EBA/GL/2021/05

2 de julho de 2021

Orientações

sobre governo interno

1. Obrigações de cumprimento e de reporte

Natureza das presentes orientações

1. As presentes orientações foram 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 Regulamento (UE) n.º 1093/2010, as autoridades competentes e as instituições financeiras, incluindo as instituições, 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 se aplicam as presentes orientações devem dar cumprimento às mesmas, incorporando-as nas suas práticas de supervisão conforme adequado (por exemplo, alterando o respetivo enquadramento jurídico ou os respetivos processos de supervisão), nomeadamente sempre que as orientações se dirijam, em primeira instância, às instituições.

Requisitos de reporte

3. Nos termos do artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes devem notificar a EBA de que dão ou tencionam dar cumprimento às presentes orientações, ou, caso contrário, notificá-la das razões do não cumprimento, até (05.12.2021). Na ausência de qualquer notificação até à referida data, a EBA considerará que a autoridade competente em causa não cumpre as orientações. As notificações devem ser efetuadas mediante o envio do modelo disponível no sítio Web da EBA para compliance@eba.europa.eu com a referência «EBA/GL/2021/05». As notificações devem ser efetuadas por pessoas devidamente autorizadas para o reporte da verificação do cumprimento em nome das 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 artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010.

[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 de 15.12.2010, p. 12).

2. Objeto, âmbito de aplicação e definições

Objeto

5. As presentes orientações especificam mais pormenorizadamente as disposições, processos e mecanismos de governação interna que as instituições abrangidas pela Diretiva 2013/36/UE[2] e as empresas de investimento abrangidas pelo Título VII da Diretiva 2013/36/UE em aplicação do artigo 1.º, n.os 2 e 5, do Regulamento 2019/2033/UE devem aplicar, de acordo com o artigo 74.º, n.º 1, da Diretiva 2013/36/UE, para garantir a sua gestão efetiva e prudente.

Destinatários

As presentes orientações são dirigidas às autoridades competentes na aceção do artigo 4.º, n.º 2, alínea i), do Regulamento (UE) n.º 1093/2010, e às instituições financeiras na aceção do artigo 4.º, n.º 1, do Regulamento (UE) n.º 1093/2010 que são instituições para efeitos de aplicação da Diretiva 2013/36/UE, na aceção do artigo 3.º, n.º 1, ponto 3), da mesma diretiva, também tendo em conta o artigo 3.º, n.º 3, da mesma diretiva, ou que são empresas de investimento abrangidas pelo Título VII da Diretiva 2013/36/UE, em aplicação do artigo 1.º, n.os 2 e 5, do Regulamento (UE) 2019/2033 (a seguir «instituições»).

Âmbito de aplicação

6. As presentes orientações aplicam-se às disposições de governação das instituições, incluindo a respetiva estrutura organizacional e as correspondentes linhas de responsabilidade, aos processos de identificação, gestão, monitorização, e reporte de todos os riscos[3] a que estão ou possam vir a estar expostas, e ao quadro de controlo interno.

7. As orientações pretendem abranger todas as estruturas de administração existentes e não preconizam nenhuma estrutura específica. As orientações não interferem com a repartição geral de competências de acordo com o direito das sociedades nacional. Por conseguinte, devem ser aplicadas, independentemente da estrutura de administração utilizada (monista e/ou dualista e/ou outra estrutura) nos Estados-membros. Deve pressupor-se que o «órgão de administração», tal como definido no artigo 3.º, n.º 1, pontos 7) e 8), da Diretiva 2013/36 UE, tem funções de gestão (executivas) e de fiscalização (não executivas)[4].

[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] Qualquer referência a «riscos» nas presentes orientações deve incluir os riscos de branqueamento de capitais e de financiamento do terrorismo.

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

8. 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 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 órgãos ou membros do órgão de administração e fiscalização responsáveis por essa função, nos termos do direito nacional. Ao implementarem as presentes orientações, as autoridades competentes devem ter em conta o direito das sociedades do seu país e, sempre que necessário, especificar o órgão ou os membros do órgão de administração aos quais se aplicam essas funções.

9. 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 pressupor-se que as pessoas que desempenham essas funções executivas ao abrigo 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 administrador executivo, conforme definidos nas presentes orientações, mesmo que não tenham sido propostos ou nomeados como membros formais do órgão ou dos órgãos de governo da instituição nos termos do direito nacional.

10. Nos Estados-Membros onde algumas responsabilidades são exercidas diretamente por acionistas, membros ou proprietários da instituição em lugar do órgão de administração, as instituições devem assegurar que tais responsabilidades e decisões conexas estão, tanto quanto possível, em conformidade com as orientações aplicáveis ao órgão de administração.

11. As definições utilizadas nas presentes orientações de administrador executivo [CEO], administrador financeiro [CFO] e titular de funções essenciais são puramente funcionais e não pretendem impor a nomeação destas funções ou a criação destes cargos, exceto se tal for exigido pelo direito nacional ou pelo direito da UE aplicável.

12. As instituições devem cumprir as presentes orientações e as autoridades competentes devem garantir o seu cumprimento pelas instituições, em base individual, subconsolidada e consolidada, de acordo com o nível de aplicação estabelecido no artigo 109.º da Diretiva 2013/36/UE.

Definições

13. Salvo especificação em contrário, os termos utilizados e definidos na Diretiva 2013/36/UE e no Regulamento (UE) n.º 575/2013 têm o mesmo significado nas presentes orientações. Adicionalmente, para efeitos das presentes orientações, aplicam-se as seguintes definições:

Acionista	uma pessoa que possui ações de uma instituição ou, dependendo da forma jurídica da instituição, outros proprietários ou membros da instituição.
Administrador executivo (CEO)	a pessoa responsável pela gestão e orientação global das atividades de negócio de uma instituição.
Administrador financeiro (CFO)	a pessoa que detém a responsabilidade global pela gestão de todas as seguintes atividades: gestão dos recursos financeiros, planeamento financeiro e relato financeiro.
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 suas restrições regulamentares.
Cargo de administração	uma posição como membro do órgão de administração de uma instituição ou outra entidade jurídica.
Consolidação prudencial	a aplicação das regras 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[5].
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.
Disparidade salarial entre géneros	a diferença entre a remuneração horária bruta média de homens e mulheres, expressa em percentagem da remuneração horária bruta média dos homens.
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 (UE) 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, caso aplicável, outras instituições determinadas pela autoridade competente ou pelo direito nacional, com base na avaliação da dimensão e

[5] Ver também as NTR relativas à consolidação prudencial em: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

	organização interna das instituições, e da natureza, âmbito de aplicação e complexidade das suas atividades.
Instituição cotada	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, pontos 21) e 22), da Diretiva 2014/65/UE, num ou mais Estados-Membros[6].
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.
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	As pessoas que têm uma influência significativa na gestão da instituição, mas que não são membros do órgão de administração, nem o administrador executivo. Incluem os responsáveis pelas funções de controlo interno e o administrador financeiro, se estes não forem membros do órgão de administração, e, sempre que identificados pelas instituições segundo uma abordagem baseada no risco, outros titulares de funções essenciais. Estes podem incluir responsáveis por unidades de negócio significativas, sucursais do Espaço Económico Europeu e da Associação Europeia de Comércio Livre, filiais de países terceiros e outras funções internas.

3. Implementação

Data de aplicação

14. As presentes orientações aplicam-se a partir de 31 de dezembro de 2021.

Revogação

15. As orientações da EBA sobre governo interno (EBA/GL/2017/11), de 26 de setembro de 2017, são revogadas com efeitos a partir de 31 de dezembro de 2021.

[6] 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).

4. Orientações

Título I – Proporcionalidade

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

17. No desenvolvimento e implementação de sistemas de governo interno, as instituições devem ter em conta a sua dimensão e organização interna, bem como a natureza, escala 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. As instituições devem, contudo, ter em conta, que a dimensão ou a importância sistémica da instituição não podem, por si só, ser indicativas da medida em que a instituição está exposta aos riscos.

18. Para efeitos da aplicação do princípio da proporcionalidade e a fim de assegurar a implementação adequada dos requisitos regulamentares e das presentes orientações, as instituições e as autoridades competentes devem ter em conta todos os aspetos seguintes:

    a. A dimensão em termos do total do balanço da instituição e das suas filiais no perímetro de 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 do grupo;

    d. Se a instituição está cotada;

    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 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 funções e canais de distribuição subcontratados;

l. Os sistemas de tecnologias da informação (TI) existentes, incluindo os sistemas de continuidade e as funções subcontratadas neste domínio; e

m. Se a instituição está abrangida pela definição dos pontos 145) e 146) do artigo 4.º, n.º 1, do Regulamento (UE) n.º 575/2013 de «instituição de pequena dimensão e não complexa» e de «instituição de grande dimensão».

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

1 Papel e responsabilidades do órgão de administração

19. 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 implementação de sistemas de governo na instituição que asseguram a sua gestão efetiva e prudente.

20. 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 definidos num documento escrito e devidamente aprovado pelo órgão de administração. Todos os membros do órgão de administração devem ter pleno conhecimento da estrutura e responsabilidades deste órgão, bem como da divisão de tarefas entre as diferentes funções do órgão de administração e os seus comités.

21. O órgão de administração na sua função de fiscalização e na sua função de gestão deve interagir de forma efetiva. As duas funções devem trocar informações suficientes que lhes permitam desempenhar os respetivos papéis. A fim de assegurar a existência de mecanismos adequados de controlo e equilíbrio, o processo de tomada de decisão no órgão de administração não deve ser circunscrito a um único membro ou a um número reduzido de membros.

22. As responsabilidades do órgão de administração incluem a definição, a aprovação e a fiscalização da implementação dos seguintes aspetos:

    a. A estratégia de negócio global e as políticas essenciais da instituição, tendo em conta o quadro jurídico e regulamentar aplicável, os interesses financeiros e a solvabilidade da instituição a longo prazo;

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

    c. Um quadro adequado e efetivo de governo e de controlo interno, tal como definido no Título V, que:

        i. inclui uma estrutura organizacional clara e funções internas independentes e eficientes de gestão de riscos, conformidade e auditoria, que disponham de autoridade, estatuto e recursos suficientes para exercerem as suas funções;

        ii. assegura o cumprimento dos requisitos regulamentares aplicáveis no contexto da prevenção do branqueamento de capitais e do financiamento do terrorismo;

    d. Os montantes, tipos e distribuição dos fundos próprios internos e dos fundos próprios regulamentares para cobrir de forma adequada os riscos da instituição;

    e. Os objetivos da gestão da liquidez da instituição;

    f. 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[7];

    g. Mecanismos que assegurem que a avaliação da adequação individual e coletiva do órgão de administração seja realizada de forma eficaz, que a composição e o plano de sucessão do órgão de administração sejam adequados e que o órgão de administração desempenhe as suas funções de forma eficaz[8];

    h. Um processo de seleção e avaliação da adequação dos titulares de funções essenciais[9];

[7] Orientações da EBA relativas a políticas de remuneração sãs

[8] Ver também as Orientações conjuntas da ESMA e da EBA sobre a avaliação da adequação dos membros do órgão de administração e dos titulares de funções essenciais.

[9] Ver também as Orientações conjuntas da ESMA e da EBA sobre a avaliação da adequação dos membros do órgão de administração e dos titulares de funções essenciais.

i. Os 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. 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;

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

l. Uma política em matéria de conflitos de interesses a nível institucional consentânea com a Secção 11 e em relação ao pessoal consentânea com a Secção 12; e

m. Os mecanismos destinados a garantir a integridade dos sistemas contabilístico e relato financeiro, incluindo os controlos financeiros e operacionais e o cumprimento da legislação e das normas aplicáveis.

23. Ao definir, aprovar e fiscalizar a implementação dos aspetos enumerados no n.º 22, o órgão de administração deve procurar garantir que o modelo de negócio, sistemas de governo, incluindo um quadro de gestão de riscos que tenha em conta todos os riscos. Ao terem em conta todos os riscos a que as instituições estão expostas, estas devem ter em conta todos os fatores de risco relevantes, incluindo os fatores de risco ambientais, sociais e de governação. As instituições devem considerar que estes últimos podem impulsionar os seus riscos prudenciais, incluindo riscos de crédito, por ex. através de fatores de risco relacionados com a transição para uma economia sustentável ou eventos físicos externos relacionados com o clima que podem afetar os devedores, o mercado, a liquidez, riscos operacionais e também riscos de reputação, por ex. através de fatores de risco sociais e de governação, por ex. no contexto de acordos de subcontratação[10]. Tais riscos incluem, por exemplo, riscos jurídicos no domínio do direito dos contratos ou do direito do trabalho, riscos relativos a potenciais violações dos direitos humanos ou outros fatores de risco ambientais, sociais ou de governação (ASG) que podem afetar o país onde o prestador de serviços está localizado e a sua capacidade para prestar os níveis de serviço acordados.

[10] Ver *EBA report on ESG risk management and supervision* [relatório da EBA sobre a gestão e supervisão dos riscos ASG] publicado ao abrigo do artigo 98.º, n.º 8, da Diretiva 2013/36/UE, para uma descrição do entendimento da EBA sobre os riscos ASG, canais de transmissão, e recomendações relativas a disposições, processos, mecanismos e estratégias a implementar pelas instituições para identificar, avaliar e gerir os riscos ASG.

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

25. Todos os membros do órgão de administração devem ser 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 membro do órgão de administração pode ser responsável por uma função de controlo interno, conforme referido no Título V, Secção 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 deve acompanhar, rever periodicamente e corrigir quaisquer insuficiências identificadas no que respeita à implementação dos processos, estratégias e políticas associados às responsabilidades enumeradas nos n.^{os} 22 e 23. O quadro de governo interno e a sua implementação, devem ser revistos e atualizados periodicamente tendo em conta o princípio da proporcionalidade, conforme explicado no Título I. Sempre que alterações significativas afetem a instituição , deve ser realizada uma revisão mais profunda.

2 Função de gestão do órgão de administração

28. O órgão de administração na sua função de gestão deve envolver-se ativamente na atividade da instituição e deve tomar decisões fundamentadas e com conhecimento de causa.

29. O órgão de administração na sua função de gestão é responsável pela implementação das estratégias definidas pelo órgão de administração e discute regularmente a implementação 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 deve informar 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 tomadas relativas às atividades de negócio e aos riscos incorridos), 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.

31. Sem prejuízo da transposição nacional da Diretiva 2015/849/UE, o órgão de administração deve, em conformidade com os requisitos por força do artigo 46.º, n.º 4, da Diretiva 2015/849/UE relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo (BC/FT), identificar um dos seus membros como responsável pela implementação das disposições legislativas,

regulamentares e administrativas necessárias para dar cumprimento a esta diretiva, incluindo as respetivas políticas e procedimentos de BC/FT na instituição e ao nível do órgão de administração[11].

3 Função de fiscalização do órgão de administração

32. 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.

33. 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 sobre a 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.

34. Sem prejuízo das responsabilidades atribuídas por força do direito das sociedades nacional aplicável, o órgão de administração na sua função de fiscalização:

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

    b. Critica e analisa 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 medidas adequadas para corrigir quaisquer deficiências identificadas;

    e. Supervisiona e monitoriza a implementação coerente dos objetivos estratégicos da instituição, da sua estrutura organizacional e da sua estratégia de risco, da sua apetência pelo risco e do seu quadro de gestão de riscos, bem como de outras políticas (por ex., a política de remuneração) e do quadro para a divulgação de informação;

    f. Monitoriza a implementação coerente da cultura de risco da instituição;

[11] O órgão de administração, enquanto órgão coletivo, permanece responsável no seu conjunto.

g. Supervisiona a implementação e manutenção de um código de conduta ou de um código semelhante e de políticas eficazes, a fim de identificar, gerir e mitigar conflitos de interesse reais ou potenciais;

h. Supervisiona a integridade da informação e do relato financeiro, e o quadro de controlo interno, incluindo um quadro sólido e eficaz de gestão de riscos;

i. Assegura que os responsáveis das funções de controlo interno possam atuar com independência e, sem prejuízo da obrigação de informar outros órgãos internos, unidades ou áreas de negócio, manifestar preocupações e alertar diretamente o órgão de administração na sua função de fiscalização, quando necessário, sempre que a evolução adversa do risco afete ou seja suscetível de afetar a instituição; e

j. Monitoriza a implementação do plano de auditoria interna, após o envolvimento prévio dos comités de risco e de auditoria, sempre que estes comités tenham sido constituídos.

4 Papel do presidente do órgão de administração

35. O presidente do órgão de administração deve dirigir o órgão, 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.

36. O presidente deve incentivar e promover um debate aberto e crítico e assegurar que as opiniões divergentes possam ser expressas e discutidas no âmbito do processo de tomada de decisão.

37. 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 especial, 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 da instituição não pode exercer simultaneamente funções de administrador executivo (CEO) na mesma instituição, salvo justificação pela instituição e autorização pelas autoridades competentes.

38. O presidente deve preparar as agendas das reuniões e assegurar que as questões estratégicas sejam discutidas com prioridade em relação às demais. Assegura que as decisões do órgão de administração sejam devidamente fundamentadas e tomadas com conhecimento de causa e que os documentos e informações sejam recebidos com suficiente antecedência antes da reunião.

39. presidência presidente do órgão de administração deve contribuir para uma clara alocação 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 possam contribuir de forma construtiva para os debates e exerçam os seus votos de forma fundamentada e com conhecimento de causa.

5 Comités do órgão de administração na sua função de fiscalização

5.1 Criação de comités

40. 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[12] e de remuneração[13] para aconselhar o órgão de administração na sua função de fiscalização e preparar as decisões a adotar por este órgão. As instituições não significativas, incluindo as que se encontram no no perímetro de consolidação prudencial de uma instituição significativa numa situação subconsolidada ou consolidada, não estão obrigadas a constituir esses comités.

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

42. As instituições podem, tendo em conta os critérios estabelecidos no Título I das presentes orientações, criar outros comités (p. ex., comités de prevenção do branqueamento de capitais e do financiamento do terrorismo, de ética, de conduta e de conformidade).

43. As instituições devem assegurar uma clara alocação e distribuição das funções e tarefas entre os comités especializados do órgão de administração.

44. 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.

45. Os comités devem apoiar a função de fiscalização em áreas específicas e facilitar o desenvolvimento e a implementação de um quadro de governo interno sólido. A delegação nos comités não exime o órgão de administração na sua função de fiscalização, do cumprimento coletivo das suas obrigações e responsabilidades.

[12] Ver também as orientações conjuntas da ESMA e da EBA sobre a 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.

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

5.2 Composição dos comités[14]

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

47. Os membros independentes[15] do órgão de administração na sua função de fiscalização devem participar ativamente nos comités.

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

49. 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, que os comités não sejam compostos pelo mesmo grupo de membros que formam outro comité.

50. As instituições devem ponderar a rotação ocasional 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.

51. 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[16]. 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[17].

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

53. Os membros do comité de nomeação devem possuir, individual e coletivamente, conhecimentos, competências e experiência adequados, no que respeita aos processos de

[14] Esta secção deve ser lida em conjunto com as orientações conjuntas da ESMA e da EBA sobre a 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.

[15] 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.

[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 que revoga a Diretiva 84/253/CEE do Conselho (JO L 157 de 9.6.2006, p. 87), tal como alterada pela Diretiva 2014/56/UE do Parlamento Europeu e do Conselho, de 16 de Abril de 2014.

[17] Orientações da EBA relativas a políticas de remuneração sãs, nos termos do artigo 74.º, n.º 3, e do artigo 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).

seleção e requisitos de avaliação da adequação estabelecidos nos termos da Diretiva 2013/36/UE.

54. Nas G-SII (instituições de importância sistémica global) e nas O-SII (outras instituições de importância sistémica), o comité de risco deve incluir uma maioria de membros independentes. Nas G-SII e nas O-SII, o presidente do comité de risco deve ser um membro independente. Noutras instituições significativas, determinadas pelas autoridades competentes ou pelo direito nacional, o comité de risco deve ser composto por 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 pelo presidente do órgão de administração, nem pelo presidente de qualquer outro comité.

55. Os membros do comité de risco devem possuir, individual e coletivamente, conhecimentos, competências e experiência adequados no que respeita a práticas de controlo e de gestão de riscos.

5.3 Processos dos comités

56. Os comités devem informar regularmente o órgão de administração na sua função de fiscalização.

57. Os comités devem interagir entre si, sempre que necessário. Sem prejuízo do disposto no n.º 49, essa interação poderá assumir a forma de participações cruzadas, de forma a que o presidente ou um membro de um comité possa também ser membro de outro comité.

58. Os membros dos comités devem participar em debates abertos e críticos, nos quais as divergências de opiniões sejam debatidas de uma forma construtiva.

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

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

    a. Ter acesso a todas as informações relevantes e a todos os dados necessários para desempenhar as suas funções, incluindo informações e dados das funções de controlo e das funções da instituição relevantes [por ex., jurídica, financeira, recursos humanos, TI, auditoria interna, risco, conformidade, incluindo informações sobre a conformidade em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo e informação agregada sobre reportes de transações suspeitas, e fatores de risco de branqueamento de capitais e de financiamento do terrorismo (BC/FT)];

    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 materiais [18] que possam ter ocorrido, com informações pormenorizadas e recomendações sobre medidas corretivas adotadas, a adotar ou sugeridas para corrigir essas infrações; rever periodicamente e decidir sobre o conteúdo, formato e frequência da informação sobre riscos a reportar aos mesmos;

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

5.4 Papel do comité de risco

61. 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 estratégia de risco e da apetência de risco global, atual e futura da instituição, tendo em conta todos os tipos de riscos, a fim de assegurar que estejam alinhadas 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 implementação da estratégia de risco da instituição e dos correspondentes limites fixados;

c. Supervisionar a implementação das estratégias de gestão dos fundos próprios e da liquidez, bem como de todos os restantes riscos relevantes de uma instituição, tais como os riscos de mercado, de crédito, operacional (incluindo o risco jurídico e de TI) e reputacional, a fim de avaliar a sua adequação face à estratégia de risco e apetência de risco aprovadas;

d. Apresentar recomendações ao órgão de administração na sua função de fiscalização sobre os ajustamentos necessários da 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 de apoio;

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

[18] No que diz respeito a infrações graves no domínio do BC/FT. Ver também as orientações a emitir ao abrigo do artigo 117.º, n.º 6, da Diretiva 2013/36/UE, que especificam o modo de cooperação e de troca de informações entre as autoridades a que se refere o n.º 5, do presente artigo, em particular no que respeita aos grupos transfronteiriços e no contexto da identificação de infrações graves das regras de prevenção do branqueamento de capitais.

g. Supervisionar o alinhamento entre todos os produtos e serviços financeiros importantes oferecidos aos clientes, bem como o modelo de negócio e a estratégia de risco da instituição[19]. O comité de risco deve avaliar os riscos associados aos produtos e serviços financeiros oferecidos e ter em conta o alinhamentoentre os preços atribuídos a esses produtos e serviços e os proveitos obtidos com os mesmos; e

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

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

63. Se tiver sido constituído, o comité de risco 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

64. De acordo com a Diretiva 2006/43/CE[20], caso tenha sido constituído, o comité de auditoria deve, nomeadamente:

a. Monitorizar a eficácia dos sistemas de controlo da qualidade interno e de gestão de riscos da instituição e, se aplicável, a sua função de auditoria interna, no que respeita ao relato financeiro da instituição auditada, sem violar a sua independência;

b. Supervisionar a definição das políticas contabilísticas da instituição;

c. Monitorizar o processo de relato financeiro e apresentar recomendações destinadas a garantir a sua integridade;

d. Rever e monitorizar 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[21] e,

[19] 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.

[20] 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 que revoga a Diretiva 84/253/CEE do Conselho (JO L 157 de 9.6.2006, p. 87), conforme alterada pela Diretiva 2014/56/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014.

[21] Regulamento (UE) n.º 537/2014 do Parlamento Europeu e do Conselho, de 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).

em especial, a adequação da prestação de serviços distintos da auditoria à instituição auditada nos termos do artigo 5.º do referido regulamento;

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

f. Ser responsável 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 se for aplicado o n.º 8 do mesmo artigo], a sua nomeação, remuneração ou exoneração;

g. Rever o âmbito e a frequência da revisão legal das contas anuais ou 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 das 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

65. 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 com, caso esteja constituído, o comité de auditoria referido no artigo 39.º da Diretiva 2006/43/CE.

66. Sempre que sejam constituídos comités de risco e de nomeação em instituições não significativas, os comités podem ser combinados. Nesse caso, as instituições devem documentar os motivos pelos quais optaram por combinar os comités e o modo como a abordagem adotada realiza os objetivos dos comités.

67. As instituições devem garantir, de forma permanente, que os membros de um comité combinado possuem, individual e coletivamente, os conhecimentos, competências e experiência necessária para compreenderem totalmente as funções que serão exercidas pelo comité combinado[22].

[22] Ver também as orientações conjuntas da ESMA e da EBA sobre a 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.

Título III – Quadro de governo

6 Quadro e estrutura organizacional

6.1 Quadro organizacional

68. Compete ao órgão de administração de uma instituição assegurar que esta possui uma estrutura organizacional e operacional adequada e transparente e manter uma descrição por escrito dessa estrutura. A estrutura deve promover e demonstrar uma gestão efetiva e prudente da instituição, aos níveis individual, subconsolidado e consolidado. O órgão de administração assegura que as funções de controlo interno são independentes das áreas de negócio que controlam, em especial que exista uma segregação de funções adequada e que tais funções estejam dotadas dos recursos financeiros e humanos e dos poderes adequados para desempenharem eficazmente as suas funções. As linhas de reporte e a repartição de responsabilidades, nomeadamente entre os titulares de funções essenciais, devem ser claras, bem definidas, coerentes, vinculativas e devidamente documentadas. A documentação deve ser atualizada sempre que necessário.

69. 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 o grupo, ou a capacidade da autoridade competente para supervisionar eficazmente a instituição.

70. O órgão de administração deve avaliar se e de que modo alterações significativas 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 debilidades, o órgão de administração deve proceder rapidamente a quaisquer ajustamentos necessários.

6.2 «Conheça a sua estrutura»

71. O órgão de administração conhece e compreende inteiramente a estrutura jurídica, organizacional e operacional da instituição («conheça a sua estrutura») e assegura que a mesma esteja de acordo com a estratégia de negócio e de risco e com a apetência pelo risco aprovadas e que esteja coberta pelo seu quadro de gestão de riscos.

72. O órgão de administração é responsável pela aprovação de estratégias e políticas sólidas para a criação de novas estruturas. Sempre que uma instituição crie muitas entidades jurídicas no seio do seu grupo, o número de entidades e, principalmente, as interligações e operações entre as mesmas 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, caso aplicável, as estruturas pertencentes ao grupo, tendo em conta os critérios especificados na secção 7, sejam claras, eficientes e transparentes para o pessoal da instituição, bem como para os seus acionistas e outras partes interessadas, e para a autoridade competente.

73. O órgão de administração orienta a estrutura da instituição, a sua evolução e limitações, e deve assegurando que a estrutura seja justificada e eficiente e que não apresente uma complexidade excessiva ou inadequada.

74. 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 diferentes entidades e as ligações e relações existentes entre as mesmas. Tal deve incluir os riscos operacionais específicos do grupo, as exposições intragrupo, e o modo como os perfis de financiamento, fundos próprios, liquidez e risco do grupo podem ser afetados em circunstâncias normais e em circunstâncias adversas. O órgão de administração assegura que a instituição é capaz de produzir informações oportunas sobre o tipo, as características, o organograma, a estrutura de propriedade e atividades de cada entidade jurídica, e que as instituições pertencentes ao grupo cumprem com todos os requisitos de reporte de supervisão em base individual, subconsolidada ou consolidada.

75. 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. As referidas informações e análises são documentadas e disponibilizadas às funções relevantes envolvidas, nomeadamente o órgão de administração, áreas de negócio 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. Informação 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 relação aos quais é exigida a conformidade com o quadro regulamentar a nível individual, subconsolidado e consolidado.

6.3 Estruturas complexas e atividades não convencionais ou não transparentes

76. As instituições devem evitar a criação de estruturas complexas e potencialmente não transparentes. No seu processo de tomada de decisões, as instituições têm em conta os resultados da avaliação de riscos efetuada para identificar se essas estruturas possam ser utilizadas para fins ligados ao branqueamento de capitais, financiamento do terrorismo ou

outros crimes financeiros, e os respetivos controlos e quadro jurídico em vigor[23]. Para o efeito, as instituições devem ter em conta, no mínimo, em que medida:

a. Se a jurisdição onde a estrutura será criada cumpre efetivamente com as normas europeias e internacionais em matéria de transparência fiscal, de luta contra o branqueamento de capitais e de combate ao financiamento do terrorismo[24];

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 é questionável;

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 pelas autoridades competentes.

77. Em qualquer dos casos, as instituições não devem criar estruturas opacas ou desnecessariamente complexas sem uma finalidade jurídica ou um interesse económico claros que possam suscitar preocupações quanto à possibilidade de terem sido criadas para fins associados ao crime financeiro.

78. Ao constituir tais estruturas, o órgão de administração deve compreender as estruturas e a sua finalidade, bem como os riscos específicos que lhe estão associados, e garantir o envolvimento adequado 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.

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

80. O órgão de administração assegura a adoção de medidas adequadas para evitar ou mitigar os riscos das atividades realizadas nessas estruturas. Tal inclui assegurar que:

[23] Para mais informações sobre a avaliação do risco do país e do risco associado a produtos e clientes individuais, as instituições devem igualmente consultar as Orientações conjuntas relativas aos fatores de risco BC/FT (Orientações da EBA JC/2017/37) que atualmente desse encontram em revisão.

[24] Ver também: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

a. A instituição dispõe de políticas e procedimentos adequados, bem como processos documentados (por exemplo, limites aplicáveis, fluxos de informação), com vista à análise, verificação da conformidade, 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 relativa a essas atividades e aos respetivos riscos esteja facilmente acessível para a instituição consolidante e para os seus auditores internos e externos e seja comunicada ao órgão de administração na sua função de fiscalização e à autoridade competente que concedeu a autorização; e

c. A instituição avalie periodicamente a necessidade de manutenção dessas estruturas.

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

82. As instituições adotam as mesmas medidas de gestão de riscos que adotem para as suas próprias atividades de negócio quando desempenhem atividades não convencionais ou não transparentes por conta de clientes (p. ex., auxiliando-os a constituir veículos de investimento em jurisdições *offshore*, desenvolvendo estruturas complexas, financiando-lhes operações ou prestando serviços fiduciários) que possam colocar desafios semelhantes em matéria de governo interno e gerar riscos operacional e reputacional significativos. Em particular, as instituições devem analisar o motivo pelo qual um cliente pretende constituir uma estrutura específica.

7 Quadro organizacional num contexto de grupo

83. 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 as disposições, processos e mecanismos de governo sejam coerentes e bem integrados em base consolidada e subconsolidada. Para o efeito, as empresas-mãe e as filiais incluídas no perímetro de consolidação prudencial devem implementar essas disposições, processos e mecanismos nas suas filiais não abrangidas pela Diretiva 2013/36/UE, incluindo as que estão estabelecidas em países terceiros e em estabelecimentos *offshore*, a fim de assegurar sistemas de governo robustos em base consolidada e subconsolidada. No que diz respeito aos requisitos de remuneração, aplicam-se algumas exceções de acordo com o artigo 109.º, n.os 4 e 5[25]. As funções competentes da instituição consolidante e das suas filiais devem interagir e trocar dados e informações, consoante necessário. As disposições, processos e mecanismos de governo asseguram que a instituição consolidante possua dados e informações suficientes e que seja capaz de avaliar o perfil de risco global do grupo, conforme indicado na secção 6.2.

[25] Ver também as Orientações da EBA relativas a políticas de remuneração sãs

84. O órgão de administração de uma filial abrangida pela Diretiva 2013/36/UE adota e implementa, a nível individual, as políticas de governo ao nível do grupo estabelecidas a nível consolidado ou subconsolidado de forma a que cumpra com todos os requisitos específicos nos termos do direito nacional e do direito da UE.

85. Aos níveis consolidado e subconsolidado, a instituição consolidante assegura a aplicação das políticas de governo ao nível do grupo e do quadro de controlo interno referido no Título V por todas as instituições e outras entidades no perímetro de consolidação prudencial, incluindo as respetivas filiais não abrangidas pela Diretiva 2013/36/UE. Ao implementar políticas de governo, a instituição consolidante deve assegurar que sejam estabelecidas disposições de governo robustas para cada filial e considerar a aplicação de disposições, processos e mecanismos específicos sempre que as atividades de negócio não estejam organizadas em entidades jurídicas distintas, mas numa matriz de áreas de negócio que englobe várias entidades jurídicas.

86. A instituição consolidante deve ter em conta os interesses de todas as suas filiais e a forma como as estratégias e políticas contribuem, a longo prazo, para o interesse de cada filial e para o interesse do grupo como um todo.

87. As empresas-mãe e as respetivas filiais asseguram que as instituições e as entidades pertencentes ao grupo cumpram todos os requisitos regulamentares específicos em todas as jurisdições relevantes.

88. A instituição consolidante assegura que as filiais estabelecidas em países terceiros e que estejam incluídas no perímetro de consolidação prudencial disponham de sistemas, processos e mecanismos de governo coerentes com as políticas de governo ao nível do grupo e que cumpram com 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.

89. Os requisitos em matéria de governo da Diretiva 2013/36/UE e disposições constantes das 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 num país terceiro for uma instituição consolidante, o perímetro de 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 ao nível do grupo da instituição-mãe num país terceiro seja 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 com as especificações adicionais das presentes orientações.

90. Ao definirem políticas e documentarem governação os sistemas de governo, as instituições têm em conta os aspetos enumerados no Anexo I das presentes 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[26]

91. O órgão de administração aprova, revê regularmente e atualiza a política de subcontratação da instituição, assegurando a implementação em tempo oportuno de eventuais alterações.

92. A política de subcontratação toma em consideração o impacto da subcontratação nas atividades da instituição e nos riscos que ela enfrenta (nomeadamente, o risco operacional, incluindo o risco jurídico e de TI, o risco reputacional e o risco de concentração). A política deve incluir os mecanismos de reporte e de monitorização que devem ser implementados desde o início até ao ao termo de um acordo de subcontratação (incluindo a elaboração do estudo de viabilidade, a celebração do contrato, a execução do contrato 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. Por conseguinte, a política de subcontratação deve referir expressamente que a subcontratação não exonera a instituição das suas obrigações regulamentares nem das suas responsabilidades para com os seus clientes.

93. A política deve estipular que os acordos de subcontratação não devem obstar a uma supervisão efetiva da instituição, no local ou remota, e que não devem infringir quaisquer restrições regulamentares aplicáveis aos serviços e atividades. A política deve também abranger a subcontratação intragrupo (ou seja, serviços prestados por uma entidade jurídica distinta pertencente ao grupo da instituição) e ter em conta quaisquer circunstâncias específicas do grupo.

Título IV – Cultura de risco e conduta empresarial

9 Cultura de risco

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

95. As instituições devem desenvolver, em toda a sua estrutura, uma cultura de risco integrada e global, baseada na plena compreensão e numa visão holística dos riscos que enfrentam e do modo como estes são geridos, tendo em conta a sua apetência pelo risco.

96. As instituições devem desenvolver uma cultura de risco através de políticas, comunicação e formação ao pessoal relativamente às suas atividades, estratégia e perfil de risco, e devem adaptar a comunicação e a formação do pessoal, de forma a ter em conta as responsabilidades destes em matéria de assunção e gestão de riscos.

[26] Ver também: Orientações da EBA relativas à subcontratação, disponíveis em https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

97. Os membros do pessoal devem estar plenamente cientes das suas responsabilidades na gestão de riscos, a qual não deve estar reservada a especialistas do risco, nem às funções de controlo interno. As unidades de negócio sob a supervisão do órgão de administração são as principais responsáveis pela gestão quotidiana de 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 deve incluir pelo menos os seguintes aspetos:

    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. A administração da instituição, incluindo os titulares de funções essenciais, deve contribuir para a comunicação interna dos valores fundamentais e expetativas ao pessoal. Os membros do pessoal deve agir em conformidade com a 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 participação de infrações). O órgão de administração promove, monitoriza 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 alterações quando 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 testar as 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 do comportamento de assunção de riscos com o perfil de risco da instituição e com os seus interesses de longo prazo[27].

10 Valores corporativos e código de conduta da instituição

99. O órgão de administração desenvolve, adota, cumpre e promove normas éticas e profissionais rigorosas, tendo em conta as características e necessidades específicas da instituição, e

[27] Ver 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.

assegura a sua aplicação (através de um código de conduta ou instrumento similar). Também fiscaliza o cumprimento dessas normas pelos membros do pessoal. Quando aplicável, o órgão de administração pode adotar e implementar as normas da instituição ao nível do grupo, bem como normas comuns emitidas por associações ou outras organizações relevantes.

100. As instituições asseguram que não haja discriminação do pessoal em razão do género, raça, cor, origem étnica ou social, características genéticas, língua, religião ou crença, opiniões políticas ou quaisquer outras opiniões, pertença a uma minoria nacional, riqueza, nascimento, deficiência, idade ou orientação sexual.

101. As políticas da instituição devem ser neutras do ponto de vista do género. Tal inclui, mas não se limita à remuneração, políticas de recrutamento, planos de desenvolvimento de carreira e de sucessão, acesso a formação e a possibilidade de candidaturas a vagas internas. As instituições devem assegurar a igualdade de oportunidades[28] para todos os membros do pessoal, independentemente do seu género, nomeadamente no que diz respeito às perspetivas de carreira, e procuram melhorar a representação do género sub-representado em cargos no órgão de administração, bem como no grupo de membros do pessoal com responsabilidades de gestão, tal como definido no Regulamento Delegado da Comissão [normas técnicas de regulamentação (NTR) relativas ao pessoal identificado][29]. As instituições monitorizam separadamente a evolução da disparidade salarial de género em relação ao pessoal identificado (com exclusão dos membros do órgão de administração), membros do órgão de administração na sua função de gestão, membros do órgão de administração na função de fiscalização e outro pessoal. As instituições devem ter políticas que facilitem a reintegração do pessoal depois do gozo de licença de maternidade, paternidade ou de licença parental.

102. As normas aplicadas devem ter como objetivo reforçar a robustez dos sistemas de governo e reduzir os riscos a que a instituição está exposta, nomeadamente riscos operacional e reputacional, 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.

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

a. Recordar os membros do pessoal que todas as atividades da instituição devem ser exercidas em conformidade com o direito aplicável e com os valores corporativos da instituição;

[28] Ver também a Diretiva 2006/54/CE do Parlamento Europeu e do Conselho, de 5 de Julho de 2006, relativa à implementação do princípio da igualdade de oportunidades e igualdade de tratamento entre homens e mulheres em domínios ligados ao emprego e à atividade profissional

[29] Ver também Orientações da EBA relativas às políticas de remuneração neutras do ponto de vista do género]

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

c. Estabelecer princípios, com a apresentação de exemplos, sobre os comportamentos aceitáveis e não aceitáveis associados, em especial, ao reporte de informações financeiras incorretas e à prática de irregularidades financeiras, à criminalidade económica e financeira, incluindo, designadamente fraude, branqueamento de capitais e financiamento do terrorismo, práticas anticoncorrenciais, sanções financeiras, suborno e corrupção, manipulação do mercado, vendas enganosas e outras infrações da legislação de proteção dos consumidores, infrações fiscais, cometidas direta ou indiretamente, nomeadamente mediante mecanismos de arbitragem de dividendos ilegais ou proibidos;

d. clarificar que, além da conformidade com os requisitos legais e regulamentares e com as 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.

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

11 Política de conflitos de interesses a nível institucional

105. O órgão de administração é responsável pela definição, aprovação e supervisão da implementação e manutenção de políticas eficazes para identificar, avaliar, gerir e mitigar ou prevenir conflitos de interesses reais e potenciais ao nível institucional, resultantes, p. ex., das diversas atividades e funções da instituição, de diferentes instituições no perímetro de consolidação prudencial ou de diferentes unidades ou áreas de negócio no seio de uma instituição, ou no que respeita às partes interessadas externas.

106. 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.

107. As medidas adotadas pelas instituições para gerirem ou, quando apropriado, mitigarem conflitos de interesses, devem ser documentadas e incluir, nomeadamente:

a. Uma adequada segregação de funções, por exemplo, atribuindo a diferentes pessoas as atividades que suscitam conflitos de interesses no processamento de operações ou na prestação de serviços, ou atribuindo as responsabilidades de supervisão e de reporte de atividades conflituantes a diferentes pessoas;

b. O estabelecimento de obstáculos à informação, por exemplo, através da segregação física de determinadas unidades ou áreas de negócio da instituição.

12 Política de conflitos de interesses dos membros do pessoal[30]

108. O órgão de administração estabelece, aprova e supervisiona a implementação e manutenção de políticas eficazes para identificar, avaliar, gerir e mitigar ou prevenir os conflitos de interesses atuais 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 das 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.

109. A política deve visar a identificação de conflitos de interesses dos membros do pessoal, incluindo os interesses dos seus familiares mais próximos. As instituições devem ter em consideração que os conflitos de interesses podem resultar de relações pessoais ou profissionais tanto presentes como passadas. Sempre que surjam conflitos de interesses, as instituições devem avaliar a sua materialidade e decidir implementar, se apropriado, medidas de mitigação.

110. No que respeita aos conflitos de interesses que possam resultar de relações passadas, 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 ainda possam impactar o comportamento e a participação dos membros do pessoal nos processos de tomada de decisões.

111. 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, empréstimos concedidos pela instituição a uma empresa detida por membros do pessoal, participação ou propriedade de um organismo ou entidade com interesses conflitantes);

[30] Esta secção deve ser lida em conjunto com as orientações conjuntas da ESMA e da EBA sobre a 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.

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

c. Relações pessoais ou profissionais com membros do pessoal da instituição ou entidades incluídas no perímetro de 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.

112. 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 numa instituição, ou utilizar outros serviços dessa instituição, caso se mantenham num limiar mínimo adequado, não deve significar que os membros do pessoal sejam considerados como estando em situação de conflito de interesses.

113. A política deve estabelecer os procedimentos para informação e comunicação à função 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.

114. A política deve distinguir entre conflitos de interesses que persistem e que devem ser geridos de forma permanente e conflitos de interesses que ocorrem inesperadamente em relação a um único evento (p. ex., uma operação, a seleção de um prestador de serviços, etc.) e que podem normalmente ser geridos com uma medida pontual. Em qualquer circunstância, as decisões tomadas devem privilegiar o interesse da instituição.

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

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

b. Medidas que impeçam que membros do pessoal que também exercem atividades no exterior, exerçam uma influência indevida na instituição relativamente a essas outras atividades;

c. O estabelecimento da responsabilidade dos 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. Medidas que impeçam que os membros do órgão de administração exerçam cargos de direção em instituições concorrentes, a menos que se trate 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 perímetro de consolidação prudencial.

116. 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 prejudicar a independência de espírito dos membros do órgão de administração[31].

117. Para efeitos da mitigação dos conflitos de interesses identificados dos membros do órgão de administração, as instituições devem documentar as medidas tomadas, incluindo a fundamentação da sua eficácia para assegurar a objetividade na tomada de decisões.

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

119. Todos os conflitos de interesses atuais 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.

12.1 Política de conflitos de interesses no contexto de empréstimos e outras operações com membros do órgão de administração e respetivas partes relacionadas

120. Como parte das suas políticas de conflitos de interesses para os membros do pessoal (Secção 12) e da gestão de conflitos de interesses dos membros do órgão de administração,

[31] Ver também as orientações conjuntas da ESMA e da EBA sobre a 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.

tal como estabelecido no n.º 117, o órgão de administração estabelece um quadro para a identificação e gestão de conflitos de interesses no contexto da concessão de empréstimos e da realização de outras operações (por exemplo, *factoring*, locação financeira, operações imobiliárias, etc.) com membros do órgão de administração e respetivas partes relacionadas.

121. Sem prejuízo da transposição nacional da Diretiva 2013/36/UE[32], as instituições podem ter em conta outras categorias de partes relacionadas às quais aplicam, no todo ou em parte, o respetivo quadro em matéria de conflitos de interesses no que diz respeito a empréstimos e outras operações.

122. O quadro em matéria de conflitos de interesse assegura que as decisões respeitantes à concessão de empréstimos e à realização de outras operações com membros do órgão de administração e respetivas partes relacionadas sejam tomadas com objetividade, sem influência indevida por conflitos de interesses, e que são, regra geral, efetuadas em condições de mercado.

123. O órgão de administração estabelece os processos de decisão aplicáveis à concessão de empréstimos e à realização de outras operações com membros do órgão de administração e respetivas partes relacionadas. Este quadro pode prever uma diferenciação entre as operações comerciais normais[33] realizadas no decurso normal da atividade e em condições normais de mercado e os empréstimos e operações com membros do pessoal, realizados em condições acessíveis a todos os membros do pessoal. Além disso, o quadro e o processo de tomada de decisão em matéria de conflitos de interesses pode diferenciar entre empréstimos e outras operações materiais e não materiais, diferentes tipos de empréstimos e outras operações e o nível de conflitos de interesses atuais ou potenciais que podem gerar.

124. Como parte do quadro em matéria de conflitos de interesses, o órgão de administração fixa limiares adequados (por ex., por tipo de produto, ou dependendo das condições) acima dos quais o empréstimo ou outra operação com um membro do órgão de administração ou respetivas partes relacionadas exiga sempre a aprovação do órgão de administração. As decisões sobre empréstimos materiais ou outras operações materiais com membros do órgão de administração que não são realizadas em condições normais de mercado, mas em condições acessíveis a todos os membros do pessoal, são sempre tomadas pelo órgão de administração.

125. O membro do órgão de administração que beneficie de um empréstimo material ou outra operação material ou o membro que está relacionado com a contraparte não devem participar no processo de tomada de decisão.

[32] Ver também o Princípio Fundamental 20 de Basileia

[33] As operações comerciais incluem empréstimos e outras operações (por ex., locação financeira, *factoring*, serviços no contexto de ofertas públicas iniciais), fusões e aquisições, compra e venda de imóveis).

126. Ao decidir sobre um empréstimo ou outra operação com um membro do órgão de administração ou respetivas partes relacionadas, antes de tomarem uma decisão, as instituições avaliam o risco ao qual a instituição pode ser exposta devido à operação.

127. Sempre que os empréstimos sejam concedidos sob a forma de linha de crédito (por ex., facilidade de descobertos), a decisão inicial e as respetivas alterações devem ser documentadas. Qualquer utilização dessas linhas de crédito acordadas nos limites acordados não deve ser considerada como uma nova decisão sobre um empréstimo a um membro do órgão de administração ou à respetiva parte relacionada. Se a alteração de uma linha de crédito for material, de acordo com a política da instituição, deve ser efetuada uma nova avaliação e tomada uma nova decisão.

128. Para garantir o cumprimento das suas políticas de conflitos de interesses, as instituições asseguram que todos os procedimentos de controlo interno relevantes se aplicam integralmente aos empréstimos e outras operações com membros do órgão de administração ou respetivas partes relacionadas e que esteja implementada um quadro de supervisão adequado ao nível do órgão de administração na sua função de fiscalização.

12.2 Documentação dos empréstimos a membros do órgão de administração e respetivas partes relacionadas e informação adicional

129. Para efeitos do artigo 88.º, n.º 1, da Diretiva 2013/36/UE, as instituições devem documentam adequadamente os dados sobre empréstimos[34] aos membros do órgão de administração e respetivas partes relacionadas, incluindo, no mínimo:

a. O nome do devedor e o seu estatuto (ou seja, membro do órgão de administração ou parte relacionada) e relativamente aos empréstimos a uma parte relacionada, o membro do órgão de administração com quem a parte está relacionada e a natureza da relação com a parte relacionada;

b. O tipo/natureza do empréstimo e o montante;

c. Os termos e condições aplicáveis ao empréstimo;

d. A data de aprovação do empréstimo;

e. O nome do indivíduo ou do órgão e a sua composição que tomaram a decisão de aprovar o empréstimo e as condições aplicáveis;

f. O facto (sim/não) de o empréstimo ter sido ou não concedido em condições de mercado; e

[34] Ver também as Orientações da EBA sobre a concessão e a monitorização de empréstimos, disponíveis em: https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

g. O facto (sim/não) de o empréstimo ter sido ou não concedido em condições acessíveis a todos os membros do pessoal.

130. As instituições asseguram que a documentação de todos os empréstimos a membros do órgão de administração e respetivas partes relacionadas é completa e atualizada e que a instituição seja capaz de disponibilizar às autoridades competentes a documentação completa num formato adequado, mediante solicitação, sem demora injustificada.

131. Em relação a um empréstimo a um membro do órgão de administração ou respetiva parte relacionada num montante superior a EUR 200 000, as instituições devem ser capazes de fornecer à autoridade competente, mediante solicitação, a seguinte informação adicional:

a. A percentagem do empréstimo e a percentagem da soma de todos os montantes em dívida de empréstimos ao mesmo devedor em comparação com:

i. a soma dos seus fundos próprios de nível 1 e de nível 2 e

ii. fundos próprios principais de nível 1 da instituição;

b. Se o empréstimo faz parte de um «grande risco»[35]; e

c. O peso relativo da soma agregada de todos os montantes em dívida de empréstimos ao mesmo devedor, calculado como uma percentagem dividindo o montante total em dívida pelo montante total de todos os empréstimos em dívida a membros do órgão de administração e respetivas partes relacionadas.

13 Procedimentos internos de alerta

132. As instituições estabelecem e mantêm políticas de alerta adequadas a nível interno e procedimentos departicipação pelos membros do pessoal, através de um canal específico, independente e autónomo, de infrações atuais ou potenciais dos requisitos regulamentares ou internos, nomeadamente dos requisitos previstos no Regulamento (UE) n.º 575/2013 e das disposições nacionais de transposição da Diretiva 2013/36/UE, ou de disposições internas de governo. Não deve ser necessário que os membros do pessoal estejam na posse de evidências de uma infração para efetuarem uma participação; no entanto, devem possuir um grau de certeza suficiente que forneça motivo suficiente para iniciar uma investigação. As instituições implementam igualmente processos e procedimentos adequados que assegurem que dão cumprimento às obrigações que lhes incumbem por força da transposição nacional da Diretiva (UE) 2019/1937 do Parlamento e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que comunicam infrações do direito da União.

133. A fim de evitar conflitos de interesses, deverá ser possível aos membros do pessoal participarem infrações fora dos canais normais de transmissão de informações (p. ex., através da função de conformidade, da função de auditoria interna ou de um procedimento independente de participação de infrações a nível interno). Os procedimentos de alerta

[35] Ver também a Parte IV do Regulamento (UE) n.º 575/2013 e, em especial, o artigo 392.º.

devem assegurar a proteção dos dados pessoais da pessoa que participa a infração e da pessoa singular que é alegadamente responsável pela infração, em conformidade com o Regulamento (UE) 2016/679 (RGPD)[36].

134. Todos os membros do pessoal da instituição devem ser informados dos procedimentos de alerta.

135. As informações fornecidas pelos membros do pessoal por meio de procedimentos de alerta devem ser transmitidas, se apropriado, ao órgão de administração e a outras funções responsáveis designadas no âmbito da política de alertas internos. Quando solicitado pelo membro do pessoal que comunica uma infração, as informações devem ser transmitidas de forma anónima ao órgão de administração e a outras funções responsáveis. As instituições também podem disponibilizar um procedimento de participação de infrações que permita que as informações sejam transmitidas de forma anónima.

136. As instituições devem assegurar que a pessoa que participa 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 participado uma infração e deve tomar medidas adequadas contra os responsáveis por tais ações.

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

138. Em especial, os procedimentos internos de alerta devem:

a. Ser documentados (p. ex., manuais do pessoal);

b. Fornecer regras claras que assegurem que as informações sobre a participação, as pessoas denunciadas e a infração sejam tratadas de forma confidencial, em conformidade com o Regulamento (UE) 2016/679, exceto se a sua divulgação for exigida nos termos do direito nacional, no contexto de investigações adicionais ou de um processo judicial subsequente;

c. Proteger os membros do pessoal que efetuaram participações de serem vitimizados por terem divulgado infrações ;

[36] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

d. Assegurar que as infrações potenciais ou atuais participadas 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 participou infrações potenciais ou atuais a confirmação da receção das informações;

f. Assegurar o seguimento do resultado de uma investigação relativa à participação de uma infração; e

g. Assegurar a manutenção de registos adequados.

14 Comunicação de infrações às autoridades competentes

139. As autoridades competentes estabelecem mecanismos efetivos e fiáveis que permitam aos membros pessoal das instituições participarem às autoridades competentes infrações atuais ou potenciais graves dos requisitos regulamentares, nomeadamente dos 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 de receção de participações de infrações, e do seu seguimento, por exemplo, um departamento, unidade ou função dedicados;

b. Proteção adequada, conforme referido na Secção 13;

c. Proteção dos dados pessoais da pessoa singular que participou a infração e da pessoa singular que é alegadamente responsável pela infração, em conformidade com o Regulamento (UE) 2016/679 (RGPD); e

d. Procedimentos claros, conforme indicado na Secção 13.

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

Título V – Quadro e mecanismos de controlo interno

15 Quadro de controlo interno

141. As instituições desenvolvem e mantêm uma cultura que incentive uma atitude positiva perante o controlo do risco e a conformidade na instituição, bem como um quadro de controlo interno robusto e abrangente. No âmbito deste quadro, as áreas de negócio 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 devem possuir funções de controlo interno com autoridade adequada e suficiente, estatuto e acesso ao órgão de administração para cumprirem a sua missão e um quadro de gestão de riscos.

142. O quadro de controlo interno das instituições deve ser adaptado, em base individual, à especificidade da sua atividade, da sua complexidade e dos riscos associados, tendo em conta o contexto do grupo. As instituições organizam o intercâmbio das necessárias informações de modo a garantir que cada órgão de administração, área de negócio e unidade interna, incluindo cada função de controlo interno, seja capaz de desempenhar as suas funções. Tal significa, por exemplo, estabelecer o necessário intercâmbio de informações adequadas entre as áreas de negócio, a função de conformidade e a função de controlo do cumprimento em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo, quando esta função de controlo se encontre segregada, ao nível do grupo e entre os responsáveis das funções de controlo interno ao nível do grupo e o órgão de administração da instituição.

143. As instituições implementam processos e procedimentos adequados que assegurem o cumprimento das obrigações que lhes incumbem no contexto do combate ao branqueamento de capitais e ao financiamento do terrorismo. As instituições avaliam a sua exposição ao risco de serem utilizadas para efeitos de BC/FT e, caso necessário, tomam medidas de mitigação para reduzir esses riscos, assim como os seus riscos operacional e reputacional associados. As instituições tomam medidas para assegurar que os seus membros do pessoal estão cientes dos riscos de BC/FT e do impacto que o BC/FT tem na instituição e na integridade do sistema financeiro.

144. O quadro de controlo interno abrange toda a organização, incluindo as responsabilidades e as tarefas do órgão de administração, e as atividades de todas as áreas de negócio e unidades internas, incluindo as funções de controlo interno, as atividades subcontratadas e os canais de distribuição.

145. 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, medição 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

146. O órgão de administração é responsável pelo estabelecimento e monitorização da adequação e eficácia dos processos, mecanismos e quadro de controlo interno, bem como pela supervisão de todas as áreas de negócio e unidades internas, incluindo as funções de controlo interno (tais como as funções de gestão de riscos, conformidade, controlo do cumprimento em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo, sempre que esta função esteja segregada da função de conformidade, e de auditoria interna). As instituições estabelecem, mantêm e atualizam regularmente, procedimentos, mecanismos e políticas de controlo interno, por escrito, que são aprovados pelo órgão de administração.

147. As instituições asseguram a existência de um processo de tomada de decisão claro, transparente e documentado e de uma clara alocação de responsabilidades e de autoridade no âmbito do seu quadro de controlo interno, incluindo as suas áreas de negócio, unidades internas e funções de controlo interno.

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

149. Quando implementam o quadro de controlo interno, as instituições estabelecem uma adequada segregação de funções (p. ex., atribuir a pessoas diferentes as atividades que suscitam conflitos de interesses na cadeia de processamento 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 segregação física de alguns departamentos).

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

151. 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 tomadas. O órgão de administração dá seguimento às deficiências identificadas pelas funções de controlo interno de forma eficaz e atempada e exige a adoção de medidas corretivas adequadas. Deve ser adotado um procedimento formal de seguimento das deficiências identificadas e das medidas corretivas adotadas.

17 Quadro de gestão dos riscos

152. No âmbito do quadro global de controlo interno, as instituições possuem um quadro de gestão de riscos holístico, que abrange todas as suas áreas de negócio e unidades internas, incluindo as funções de controlo interno, reconhecendo plenamente a realidade económica de todos os riscos a que estão expostas. O quadro de gestão dos riscos deve permitir à instituição a tomada de decisões com pleno conhecimento de causa sobre a assunção de riscos. O quadro de gestão de riscos deve abranger os riscos patrimoniais e extrapatrimoniais, bem como todos os riscos atuais e futuros a que a instituição pode vir a estar exposta. Os riscos são avaliados no sentido ascendente e descendente, dentro e entre as vários áreas de negócio, utilizando uma terminologia coerente e metodologias compatíveis em toda a instituição e ao nível consolidado ou subconsolidado. O quadro de gestão dos riscos inclui todos os riscos materiais, tendo em devida consideração os riscos financeiros e não financeiros, incluindo os riscos de crédito, de mercado, de liquidez, de concentração, operacional, TI, reputacional, jurídico, de conduta, de cumprimento em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo e outros crimes financeiros, ASG e risco de estratégia.

153. O quadro de gestão dos riscos da instituição inclui políticas, procedimentos, limites de risco e controlos de risco que permitam, de uma forma adequada, atempada e contínua, identificar, medir ou avaliar, monitorizar, gerir, mitigar e comunicar os riscos aos níveis das áreas de negócio, da instituição e ao nivel consolidado e sub-consolidado.

154. O quadro de gestão dos riscos da instituição deve fornecer orientações específicas sobre a implementação das suas estratégias. Essas orientações estabelecem e mantêm, quando apropriado, limites internos consentâneos com a apetência pelo risco da instituição e compatíveis com o bom funcionamento, a solidez financeira, a base de fundos próprios e os objetivos estratégicos da instituição. O perfil de risco da instituição é mantido dentro desses limites estabelecidos. O quadro de gestão dos riscos assegura que existe um processo definido para que as infrações dos limites de risco sejam transmitidas ao nível hierárquico superior e tratadas através de um procedimento de acompanhamento adequado.

155. O quadro de gestão dos 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 riscos 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 nos proveitos, qualquer aumento na complexidade da atividade, no perfil de risco ou na estrutura operacional da instituição, expansão geográfica, fusões e aquisições e a introdução de novos produtos ou áreas de negócio.

156. Para efeitos da identificação e da medição ou avaliação dos riscos, as instituições devem desenvolver metodologias adequadas, incluindo instrumentos prospetivos e retrospetivos. As metodologias permitem agregar as exposições ao risco das diversas áreas de negócio e

ajudam a identificar concentrações de riscos. Os instrumentos incluem a avaliação do perfil de risco atual em relação à apetência pelo risco da instituição, bem como a identificação e avaliação de exposições de risco potenciais e excessivas em relação à capacidade de risco da instituição com base num conjunto de circunstâncias adversas presumidas. 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.

157. 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 docapital económico 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 assumido não deve basear-se apenas em informações quantitativas ou em resultados de modelos, mas incluir também uma abordagem qualitativa (incluindo pareceres especializados e análises críticas). As tendências e os dados relevantes da conjuntura macroeconómica são explicitamente considerados para identificar o seu potencial impacto nas exposições e carteiras.

158. A responsabilidade final pela avaliação dos riscos cabe exclusivamente à instituição, a qual avalia, assim, os seus riscos de forma crítica e não depende exclusivamente 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.

159. As instituições devem ter pleno conhecimento das limitações dos modelos e das métricas e utilizar não apenas instrumentos de avaliação quantitativa mas também instrumentos de avaliação qualitativa dos riscos (incluindo pareceres especializados e análises críticas).

160. 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 preciso dessas avaliações, bem como das suas limitações.

161. São estabelecidos 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, monitorização e gestão dos riscos. O quadro de reporte é claramente definido e documentado.

162. A comunicação e sensibilização eficazes 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 o risco. A comunicação eficaz dos riscos envolve uma adequada consideração e uma comunicação a nível interno da estratégia de risco e dos dados de risco relevantes (p. ex., exposições e principais indicadores de risco), tanto horizontalmente, por toda a instituição, como verticalmente, no sentido ascendente e descendente, ao longo da cadeia de gestão.

18 Novos produtos e alterações significativas[37]

163. 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 acordos de subcontratação) e sistemas (p. ex., processos de alteração dos sistemas de TI). A PANP assegura que os produtos e alterações aprovados sejam coerentes com a estratégia e a apetência pelo risco da instituição e com os limites correspondentes da instituição, ou que sejam efetuadas as necessárias revisões.

164. As alterações significativas ou as operações excecionais podem incluir fusões e aquisições [nomeadamente as possíveis consequências da realização de um exame prévio (*due diligence*) insuficiente para identificar os riscos e as responsabilidades decorrentes das operações de fusão], 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.

165. 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 conformidade, no que respeita a novos produtos ou alterações significativas aos produtos existentes.

166. 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 serem utilizadas na organização e as funções internas a serem envolvidas no processo de tomada de decisão.

[37] Ver também as Orientações da EBA relativas aos procedimentos de governo e monitorização 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.

167. A PANP inclui as principais questões que devem ser endereçadas 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. Além disso, para cumprir as obrigações por força da Diretiva (UE) 2015/849, as instituições identificam e avaliam o risco de BC/FT associado ao novo produto ou prática comercial, e definem as medidas a serem tomadas para mitigar esses riscos. A decisão de lançar uma nova atividade deve indicar claramente a unidade da instituição e os indivíduos responsáveis pela mesma. Não se iniciarão novas atividades enquanto não estiverem disponíveis recursos suficientes para compreender e gerir os riscos associados.

168. As funções de gestão de riscos e conformidade devem ser envolvidas na aprovação de novos produtos ou nas alterações significativas de produtos, processos e sistemas existentes. A sua contribuição deve incluir 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) nas diversas áreas de atividade e carteiras, e poderes para exigir que alterações aos produtos existentes sejam submetidas ao processo formal previsto na PANP.

19 Funções de controlo interno

169. As funções de controlo interno devem incluir uma função de gestão de riscos (ver a Secção 20), uma função de conformidade (ver a Secção 21) e uma função de auditoria interna (ver a Secção 22). As funções de gestão de riscos e de conformidade são sujeitas a revisão pela função de auditoria interna. As responsabilidades das funções de controlo incluem também assegurar o cumprimento dos requisitos em matéria de BC/FT.

170. 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 operacionais de controlo interno 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.

171. Sem prejuízo da legislação nacional que transpôs a Diretiva 2015/849/UE, as instituições atribuem a um membro do pessoal a responsabilidade por assegurar o cumprimento pela

instituição dos requisitos da referida diretiva e das suas políticas e procedimentos (por ex., responsável pela conformidade). As instituições podem estabelecer uma função de controlo do cumprimento em matéria de BC/CFT segregada, como uma função de controlo independente.[38] A pessoa responsável pelo BC/FT deve, caso necessário, poder reportar diretamente ao órgão de administração nas suas funções de gestão e de supervisão.

19.1 Responsáveis pelas funções de controlo interno

172. As funções de controlo interno são estabelecidas a um nível hierárquico adequado que lhes confira as seus responsáveis 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 das áreas de negócio ou unidades que controlam. Para este efeito, os responsáveis pelas funções de gestão de riscos, conformidade e auditoria interna reportam e respondem diretamente perante o órgão de administração, que também avalia o seu desempenho.

173. Caso necessário, os responsáveis das funções de controlo interno devem poder ter acesso e reportar diretamente ao órgão de administração na sua função de fiscalização para manifestarem preocupações e alertar este órgão, se for caso disso, no caso de uma evolução específica que afete ou possa afetar a instituição. Tal não deve impedir que os responsáveis pelas funções de controlo interno também utilizem as linhas de reporte regulares.

174. As instituições têm estabelecidos processos documentados de nomeação e destituição do responsável por uma função de controlo interno. Em qualquer caso, os responsáveis pelas funções de controlo interno (e, nos termos do artigo 76.º, n.º 5, da Diretiva 2013/36/UE, o responsável pela função de gestão de riscos) não podem ser destituídos sem a aprovação prévia do órgão de administração na sua função de fiscalização. Nas instituições significativas, as autoridades competentes são informadas de imediato da aprovação e das razões da substituição do responsável por uma função de controlo interno.

19.2 Independência das funções de controlo interno

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

a. Os seus membros do pessoal não desempenham quaisquer tarefas operacionais abrangidas pelas atividades que as funções de controlo interno devem monitorizar e controlar;

b. Estão separadas, do ponto de vista organizacional, das atividades que lhes compete monitorizar e controlar;

[38] Ver também *EBA Guidelines on the AML/CTF compliance function* [Orientações da EBA sobre a função de controlo do cumprimento em matéria de BC/FT] (atualmente em elaboração)

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 pela gestão das atividades que a função de controlo interno monitoriza e controla; e

d. A remuneração dos membros do pessoal das funções de controlo interno não deve estar associada aos resultados das atividades que estas monitorizam e controlam, nem pode comprometer de outro modo a sua objetividade[39].

19.3 Combinação de funções de controlo interno

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

19.4 Recursos das funções de controlo interno

177. As funções de controlo interno devem estar dotadas de recursos suficientes e dispor de um número adequado de colaboradores qualificados (tanto a nível da empresa-mãe como das filiais). As qualificações dos seus membros do pessoal devem ser permanentemente atualizadas e estes devem receber formação adequada, sempre que necessário.

178. As funções de controlo interno devem dispor também de sistemas informáticos e de 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 todas as áreas de atividade e às filiais com assunção de riscos relevantes, em especial as que possam originar riscos significativos para a instituição.

20 Função de gestão de riscos

179. As instituições estabelecem uma função de gestão de riscos (FGR) que abrange toda a instituição. A FGR deve ter 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 definido na Secção 17.

180. Sempre que 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 risco.

181. A FGR tem acesso a todos as áreas de negócio e outras unidades internas suscetíveis de gerar risco, bem como às filiais e entidades associadas relevantes.

[39] 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.

182. 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, mercados e produtos, e devem ter acesso a formação regular.

183. A FGR é independente das áreas de negócio e unidades cujos riscos controla, mas não está impedida de interagir com as mesmas. 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.

184. A FGR deve ser um elemento organizativo essencial da instituição e estar estruturada de modo a poder implementar políticas de risco e controlar o quadro de gestão de riscos. A FGR deve desempenhar um papel fundamental assegurando que a instituição tenha estabelecidos processos eficazes de gestão de riscos. A FGR participa ativamente em todas as decisões de gestão de riscos significativos.

185. As instituições significativas podem ponderar estabelecer FGR específicas para cada área de negócio material, mas deve haver sempre uma FGR a nível central (incluindo uma FGR do grupo na instituição consolidante), para a obtenção de uma perspetiva holística da totalidade dos riscos ao nível da instituição e do grupo, e para assegurar que a estratégia de risco é cumprida.

186. A FGR fornece informações, análises e pareceres específicos pertinentes e independentes sobre as exposições ao risco, emite pareceres sobre propostas e decisões de rusci tomadas pelas áreas de negócio ou unidades internas e informa o órgão de administração da compatibilidade dessas propostas e decisões com a apetência pelo risco e a estratégia de risco da instituição. A FGR pode recomendar melhorias do quadro de gestão de riscos e medidas corretivas para remediar infrações de políticas, procedimentos e dos limites de risco.

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

187. A FGR participa ativamente numa fase inicial, na elaboração da estratégia de risco da instituição e assegura que a instituição tem estabelecidos processos eficazes de gestão de riscos. A FGR faculta ao órgão de administração todas as informações relevantes em matéria de riscos para que este possa determinar o nível de apetência pelo risco da instituição. A FGR avalia a solidez e a sustentabilidade da estratégia de risco e da apetência pelo risco. Deve assegurar que a apetência pelo risco se traduza de forma adequada em limites de risco específicos. A FGR avalia igualmente a estratégia de risco e a apetência pelo risco das unidades de negócio, incluindo os objetivos que estas propõem, e é envolvida antes de o órgão de administração tomar decisões relativas às estratégias de risco e à apetência pelo risco. Os objetivos devem ser plausíveis e coerentes com a estratégia de risco da instituição.

188. O envolvimento da FGR nos processos de tomada de decisão deve garantir que as considerações de risco sejam tidas em conta de forma adequada. Contudo, a

responsabilidade pelas decisões tomadas deve continuar a pertencer às unidades de negócio e às unidades internas e, em última análise, ao órgão de administração.

20.2 Papel da FGR nas alterações significativas

189. 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 tomada da decisão.

190. 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 solidez dos seus fundos próprios, em circunstâncias normais e adversas.

20.3 Papel da FGR na identificação, medição, avaliação, gestão, mitigação, monitorização e reporte dos riscos

191. A FGR assegura a existência de um quadro de gestão de riscos adequado e que todos os riscos sejam identificados, avaliados, medidos, monitorizados, geridos e adequadamente reportados pelas unidades pertinentes na instituição.

192. A FGR assegura que a identificação e a avaliação não se baseiam apenas em informações quantitativas ou em resultados de modelos, mas 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.

193. 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.

194. A FGR assegura que todos os riscos identificados são efetivamente acompanhados pelas unidades de negócio.

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

196. A FGR analisa as tendências e reconhece os riscos novos ou emergentes e os aumentos de riscos suscitados pela alteração das circunstâncias e condições. Também deve rever regularmente os resultados atuais em termos de riscos face às estimativas anteriores (verificações *a posteriori*) para avaliar e melhorar a precisão e a eficácia do processo de gestão de riscos.

197. 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

198. A FGR avalia de forma independente as infrações aos limites de risco ou à apetência pelo risco (incluindo a determinação das suas causas e a realização de uma análise jurídica e económica do custo real do encerramento, redução ou cobertura da exposição face ao possível custo da sua manutenção), informando as unidades de negócio 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 comités.

199. A FGR tem um papel fundamental no sentido de assegurar que as decisões sobre as suas recomendações sejam adotadas ao nível pertinente, cumpridas pelas unidades de negócio 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

200. 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 compreenda o perfil de risco global da instituição. O mesmo se aplica ao responsável pela FGR de uma empresa-mãe em relação à situação consolidada.

201. O responsável pela FGR possui conhecimentos especializados, independência e senioridade 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 em exclusividade 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 conformidade ou ser desempenhada por outro quadro superior, desde que seja salvaguardada a inexistência de quaisquer conflitos 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).

202. 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.

203. As instituições estabelecem procedimentos reforçados para a aprovação de decisões sobre as quais o responsável pela FGR tenha manifestado 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 de risco e a apetência pelo risco da instituição.

21 Função de conformidade

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

205. Caso não seja adequado nomear uma pessoa para desempenhar em exclusividade o cargo de responsável pela conformidade, tendo em conta o princípio da proporcionalidade estabelecido no Título I, esta função pode ser combinada com a função de responsável da FGR ou pode ser desempenhada por outro quadro superior (p. ex., o responsável do departamento jurídico), desde que seja salvaguardada a inexistência de quaisquer conflitos de interesses entre as funções combinadas.

206. A função de verificação do cumprimento, incluindo o seu responsável, é independente das áreas de negócio 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 pela FGR ou combinada com a mesma ou outras funções adequadas, p. ex., o departamento jurídico ou os recursos humanos.

207. Os membros do pessoal da função de conformidade devem possuir conhecimentos, competência e experiência suficientes, no que respeita à verificação do cumprimento e aos procedimentos relevantes, e devem ter acesso a formação regular.

208. O órgão de administração na sua função de fiscalização supervisiona a implementação de uma política de conformidade 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.

209. A função de conformidade aconselha o órgão de administração sobre as medidas a tomar 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 de conformidade.

210. A função de conformidade assegura que a monitorização da conformidade é efetuada através de um programa bem estruturado e definido e que a política em conformidade é observada. A função de conformidade 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. A função de conformidade e a FGR cooperam e trocam informações necessárias para o

desempenho das respetivas funções. As conclusões da função de conformidade são tidas em conta pelo órgão de administração e pela FGR no âmbito do processo de tomada de decisão.

211. De acordo com a Secção 18 das presentes orientações, a função de conformidade verifica também, em estreita cooperação com a FGR e o departamento jurídico, se os novos produtos e os novos procedimentos respeitam o quadro jurídico em vigor e, quando apropriado, e as futuras alterações conhecidas da legislação, da regulamentação e dos requisitos de supervisão.

212. As instituições tomam medidas adequadas contra comportamentos internos ou externos que possam facilitar ou permitir a fraude, BC/FT ou outros crimes financeiros e infrações disciplinares (por ex., infrações de procedimentos internos ou de limites).

213. As instituições asseguram que as suas filiais e sucursais tomam medidas para assegurarem que as suas operações cumprem com 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 função de conformidade da instituição consolidante.

22 Função de auditoria interna

214. 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.

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

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

217. 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 risco, controlos internos e conformidade com as regras aplicáveis.

218. A FAI avalia se o quadro de controlo interno da instituição, tal como definido na Secção 15, é efetivo e eficiente. Em especial, a FAI avalia:

a. A adequação do quadro de governo da instituição;

b. Se as políticas e os procedimentos existentes permanecem adequados e cumprem os requisitos legais e regulamentares, bem como a estratégia de risco e a apetência pelo risco 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, qualidade e eficácia dos controlos efetuados e do reporte realizado pelas unidades de negócio de defesa, e pelas funções de gestão de riscos e de conformidade.

219. 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 tomadas.

220. A FAI deve ter livre acesso, ao nível de toda a instituição, a todos os registos, documentos, informações e instalações da instituição. Tal deve incluir o acesso a sistemas informáticos de gestão e a atas de todos os comités e órgãos de decisão.

221. 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).

222. 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.

223. 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.

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

Título VI – Gestão da continuidade do negócio[40]

225. As instituições estabelecem um plano sólido de gestão da continuidade e de recuperação do negócio para assegurar a sua capacidade de funcionar em permanência e para limitarem as perdas em caso de perturbação grave das atividades.

226. As instituições podem estabelecer uma função independente específica de continuidade do negócio, p. ex., como parte da função de gestão dos riscos[41].

227. A atividade de uma instituição depende de vários recursos críticos (por exemplo, sistemas de TI, incluindo serviços de computação em nuvem, sistemas de comunicação, pessoal essencial e instalações). O objetivo da gestão da continuidade do negócio é minimizar as consequências operacionais, financeiras, jurídicas e reputacionais, bem como outras consequências materiais decorrentes de uma catástrofe ou de uma interrupção prolongada destes recursos e a perturbação consequente dos procedimentos operacionais 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).

228. A fim de estabelecer um plano sólido de gestão da continuidade do negócio, a instituição analisa cuidadosamente fatores de risco e 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 todas as áreas de negócio 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.

229. Com base na análise anterior, a instituição estabelece:

a. Planos de contingência e de continuidade de negócio para assegurar uma reação adequada às emergências e ter a capacidade de manter as suas atividades mais importantes em caso de perturbação dos procedimentos operacionais normais; e

b. Planos de recuperação de recursos críticos para possibilitar a retoma dos procedimentos operacionais normais num prazo adequado. Os eventuais riscos residuais resultantes de potenciais perturbações da atividade serão compatíveis com a apetência pelo risco da instituição.

230. Os planos de contingência, de continuidade do negócio e de recuperação são documentados e cuidadosamente implementados. A documentação está disponível nas áreas de negócio, nas unidades internas e na função de gestão de riscos e é armazenada em

[40] As instituições devem também consultar as Orientações da EBA relativas ao risco das TIC, disponíveis em:https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[41] Ver também o artigo 312.º do Regulamento (UE) n.º 575/2013.

sistemas fisicamente segregados e facilmente acessíveis em caso de contingência. Deve ser proporcionada formação adequada. Os planos devem ser testados e atualizados regularmente. Quaisquer desafios ou falhas detetados nos testes são documentados e analisados, e os planos revistos em conformidade.

Título VII – Transparência

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

232. Deste modo, o órgão de administração informa e mantém o pessoal relevante 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.

233. Sempre que as autoridades competentes exijam, nos termos do artigo 106.º, n.º 2, da Diretiva 2013/36/UE, que as empresas-mãe publiquem anualmente uma descrição da sua estrutura jurídica e de governo e a 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[42].

234. 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 qualificados como 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;

[42] 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).

g. Uma descrição da política em matéria de conflitos de interesses aplicável à instituição e ao órgão de administração;

h. Uma descrição do quadro de controlo interno; e

i. Uma descrição do quadro de gestão da continuidade do negócio.

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

De acordo com o Título III, as instituições devem considerar os seguintes aspetos para efeitos de documentação das políticas e e disposições de governo interno:

1. Estrutura acionista
2. Estrutura organizativa do grupo, se aplicável (estrutura jurídica e funcional)
3. Composição e funcionamento do órgão de administração
   a) Critérios de seleção, incluindo o modo como é tida em conta a diversidade
   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 organograma (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 conformidade
   c) Responsável pela função de auditoria interna
   d) Administrador 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
7. Descrição da estratégia de risco e do quadro de gestão de riscos

8. Estrutura organizacional (com impacto no grupo, se aplicável)
    a) Estrutura operacional, unidades de negócio e atribuição de competências e responsabilidades
    b) Subcontratação
    c) Gama de produtos e serviços
    d) Âmbito geográfico da atividade
    e) Prestação de serviços ao abrigo do regime da liberdade de prestação de serviços
    f) Sucursais
    g) Filiais, sociedades mistas, etc.
    h) Utilização de estabelecimentos *offshore*
9. 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 de conflito de interesses
    d) Participação de infrações
10. Estado da política de governo interno, com a data de:
    a) Elaboração
    b) Última alteração
    c) Última avaliação
    d) Aprovação pelo órgão de administração.