risco desempenha as suas funções de forma independente dos segmentos de atividade e unidades cujos riscos supervisiona, mas não deve ser impedida de interagir com os mesmos.
- 2.2.2** A Função de Gestão de Risco deve garantir que todos os riscos que possam afetar a capacidade de uma entidade supervisionada de cumprir as suas obrigações nos termos dos regulamentos aplicáveis, ou a sua continuidade operacional, sejam identificados, avaliados e medidos. Os riscos materialmente relevantes para estes objetivos devem, então, ser acompanhados, geridos, mitigados e devidamente reportados às unidades relevantes da entidade supervisionada, em tempo útil.

- 2.2.3** A Função de Gestão de Risco controla o perfil de risco da entidade supervisionada tendo em conta a apetência pelo risco da mesma, a fim de permitir a tomada de decisões.
- 2.2.4** A Função de Gestão de Risco presta aconselhamento sobre propostas e decisões relacionadas com o risco tomadas pelos diferentes segmentos de atividade e informa o órgão de gestão sobre a conformidade das mesmas com a apetência pelo risco e os objetivos da entidade supervisionada.
- 2.2.5** Sempre que necessário, a Função de Gestão de Risco recomenda melhorias ao quadro de gestão de risco e alterações às políticas e procedimentos de risco. A Função de Gestão de Risco deve rever os limites de risco de acordo com quaisquer alterações na apetência pelo risco da organização.

### **Componente 2.3 Função de Gestão da Segurança da Informação (apenas para entidades supervisionadas não sujeitas ao Regulamento DORA)**

- 35. A Função de Gestão da Segurança da Informação de uma entidade supervisionada é responsável pelo desenvolvimento e implementação da segurança da informação no seio da entidade supervisionada. A entidade supervisionada deve criar uma função que promova uma cultura de segurança da informação no seu próprio seio.

#### **Características**

- 2.3.1** A Função de Gestão da Segurança da Informação é responsável pela revisão e acompanhamento do cumprimento, por parte da entidade supervisionada, das políticas e procedimentos de segurança da informação da entidade supervisionada.
- 2.3.2** A Função de Gestão da Segurança da Informação deve gerir as atividades de segurança da informação da entidade supervisionada.
- 2.3.3** A Função de Gestão da Segurança da Informação deve criar e implementar um programa de sensibilização para a segurança da informação destinado ao pessoal, a fim de reforçar a cultura de segurança e desenvolver uma ampla compreensão do quadro de segurança da informação da entidade supervisionada.
- 2.3.4** A Função de Gestão da Segurança da Informação deve reportar e aconselhar o órgão de gestão e a direção sobre o estado do sistema de gestão da segurança da informação e sobre os riscos (por exemplo, informações sobre projetos de segurança da informação, incidentes de segurança da informação e os resultados das revisões de segurança da informação).

## **Componente 2.4 Função de Auditoria Interna**

36. A Função de Auditoria Interna de uma entidade supervisionada é responsável por prestar uma garantia independente e objetiva e uma atividade de aconselhamento destinada a melhorar o funcionamento da organização. Ajuda a organização a cumprir os seus objetivos através de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia do sistema de controlo interno.

### **Características**

- 2.4.1** A Função de Auditoria Interna deve desempenhar as suas funções de forma independente dos segmentos de atividade e de outras funções do setor das informações. Esta estrutura deve ser regida por uma carta de auditoria interna que define a sua função e responsabilidades e está sujeita a supervisão pelo órgão de gestão.
- 2.4.2** A Função de Auditoria Interna deve seguir uma abordagem baseada no risco e aderir às normas internacionais de auditoria interna.
- 2.4.3** A Função de Auditoria Interna analisa de forma independente e dá garantias objetivas de que as atividades da entidade supervisionada, incluindo as atividades subcontratadas, cumprem as políticas e os procedimentos da entidade supervisionada, bem como os requisitos legais e regulamentares aplicáveis.
- 2.4.4** A Função de Auditoria Interna estabelece, pelo menos uma vez por ano, com base nos objetivos anuais de controlo da auditoria interna, um plano de auditoria sujeitos à supervisão do órgão de gestão.
- 2.4.5** A Função de Auditoria Interna apresenta relatórios periódicos aos membros independentes do órgão de gestão ou ao Comité de Auditoria, caso existam.
- 2.4.6** A Função de Auditoria Interna comunica as suas recomendações de forma clara e coerente, permitindo ao órgão de gestão e à direção compreender a sua materialidade e definir prioridades em conformidade.
- 2.4.7** As recomendações da auditoria interna são objeto de um procedimento de acompanhamento formal por parte dos níveis de gestão adequados, tendo em vista a elaboração de relatórios e a garantia da sua aplicação efetiva e atempada.

## **Componente 2.5 Função de Revisão (apenas para as ANR)**

37. A Função de Revisão de uma ANR deve proceder à revisão das metodologias de notação de risco, pelo menos, uma vez por ano. A Função de Revisão da ANR deve também assegurar a validação e a revisão de novas metodologias, bem como de quaisquer alterações às metodologias existentes.

### **Características**

- 2.5.1** A Função de Revisão desempenha as suas funções de forma independente dos segmentos de atividade responsáveis pelas atividades de notação de risco e apresenta relatórios periódicos aos ANEI da ANR.
- 2.5.2** Os acionistas ou o pessoal da ANR envolvido no desenvolvimento empresarial não podem exercer as tarefas da Função de Revisão.
- 2.5.3** Os analistas não devem participar na aprovação de novas metodologias, nem na validação e revisão de metodologias, modelos e principais pressupostos de notação que tenham desenvolvido.
- 2.5.4** O pessoal afeto à Função de Revisão deve assegurar a responsabilidade exclusiva, ou deter a maioria dos direitos de voto, nas comissões responsáveis pela aprovação das metodologias, modelos e principais pressupostos de notação.
- 2.5.5** Os colaboradores da Função de Revisão responsáveis pela validação e/ou revisão de uma metodologia, e que também estão envolvidos na sua fase de desenvolvimento, não devem assegurar a responsabilidade exclusiva, ou deter a maioria dos direitos de voto, nas comissões responsáveis pela aprovação das metodologias.
- 2.5.6** Em caso de externalização da Função de Revisão, a ANR deve ter em conta a Orientação 1.5.6. Além disso, a ANR deve dispor de mecanismos de controlo interno adequados para garantir que cumpre de forma consistente os requisitos regulamentares e mantém padrões de qualidade analítica adequados.

## **Componente 2.6 Função de supervisão (apenas para AIR)<sup>12</sup>**

38. A Função de Supervisão supervisiona os principais aspetos do fornecimento de índices de referência. Isso inclui, entre outros, a revisão da definição e metodologia do índice de referência, a gestão de terceiros envolvidos no fornecimento do índice, a avaliação de

---

<sup>12</sup> Os AIR não significativos que aplicam o artigo 26.º do Regulamento IR devem aplicar as presentes Orientações de forma proporcional aos requisitos do artigo 26.º.

auditorias internas e externas ou revisões da estrutura de controlo do administrador e a comunicação às autoridades competentes de qualquer conduta indevida relevante.

### **Características**

- 2.6.1** A Função de Supervisão do AIR mantém a sua independência face a qualquer órgão de gestão ou função dos AIR e a qualquer entidade externa dos AIR. A independência parte do princípio de que os membros da Função de Supervisão não estão sujeitos a conflitos de interesses entre as suas atividades enquanto membros da Função de Supervisão e as suas outras atividades. O AIR deve implementar um quadro operacional de controlo interno para prevenir e atenuar eventuais conflitos de interesses.
- 2.6.2** O AIR deve dispor de políticas e procedimentos claros no que diz respeito à criação e às responsabilidades da Função de Supervisão e respetivos membros, incluindo políticas e procedimentos para as atualizações da metodologia dos índices de referência e as análises da integridade dos dados.
- 2.6.3** A Função de Supervisão dos AIR deve realizar uma autoavaliação periódica para avaliar a sua eficácia e a adequação dos seus membros para efeitos da função, bem como para identificar potenciais conflitos de interesses e propor domínios a melhorar, se necessário.
- 2.6.4** A Função de Supervisão dos AIR deve manter um canal de comunicação definido e regular com o órgão de gestão, a direção e outras funções-chave. A Função de Supervisão dos AIR deve também poder aceder e questionar as informações de gestão e receber atualizações sobre o estado das medidas corretivas na sequência de auditorias internas e externas, relatórios de risco e de conformidade.
- 2.6.5** A Função de Supervisão dos AIR deve manter um canal de comunicação definido com as autoridades competentes relevantes, incluindo a comunicação de qualquer má conduta ou violação por parte de administradores ou contribuintes.