EBA/GL/2017/11

21/03/2018

Orientações

sobre governo interno

1. Obrigações de cumprimento e de comunicação de informação

Natureza das presentes Orientações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1093/2010[1]. Nos termos do artigo 16.º, n.º 3, do referido Regulamento, as autoridades competentes e as instituições financeiras devem desenvolver todos os esforços para dar cumprimento às Orientações.

2. As Orientações refletem a posição da EBA sobre práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União deve ser aplicada num domínio específico. As autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010, às quais as presentes Orientações se aplicam devem dar cumprimento às mesmas, incorporando-as nas suas práticas de supervisão conforme for mais adequado (por exemplo, alterando o seu enquadramento jurídico ou os seus processos de supervisão), incluindo nos casos em que as orientações são aplicáveis, em primeira instância, a instituições.

Requisitos de notificação

3. Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes confirmam à EBA se dão ou tencionam dar cumprimento às presentes Orientações, ou, caso contrário, indicam as razões para o não cumprimento até 21/05/2018. Na ausência de qualquer notificação até à referida data, a EBA considerará que as autoridades competentes em causa não cumprem as Orientações. As notificações efetuam-se mediante o envio do modelo disponível no sítio Web da EBA para o endereço compliance@eba.europa.eu com a referência «EBA/GL/2017/11». As notificações devem ser apresentadas por pessoas devidamente autorizadas para o efeito pelas respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deve igualmente ser comunicada à EBA.

4. As notificações serão publicadas no sítio Web da EBA, em conformidade com o disposto no artigo 16.º, n.º 3.

[1] Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão (JO L 331, 15.12.2010, p.12).

2. Objeto, âmbito de aplicação e definições

Objeto

5. As presentes orientações especificam os sistemas, processos e mecanismos de governo interno que as instituições de crédito e as empresas de investimento devem aplicar em conformidade com o artigo 74.º, n.º 1, da Diretiva 2013/36/UE[2], a fim de assegurar a gestão efetiva e prudente da instituição.

Destinatários

6. As presentes orientações destinam-se às autoridades competentes, na aceção do artigo 4.º, n.º 1, ponto 40, do Regulamento 575/2013/UE[3], incluindo o Banco Central Europeu no âmbito das matérias relacionadas com as funções conferidas pelo Regulamento (UE) n.º 1024/2013, e às instituições definidas no artigo 4.º, n.º 1, ponto 3, do Regulamento UE n.º 575/2013.

Âmbito de aplicação

7. As presentes orientações são aplicáveis aos sistemas de governo das instituições, incluindo a sua estrutura organizacional e a correspondente delimitação de responsabilidades, aos processos destinados à identificação, gestão, monitorização, e reporte dos riscos a que estão ou possam vir a estar expostas, e à estrutura de controlo interno.

8. As orientações pretendem abranger todas as diferentes estruturas de administração e fiscalização existentes e não defendem nenhuma estrutura em particular. As orientações não interferem na atribuição geral de competências à luz do direito das sociedades nacional. Por conseguinte, devem ser aplicadas, independentemente da estrutura de administração e fiscalização utilizada (uma estrutura monista e/ou dualista e/ou outra estrutura) nos Estados-membros. O órgão de administração, tal como definido no artigo 3.º, n.º 1, pontos 7 e 8, da Diretiva 2013/36 UE, deve ser entendido como tendo funções de gestão (executivas) e de fiscalização (não executivas) [4].

9. As expressões «órgão de administração na sua função de gestão» e «órgão de administração na sua função de fiscalização» são utilizadas nas presentes orientações sem qualquer

[2] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

[3] Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1-337).

[4] Ver também o considerando 56 da Diretiva 2013/36/UE.

referência a uma estrutura de governo específica. As referências à função de gestão (executiva) ou à função de fiscalização (não executiva) devem ser entendidas como aplicáveis às entidades ou membros do órgão de administração e fiscalização responsáveis por essa função, nos termos do direito nacional. Quando implementam as presentes orientações, as autoridades competentes devem ter em conta o direito das sociedades do seu país e, sempre que necessário, especificar a que órgão social ou membros do órgão de administração se aplicam essas funções.

10. Nos Estados-Membros onde o órgão de administração delega, em parte ou na totalidade, as funções executivas numa pessoa ou num órgão executivo interno (p. ex., um administrador executivo [CEO], uma equipa de gestão ou um comité executivo), deve considerar-se que as pessoas que desempenham essas funções executivas em virtude dessa delegação integram a função de gestão do órgão de administração. Para efeito das presentes orientações, qualquer referência ao órgão de administração na sua função de gestão deve ser entendida como incluindo igualmente os membros do órgão executivo ou o CEO, na aceção das presentes orientações, mesmo que não tenham sido propostos ou formalmente nomeados como membros dos órgãos sociais ou do órgão de administração da instituição, nos termos do direito nacional.

11. Nos Estados-Membros onde algumas responsabilidades são exercidas diretamente por acionistas, membros ou proprietários da instituição e não pelo órgão de administração, as instituições devem assegurar que essas responsabilidades e as decisões conexas estão, tanto quanto possível, harmonizadas com as orientações aplicáveis ao órgão de administração.

12. As definições de CEO, administrador com o pelouro financeiro (CFO) e titular de funções essenciais utilizadas nas presentes orientações não pretendem impor a nomeação desses intervenientes nem a criação dessas funções, exceto se forem exigidas pelo direito nacional ou direito da UE aplicável.

13. As instituições cumprem as presentes orientações, e as autoridades competentes garantem que as instituições as cumprem, em base individual, subconsolidada e consolidada, nos termos do artigo 109.º da Diretiva 2013/36/UE.

Definições

14. Salvo especificação em contrário, os termos utilizados e definidos na Diretiva 2013/36/UE têm o mesmo significado nas presentes orientações. Adicionalmente, para efeito das presentes orientações, aplicam-se as seguintes definições:

Apetência pelo risco	o nível agregado e os tipos de risco que uma instituição está disposta a assumir no contexto da sua capacidade de risco e de acordo com o seu modelo de negócio, para atingir os seus objetivos estratégicos.

Capacidade de risco	o nível máximo de risco que uma instituição pode assumir em função da sua base de fundos próprios, das suas capacidades de controlo e gestão de riscos e das restrições impostas pela regulação.
Cultura de risco	as normas, as atitudes e os comportamentos de uma instituição em matéria de sensibilização para o risco, assunção de riscos e gestão de riscos, bem como os controlos que influenciam as decisões em matéria de risco. A cultura de risco influencia as decisões da administração e dos funcionários nas atividades quotidianas e tem impacto nos riscos que estes assumem.
Instituições	instituições de crédito e empresas de investimento na aceção do artigo 4.º, n.º 1, ponto 3 do Regulamento (UE) n.º 575/2013.
Pessoal	todos os funcionários de uma instituição e das respetivas filiais no seu perímetro de consolidação, incluindo as filiais não abrangidas pela Diretiva 2013/36/UE e todos os membros do órgão de administração na sua função de gestão e na sua função de fiscalização.
Presidente da Comissão Executiva (CEO)	a pessoa responsável pela gestão e orientação global das atividades de negócio de uma instituição.
Administrador com o pelouro financeiro (CFO)	a pessoa que detém a responsabilidade global pela gestão de todas as seguintes atividades: gestão dos recursos financeiros, planeamento financeiro e informação financeira.
Responsáveis das funções de controlo interno	as pessoas ao mais alto nível hierárquico responsáveis pela gestão efetiva do funcionamento quotidiano das funções independentes de gestão de riscos, de verificação do cumprimento e de auditoria interna.
Titulares de funções essenciais	pessoas com uma influência significativa na direção da instituição, mas que não são membros do órgão de administração nem são o CEO. Incluem os responsáveispelas funções de controlo interno e o CFO, se estes não forem membros do órgão de administração, e, desde que identificadas pelas instituições numa abordagem baseado no risco, outras pessoas que exercem funções essenciais. Estas podem incluir os responsáveis dos segmentos de atividade significativas, sucursais no Espaço Económico Europeu/na Associação Europeia de Comércio Livre, filiais em países terceiros e outras funções internas.
Consolidação prudencial	a aplicação das normas prudenciais estabelecidas na Diretiva 2013/36/UE e no Regulamento (UE) n.º 575/2013 em base consolidada ou subconsolidada, nos termos da Parte I, Título II, Capítulo 2, do Regulamento n.º 575/2013. Inclui todas as filiais que

	sejam instituições ou instituições financeiras, na aceção do artigo 4.º, n.º 3, e do artigo 26.º, respetivamente, do Regulamento (UE) n.º 575/2013, e pode incluir as empresas de serviços auxiliares, na aceção do artigo 2.º, n.º 18, desse Regulamento, estabelecidas na UE e em países terceiros.
Instituição consolidante	uma instituição que é obrigada a cumprir os requisitos prudenciais com base na situação consolidada, em conformidade com a Parte I, Título II, Capítulo 2, do Regulamento n.º 575/2013.
Instituições significativas	as instituições referidas no artigo 131.º da Diretiva 2013/36/UE (instituições de importância sistémica global [G-SII] e outras instituições de importância sistémica [O-SII]) e, se for caso disso, outras instituições determinadas pela autoridade competente ou pelo direito nacional, com base numa avaliação da dimensão das instituições, da natureza e organização interna, do âmbito de aplicação e da complexidade das suas atividades.
Instituição cotada abrangida pela Diretiva 2013/36/EU	uma instituição cujos instrumentos financeiros são admitidos à negociação num mercado regulamentado ou num sistema de negociação multilateral, na aceção do artigo 4.º, n.º, 1, alíneas 21 e 22, da Diretiva 2014/65/UE, num ou mais Estados-Membros[5].
Acionista	uma pessoa que possui ações de uma instituição ou, dependendo da forma jurídica de uma instituição, outros proprietários ou membros da instituição.
Cargo de administração	uma posição como membro do órgão de administração de uma instituição ou outra entidade jurídica.

3. Implementação

Data de aplicação

15. As presentes orientações são aplicáveis a partir de 30 de junho de 2018.

Revogação

[5] Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE (JO L 173 de 12.6.2014, p. 349).

16. As orientações da EBA sobre a governação interna (GL 44), de 27 de setembro de 2011, são revogadas com efeito a partir de 30 de junho de 2018.

4. Orientações

Título I – Proporcionalidade

17. O princípio da proporcionalidade enunciado no artigo 74.º, nº. 2, da Diretiva 2013/36/UE tem por objetivo assegurar a coerência entre os sistemas de governo interno e o perfil de risco e o modelo de negócio de uma instituição a nível individual, de modo a que os objetivos dos requisitos regulamentares sejam efetivamente atingidos.

18. Quando desenvolvem e implementam sistemas de governo interno, as instituições devem ter em conta a sua dimensão e a sua organização interna, bem como a natureza, dimensão e complexidade das suas atividades. As instituições significativas devem dispor de sistemas de governo mais sofisticados, enquanto as instituições de menor dimensão e complexidade podem implementar sistemas de governo mais simples.

19. Para efeito da aplicação do princípio da proporcionalidade e a fim de assegurar a aplicação adequada dos requisitos, as instituições e as autoridades competentes devem ter em conta os critérios seguintes:

    a. a dimensão, em termos do total do balanço, da instituição e das suas filiais no âmbito da consolidação prudencial;

    b. a presença geográfica da instituição e a dimensão das suas operações em cada jurisdição;

    c. a forma jurídica da instituição, incluindo se faz parte de um grupo e, em caso afirmativo, a avaliação da proporcionalidade realizada pelo grupo;

    d. se a instituição está ou não cotada em bolsa;

    e. se a instituição está autorizada a utilizar modelos internos para medir os requisitos de fundos próprios (p. ex., o Método das Notações Internas);

    f. o tipo de atividades e serviços autorizados realizados pela instituição (p. ex., ver o Anexo I da Diretiva 2013/36/UE e o Anexo I da Diretiva 2014/65/UE);

    g. a estratégia e o modelo de negócio subjacentes, a natureza e complexidade das atividades de negócio e a estrutura organizacional da instituição;

    h. a estratégia de risco, a apetência pelo risco e o perfil de risco real da instituição, tendo igualmente em conta o resultado das avaliações SREP dos fundos próprios e da liquidez;

i. a titularidade e a estrutura de financiamento da instituição;

j. o tipo de clientes (p. ex., retalho, empresariais, institucionais, pequenas empresas, entidades públicas) e a complexidade dos produtos ou dos contratos;

k. as atividades subcontratadas e os canais de distribuição; e

l. os sistemas de tecnologias da informação (TI) existentes, incluindo os sistemas de continuidade e as atividades subcontratadasneste domínio.

Título II – Papel e composição do órgão de administração e dos comités

1 Papel e responsabilidades do órgão de administração

20. Nos termos do artigo 88.º, n.º 1, da Diretiva 2013/36/UE, o órgão de administração assume a responsabilidade última e global pela instituição e define, supervisiona e é responsável pela aplicação de sistemas de governo que assegurem a gestão efetiva e prudente da instituição.

21. Os deveres do órgão de administração devem ser claramente definidos e deve ser feita distinção entre os deveres da função de gestão (executiva) e os da função de fiscalização (não executiva). Os deveres e responsabilidades do órgão de administração devem ser descritos num documento escrito e devidamente aprovado pelo órgão de administração.

22. Os membros do órgão de administração têm pleno conhecimento da sua estrutura e responsabilidades, bem como da divisão de tarefas entre as diferentes funções do órgão de administração e dos seus comités. A fim de assegurar a existência de mecanismos adequados de controlo e equilíbrio, o processo de tomada decisão do órgão de administração não deve ser circunscrito a um único membro ou a um número reduzido de membros. O órgão de administração, no exercício da sua função de gestão e da sua função de fiscalização, deve interagir de forma efetiva. As duas funções devem trocar informações suficientes que lhes permitam desempenhar os respetivos papéis.

23. As responsabilidades do órgão de administração incluem a definição, a aprovação e a fiscalização da aplicação:

a. da estratégia comercial global e das políticas essenciais da instituição no quadro jurídico e regulamentar aplicável, tendo em conta os interesses financeiros e a solvabilidade da instituição a longo prazo;

b. da estratégia de risco global da instituição, incluindo a sua apetência pelo risco e o seu quadro de gestão de riscos, bem como de medidas destinadas a assegurar que o órgão de administração dedica tempo suficiente a questões em matéria de risco;

c. de um sistema de governo interno adequado e eficiente e de um sistema de controlo interno com uma estrutura organizacional clara e funções independentes e eficientes em matéria de gestão de riscos, verificação do cumprimento e auditoria, que tenham autoridade, estatuto e recursos suficientes para exercerem as suas funções;

d. dos montantes, tipos e distribuição dos fundos próprios internos e dos fundos próprios regulamentares adequados para cobrir os riscos da instituição;

e. de objetivos para a gestão da liquidez da instituição;

f. de uma política de remuneração consentânea com os princípios estabelecidos nos artigos 92.º a 95.º da Diretiva 2013/36/UE e com as orientações da EBA relativas a políticas de remuneração sãs, nos termos dos artigos 74.º, n.º 3, e 75.º, n.º 2, da Diretiva 2013/36/UE[6];

g. de mecanismos que assegurem que a avaliação da adequação individual e coletiva do órgão de administração é realizada de forma eficaz, que a composição e o plano de sucessão do órgão de administração são adequados e que o órgão de administração desempenha as suas funções de forma eficaz[7];

h. de um processo de seleção e avaliação da adequação dos titulares de funções essenciais[8];

i. de mecanismos destinados a garantir o funcionamento interno de cada comité do órgão de administração, caso tenha sido constituído, discriminando:

    i. o papel, a composição e as tarefas de cada um deles;

    ii. um fluxo de informação adequado, incluindo a documentação de recomendações e conclusões, e linhas de reporte adequadas entre cada comité e o órgão de administração, as autoridades competentes e outras partes;

j. de uma cultura de risco consentânea com a secção 9 das presentes orientações, que inclua a sensibilização para o risco e os comportamentos de risco da instituição;

[6] Orientações da EBA relativas a políticas de remuneração sãs, nos termos dos artigos 74.º, n.º 3, e 75.º, n.º 2, da Diretiva 2013/36/UE, e à divulgação de informações, nos termos do artigo 450.º do Regulamento (UE) n.º 575/2013 (EBA/GL/2015/22).

[7] Ver também as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

[8] Ver também as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

k. de uma cultura empresarial e de valores consentâneos com a secção 10, que promovam comportamentos éticos e responsáveis, incluindo um código de conduta ou um instrumento semelhante;

l. de uma política em matéria de conflitos de interesses a nível institucional consentânea com a secção 11 e de uma política de pessoal consentânea com a secção 12; e

m. de mecanismos que garantam a integridade dos sistemas contabilístico e de informação financeira, incluindo os controlos financeiros e operacionais e o cumprimento da lei e das normas relevantes aplicáveis.

24. O órgão de administração supervisiona o processo de divulgação e as comunicações com as partes interessadas externas e as autoridades competentes.

25. Todos os membros do órgão de administração são informados sobre a atividade global e a situação financeira e de risco da instituição, tendo em conta a conjuntura económica, bem como sobre as decisões adotadas que tenham um impacto significativo na atividade da instituição.

26. Um dos membros do órgão de administração pode ser responsável por uma função de controlo interno a que se refere o Título V, ponto 19.1, desde que esse membro não acumule outras funções que possam comprometer as suas atividades de controlo interno e a independência da função de controlo interno.

27. O órgão de administração acompanha, revê periodicamente e corrig quaisquer insuficiências identificadas, no que respeita à execução dos processos, estratégias e políticas associados às obrigações enumeradas nos pontos 23 e 24. O quadro de governo interno, bem como a sua aplicação, deve ser revisto e atualizado periodicamente tendo em conta o princípio da proporcionalidade, conforme explicado no Título I. Deve ser efetuada uma revisão mais aprofundada sempre que alterações significativas afetem a instituição.

2 Função de gestão do órgão de administração

28. O órgão de administração de uma instituição na sua função de gestão envolve-se ativamente na atividade da mesma e adota decisões fundamentadas e com conhecimento de causa.

29. O órgão de administração na sua função de gestão é responsável pela aplicação das estratégias definidas pelo órgão de administração e discute regularmente a aplicação e adequação dessas estratégias com o órgão de administração na sua função de fiscalização. A implementação operacional pode ser executada pela função de gestão da instituição.

30. O órgão de administração na sua função de gestão, analisa de forma construtiva e crítica as propostas, explicações e informações recebidas quando exerce o seu julgamento e toma decisões. O órgão de administração na sua função de gestão informa o órgão de administração na sua função de fiscalização, de forma exaustiva e regular e, sempre que necessário, sem

demora indevida, sobre os elementos relevantes para a avaliação de uma situação, os riscos e desenvolvimentos suscetíveis de afetar a instituição (p. ex., decisões importantes adotadas relativas às atividades de negócio e aos riscos), a avaliação da situação económica e comercial da instituição, a liquidez e a base sólida de fundos próprios, bem como a avaliação das suas posições de risco significativas.

3 Função de fiscalização do órgão de administração

31. O papel dos membros do órgão de administração na sua função de fiscalização deve incluir a monitorização e a crítica construtiva da estratégia da instituição.

32. Sem prejuízo da aplicação do direito nacional, o órgão de administração na sua função de fiscalização deve incluir membros independentes, conforme previsto na secção 9.3 das orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros do órgão de administração e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

33. Sem prejuízo das obrigações decorrentes do direito das sociedades nacional aplicável, o órgão de administração na sua função de fiscalização:

    a. supervisiona e monitoriza as ações e tomadas de decisão em matéria de gestão e supervisiona eficazmente o órgão de administração na sua função de gestão, incluindo a monitorização e análise do seu desempenho individual e coletivo e a execução das estratégias e dos objetivos da instituição;

    b. desafia e critica de forma construtiva as propostas e informações fornecidas pelos membros do órgão de administração na sua função de gestão, bem como as suas decisões;

    c. tendo em conta o princípio da proporcionalidade estabelecido no Título I, desempenha adequadamente as funções e o papel do comité de risco, do comité de remuneração e do comité de nomeação, sempre que estes comités não tenham sido constituídos;

    d. assegura e avalia periodicamente a eficácia do quadro de governo interno da instituição e adota as medidas adequadas para corrigir quaisquer deficiências identificadas;

    e. supervisiona e monitoriza a execução coerente dos objetivos estratégicos da instituição, da sua estrutura organizacional e estratégia de risco, incluindo a sua apetência pelo risco e o seu quadro de gestão do risco, bem como outras políticas (p. ex., política de remuneração) e o quadro de comunicação de informações;

    f. monitoriza a aplicação coerente da cultura de risco da instituição;

g. supervisiona a aplicação e manutenção de um código de conduta ou de políticas semelhantes e eficazes, a fim de identificar, gerir e mitigar conflitos de interesse reais ou potenciais;

h. supervisiona a integridade da informação financeira e do reporte, bem como o sistema de controlo, incluindo um quadro de gestão sã e efetiva dos riscos;

i. assegura que os responsáveis das funções de controlo interno têm condições para atuar com independência e, sem prejuízo da obrigação de informar outros órgãos internos, unidades ou segmentos de atividade, pode criticar e alertar diretamente o órgão de administração no exercício da sua função de fiscalização, quando necessário, sempre que a evolução do risco afete ou seja suscetível de afetar a instituição; e

j. monitoriza a execução do plano de auditoria interna, após o envolvimento prévio do comité de risco e do comité de auditoria, sempre que estes comités estejam constituídos.

4 Papel da presidência do órgão de administração

34. A presidência do órgão de administração deve dirigir o órgão e contribuir para um fluxo eficiente das informações entre os seus membros e entre o órgão de administração e os seus comités, caso tenham sido constituídos, e é responsável pelo seu funcionamento global efetivo.

35. A presidência incentiva e promove um debate aberto e crítico e assegura que as opiniões divergentes possam ser expressas e discutidas no âmbito do processo de tomada de decisão.

36. Como princípio geral, o presidente do órgão de administração deve ser um membro não executivo. Nos casos em que o presidente seja autorizado a exercer funções executivas, a instituição deve tomar medidas para mitigar eventuais impactos negativos sobre os seus mecanismos de controlo e equilíbrio (p. ex., designando um membro principal ou um membro independente do órgão de administração numa posição hierárquica superior, ou aumentando o número de membros não executivos do órgão de administração na sua função de fiscalização). Em particular, nos termos do artigo 88.º, n.º 1, alínea e), da Diretiva 2013/36/UE, o presidente do órgão de administração na sua função de fiscalização de uma instituição não pode exercer simultaneamente funções de administrador executivo na mesma instituição, salvo justificação pela instituição e autorização pelas autoridades competentes.

37. A presidência prepara as agendas das reuniões e assegura que as questões estratégicas são discutidas com prioridade em relação às demais. Assegura que as decisões do órgão de administração e fiscalização são devidamente fundamentadas e tomadas com conhecimento de causa e que os documentos e as informações são recebidos com antecedência suficiente antes da reunião.

38. A presidência contribui para uma clara atribuição de funções entre os membros do órgão de administração e para a existência de um fluxo de informação eficiente entre os seus membros, por forma a que os membros do órgão de administração na sua função de fiscalização tenham um contributo construtivo para os debates e tomem decisões de voto bem fundamentadas e com conhecimento de causa.

5 Comités do órgão de administração na sua função de fiscalização

5.1 Criação dos comités

39. Nos termos do artigo 109.º, n.º 1, da Diretiva 2013/36/UE, conjugado com o artigo 76.º, n.º 3, o artigo 88.º, n.º 2, e o artigo 95.º, n.º 1, da Diretiva 2013/36/UE, todas as instituições que sejam elas próprias significativas, tendo em conta a sua dimensão a nível individual, a nível subconsolidado e a nível consolidado, devem constituir comités de risco, de nomeação[9] e de remuneração[10], cuja função consistirá em aconselhar o órgão de administração na sua função de fiscalização e preparar as decisões que serão adotadas por este órgão. As instituições não significativas, incluindo as que são abrangidas pelo âmbito da consolidação prudencial de uma instituição que seja significativa numa situação subconsolidada e consolidada, não são obrigadas a constituir esses comités.

40. Sempre que não seja criado um comité de risco ou de nomeação, as referências a esses comités nas presentes orientações devem ser entendidas como aplicáveis ao órgão de administração na sua função de fiscalização, tendo em conta o princípio da proporcionalidade estabelecido no Título I.

41. As instituições podem, tendo em conta os critérios estabelecidos no Título I das presentes orientações, criar outros comités (p. ex., comités de ética, de conduta e de verificação do cumprimento).

42. As instituições devem assegurar uma clara atribuição e distribuição de funções e tarefas entre os comités especializados do órgão de administração.

43. Cada comité deve ter um mandato documentado, que inclua o âmbito das suas responsabilidades, conferido pelo órgão de administração na sua função de fiscalização, e estabelecer procedimentos de trabalho adequados.

44. Os comités devem apoiar a função de fiscalização em áreas específicas e facilitar o desenvolvimento e a aplicação de um quadro de governo interno sólido. A delegação nos

[9] Ver também as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

[10] No que respeita ao comité de remuneração, consulte as orientações da EBA relativas a políticas de remuneração sãs.

comités não exime o órgão de administração, nas suas funções de fiscalização, do cumprimento coletivo das suas obrigações e responsabilidades.

5.2 Composição dos comités[11]

45. Todos os comités devem ser presididos por um membro não executivo do órgão de administração com capacidade de formular juízos objetivos.

46. Os membros independentes[12] do órgão de administração na sua função de fiscalização devem ser envolvidos ativamente nos comités.

47. Os comités criados nos termos da Diretiva 2013/36/UE ou do direito nacional devem ser compostos por um mínimo de três membros.

48. As instituições devem certificar-se, tendo em conta a dimensão do órgão de administração e o número de membros independentes do órgão de administração na sua função de fiscalização, de que os comités não são compostos pelo mesmo grupo de membros que forma outro comité.

49. As instituições devem ponderar a rotação periódica das presidências e dos membros dos comités, tendo em conta a experiência, as competências e os conhecimentos específicos que são exigidos para esses comités, a nível individual ou coletivo.

50. Os comités de risco e de nomeação devem ser compostos por membros não executivos do órgão de administração, na sua função de fiscalização, da instituição em causa. O comité de auditoria deve ser composto em conformidade com o artigo 41.º da Diretiva 2006/43/CE[13]. O comité de remuneração deve ser composto de acordo com a secção 2.4.1 das orientações da EBA relativas a políticas de remuneração sãs[14].

51. Nas G-SII (instituições de importância sistémica global) e nas O-SII (outras instituições de importância sistémica), o comité de nomeação deve incluir uma maioria de membros independentes e ser presidido por um membro independente. Noutras instituições significativas, determinadas pelas autoridades competentes ou pelo direito nacional, o comité de nomeação deve incluir um número suficiente de membros independentes; essas

[11] Esta secção deve ser lida em conjunto com as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

[12] Conforme definido na secção 9.3 das orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

[13] Diretiva 2006/43/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa à revisão legal das contas anuais e consolidadas, que altera as Diretivas 78/660/CEE e 83/349/CEE do Conselho e revoga a Diretiva 84/253/CEE do Conselho (JO L 157, de 9.6.2006, p. 8756), com a última redação que lhe é dada pela Diretiva 2014/56/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014.

[14] Orientações da EBA relativas a políticas de remuneração sãs, nos termos dos artigos 74.º, n.º 3, e 75.º, n.º 2, da Diretiva 2013/36/UE, e à divulgação de informações, nos termos do artigo 450.º do Regulamento (UE) n.º 575/2013 (EBA/GL/2015/22).

instituições também podem considerar como boa prática que a presidência do comité de nomeação seja exercida por um membro independente.

52. Os membros do comité de nomeação devem possuir, individual e coletivamente, conhecimentos, competências e experiência adequados, no que respeita ao processo de seleção e aos requisitos de adequação.

53. Nas G-SII e nas O-SII, o comité de risco deve incluir uma maioria de membros independentes e ser presidido por um membro independente. Noutras instituições significativas, determinadas pelas autoridades competentes ou pelo direito nacional, o comité de risco deve incluir um número suficiente de membros independentes e a presidência deve, sempre que possível, ser exercida por um membro independente. Em todas as instituições, a presidência do comité de risco não deve ser exercida nem pelo presidente do órgão de administração nem pelo presidente de qualquer outro comité.

54. Os membros do comité de nomeação devem possuir, individual e coletivamente, conhecimentos, competências e experiência adequados no que respeita no que respeita às práticas de controlo e gestão de riscos.

5.3 Processos dos comités

55. Os comités devem reportar regularmente ao órgão de administração na sua função de fiscalização.

56. Os comités devem ainda interagir entre si, sempre que necessário. Sem prejuízo do disposto no ponto 48, essa interação poderá assumir a forma de participação cruzada, de forma a que o presidente ou um membro de um comité possa também ser membro de outro comité.

57. Os membros dos comités devem empenhar-se em debates abertos e críticos, nos quais as divergências sejam debatidas de uma forma construtiva.

58. Os comités devem documentar as agendas das suas reuniões, bem como os principais resultados e conclusões.

59. Os comités de risco e de nomeação devem, no mínimo:

    a. ter acesso a todos os dados e informações necessários para o desempenho da sua função, incluindo dados e informações de áreas empresariais e de controlo relevantes (p. ex., área jurídica, financeira, recursos humanos, TI, risco, controlo do cumprimento, auditoria, etc.);

    b. receber relatórios periódicos, informação *ad hoc*, comunicações e pareceres dos responsáveis das funções de controlo interno, no que respeita ao perfil de risco atual da instituição, à sua cultura de risco e aos seus limites de risco, bem como sobre quaisquer infrações importantes que possam ter ocorrido, com informações

pormenorizadas sobre, e recomendações de, medidas corretivas adotadas, a adotar ou sugeridas para corrigir essas infrações;

c. analisar periodicamente e decidir sobre o conteúdo, o formato e a frequência das informações sobre o risco que lhes serão transmitidas; e

d. sempre que necessário, assegurar o envolvimento adequado das funções de controlo interno e de outras funções relevantes (recursos humanos, área jurídica, área financeira) no âmbito das respetivas áreas de especialização e/ou obter aconselhamento de peritos externos.

5.4 Papel do comité de risco

60. Caso tenha sido constituído, o comité de risco deve, no mínimo:

a. aconselhar e apoiar o órgão de administração na sua função de fiscalização, no que respeita à monitorização da apetência e estratégia de risco gerais, atuais e futuras da instituição, tendo em conta todos os tipos de riscos, a fim de assegurar que estão harmonizadas com a estratégia empresarial, os objetivos, a cultura e os valores empresariais da instituição;

b. assistir o órgão de administração na sua função de fiscalização, na supervisão da execução da estratégia de risco da instituição e dos correspondentes limites fixados;

c. supervisionar a execução das estratégias em matéria de gestão de fundos próprios e de liquidez, bem como de todos os restantes riscos significativos de uma instituição, como os riscos de mercado, de crédito, operacionais (incluindo os riscos jurídicos e os riscos das TI) e de reputação, a fim de avaliar a sua adequação face à apetência e estratégia de risco aprovadas;

d. formular recomendações ao órgão de administração na sua função de fiscalização sobre os ajustamentos necessários à estratégia de risco resultantes, nomeadamente, de alterações do modelo de negócio da instituição, da evolução dos mercados ou de recomendações formuladas pela função de gestão de riscos;

e. prestar aconselhamento sobre a nomeação de consultores externos que a função de fiscalização decida contratar para prestação de aconselhamento ou apoio;

f. analisar um conjunto de possíveis cenários, incluindo cenários de esforço, para avaliar a forma como o perfil de risco da instituição reagiria a acontecimentos externos e internos;

g. supervisionar a coerência entre todos os produtos e serviços financeiros importantes oferecidos aos clientes, bem como o modelo de negócio e a estratégia de risco da

instituição[15]. O comité de risco deve avaliar os riscos associados aos produtos e serviços financeiros oferecidos e ter em conta a coerência entre os preços atribuídos a esses produtos e serviços e os lucros obtidos com os mesmos; e

h. avaliar as recomendações formuladas pelos auditores internos e externos e acompanhar a adequada aplicação das medidas adotadas.

61. O comité de risco deve colaborar com outros comités cujas atividades possam ter impacto na estratégia de risco (p. ex., comités de auditoria e de remuneração) e comunicar regularmente com as funções de controlo interno da instituição, em particular, a função de gestão de riscos.

62. Se tiver sido constituído, o comité de riscos deve, sem prejuízo das tarefas do comité de remuneração, examinar se os incentivos proporcionados pelas políticas e práticas de remuneração têm em consideração o risco, os fundos próprios e a liquidez da instituição, bem como a probabilidade e o momento da existência de lucros.

5.5 Papel do comité de auditoria

63. Nos termos da Diretiva 2006/43/CE[16], caso tenha sido constituído, o comité de auditoria deve, nomeadamente:

a. controlar a eficácia dos sistemas de controlo de qualidade interno e de gestão do risco da instituição e, se aplicável, da sua função de auditoria interna, no que respeita à informação financeira da instituição auditada, sem violar a sua independência;

b. supervisionar a definição das políticas contabilísticas da instituição;

c. acompanhar o processo de informação financeira e apresentar recomendações para garantir a sua integridade;

d. verificar e acompanhar a independência dos revisores oficiais de contas ou das sociedades de revisores oficiais de contas nos termos dos artigos 22.º, 22.º-A, 22.º-B, 24.º-A e 24.º-B da Diretiva 2006/43/UE e do artigo 6.º do Regulamento (UE) n.º 537/2014[17], e, em especial, a adequação da prestação de serviços que não sejam serviços de auditoria à entidade auditada nos termos do artigo 5.º desse regulamento;

[15] Ver também as orientações da EBA relativas aos procedimentos de governação e monitorização de produtos bancários de retalho, disponíveis em http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

[16] Diretiva 2006/43/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa à revisão legal das contas anuais e consolidadas, que altera as Diretivas 78/660/CEE e 83/349/CEE do Conselho e revoga a Diretiva 84/253/CEE do Conselho (JO L 157, de 9.6.2006, p. 8756), com a última redação que lhe é dada pela Diretiva 2014/56/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014.

[17] Regulamento (UE) n.º 537/2014 do Parlamento Europeu e do Conselho, 16 de abril de 2014, relativo aos requisitos específicos para a revisão legal de contas das entidades de interesse público e que revoga a Decisão 2005/909/CE da Comissão (JO L 158 de 27.5.2014, p. 77).

e. acompanhar a revisão legal de demonstrações financeiras anuais e consolidadas, nomeadamente a sua execução, tendo em conta as eventuais constatações e conclusões da autoridade competente nos termos do artigo 26.º, n.º 6, do Regulamento (UE) n.º 537/2014;

f. assumir a responsabilidade pelo processo de seleção do revisor ou dos revisores oficiais de contas ou da sociedade ou das sociedades de revisores oficiais de contas e recomendar, para aprovação pelo órgão competente da instituição (nos termos do artigo 16.º do Regulamento (UE) n.º 537/2014, salvo quando for aplicado o n.º 8 do mesmo artigo), a sua nomeação, remuneração ou exoneração;

g. rever o âmbito e a frequência de auditoria da revisão legal das contas anuais e das contas consolidadas;

h. nos termos do artigo 39.º, n.º 6, alínea a), da Diretiva 2006/43/UE, informar o órgão de administração ou de fiscalização da entidade auditada dos resultados da revisão legal de contas e explicar o modo como a revisão legal das contas contribuiu para a integridade do relato financeiro e o papel que o comité de auditoria desempenhou nesse processo; e

i. receber e ter em conta os relatórios das auditorias.

5.6 Comités combinados

64. Nos termos do artigo 76.º, n.º 3, da Diretiva 2013/36/UE, as autoridades competentes podem autorizar as instituições que não sejam consideradas significativas a combinar o comité de risco e, caso esteja constituído, o comité de auditoria referido no artigo 39.º da Diretiva 2006/43/CE.

65. Sempre que sejam constituídos comités de risco e de nomeação em instituições não significativas, estas podem combinar os comités. Se o fizerem, essas instituições devem documentar os motivos que presidiram à opção de combinar os comités e a forma como a abordagem realiza os objetivos dos comités.

66. As instituições devem garantir, de forma permanente, que os membros de um comité combinado possuem, individual e coletivamente, a conjugação de conhecimentos, competências e experiência necessária para compreenderem totalmente as funções que serão exercidas pelo comité combinado[18].

Título III – Quadro de governo

[18] Ver também as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

6 Quadro organizacional e estrutura

6.1 Quadro organizacional

67. Compete ao órgão de administração de uma instituição assegurar que esta possui uma estrutura organizacional e operacional adequada e transparente e manter uma descrição escrita dessa estrutura. A estrutura deve ser capaz de promover e demonstrar uma gestão efetiva e prudente da instituição, a nível individual, a nível subconsolidado e a nível consolidado. O órgão de administração assegura que as funções de controlo interno são independentes dos segmentos de atividade que controla, em especial, que existe uma segregação de funções adequada e que aquelas funções estão dotadas dos recursos financeiros e humanos e dos poderes adequados para desempenharem eficazmente a sua função. Os canais de transmissão de informações e a atribuição de responsabilidades no interior de uma instituição, nomeadamente entre os titulares de funções essenciais, devem ser claros, bem definidos, coerentes, vinculativos e devidamente documentados. A documentação deve ser atualizada consoante necessário.

68. A estrutura da instituição não pode prejudicar a capacidade do órgão de administração para supervisionar e gerir eficazmente os riscos que afetam a instituição ou do grupo nem a capacidade da autoridade competente para supervisionar eficazmente a instituição.

69. O órgão de administração deve avaliar a forma como as alterações materiais à estrutura do grupo (p. ex., estabelecimento de novas filiais, fusões e aquisições, venda ou liquidação de partes do grupo, ou acontecimentos externos) afetam a solidez do quadro organizacional da instituição. Sempre que forem identificadas deficiências, o órgão de administração procede rapidamente a quaisquer ajustamentos necessários.

6.2 «Conheça a sua estrutura»

70. O órgão de administração conhece e compreende inteiramente a estrutura jurídica, organizacional e operacional da instituição («conheça a sua estrutura») e assegura a conformidade da mesma com a estratégia comercial e de risco e a apetência pelo risco aprovadas.

71. O órgão de administração é responsável pela aprovação de estratégias e políticas sólidas para a criação de novas estruturas. Quando uma instituição cria muitas entidades jurídicas no seio do seu grupo, o número de entidades e, principalmente, as interligações e operações entre elas, não devem dificultar a conceção do seu governo interno nem a gestão e supervisão eficaz dos riscos do grupo como um todo. O órgão de administração assegura que a estrutura de uma instituição e, quando aplicável, as estruturas pertencentes a um grupo, tendo em conta os critérios especificados na secção 7, são claras, eficientes e transparentes para o pessoal da instituição, bem como para os seus acionistas e outras partes interessadas, e para a autoridade competente.

72. O órgão de administração orienta a estrutura da instituição, a sua evolução e limitações, assegurando que essa estrutura se justifica e é eficiente e não implica uma complexidade excessiva ou inadequada.

73. O órgão de administração de uma instituição consolidante deve compreender não só a estrutura jurídica, organizacional e operacional do grupo, mas também a finalidade e as atividades das suas diversas entidades e as ligações e relações existentes entre elas. Essa compreensão inclui os riscos operacionais específicos do grupo, as exposições intragrupo, bem como o modo como os perfis de financiamento, fundos próprios, liquidez e risco do grupo podem ser afetados em circunstâncias normais e adversas. O órgão de administração assegura que a instituição é capaz de produzir informações oportunas sobre o tipo, as características, o organigrama, a estrutura de propriedade e atividades de cada entidade jurídica, e que as instituições pertencentes ao grupo cumprem com todos os requisitos em matéria de elaboração de relatórios de supervisão em base individual, subconsolidada ou consolidada.

74. O órgão de administração de uma instituição consolidante assegura que as diferentes entidades do grupo (incluindo a própria instituição consolidante) recebem informações suficientes para terem uma perceção clara dos objetivos gerais, das estratégias e do perfil de risco do grupo e da forma como a entidade do grupo em causa está integrada na estrutura e no funcionamento operacional do grupo. Essas informações e análises são documentadas e disponibilizadas às funções pertinentes envolvidas, nomeadamente o órgão de administração, segmentos de atividade e funções de controlo interno. Os membros do órgão de administração de uma instituição consolidante mantêm-se ao corrente dos riscos suscitados pela estrutura do grupo, tendo em conta os critérios especificados na secção 7 das orientações. Tal inclui a receção de:

    a. informações sobre os principais fatores de risco;

    b. relatórios periódicos de avaliação da estrutura global da instituição e da conformidade das atividades de cada uma das entidades com a estratégia aprovada ao nível do grupo; e

    c. relatórios periódicos sobre tópicos em que o quadro regulamentar exige conformidade a nível individual, a nível subconsolidado e a nível consolidado.

6.3 Estruturas complexas e atividades não convencionais ou não transparentes

75. As instituições devem evitar a criação de estruturas complexas e suscetíveis de não serem transparentes. No seu processo de tomada de decisões, as instituições têm em conta não só os resultados de uma avaliação dos riscos efetuada para determinar se essas estruturas podem ser utilizadas para uma finalidade associada a branqueamento de capitais ou outros crimes

financeiros, mas também os respetivos controlos e quadro jurídico em vigor[19]. Para o efeito, as instituições têm em conta, no mínimo, em que medida:

a. a jurisdição na qual a estrutura será criada cumpre efetivamente as normas europeias e internacionais em matéria de transparência fiscal, de luta contra o branqueamento de capitais e de combate ao financiamento do terrorismo;

b. a estrutura serve uma finalidade económica e lícita óbvia;

c. a estrutura pode ser utilizada para ocultar a identidade do beneficiário efetivo final;

d. o pedido de um cliente que está na base da possível criação de uma estrutura suscita preocupação;

e. a estrutura pode impedir a supervisão adequada pelo órgão de administração da instituição ou a capacidade desta para gerir o risco associado; e

f. a estrutura dificulta a supervisão efetiva das autoridades competentes.

76. Em qualquer dos casos, as instituições não devem constituir estruturas opacas ou desnecessariamente complexas que não tenham uma finalidade jurídica ou um interesse económico claros, ou se suspeitarem de que tais estruturas possam ser utilizadas para fins associados ao crime financeiro.

77. Quando constitui essas estruturas, o órgão de administração compreende a sua finalidade e estrutura, bem como os riscos específicos que lhe estão associados, e assegura o correto envolvimento das funções de controlo interno. Tais estruturas apenas devem ser aprovadas e mantidas quando a sua finalidade tiver sido claramente definida e compreendida e quando o órgão de administração se tiver certificado de que todos os riscos materiais, incluindo o risco reputacional, foram identificados, podem ser geridos eficientemente e comunicados de forma adequada, e de que foi assegurada uma supervisão efetiva. Quanto mais complexa e opaca for a estrutura organizacional e operacional e maiores forem os riscos, mais intensa deverá ser a supervisão da estrutura.

78. As instituições devem documentar as suas decisões e ser capazes de as justificar às autoridades competentes.

79. O órgão de administração assegura a adoção de medidas adequadas para evitar ou mitigar os riscos das atividades realizadas nessas estruturas, nomeadamente que:

[19] Para mais informações sobre a avaliação do risco do país e o risco associado a produtos e clientes individualizados, as instituições devem igualmente consultar as orientações conjuntas finais (quando publicadas) sobre os fatores de risco: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

a. a instituição possui políticas e procedimentos adequados, bem como processos documentados (por exemplo, limites aplicáveis, requisitos de informação), com vista à análise, verificação do cumprimento, aprovação e gestão dos riscos dessas atividades, tendo em conta as consequências para a estrutura operacional e organizacional do grupo, o seu perfil de risco e o seu risco reputacional;

b. a informação referente a essas atividades e o risco da mesma está facilmente acessível para a instituição consolidante e para os seus auditores internos e externos e é comunicada ao órgão de administração na sua função de fiscalização e à autoridade competente que concedeu a autorização; e

c. a instituição avalia periodicamente se continua a ser necessário manter tais atividades.

80. Todas estas estruturas e atividades, incluindo o cumprimento da legislação e das normas profissionais, são objeto de análise regular por parte da função de auditoria interna, seguindo uma abordagem baseada no risco.

81. As instituições adotam as mesmas medidas de gestão de riscos adotadas para as suas próprias atividades comerciais quando desempenham atividades não convencionais ou não transparentes por conta de clientes (p. ex., auxiliando-os a constituir veículos de investimento em jurisdições *offshore*, desenvolvendo estruturas e operações financeiras complexas por sua conta ou prestando serviços de mandatário) que possam colocar desafios semelhantes em matéria de governo interno e criar riscos operacionais e de reputação significativos. Em particular, as instituições devem analisar o motivo pelo qual o cliente pretende constituir uma estrutura específica.

7 Quadro organizacional num contexto de grupo

82. Nos termos do artigo 109.º, n.º 2, da Diretiva 2013/36/UE, as empresas-mãe e as filiais abrangidas por essa diretiva devem assegurar que os seus sistemas, processos e mecanismos de governo sejam coerentes e bem integrados em base consolidada e subconsolidada. Para o efeito, as empresas-mãe e as filiais abrangidas pelo âmbito da consolidação prudencial aplicam esses sistemas, processos e mecanismos nas suas filiais não abrangidas pela Diretiva 2013/36/UE, a fim de assegurar sistemas de governo robustos em base consolidada e subconsolidada. As funções competentes no âmbito da instituição consolidante e das suas filiais devem interagir e trocar dados e informações, consoante necessário. Os sistemas, os processos e os mecanismos de governo asseguram que a instituição consolidante possui dados e informações suficientes e é capaz de avaliar o perfil de risco do grupo, conforme indicado na secção 6.2.

83. O órgão de administração de uma filial abrangida pela Diretiva 2013/36/UE adota e aplica, a nível individual, as políticas de governo ao nível do grupo estabelecidas em nível consolidado ou subconsolidado, de uma forma que cumpra com todos os requisitos específicos no âmbito do direito nacional e do direito da UE.

84. Aos níveis consolidado e subconsolidado, a instituição consolidante assegura a aplicação das políticas de governo ao nível do grupo por todas as instituições e outras entidades abrangidas pelo âmbito de consolidação prudencial, incluindo as suas filiais não abrangidas pela Diretiva 2013/36/UE. Quando implementa políticas de governo, a instituição consolidante garante que são estabelecidos sistemas de governo robustos para cada filial e considera a aplicação de sistemas, processos e mecanismos específicos sempre que as atividades comerciais estejam organizadas não em entidades jurídicas distintas, mas numa matriz de segmentos de atividade que englobe várias entidades jurídicas.

85. As instituições consolidantes têm em conta os interesses de todas as suas filiais e a forma como as estratégias e políticas contribuíram, a longo prazo, para o interesse de cada filial e para o interesse do grupo como um todo.

86. As empresas-mãe e as suas filiais asseguram que as instituições e as entidades pertencentes ao grupo cumpram com todos os requisitos específicos em qualquer jurisdição relevante.

87. A instituição consolidante assegura que as filiais estabelecidas em países terceiros e que estejam incluídas no âmbito da consolidação prudencial dispõem de sistemas, processos e mecanismos de governo que sejam coerentes com as políticas de governo ao nível do grupo e cumpram os requisitos dos artigos 74.º a 96.º da Diretiva 2013/36/UE e com as presentes orientações, desde que a sua aplicação não infrinja a legislação do país terceiro.

88. Os requisitos da Diretiva 2013/36/UE em matéria de governo e as presentes orientações são aplicáveis às instituições, independentemente do facto de poderem ser filiais de uma empresa-mãe num país terceiro. Sempre que uma filial na UE de uma empresa-mãe de um país terceiro for uma instituição consolidante, o âmbito da consolidação prudencial não inclui o nível da empresa-mãe situada no país terceiro nem outras filiais diretas dessa empresa-mãe. A instituição consolidante assegura que a política de governo a nível de grupo da instituição-mãe num país terceiro é tida em consideração nas suas próprias políticas de governo, desde que tal seja compatível com os requisitos estabelecidos no direito da UE aplicável, incluindo a Diretiva 2013/36/UE e as presentes orientações.

89. Quando definem políticas e documentam os sistemas de governo, as instituições têm em conta os aspetos enumerados no Anexo I das orientações. Embora as políticas e a documentação possam ser incluídas em documentos distintos, as instituições devem ponderar combiná-las ou incluí-las num único documento relativo ao quadro de governo.

8 Política de subcontratação[20]

90. O órgão de administração aprova, revê regularmente e atualiza a política de subcontratação da instituição, assegurando a aplicação oportuna de eventuais alterações.

[20] As presentes orientações referem-se apenas à política de subcontratação, sendo os aspetos específicos desta última tratados nas orientações sobre subcontratação do CAESB, que serão objeto de revisão. Essas orientações estão disponíveis em https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

91. A política de subcontratação toma em consideração o impacto que esta produz na atividade da instituição e nos riscos que ela enfrenta (nomeadamente, os riscos operacionais, incluindo riscos jurídicos e de TI, os riscos de reputação e os riscos de concentração). A política inclui os mecanismos de informação e acompanhamento que devem ser aplicados do princípio ao fim de um contrato de subcontratação (incluindo a elaboração do estudo de viabilidade, a celebração do contrato, a execução do mesmo até ao seu termo, os planos de contingência e as estratégias de saída). A instituição continua a ser inteiramente responsável por todos os serviços e atividades subcontratados, bem como pelas decisões de gestão deles decorrentes. A referida política deve indicar, por isso, claramente, que a subcontratação não exonera a instituição das suas obrigações regulamentares nem das responsabilidades para com os seus clientes.

92. A política estipula que as condições de subcontratação não obstam a uma supervisão efetiva da instituição, *in situ* ou noutro local, nem infringem quaisquer restrições regulamentares aplicáveis aos serviços e atividades. A política também abrange a subcontratação intragrupo (ou seja, serviços prestados por uma entidade jurídica distinta pertencente ao grupo da instituição) e tem em conta quaisquer circunstâncias específicas do grupo.

93. A política especifica que, quando seleciona prestadores de serviços externos relevantes ou subcontrata atividades, a instituição tem em conta se o prestador de serviços dispõe ou não de normas éticas adequadas ou um código de conduta.

Título IV – Cultura de risco e conduta empresarial

9 Cultura de risco

94. Um dos elementos fundamentais de uma gestão dos riscos eficaz é uma cultura de risco forte e coerente, que permita às instituições tomar decisões fundamentadas e bem informadas.

95. As instituições desenvolvem, em toda a sua estrutura, uma cultura de risco integrada e global, baseada na plena compreensão e numa perspetiva holística dos riscos que enfrenta e do modo como podem ser geridos, tendo em conta a suaapetência pelo risco.

96. As instituições desenvolvem uma cultura de risco através de políticas, comunicação e formação dos membros do pessoal, no que respeita às atividades, estratégia e perfil de risco, e adaptam a comunicação e a formação dos membros do pessoal, de forma a ter em conta as responsabilidades destes em matéria de tomada e gestão dos riscos.

97. Todos os membros do pessoal estão plenamente cientes das suas responsabilidades na gestão dos riscos, a qual não está confinada a especialistas de risco nem às funções de controlo interno. As unidades de negociação, sob a supervisão do órgão de administração, são as principais responsáveis pela gestão quotidiana dos riscos, em consonância com as políticas,

procedimentos e controlos da instituição e tendo em conta a sua capacidade de risco e apetência pelo risco.

98. Uma cultura de risco sólida inclui mas não está necessariamente limitada a:

a. Exemplo vindo de cima ("*tone from the top*"): o órgão de administração é responsável pela definição e comunicação dos valores fundamentais e expectativas da instituição. O comportamento dos seus membros deve refletir os valores defendidos. A administração das instituições, incluindo os titulares de funções essenciais, contribui para a comunicação interna dos valores fundamentais e expectativas aos membros do pessoal. Estes devem agir no respeito da legislação e regulamentação aplicável e transmitir de imediato ao nível hierárquico superior qualquer incumprimento observado dentro ou fora da instituição (p. ex., à autoridade competente, através de um processo de comunicação de irregularidades). O órgão de administração promove, controla e avalia continuamente a cultura de risco da instituição, tem em consideração o impacto da cultura de risco na estabilidade financeira, no perfil de risco e na solidez do governo da instituição, e promove as alterações necessárias.

b. Responsabilidade: os membros relevantes do pessoal a todos os níveis devem conhecer e compreender os valores fundamentais da instituição e, na medida necessária para a sua função, a sua capacidade de risco e apetência pelo risco. Devem ser capazes de desempenhar as suas funções e estar cientes de que serão responsáveis pelas suas ações, no que respeita ao comportamento de assunção de riscos da instituição.

c. Comunicação eficaz e crítica: uma cultura de risco sólida deve promover um ambiente de comunicação aberta e de crítica construtiva, no qual os processos de tomada de decisão incentivem a partilha de um amplo conjunto de perspetivas, permitam a experimentação de práticas correntes, estimulem uma atitude crítica construtiva entre o pessoal e promovam um ambiente de compromisso aberto e construtivo em toda a organização.

d. Incentivos: uma política de incentivos adequada desempenha um papel fundamental no alinhamento entre a tomada de riscos, o perfil de risco da instituição e os seus interesses a longo prazo[21].

10 Valores e código de conduta da instituição

99. O órgão de administração desenvolve, adota, cumpre e promove elevadas normas éticas e profissionais, tendo em conta as características e necessidades específicas da instituição, assegura a sua aplicação (através de um código de conduta ou instrumento similar) e fiscaliza o cumprimento dessas normas pelos membros do pessoal. Quando aplicável, o órgão de

[21] Consulte também as orientações da EBA relativas a políticas de remuneração sãs, nos termos dos artigos 74.º, n.º 3, e 75.º, n.º 2, da Diretiva 2013/36/UE, e à divulgação de informações, nos termos do artigo 450.º do Regulamento (UE) n.º 575/2013 (EBA/GL/2015/22), disponíveis em https://www.eba.europa.eu/regulation-and-policy/remuneration.

administração pode adotar e aplicar as normas da instituição ao nível do grupo, bem como normas comuns emitidas por associações ou outras organizações relevantes.

100. As normas aplicadas devem ter como objetivo reduzir os riscos a que a instituição está exposta, nomeadamente riscos operacionais e reputacionais, que podem ter um efeito negativo considerável na rendibilidade e sustentabilidade de uma instituição através de multas, custos de resolução de litígios, restrições impostas pelas autoridades competentes, outras sanções financeiras e criminais, e a perda de valor da marca e da confiança dos consumidores.

101. O órgão de administração tem políticas claras e documentadas sobre a forma como estas normas devem ser cumpridas. Essas políticas devem:

a. Recordar os seus destinatários que todas as atividades da instituição devem ser exercidas em conformidade com o direito aplicável e com os valores da instituição;

b. promover a sensibilização para o risco, através de uma cultura de risco sólida, em consonância com a secção 9 das orientações, que transmita as expectativas do órgão de administração de que as atividades são exercidas dentro da apetência pelo risco e dos limites definidos pela instituição e pelas responsabilidades dos membros do pessoal;

c. estabelecer princípios sobre, e fornecer exemplos de, comportamentos aceitáveis e não aceitáveis associados, em particular, quanto à comunicação de informações e práticas financeiras incorretas, conduta errada, crime económico e financeiro (incluindo, fraude, branqueamento de capitais e práticas anti-concorrenciais, sanções financeiras, suborno e corrupção, manipulação de mercado, venda enganosa e outras infrações à legislação em matéria de proteção dos consumidores);

d. clarificar que, além da conformidade com os requisitos legais e regulamentares e das políticas internas, os membros do pessoal devem assumir uma conduta honesta e íntegra e exercer as suas funções com o devido profissionalismo, zelo e diligência; e

e. assegurar que os membros do pessoal estão cientes das potenciais medidas disciplinares, ações legais e sanções decorrentes de comportamentos incorretos e inaceitáveis, tanto a nível interno como externo.

102. As instituições devem certificar-se do cumprimento dessas normas e assegurar a sensibilização dos membros do pessoal, por exemplo, através de formação. Devem também definir o órgão responsável pelo controlo do cumprimento e pela análise de violações do código de conduta ou instrumento similar, bem como um procedimento para tratar questões de não conformidade. Os resultados devem ser comunicados periodicamente ao órgão de administração.

11 Política em matéria de conflitos de interesses a nível institucional

103. O órgão de administração adota, aprova e supervisiona a aplicação e manutenção de políticas eficazes para identificar, avaliar, gerir e mitigar ou prevenir os conflitos de interesses reais e potenciais ao nível da instituição, resultantes, p. ex., das diversas atividades e funções da instituição, de diferentes instituições no âmbito da consolidação prudencial ou de diferentes unidades ou segmentos de atividade no seio de uma instituição, ou no que respeita às partes interessadas externas.

104. As instituições adotam, no âmbito dos seus sistemas organizacionais e administrativos, medidas adequadas para prevenir que os interesses dos seus clientes sejam afetados, de forma adversa, por conflitos de interesses.

105. As medidas adotadas pela instituição para gerir ou, quando necessário, mitigar conflitos de interesses, devem ser documentadas e incluir, nomeadamente:

    a. uma adequada segregação de funções, por exemplo, ao confiar a pessoas diferentes as atividades que suscitam conflitos de interesses na cadeia de tratamento de operações ou de prestação de serviços, ou as responsabilidades de supervisão e de informação referentes a essas atividades;

    b. o estabelecimento de barreiras à informação, por exemplo, através da separação física de certos segmentos de atividade ou unidades; e

    c. o estabelecimento de procedimentos adequados para as operações com partes relacionadas, p. ex., exigindo que as operações sejam realizadas em condições de mercado.

12 Política em matéria de conflitos de interesses ao nível dos membros do pessoal[22]

106. O órgão de administração adota, aprova e supervisiona a aplicação e manutenção de políticas eficazes para identificar, avaliar, gerir e mitigar os conflitos de interesses reais e potenciais entre os interesses da instituição e os interesses privados dos membros do pessoal, incluindo os membros do órgão de administração, que possam influenciar negativamente o desempenho as suas funções e responsabilidades. As instituições consolidantes devem considerar os interesses no âmbito de uma política em matéria de conflitos de interesses a nível do grupo em base consolidada ou subconsolidada.

107. A política deve visar a identificação de conflitos de interesses dos membros do pessoal, incluindo os interesses dos seus familiares diretos. As instituições devem ter em consideração que os conflitos de interesses podem resultar de relações pessoais ou profissionais tanto

[22] Esta secção deve ser lida em conjunto com as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

presentes como passados. Sempre que surjam conflitos de interesses, as instituições devem avaliar a sua materialidade e decidir e aplicar, se adequado, medidas apropriadas de mitigação.

108. No que respeita aos conflitos de interesses que possam resultar de relações anteriores, as instituições devem estabelecer um período temporal adequado para o qual pretendam que o pessoal comunique possíveis conflitos de interesses, com o fundamento de que estes podem afetar o comportamento e a participação dos membros dos pessoal no processo de tomada de decisões.

109. A política deve abranger, pelo menos, as seguintes situações ou relações nas quais podem surgir conflitos de interesses:

    a. interesses económicos: (p. ex., ações, outros direitos de propriedade e participações, participações financeiras e outros interesses económicos em clientes comerciais, direitos de propriedade intelectual, créditos concedidos pela instituição a uma empresa detida por membros do pessoal, participação ou propriedade de um organismo ou entidade com interesses conflitantes);

    b. relações pessoais ou profissionais com os titulares de participações qualificadas na instituição;

    c. relações pessoais ou profissionais com o pessoal da instituição ou de entidades incluídas no âmbito da consolidação prudencial (p. ex., relações familiares);

    d. outros empregos e empregos anteriores num passado recente (p. ex., cinco anos);

    e. relações pessoais ou profissionais com partes interessadas externas relevantes (p. ex., estar associado a fornecedores materiais, consultores ou outros prestadores de serviços); e

    f. influência política ou relações políticas.

110. Sem prejuízo do acima exposto, as instituições devem ter em consideração que o facto de ser acionista de uma instituição ou deter contas privadas ou empréstimos de uma instituição, ou manter outros serviços dessa instituição, caso não atinjam um limiar mínimo adequado, não deve significar que os membros do pessoal sejam considerados como estando em situação de conflito de interesses.

111. A política deve estabelecer os procedimentos para informação e comunicação ao órgão responsável no âmbito da política. Os membros do pessoal devem ter a obrigação de divulgar internamente e de imediato quaisquer questões que possam resultar, ou já tenham resultado, num conflito de interesses.

112. A política deve distinguir entre conflitos de interesses que persistem e devem ser geridos de forma permanente e conflitos de interesses que ocorrem inesperadamente em relação a um

único acontecimento (p. ex., uma operação, a seleção de um prestador de serviços, etc.) e podem normalmente ser geridos com uma medida pontual. Em qualquer circunstância, as decisões adotadas devem privilegiar o interesse da instituição.

113. A política deve definir procedimentos, medidas, requisitos de documentação e responsabilidades para a identificação e prevenção de conflitos de interesses, para a avaliação da sua materialidade e a adoção de medidas de mitigação. Tais procedimentos, requisitos, responsabilidades e medidas devem incluir:

a. a atribuição das atividades ou operações que suscitam conflitos de interesses a pessoas diferentes;

b. medidas que evitem que membros do pessoal que também exerçam atividades no exterior, exerçam uma influência indevida na instituição relativamente a essas outras atividades exercidas no exterior de;

c. o estabelecimento da responsabilidade que incumbe aos membros do órgão de administração de se absterem de participar na votação de quaisquer matérias em que tenham, ou possam ter, conflitos de interesses, ou em relação às quais a sua objetividade ou capacidade para cumprirem adequadamente as suas obrigações para com a instituição possam estar comprometidas;

d. a criação de procedimentos adequados para efetuar operações com partes relacionadas (as instituições podem considerar, nomeadamente, a exigência de que as operações sejam realizadas em condições de mercado, a exigência de que sejam plenamente aplicados a essas operações todos os procedimentos de controlo interno relevantes, a exigência de um processo consultivo vinculativo dos membros independentes do órgão de administração, a exigência de aprovação das operações mais relevantes pelos acionistas e a limitação da exposição a essas operações); e

e. impedir que os membros do órgão de administração exerçam cargos de direção em instituições concorrentes, a menos que estas façam parte de instituições que integrem o mesmo sistema de proteção institucional, conforme referido no artigo 113.º, n.º 7, do Regulamento (UE) n.º 575/2013, de instituições de crédito associadas de modo permanente a um organismo central, conforme referido no artigo 10.º do mesmo regulamento, ou de instituições incluídas no âmbito da consolidação prudencial.

114. A política deve abranger especificamente o risco em matéria de conflitos de interesses ao nível do órgão de administração e prestar orientações suficientes sobre a identificação e gestão de conflitos de interesses que possam prejudicar a capacidade dos membros do órgão de administração para tomar decisões objetivas e imparciais que defendam os melhores

interesses da instituição. As instituições devem ter em conta que os conflitos de interesses podem influenciar a independência de espírito dos membros do órgão de administração[23].

115. Os conflitos de interesses reais ou potenciais que tenham sido comunicados ao órgão responsável na instituição devem ser avaliados e geridos de forma adequada. Caso seja identificado um conflito de interesses nos membros do pessoal, a instituição documenta a decisão tomada, nomeadamente se o conflito de interesses e os riscos associados tiverem sido aceites, e, se for esse o caso, a forma como o conflito foi satisfatoriamente mitigado ou solucionado.

116. Todos os conflitos de interesses reais e potenciais ao nível do órgão de administração, sejam de natureza individual ou coletiva, são devidamente documentados, comunicados ao órgão de administração, e debatidos, decididos e devidamente geridos pelo órgão de administração.

13 Procedimentos de alerta a nível interno

117. As instituições aplicam e mantêm políticas de alerta adequadas a nível interno e procedimentos para o pessoal comunicar, através de um canal independente e autónomo, infrações potenciais ou reais aos requisitos regulamentares ou internos, nomeadamente aos requisitos previstos no Regulamento (UE) n.º 575/2013 e às disposições nacionais de transposição da Diretiva 2013/36/UE, ou dos sistemas de governo interno. Não deve ser necessário que os membros do pessoal estejam na posse de provas de uma infração para efetuarem uma comunicação; no entanto, devem possuir um grau de certeza suficiente que forneça motivo suficiente para iniciar uma investigação.

118. A fim de evitar conflitos de interesses, deverá ser possível comunicar infrações fora dos canais normais de transmissão de informações (p. ex., através da função de verificação do cumprimento, da função de auditoria interna ou de um procedimento independente de denúncia a nível interno). Os procedimentos de alerta devem assegurar a proteção dos dados pessoais quer da pessoa que comunica a infração quer da pessoa singular que é alegadamente responsável pela infração, nos termos da Diretiva 95/46/CE.

119. Todo o pessoal no seio da instituição deve ser informado dos procedimentos de alerta e

120. As informações fornecidas por meio do presente procedimento de alerta devem ser transmitidas, se apropriado, ao órgão de administração e a outros órgãos responsáveis designados no âmbito da política de alerta a nível interno. Quando solicitado pelo membro do pessoal que comunica uma infração, as informações devem ser transmitidas de forma anónima ao órgão de administração e a outros órgãos responsáveis. As instituições também podem disponibilizar um procedimento de denúncia que permita que as informações sejam transmitidas de forma anónima.

[23] Ver também as orientações conjuntas da ESMA e da EBA relativas à avaliação da adequação dos membros dos órgãos de administração e fiscalização e dos titulares de funções essenciais, nos termos da Diretiva 2013/36/UE e da Diretiva 2014/65/UE.

121. As instituições devem assegurar que a pessoa que comunica a infração é devidamente protegida de qualquer impacto negativo, p. ex., retaliação, discriminação ou outros tipos de tratamento injusto. A instituição deve assegurar que nenhuma pessoa sujeita ao seu controlo exerce retaliações sobre alguém que tenha comunicado uma infração e deve adotar medidas adequadas contra os responsáveis por tais ações.

122. As instituições devem igualmente proteger as pessoas que tenham sido alvo de comunicação de infrações contra quaisquer efeitos negativos, caso a investigação conclua que não existem motivos para adotar medidas contra essa pessoa. Caso sejam tomadas medidas, a instituição deve tomá-las de uma forma que vise proteger a pessoa em causa de efeitos negativos não intencionais que excedam o objetivo da medida adotada.

123. Em especial, os procedimentos de alerta a nível interno devem:

a. ser documentados (p. ex., manuais para os membros do pessoal);

b. fornecer regras claras que assegurem que as informações relativas à comunicação, às pessoas denunciadas e à infração são tratadas confidencialmente, em conformidade com a Diretiva 95/46/CE, exceto se a sua divulgação for exigida nos termos do direito nacional, no âmbito de outras investigações ou de procedimentos judiciais subsequentes;

c. proteger os membros do pessoal de serem vitimizados por terem divulgado infrações passíveis de denúncia;

d. assegurar que as infrações potenciais ou reais denunciadas são avaliadas e transmitidas ao nível hierárquico superior, incluindo, se for caso disso, à respetiva autoridade competente ou agência responsável pela aplicação da lei;

e. assegurar, sempre que possível, que é fornecida ao membro do pessoal que denunciou infrações potenciais ou reais uma confirmação da receção das informações;

f. assegurar o acompanhamento do resultado de uma investigação relativa a uma infração comunicada; e

g. assegurar a manutenção de registos adequados.

14 Comunicação de infrações às autoridades competentes

124. As autoridades competentes estabelecem mecanismos efetivos e confiáveis que permitam ao pessoal das instituições comunicar às autoridades competentes infrações potenciais ou reais relevantes aos requisitos regulamentares, incluindo, mas não se limitando, aos previstos no Regulamento (UE) n.º 575/2013 e nas disposições nacionais de transposição da Diretiva 2013/36/UE. Estes mecanismos devem incluir, no mínimo:

a. procedimentos específicos para a receção de comunicações sobre infrações, bem como o seu acompanhamento, por exemplo, um departamento, uma unidade ou uma função específicos para receber a denúncia;

b. proteção adequada, conforme indicado na secção 13;

c. proteção dos dados pessoais da pessoa que comunica a infração e da pessoa singular que é alegadamente responsável pela infração, nos termos da Diretiva 95/46/CE; e

d. procedimentos claros, conforme indicado no ponto 123;

125. Sem prejuízo da possibilidade de comunicação de infrações através dos seus mecanismos, as autoridades competentes devem incentivar os membros do pessoal a tentar utilizar em primeira instância os procedimentos de alerta internos das suas instituições.

Título V – Quadro de controlo interno e mecanismos

15 Quadro de controlo interno

126. As instituições desenvolvem e mantêm uma cultura que incentive uma atitude positiva perante o controlo do risco e o seu cumprimento , bem como um quadro de controlo interno robusto e amplo. No âmbito deste quadro, os segmentos de atividade das instituições são responsáveis pela gestão dos riscos que incorrem ao exercerem as suas atividades e devem dispor de controlos implementados destinados a assegurar a conformidade com os requisitos internos e externos. Ainda no âmbito deste quadro, as instituições possuem um quadro de gestão de riscos e funções de controlo interno com uma adequada e suficiente autoridade, estatuto e acesso ao órgão de administração de modo adequado e suficiente para cumprirem a sua missão.

127. O quadro de controlo interno da instituição em causa deve ser adaptado individualmente à especificidade da sua atividade, da sua complexidade e dos riscos associados, tendo em conta o contexto do grupo. As instituições em causa organizam o intercâmbio das informações necessárias de um modo que garanta que cada órgão de administração, segmento de atividade e unidade interna, incluindo cada função de controlo interno, é capaz de desempenhar as suas funções. Tal significa, por exemplo, estabelecer o necessário intercâmbio de informações adequadas entre os segmentos de atividade e a função de verificação do cumprimento ao nível do grupo e entre os responsáveis pelas funções de controlo interno ao nível do grupo e o órgão de administração da instituição.

128. O quadro de controlo interno abrange toda a organização, incluindo as responsabilidades e as tarefas do órgão de administração, e as atividades de todos os segmentos de atividade e unidades internas, incluindo as funções de controlo interno, as atividades subcontratadas e os canais de distribuição.

129. O quadro de controlo interno de uma instituição deve assegurar:

a. operações eficazes e eficientes;

b. o exercício prudente da atividade;

c. a adequada identificação, aferição e mitigação dos riscos;

d. a fiabilidade das informações financeiras e não financeiras comunicadas a nível interno e externo;

e. procedimentos administrativos e contabilísticos sólidos; e

f. o cumprimento da legislação, da regulamentação, dos requisitos de supervisão e dos processos, políticas, regras e decisões internos da instituição.

16 Implementação de um quadro de controlo interno

130. O órgão de administração é responsável pelo estabelecimento e monitorização da adequação e eficácia dos processos, dos mecanismos e do quadro de controlo interno, bem como pela supervisão de todos os segmentos de atividade e unidades internas, incluindo as funções de controlo interno (como as funções de gestão de risco, verificação do cumprimento e auditoria interna). As instituições estabelecem, mantêm e atualizam regularmente, por escrito, procedimentos, mecanismos e políticas de controlo interno, que são aprovados pelo órgão de administração.

131. As instituições asseguram a existência de um processo de tomada de decisão claro, transparente e documentado e de uma clara atribuição de responsabilidades e autoridade no âmbito do seu quadro de controlo interno, incluindo os seus segmentos de atividade, unidades internas e funções de controlo interno.

132. As instituições devem comunicar esses mecanismos, procedimentos e políticas a todos os membros do pessoal e sempre que sejam efetuadas alterações significativas.

133. Quando implementam o quadro de controlo interno, as instituições estabelecem uma segregação de funções adequada (p. ex., confiar a pessoas diferentes as atividades que suscitam conflitos de interesses na cadeia de tratamento de operações ou de prestação de serviços, ou as responsabilidades de supervisão e de reporte referentes a essas atividades) e barreiras à informação (p. ex., através da separação física de certos departamentos).

134. As funções de controlo interno verificam se as políticas, os mecanismos e os procedimentos estabelecidos no quadro de controlo interno são corretamente aplicados nas respetivas áreas de competência.

135. As funções de controlo interno apresentam ao órgão de administração relatórios periódicos, por escrito, sobre as principais deficiências identificadas. Esses relatórios devem incluir, para cada nova deficiência importante identificada, os riscos relevantes envolvidos, uma avaliação do seu impacto, recomendações e medidas corretivas a serem adotadas. O órgão de administração acompanha as conclusões das funções de controlo interno em devido tempo e de forma eficaz e exige a adoção de medidas corretivas adequadas. Deve ser adotado um procedimento formal de acompanhamento das conclusões e das medidas corretivas adotadas.

17 Quadro de gestão de riscos

136. No âmbito do quadro de gestão do risco global, as instituições possuem um quadro de gestão de riscos holístico, que abrange todos os seus segmentos de atividade e unidades internas, incluindo as funções de controlo interno, reconhecendo inteiramente a realidade económica dos riscos a que estão expostas. O quadro de gestão de riscos permite que a instituição tome decisões plenamente informadas sobre a tomada de riscos e inclui os riscos patrimoniais e extrapatrimoniais, bem como todos os riscos atuais e futuros a que a instituição pode estar exposta. Os riscos são avaliados no sentido ascendente e descendente, dentro e entre os vários segmentos de atividade, utilizando uma terminologia coerente e metodologias compatíveis em toda a instituição e em nível consolidado ou subconsolidado. O quadro de gestão de riscos inclui todos os riscos relevantes, tendo especialmente em consideração os riscos financeiros e não financeiros, incluindo os riscos de crédito, de mercado, de liquidez, de concentração, operacional, de TI, reputacional, jurídico, de conduta, de conformidade e estratégico.

137. O quadro de gestão de riscos da instituição inclui políticas, procedimentos, limites de risco e controlos de risco que permitam, de uma forma adequada, oportuna e permanente, identificar, medir ou avaliar, acompanhar, gerir, mitigar e comunicar os riscos aos níveis de segmento de atividade, instituição e consolidado e não consolidado.

138. O quadro de gestão de riscos da instituição deve fornecer orientações específicas sobre a execução das suas estratégias. Essas orientações definem e mantêm, se for caso disso, limites internos consentâneos com a apetência pelo risco e compatíveis com o bom funcionamento, a solidez financeira, a base de fundos próprios e os objetivos estratégicos da instituição. O perfil de risco desta última é mantido dentro desses limites. O quadro de gestão de riscos assegura que existe um processo definido para que as infrações aos limites de risco sejam transmitidas ao nível hierárquico superior e endereçadas através de um procedimento de acompanhamento adequado.

139. O quadro de gestão de riscos é objeto de uma análise interna independente, p. ex., realizada pela função de auditoria interna, e é reavaliado periodicamente quanto à apetência pelo risco da instituição, tendo em conta as informações da função de gestão de risco e, caso tenha sido constituído, do comité de risco. Os fatores a ter em conta incluem acontecimentos internos e externos, nomeadamente alterações no balanço ou nas demonstrações financeiras, qualquer aumento na complexidade da atividade, do perfil de risco ou da estrutura operacional da

instituição, expansão geográfica, fusões e aquisições e a introdução de novos produtos ou segmentos de atividade.

140. Quando identificam e aferem ou avaliam os riscos, as instituições desenvolvem metodologias adequadas, incluindo instrumentos prospetivos e retrospetivos. As metodologias permitem agregar as posições em risco dos diversos segmentos de atividade e ajudam a identificar concentrações de riscos. Os instrumentos incluem a análise do perfil de risco real em relação à apetência pelo risco da instituição, bem como a identificação e avaliação de riscos potenciais e excessivos em relação à capacidade de risco da instituição em diferentes circunstâncias adversas. Os instrumentos fornecem informações sobre eventuais ajustamentos do perfil de risco que possam ser necessários. Quando elaboram cenários de esforço, as instituições devem basear-se em pressupostos conservadores adequados.

141. As instituições devem ter em consideração que os resultados das metodologias de avaliação quantitativas, incluindo os testes de esforço, dependem muito das limitações e dos pressupostos dos modelos (incluindo a gravidade e a duração do choque e os riscos subjacentes). Por exemplo, o facto de os modelos indicarem uma rendibilidade muito elevada dos fundos próprios pode dever-se a uma deficiência inerente a esses modelos (por exemplo, a exclusão de alguns riscos relevantes) e não a uma estratégia excecional ou a uma execução excelente de uma estratégia por parte da instituição. Assim, a determinação do nível de risco não deve basear-se apenas em informações quantitativas ou em resultados de modelos, mas incluir também uma abordagem qualitativa (incluindo pareceres de peritos e análise crítica). As tendências e os dados relevantes da conjuntura macroeconómica são explicitamente considerados para identificar o seu potencial impacto nas posições em risco e nas carteiras.

142. A responsabilidade final pela avaliação dos riscos cabe exclusivamente à instituição, a qual avalia, assim, os seus riscos de forma crítica e não depende apenas de avaliações externas. Por exemplo, as instituições devem validar os modelos de risco que adquirem e calibrá-los em função das suas próprias circunstâncias específicas para assegurar que o modelo capta e analisa o risco de forma precisa e exaustiva.

143. As instituições devem ter pleno conhecimento das limitações dos modelos e das métricas e utilizar instrumentos de avaliação quantitativa e qualitativa dos riscos (incluindo pareceres de peritos e análise crítica).

144. Além das suas próprias avaliações, as instituições podem utilizar avaliações de risco externas (incluindo notações de crédito externas ou modelos de risco adquiridos no exterior). As instituições devem ter total conhecimento do âmbito dessas avaliações, bem como das suas limitações.

145. São criados mecanismos de informação regulares e transparentes para que o órgão de administração, o seu comité de risco, caso tenha sido constituído, e todas as unidades relevantes da instituição recebam relatórios oportunos, precisos, concisos, compreensíveis e significativos, e possam partilhar informações relevantes sobre a identificação, medição ou

avaliação, acompanhamento e gestão dos riscos. O quadro de transmissão de informação é claramente definido e documentado.

146. A comunicação e sensibilização eficaz no que respeita aos riscos e à estratégia de risco são essenciais para o processo de gestão de riscos no seu conjunto, incluindo os processos de revisão e de tomada de decisão, e contribuem para que não se adotem decisões suscetíveis de aumentar inadvertidamente os riscos. A comunicação eficaz dos riscos envolve uma análise e uma comunicação fiáveis da estratégia de gestão de riscos e dos dados pertinentes (p. ex., posições em risco e principais indicadores de risco) a nível interno, tanto horizontalmente, em todos os setores da instituição, como verticalmente, no sentido ascendente e descendente, ao longo da cadeia de gestão.

18 Novos produtos e alterações significativas[24]

147. A instituição dispõe de uma política de aprovação de novos produtos («PANP») bem documentada, aprovada pelo órgão de administração, direcionada para o desenvolvimento de novos mercados, produtos e serviços e para a introdução de alterações significativas nos já existentes, bem como de operações excecionais. Adicionalmente, a política deve englobar as alterações significativas dos processos (p. ex., novos contratos de atividades subcontratadas) e sistemas conexos (p. ex., processos de alteração dos sistemas de TI). A PANP assegura que os produtos e alterações aprovados são coerentes com a estratégia e a apetência pelo risco da instituição e os limites correspondentes, ou que são efetuadas as avaliações necessárias.

148. As alterações significativas ou operações excecionais podem incluir fusões e aquisições (incluindo as possíveis consequências de não efetuar uma auditoria (*due diligence*) suficientemente profunda para identificar os riscos e responsabilidades decorrentes das operações de concentração), a criação de estruturas (p. ex., novas filiais ou entidades instrumentais), novos produtos, alterações nos sistemas ou no quadro de gestão de riscos e respetivos procedimentos, e alterações na organização da instituição.

149. A instituição dispõe de procedimentos específicos para avaliar a conformidade com estas políticas, tendo em conta as informações fornecidas pela função de gestão de riscos. Esses procedimentos incluem uma avaliação sistemática prévia e um parecer fundamentado da função de verificação do cumprimento, no que respeita a novos produtos ou alterações significativas nos produtos existentes.

150. A PANP da instituição abrange todas as considerações que esta deve ter em conta antes de decidir entrar em novos mercados, negociar novos produtos, lançar um novo serviço ou introduzir alterações significativas nos produtos ou serviços existentes. A PANP também inclui as definições de «novo produto/mercado/atividade» e «alterações significativas» a utilizar na organização e as funções internas a serem envolvidos no processo de tomada de decisão.

[24] Ver também as orientações da EBA relativas aos requisitos de governo e monitorização aplicáveis aos fabricantes e distribuidores de produtos bancários de retalho, disponíveis em https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

151. A PANP indica as principais questões que devem ser abordadas antes de se tomar uma decisão. Entre elas figuram a observância da regulamentação, o sistema contabilístico, os modelos de determinação de preços, o impacto no perfil de risco, a adequação e rendibilidade dos fundos próprios, a disponibilidade de recursos suficientes nos serviços de sala de negociação (*front office*), apoio administrativo (*back office*) e apoio organizativo às operações de mercado e controlo de riscos (*middle office*), bem como de instrumentos e conhecimentos especializados adequados a nível interno para compreender e monitorizar os riscos associados. A decisão de lançar uma nova atividade define claramente a unidade de negociação e as pessoas que por ela ficam responsáveis. Não se iniciarão novas atividades até estarem disponíveis recursos suficientes para conhecer e gerir os riscos associados.

152. A função de gestão de riscos e a função de verificação do cumprimento são envolvidas na aprovação de novos produtos ou de alterações significativas em produtos, processos e sistemas existentes, contribuindo, nomeadamente, com uma avaliação completa e objetiva dos riscos suscitados pelas novas atividades em vários cenários, das eventuais insuficiências dos quadros de gestão de riscos e de controlo interno da instituição, e da capacidade desta última para gerir de forma efetiva os novos riscos que possam surgir. A função de gestão de riscos também possui uma perspetiva clara do lançamento de novos produtos (ou da introdução de alterações significativas em produtos, processos e sistemas existentes) pelos diversos segmentos de atividade e carteiras, e poderes para exigir que a alteração dos produtos existentes passe pelo processo formal previsto na PANP.

19 Funções de controlo interno

153. As funções de controlo interno incluem uma função de gestão de riscos (ver a secção 20), uma função de verificação do cumprimento (ver a secção 21) e uma função de auditoria interna (ver a secção 22). As funções de gestão de riscos e de verificação do cumprimento são sujeitas a revisão por parte da função de auditoria interna.

154. As tarefas operacionais das funções de controlo interno podem ser subcontratadas, tendo em conta os critérios de proporcionalidade enumerados no Título I, à instituição consolidante ou a outra entidade pertencente ou não ao grupo, com a aprovação dos órgãos de administração das instituições envolvidas. Mesmo nos casos em que as tarefas de controlo interno operacionais são subcontratadas na totalidade ou em parte, o responsável pela função de controlo interno em causa e o órgão de administração continuam a ser responsáveis por estas atividades, bem como pela manutenção de uma função de controlo interno na instituição.

19.1 Responsáveis pelas funções de controlo interno

155. As funções de controlo interno são estabelecidas a um nível hierárquico adequado que lhes confira a autoridade e o estatuto necessários para cumprirem com as suas responsabilidades. Sem prejuízo da responsabilidade global do órgão de administração, as funções de controlo interno devem ser independentes dos segmentos de atividade ou unidades que controlam. Para este efeito, as direções das funções de gestão de riscos, verificação do cumprimento e

auditoria interna comunicam e respondem diretamente perante o órgão de administração, que também avalia o seu desempenho.

156. Quando necessário, os responsáveis pelas funções de controlo interno devem poder ter acesso e reportar diretamente ao órgão de administração na sua função de fiscalização, a fim de suscitarem preocupações e alertarem a função de supervisão, se for caso disso, para acontecimentos específicos que afetem ou possam afetar a instituição, sem prejuízo de poderem continuar a utilizar as suas linhas de reporte regulares.

157. As instituições têm em vigor processos documentados de nomeação e destituição do responsável por uma função de controlo interno. Em qualquer caso, os responsáveis pelas funções de controlo interno não devem ser substituídos (e, nos termos do artigo 76.º, n.º 5, da Diretiva 2013/36/UE, o responsável pela função de gestão de riscos não pode ser substituído) sem a prévia aprovação do órgão de administração na sua função de fiscalização. Nas instituições significativas, as autoridades competentes são informadas de imediato da aprovação e dos principais motivos da substituição do responsável por uma função de controlo interno.

19.2 Independência das funções de controlo interno

158. Para as funções de controlo interno poderem ser consideradas independentes, têm de preencher as seguintes condições:

a. o seu pessoal não desempenha tarefas operacionais abrangidas pelas atividades que as funções de controlo interno devem fiscalizar e controlar;

b. estão organizativamente separadas das atividades que lhes compete fiscalizar e controlar;

c. sem prejuízo da responsabilidade global dos membros do órgão de administração da instituição, o responsável por uma função de controlo interno não deve estar subordinado a uma pessoa com responsabilidades na gestão das atividades que a função de controlo interno fiscaliza e controla; e

d. a remuneração dos membros do pessoal das funções de controlo interno não está associada aos resultados das atividades que estas fiscalizam e controlam, nem pode comprometer de outro modo a sua objetividade[25].

[25] Ver também as orientações da EBA relativas a políticas de remuneração sãs, disponíveis em https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

19.3 Combinação de funções de controlo interno

159. Tendo em conta os critérios de proporcionalidade estabelecidos no Título I, a função de gestão de riscos pode ser combinada com a função de verificação do cumprimento. A função de auditoria interna não deve ser combinada com outra função de controlo interno.

19.4 Recursos das funções de controlo interno

160. As funções de controlo interno devem ter recursos suficientes e dispor de um número adequado de trabalhadores qualificados (tanto a nível da instituição-mãe como das filiais). As qualificações desses trabalhadores são permanentemente atualizadas e estes recebem uma formação adequada, sempre que necessário.

161. As funções de controlo interno devem dispor também de sistemas informáticos e apoio adequados, com acesso às informações internas e externas necessárias para o exercício das suas responsabilidades. Devem ter acesso a todas as informações necessárias relativas a todos os segmentos de atividade e às filiais de risco relevantes, em particular, as que podem originar riscos significativos para a instituição.

20 Função de gestão de riscos

162. As instituições estabelecem uma função de gestão de riscos (FGR) que abrange toda a instituição. A FGR tem autoridade, estatuto e recursos suficientes, tendo em conta os critérios de proporcionalidade enumerados no Título I, para implementar as políticas de risco e o quadro de gestão de riscos definidos na secção 17.

163. Quando necessário, a FGR tem acesso direto ao órgão de administração na sua função de fiscalização e aos seus comités, se estiverem constituídos, incluindo, em particular, o comité de riscos.

164. A FGR tem acesso a todos os segmentos de negócio e outras unidades internas suscetíveis de gerar riscos, bem como às filiais e sucursais relevantes.

165. Os membros do pessoal da FGR devem possuir conhecimentos, competência e experiência suficientes, no que respeita às técnicas e procedimentos em matéria de gestão de riscos, aos mercados e aos produtos, e devem ter acesso a formação regular.

166. A FGR é independente dos segmentos de atividade e unidades cujos riscos controla, mas não está impedida de interagir com os mesmos. A interação entre as funções operacionais e a FGR facilita o objetivo de responsabilizar todos os membros do pessoal da instituição pela gestão de riscos.

167. A FGR é um elemento organizativo essencial da instituição e está estruturada de modo a poder aplicar políticas em matéria de risco e controlar o quadro de gestão de riscos. A FGR desempenha um papel fundamental para assegurar que a instituição tem em vigor processos

eficazes em matéria de gestão de riscos e deve ser envolvida em todas as decisões relevantes nesta matéria.

168. As instituições significativas podem ponderar a possibilidade de criar FGR específicas para cada segmento de atividade concreto, mas terão sempre de possuir uma FGR a nível central (incluindo uma FGR a nível de grupo na instituição consolidante), para obterem uma perspetiva holística da totalidade dos riscos, a nível da instituição e do grupo, e assegurar que estratégia de risco é cumprida.

169. A FGR fornece informações, análises e avaliações periciais pertinentes e independentes sobre a exposição ao risco, emite pareceres sobre propostas e decisões relativas aos riscos adotadas pelos segmentos de atividade ou pelas unidades internas e informa o órgão de administração da compatibilidade dessas propostas e decisões com a apetência pelo risco e a estratégia da instituição. A FGR pode recomendar melhorias ao quadro de gestão de riscos e medidas corretivas para remediar as violações das políticas, procedimentos e limites de risco.

20.1 Papel da FGR na estratégia e nas decisões em matéria de risco

170. A FGR participa ativamente, desde uma fase inicial, na elaboração da estratégia de risco da instituição e assegura que a instituição tem em vigor processos eficazes de gestão de riscos. A FGR faculta ao órgão de administração todas as informações relevantes a respeito dos riscos para que este possa determinar o nível de apetência pelo risco da instituição. A FGR avalia a solidez e a sustentabilidade da estratégia e da apetência pelo risco e assegura que esta se traduz em limites de risco específicos. A FGR avalia igualmente a estratégia de risco das unidades de negociação, incluindo os objetivos que estas propõem, e é envolvida antes de o órgão de administração tomar decisões relativas às estratégias de risco. Esses objetivos devem ser plausíveis e coerentes com a estratégia de risco das instituições.

171. O envolvimento da FGR nos processos de tomada de decisão assegura que as considerações de risco são devidamente tidas em conta, contudo a responsabilidade pelas decisões tomadas continua a caber às unidades de negociação e internas e, em última instância, ao órgão de administração.

20.2 Papel da FGR nas alterações significativas

172. De acordo com a secção 18, antes da tomada de decisões sobre alterações significativas ou operações excecionais, a FGR é envolvida na avaliação do impacto das mesmas no risco global da instituição e do grupo e comunica as suas conclusões diretamente ao órgão de administração antes da adoção de uma decisão.

173. A FGR avalia a forma como os riscos identificados podem afetar a capacidade da instituição ou do grupo para gerir o seu perfil de risco, a sua liquidez e a sua base sólida de fundos próprios, em circunstâncias normais e adversas.

20.3 Papel da FGR na identificação, medição, avaliação, gestão, mitigação, acompanhamento e reporte de riscos

174. A FGR assegura que todos os riscos são identificados, avaliados, medidos, monitorizados, geridos e adequadamente reportados pelas unidades pertinentes na instituição.

175. A FGR assegura que a identificação e a avaliação não se baseiam apenas em informações quantitativas ou em resultados de modelos e também têm em conta abordagens qualitativas. A FGR mantém o órgão de administração informado dos pressupostos utilizados, bem como de eventuais insuficiências da análise e dos modelos de risco.

176. A FGR assegura que as operações com partes relacionadas são revistas e que os riscos para a instituição por elas suscitados são identificados e adequadamente avaliados.

177. A FGR assegura que todos os riscos identificados são efetivamente acompanhados pelas unidades de negociação.

178. A FGR monitoriza de forma regular o perfil de risco real da instituição e examina-o em relação aos seus objetivos estratégicos e apetência pelo risco, a fim de permitir que o órgão de administração, na sua função de gestão, tome decisões, e o órgão de administração, na sua função de fiscalização, as conteste.

179. A FGR analisa as tendências e reconhece os riscos novos ou emergentes e os aumentos dos riscos suscitados pela alteração das circunstâncias e condições. Revê também regularmente os resultados referentes aos riscos reais em relação às estimativas anteriores (isto é, verificações a posteriori) para avaliar e melhorar a precisão e a eficácia do processo de gestão de riscos.

180. A FGR avalia as possíveis formas de mitigar os riscos. O reporte ao órgão de administração deve incluir propostas de medidas de mitigação dos riscos adequadas.

20.4 Papel da FGR nas exposições não aprovadas

181. A FGR avalia de forma independente qualquer infração dos limites ou da apetência pelo risco (incluindo determinar as suas causas e efetuar uma análise jurídica e económica do custo real de fechar, reduzir ou cobrir a posição em risco face ao possível custo da sua manutenção), informando as unidades de negociação em causa e o órgão de administração e recomendando possíveis soluções. A FGR reporta diretamente as infrações significativas ao órgão de administração na sua função de fiscalização, sem prejuízo do reporte a outras funções internas e aos comités.

182. A FGR tem um papel fundamental no sentido de assegurar que as decisões relativas às suas recomendações são tomadas ao nível pertinente, cumpridas pelas unidades de negociação em causa e adequadamente comunicadas ao órgão de administração e, se tiver sido constituído, ao comité de risco.

20.5 Responsável pela função de gestão de riscos

183. O responsável pela FGR é responsável por fornecer informações exaustivas e compreensíveis sobre os riscos e aconselha o órgão de administração, a fim de permitir que este conheça o perfil de risco global da instituição. O mesmo se aplica ao responsável pela FGR de uma instituição-mãe em relação à situação consolidada.

184. O responsável pela FGR possui conhecimentos especializados, independência e o nível hierárquico suficientes para contestar as decisões que afetem a exposição da instituição aos riscos. Quando o responsável pela FGR não integra o órgão de administração, as instituições significativas nomeiam um responsável independente para a FGR que não tenha responsabilidades por outras funções e que reporte diretamente ao órgão de administração. Caso não seja adequado nomear uma pessoa para desempenhar exclusivamente o cargo de responsável pela FGR, tendo em conta o princípio da proporcionalidade estabelecido no Título I, esta função pode ser combinada com a função de responsável pela função de verificação do cumprimento ou ser desempenhada por outra pessoa de nível hierárquico superior, desde que não exista qualquer conflito de interesses entre as funções combinadas. Em qualquer dos casos, esta pessoa deve ter autoridade, estatuto e independência suficientes (p. ex., responsável pelo departamento jurídico).

185. O responsável pela FGR deve poder contestar decisões adotadas pela gestão da instituição e pelo seu órgão de administração, e os fundamentos das suas objeções devem ser formalmente documentados. Se a instituição quiser conceder ao responsável pela FGR o direito de vetar decisões (p. ex., uma decisão de crédito ou de investimento ou a fixação de um limite) tomadas em níveis inferiores ao órgão de administração, deve especificar o âmbito desse direito de veto, os procedimentos de escalamento ou de recurso e a forma como o órgão de administração é envolvido.

186. As instituições estabelecem procedimentos reforçados para a aprovação de decisões sobre as quais o responsável pela FGR manifestou uma opinião negativa. O órgão de administração na sua função de fiscalização deve poder comunicar diretamente com o responsável pela FGR sobre as principais questões relacionadas com os riscos, incluindo evoluções que possam ser incompatíveis com a estratégia e a apetência pelo risco da instituição.

21 Função de verificação do cumprimento

187. As instituições estabelecem uma função de verificação do cumprimento (FVC) permanente e eficaz para gerir o risco de conformidade e nomeiam uma pessoa responsável por esta função a nível da instituição (o responsável pela verificação do cumprimento ou o diretor de conformidade).

188. Caso não seja adequado nomear uma pessoa para desempenhar exclusivamente o cargo de diretor da FVC, tendo em conta o princípio da proporcionalidade estabelecido no Título I, esta função pode ser combinada com a função de responsável pela FGR ou ser executada por outra

pessoa de nível hierárquico superior (p. ex., o responsável pelo departamento jurídico), desde que não exista qualquer conflito de interesses entre as funções combinadas.

189. A FVC, incluindo o seu responsável, é independente dos segmentos de atividade e unidades internas que controla e tem autoridade, estatuto e recursos suficientes. Tendo em conta os critérios de proporcionalidade estabelecidos no Título I, esta função pode ser assistida ou combinada com a FGR ou outras funções adequadas, p. ex., o departamento jurídico ou os recursos humanos.

190. Os membros do pessoal da FVC devem possuir conhecimentos, competência e experiência suficientes, no que respeita à verificação do cumprimento e aos procedimentos, e devem ter acesso a formação regular.

191. O órgão de administração na sua função de fiscalização supervisiona a implementação de uma política de verificação do cumprimento bem documentada, que é comunicada a todos os membros do pessoal. A instituição estabelece um processo para avaliar regularmente alterações na legislação e nos regulamentos aplicáveis às suas atividades.

192. A FVC aconselha o órgão de administração sobre as medidas a adotar para assegurar o cumprimento em matéria de legislação, regulamentação e normas aplicáveis e avalia o possível impacto de eventuais alterações ao quadro jurídico ou regulamentar nas atividades da instituição e no quadro da verificação do cumprimento.

193. A FVC assegura que o controlo é efetuado através de um programa de acompanhamento da verificação do cumprimento estruturado e bem definido e que a política em matéria de verificação do cumprimento é observada. A FVC deve reportar ao órgão de administração e, se for caso disso, comunicar com a FGR, sobre o risco de conformidade da instituição e a sua gestão. Se for caso disso, a FVC e a FGR cooperam e trocam informações necessárias para o desempenho das respetivas funções. As conclusões da FVC são tidas em conta pelo órgão de administração e pela FGR no âmbito do processo de tomada de decisões.

194. Em consonância com a secção 18 das presentes orientações, a FVC certifica-se também, em estreita cooperação com a FGR e o departamento jurídico, de que os novos produtos e os novos procedimentos respeitam o quadro jurídico em vigor e, se for caso disso, as futuras alterações conhecidas à legislação, à regulamentação e aos requisitos de supervisão.

195. As instituições adotam medidas adequadas contra qualquer comportamento fraudulento e infrações disciplinares a nível interno ou externo (p. ex., infrações de procedimentos internos ou violações dos limites).

196. As instituições asseguram que as suas filiais e sucursais adotam medidas para garantir que as suas operações cumprem a legislação e os regulamentos locais. Caso a legislação e os regulamentos locais impeçam a aplicação de procedimentos e sistemas de verificação do cumprimento mais rigorosos implementados pelo grupo, em especial, se impedirem a

divulgação e o intercâmbio de informações necessárias entre entidades do grupo, as filiais e as sucursais devem informar o responsável pela FVC da instituição consolidante.

22 Função de auditoria interna

197. As instituições estabelecem uma função de auditoria interna (FAI) independente e efetiva, tendo em conta os critérios de proporcionalidade estabelecidos no Título I, e nomeiam uma pessoa responsável por esta função em toda a instituição. A FAI deve ser independente e ter autoridade, estatuto e recursos suficientes. Em particular, a instituição assegura que as qualificações dos membros do pessoal da FAI e os recursos da FAI, nomeadamente as suas ferramentas de auditoria e métodos de análises de risco, são adequados à dimensão e às localizações da instituição, bem como à natureza, escala e complexidade dos riscos associados ao modelo de negócio, às atividades, à cultura de risco e à apetência pelo risco da instituição.

198. A FAI deve ser independente em relação às atividades auditadas. Por conseguinte, não deve ser combinada com outras funções.

199. A FAI, segundo uma abordagem baseada no risco, avalia com independência e fornece uma garantia objetiva da conformidade de todas as atividades e unidades de uma instituição, incluindo as atividades subcontratadas, com as políticas e os procedimentos da instituição e com requisitos externos. Todas as entidades do grupo são consideradas no âmbito da FAI.

200. A FAI não é envolvida no desenho, seleção, definição e implementação de políticas, mecanismos e procedimentos específicos de controlo interno e limites de risco. Contudo, tal não deve impedir o órgão de administração na sua função de gestão de solicitar o parecer da auditoria interna sobre questões relacionadas com o risco, controlos internos e cumprimento das regras aplicáveis.

201. A FAI avalia se o quadro de controlo interno da instituição, tal como definido na secção 15, é efetivo e eficiente. Em particular, a função de auditoria interna avalia:

    a. a adequação do quadro de governo da instituição;

    b. se as políticas e os procedimentos existentes continuam a ser adequados e cumprem os requisitos jurídicos e regulamentares, bem como a apetência pelo risco e a estratégia da instituição;

    c. a conformidade dos procedimentos com as leis e os regulamentos aplicáveis e com as decisões do órgão de administração;

    d. se os procedimentos são implementados de forma correta e efetiva (p. ex., a conformidade das operações, o nível do risco efetivamente incorrido, etc.); e

e. a adequação, a qualidade e a efetividade dos controlos efetuados e do reporte realizado pelas unidades de negociação, pela função de gestão de riscos e pela função de verificação do cumprimento.

202. A FAI verifica, em particular, a integridade dos processos que garantem a fiabilidade dos métodos e técnicas da instituição, bem como dos pressupostos e fontes de informação utilizados nos seus modelos internos (p. ex., modelização do risco e mensuração contabilística). Avalia igualmente a qualidade e a utilização de ferramentas qualitativas de identificação e avaliação dos riscos e as medidas de mitigação dos riscos adotadas.

203. A FAI tem livre acesso a todos os registos, documentos, informações e edifícios da instituição, incluindo o acesso aos sistemas de informação de gestão e às atas de todas as reuniões dos comités e dos órgãos de decisão.

204. A FAI deve observar as normas profissionais nacionais e internacionais. São exemplo das normas profissionais aqui referidas as normas estabelecidas pelo Instituto de Auditores Internos (Institute of Internal Auditors - IIA).

205. O trabalho de auditoria interna é efetuado de acordo com um plano de auditoria e com programas de auditoria pormenorizados, utilizando uma abordagem baseada no risco.

206. Deve ser elaborado um plano de auditoria interna, pelo menos, uma vez por ano, com base nos objetivos anuais de controlo da auditoria interna. O plano de auditoria interna é aprovado pelo órgão de administração.

207. Todas as recomendações de auditoria são objeto de um procedimento de acompanhamento formal por parte dos níveis de gestão adequados, a fim de garantir e apresentar relatórios sobre a sua resolução eficiente e atempada.

Título VI – Gestão da continuidade da atividade

208. As instituições estabelecem um plano sólido de gestão da continuidade da atividade para poderem funcionar em permanência e para limitarem as perdas em caso de perturbação grave das atividades.

209. As instituições podem estabelecer uma função independente específica de continuidade da atividade, p. ex., como parte da função de gestão de riscos[26].

210. A atividade de uma instituição está dependente de vários recursos críticos (por exemplo, sistemas informáticos, incluindo serviços em nuvem, sistemas de comunicação e edifícios). O objetivo da gestão da continuidade da atividade é minimizar as consequências operacionais, financeiras, jurídicas e reputacionais, bem como outras consequências materiais

[26] Consultar também o artigo 315.º do Regulamento (UE) n.º 575/2013,

decorrentes de uma catástrofe ou de uma interrupção prolongada destes recursos e a perturbação consequente dos procedimentos comerciais normais da instituição. Outras medidas de gestão de riscos poderão destinar-se a reduzir a probabilidade da ocorrência de tais incidentes ou transferir o seu impacto financeiro para terceiros (por exemplo, através de seguros).

211. A fim de estabelecer um plano sólido de gestão da continuidade da atividade, a instituição analisa cuidadosamente a sua exposição a perturbações graves das atividades e avalia (quantitativa e qualitativamente) o seu potencial impacto, utilizando dados internos e/ou externos e análise de cenários. Esta análise abrange todos os segmentos de atividades e unidades internas, incluindo a função de gestão de riscos, e tem em conta a interdependência das mesmas. Os resultados da análise contribuem para definir as prioridades e os objetivos de recuperação da instituição.

212. Com base na análise anterior, uma instituição estabelece:

a. planos de emergência e de continuidade da atividade para assegurar uma reação adequada às emergências e ter a capacidade de manter as suas atividades comerciais mais importantes em caso de perturbação dos procedimentos comerciais normais; e

b. planos de recuperação de recursos críticos para poder retomar os procedimentos comerciais normais num prazo adequado. Os eventuais riscos residuais resultantes de potenciais perturbações da atividade serão compatíveis com a apetência pelo risco da instituição.

213. Os planos de emergência, de continuidade da atividade e de recuperação são documentados e cuidadosamente executados. A documentação está disponível nos segmentos de atividade, nas unidades internas e na função de gestão de riscos e é armazenada em sistemas fisicamente separados e facilmente acessíveis em caso de emergência. É ministrada formação adequada e os planos são periodicamente testados e atualizados. Quaisquer desafios ou falhas detetados nos testes são documentados e analisados, e os planos revistos em conformidade.

Título VII – Transparência

214. As estratégias, políticas e procedimentos são comunicados a todo o pessoal pertinente da instituição. O pessoal da instituição compreende e respeita as políticas e os procedimentos referentes às suas funções e responsabilidades.

215. Deste modo, o órgão de administração informa e mantém o pessoal pertinente ao corrente das estratégias e políticas da instituição, de uma forma clara e coerente, pelo menos ao nível necessário para desempenharem as suas funções específicas. Podem utilizar-se para o efeito orientações escritas, manuais ou outros meios.

216. Nos casos em que as autoridades competentes, nos termos do artigo 106.º, n.º 2, da Diretiva 2013/36/UE, exijam que as empresas-mãe publiquem anualmente uma descrição da sua

estrutura jurídica e de governo e da estrutura organizacional do grupo de instituições, as informações devem incluir todas as entidades da estrutura do grupo por país, conforme definido na Diretiva 2013/34/UE[27].

217. A publicação deve incluir, no mínimo:

a. uma descrição da organização interna das instituições e da estrutura do grupo, conforme definido na Diretiva 2013/34/UE e respetivas alterações, incluindo as principais linhas de reporte e responsabilidades;

b. quaisquer alterações significativas desde a publicação anterior e as datas dessas alterações;

c. novas estruturas jurídicas, de governo ou organizacionais;

d. informações sobre a estrutura, a organização e os membros do órgão de administração, incluindo o número total de membros e o número de membros que são considerados independentes, especificando o género e a duração do mandato de cada membro do órgão de administração;

e. as principais responsabilidades do órgão de administração;

f. uma lista dos comités do órgão de administração na sua função de fiscalização e a sua composição;

g. uma descrição da política em matéria de conflitos de interesses aplicável às instituições e ao órgão de administração;

h. uma descrição do quadro de controlo interno; e

i. uma descrição do quadro de gestão da continuidade da atividade.

Anexo I – Aspetos a ter em conta ao elaborar uma política de governo interno

Em consonância com o Título III, as instituições devem considerar os seguintes aspetos quando documentam as políticas e os sistemas de governo interno:

[27] Diretiva 2013/34/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa às demonstrações financeiras anuais, às demonstrações financeiras consolidadas e aos relatórios conexos de certas formas de empresas, que altera a Diretiva 2006/43/CE do Parlamento Europeu e do Conselho e revoga as Diretivas 78/660/CEE e 83/349/CEE do Conselho (JO L 182 de 29.6.2013, p. 19).

1. Estrutura acionista
2. Estrutura do grupo, se aplicável (estrutura jurídica e funcional)
3. Composição e funcionamento do órgão de administração
    a) critérios de seleção
    b) número, duração do mandato, rotação, idade
    c) membros independentes do órgão de administração
    d) membros executivos do órgão de administração
    e) membros não executivos do órgão de administração
    f) distribuição de pelouros, se aplicável
4. Estrutura de governo e organigrama (com impacto no grupo, se aplicável)
    a) comités especializados
        i. composição
        ii. funcionamento
    b) comité executivo, se existir
        i. composição
        ii. funcionamento
5. Titulares de funções essenciais
    a) Responsável pela função de gestão de riscos
    b) Responsável pela função de verificação do cumprimento
    c) Responsável pela função de auditoria interna
    d) Administrador com o pelouro financeiro (CFO)
    e) outros titulares de funções essenciais
6. Quadro de controlo interno
    a) descrição de cada função, incluindo a sua organização, recursos, estatuto e autoridade
    b) descrição do quadro de gestão de riscos, incluindo a estratégia de risco
7. Estrutura organizacional (com impacto no grupo, se aplicável)
    a) estrutura operacional, segmentos de atividade e atribuição de competências e responsabilidades
    b) subcontratação
    c) gama de produtos e serviços
    d) âmbito geográfico da atividade
    e) prestação gratuita de serviços
    f) sucursais

g) filiais, sociedades mistas, etc.

h) utilização de centros offshore

8. Código de conduta e comportamento (com impacto no grupo, se aplicável)
   a) objetivos estratégicos e valores empresariais
   b) códigos e regulamentos internos, política de prevenção
   c) política em matéria de conflito de interesses
   d) denúncia
9. Estado da política de governo interno, com a data de:
   a) elaboração
   b) última alteração
   c) última avaliação
   d) aprovação pelo órgão de administração.