EBA/GL/2021/14

22 november 2021

Riktlinjer

för intern styrning enligt direktiv (EU) 2019/2034

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Dessa riktlinjer utfärdas i enlighet med artikel 16 i förordning (EU) nr 1093/2010[1]. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 ska behöriga myndigheter och finansinstitut, inklusive värdepappersföretag, med alla tillgängliga medel söka följa riktlinjerna.

2. I riktlinjerna ger Europeiska bankmyndigheten (EBA) sin syn på vad som är lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och på hur unionsrätten bör tillämpas inom ett visst område. De behöriga myndigheter, enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010, som berörs av riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till värdepappersföretag.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste en behörig myndighet meddela EBA att den följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att den inte gör det, senast den 16.05.2022. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att den behöriga myndigheten inte följer riktlinjerna. Anmälningar ska lämnas genom att det formulär som tillhandahålls på EBA:s webbplats skickas in till compliance@eba.europa.eu med hänvisningen ”EBA/GL/2021/14”. Anmälningar ska lämnas in av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas vägnar. Alla förändringar i graden av efterlevnad måste rapporteras till EBA.

4. Anmälningarna kommer att publiceras på EBA:s webbplats i enlighet med artikel 16.3 i förordning (EU) nr 1093/2010.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12)

2. Syfte, tillämpningsområde och definitioner

Syfte

5. I dessa riktlinjer anges, i enlighet med artikel 26.4 i direktiv (EU) 2019/2034[2], de former, processer och mekanismer för intern styrning som värdepappersföretag ska tillämpa enligt avdelning IV kapitel 2 avsnitt 2 i direktivet för att säkerställa en effektiv och ansvarsfull ledning.

6. Riktlinjerna gäller utan att det påverkar tillämpningen av de bestämmelser som anges i artiklarna 9, 16, 23 och 24 i direktiv 2014/65/EU, i kommissionens delegerade förordning (EU) 2017/565 och i kommissionens delegerade direktiv (EU) 2017/593.

Adressater

7. Dessa riktlinjer riktar sig till de behöriga myndigheter som avses i artikel 4.2 viii i förordning (EU) nr 1093/2010 och definieras i artikel 3.1.5 i direktiv (EU) 2019/2034, och till de finansinstitut som avses i artikel 4.1 i förordning (EU) nr 1093/2010 som är värdepappersföretag enligt definitionen i artikel 4.1.1 i direktiv 2014/65/EU, som inte omfattas av artikel 2.2 i direktiv (EU) 2019/2034 och som inte uppfyller samtliga villkor för att betraktas som små och icke-sammanlänkade värdepappersföretag enligt artikel 12.1 i förordning (EU) 2019/2033.

Tillämpningsområde

8. Dessa riktlinjer är tillämpliga på värdepappersföretags styrningsformer enligt kraven i direktiv (EU) 2019/2034, inbegripet deras organisationsstruktur och motsvarande ansvarskedjor, samt på processerna för att identifiera, hantera, övervaka och rapportera alla risker[3] som de är eller kan bli exponerade för, och på ramen för intern kontroll.

9. Riktlinjerna tillämpas på individuell nivå och gruppnivå enligt det tillämpningsområde som anges i artikel 25 i direktiv (EU) 2019/2034.

10. Riktlinjerna är avsedda att omfatta alla befintliga ledningsstrukturer, och ingen särskild struktur förordas. Riktlinjerna påverkar inte den allmänna fördelningen av befogenheter enligt

[2] Europaparlamentets och rådets direktiv (EU) 2019/2034 av den 27 november 2019 om tillsyn av värdepappersföretag och om ändring av direktiven 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU och 2014/65/EU.

[3] Alla hänvisningar till risker i dessa riktlinjer ska omfatta alla risker som värdepappersföretag är eller kan bli exponerade för, inbegripet risker för kunder, marknadsrisker, risker för värdepappersföretaget och likviditetsrisker, operativa risker, inklusive rättsliga risker, it-risker och anseenderisker, miljömässiga, sociala och styrningsrelaterade risker (ESG-risker) samt risker för penningtvätt och finansiering av terrorism.

nationell bolagsrätt. De ska följaktligen tillämpas oavsett ledningsstruktur (monistisk och/eller dualistisk ledningsstruktur och/eller annan struktur) i alla medlemsstater. Ledningsorganet, enligt definitionen i artikel 3.1.23 och 3.1.24 i direktiv (EU) 2019/2034, ska förstås som ett organ med ledningsfunktioner (verkställande funktioner) och tillsynsfunktioner (icke verkställande funktioner)[4].

11. Begreppen ”ledningsorgan i dess ledningsfunktion” och ”ledningsorgan i dess tillsynsfunktion” används genomgående i riktlinjerna och syftar inte på någon särskild styrningsstruktur, och hänvisningar till ledningsfunktionen (verkställande funktion) eller tillsynsfunktionen (icke verkställande funktion) ska förstås som de organ eller ledamöter i ledningsorganet som enligt nationell rätt ansvarar för den berörda funktionen. Vid genomförandet av dessa riktlinjer ska de behöriga myndigheterna beakta nationell bolagsrätt och, när så är nödvändigt, ange på vilket organ eller vilka av ledningsorganets ledamöter dessa funktioner ska åläggas.

12. I medlemsstater där ledningsorganet helt eller delvis delegerar den verkställande funktionen till en person eller ett internt verkställande organ (t.ex. en verkställande direktör, ledningsgrupp eller verkställande kommitté) ska de personer som utför dessa verkställande funktioner och leder institutets verksamhet på grundval av denna delegering anses utgöra ledningsorganets ledningsfunktion. Vid tillämpningen av dessa riktlinjer ska alla hänvisningar till ledningsorganet i dess ledningsfunktion anses omfatta ledamöterna i det verkställande organet eller den verkställande direktören, enligt definitionerna i dessa riktlinjer, även om de inte har föreslagits eller utsetts till formella ledamöter i värdepappersföretagets ledningsorgan enligt nationell rätt.

13. I medlemsstater där vissa ansvarsområden utövas direkt av värdepappersföretagets aktieägare, ledamöter eller ägare i stället för av ledningsorganet, ska värdepappersföretagen se till att sådana ansvarsområden och relaterade beslut i möjligaste mån överensstämmer med de riktlinjer som gäller för ledningsorganet.

14. De definitioner av verkställande direktör, finansdirektör och person som innehar nyckelfunktion som används i dessa riktlinjer är rent funktionella och syftar inte till att utgöra ett krav på att sådana befattningshavare utses eller att sådana befattningar inrättas, såvida detta inte föreskrivs i relevant unionsrätt eller nationell rätt.

Definitioner

15. Om inte annat anges har de termer som används och definieras i direktiv (EU) 2019/2034 och förordning (EU) 2019/2033 samma innebörd i riktlinjerna. Dessutom gäller följande definitioner i dessa riktlinjer:

[4] Se även skäl 27 i direktiv (EU) 2019/2034.

***riskaptit*:**	den aggregerade risknivå och de risktyper som ett värdepappersföretag är villigt att utsätta sig för inom ramen för sin riskkapacitet, i enlighet med sin affärsmodell, för att uppnå sina strategiska mål.
***riskkapacitet*:**	den maximala risknivå som ett värdepappersföretag kan utsätta sig för utifrån sin kapitalbas, sin riskhanterings- och kontrollkapacitet samt sina regleringsmässiga begränsningar.
***riskkultur*:**	ett värdepappersföretags normer, attityder och beteenden som rör riskmedvetenhet, risktagande och riskhantering samt de kontroller som ligger till grund för beslut om risker. Riskkulturen inverkar på de beslut som ledningen och de anställda fattar i den dagliga verksamheten och påverkar vilka risker de tar.
***personal*:**	alla anställda vid ett värdepappersföretag och dess dotterföretag på gruppnivå och samtliga ledamöter i respektive ledningsorgan i deras ledningsfunktion och deras tillsynsfunktion.
***verkställande direktör (vd)*:**	den person som ansvarar för att leda och styra ett värdepappersföretags övergripande affärsverksamhet.
***finansdirektör*:**	den person som har det övergripande ansvaret för ledningen av följande verksamhet: hantering av finansiella resurser, finansiell planering och finansiell rapportering.
***chefer för interna kontrollfunktioner*:**	de personer högst upp i hierarkin som ansvarar för att på ett effektivt sätt leda den dagliga verksamheten inom de oberoende funktionerna för riskhantering, regelefterlevnad och internrevision.
***personer som innehar nyckelfunktioner*:**	de personer som har ett väsentligt inflytande över värdepappersföretagens ledning men som varken är ledamöter i ledningsorganet eller den verkställande direktören. Här ingår chefer för interna kontrollfunktioner och finansdirektörer, om dessa inte ingår i ledningsorganet, samt andra personer som innehar nyckelfunktioner när sådana identifieras utifrån en riskbaserad metod av värdepappersföretagen. Andra personer som innehar nyckelfunktioner kan vara chefer för viktiga affärsområden, för filialer i EES-/Eftaområdet, för dotterföretag i tredjeländer eller andra interna funktioner.
***moderföretag inom unionen*:**	ett modervärdepappersföretag inom unionen, ett värdepappersinriktat moderholdingföretag inom unionen eller ett blandat finansiellt moderholdingföretag inom unionen som måste uppfylla de tillsynskrav som gäller för den konsoliderade situationen enligt artikel 7 i förordning (EU) 2019/2033.

***konsolidering under tillsyn*:**	tillämpningen av de tillsynsregler som anges i artikel 25 i direktiv (EU) 2019/2034 och artikel 7 i förordning (EU) 2019/2033[5].
***börsnoterade värdepappersföretag*:**	de värdepappersföretag vars finansiella instrument har upptagits till handel på en reglerad marknad eller en multilateral handelsplattform, enligt definitionerna i artikel 4.21 och 4.22 i direktiv 2014/65/EU, i en eller flera medlemsstater[6].
***aktieägare*:**	den person som äger aktier i ett värdepappersföretag eller, beroende på värdepappersföretagets juridiska form, andra ägare eller ledamöter i värdepappersföretaget.
***uppdrag i ledningsorgan*:**	en befattning som ledamot i ett värdepappersföretags ledningsorgan eller en annan juridisk person.

3. Genomförande

Datum för ikraftträdande

16. Dessa riktlinjer gäller från och med den 30 april 2022.

[5] Se även de tekniska tillsynsstandarderna om konsolidering av värdepappersföretag enligt direktiv (EU) 2019/2034.

[6] Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

4. Riktlinjer

Avdelning I – proportionalitet

17. Vid tillämpningen av dessa riktlinjer ska de behöriga myndigheterna och värdepappersföretagen beakta den proportionalitetsprincip som anges i artikel 26.3 i direktiv (EU) 2019/2034 och som specificeras närmare i avdelning I i dessa riktlinjer, i syfte att säkerställa att de interna styrningsformer som inrättas av värdepappersföretagen, inbegripet när det gäller värdepappersföretagskoncerner, är förenliga med företagets och koncernens enskilda riskprofil, är proportionerliga till deras storlek och interna organisation, är relevanta för deras affärsmodell, är lämpliga för verksamhetens art, omfattning och komplexitet samt är tillräckliga för att effektivt uppnå målen i de relevanta regelkraven och bestämmelserna.

18. Inom ramen för föregående punkt ska hänsyn tas till de olika affärsmodeller som värdepappersföretag och värdepappersföretagskoncerner använder sig av, det vill säga huruvida de är verksamma som investeringsrådgivare, portföljförvaltare, handelsplatsoperatörer, förvaringsinstitut, verkställande mäklare, handelsmäklare, handelsföretag eller annan funktion. För att de interna styrningsformerna ska anses vara förenliga med företagets och koncernens enskilda riskprofil, vara proportionerliga till deras storlek och interna organisation, vara relevanta för deras affärsmodell, vara lämpliga för verksamhetens art, omfattning och komplexitet samt vara tillräckliga för att effektivt uppnå målen i de relevanta regelkraven och bestämmelserna ska det säkerställas att värdepappersföretag som har en mer komplex organisation eller verkar i större skala har mer sofistikerade styrningsformer, medan värdepappersföretag som har en enklare organisation eller verkar i mindre skala kan inrätta enklare styrningsformer. Värdepappersföretag ska dock vara medvetna om att ett företags storlek eller systemvikt inte i sig är en indikation på omfattningen av värdepappersföretagets riskexponering.

19. När de behöriga myndigheterna och värdepappersföretagen tillämpar den proportionalitetsprincip som anges i artikel 26.3 i direktiv (EU) 2019/2034, och som specificeras närmare i punkt 20 i dessa riktlinjer, ska de säkerställa att tillämpningen inte leder till att lagstadgade krav för värdepappersföretag åsidosätts eller att principen tillämpas på ett sätt som underlåter att säkerställa stabila styrningsformer, en tydlig organisationsstruktur, lämpliga interna kontrollmekanismer, en sund och effektiv riskhantering och lämpliga ersättningspolicyer.

20. Vid tillämpningen av proportionalitetsprincipen och för att säkerställa ett korrekt genomförande av de lagstadgade kraven och av dessa riktlinjer ska värdepappersföretagen och de behöriga myndigheterna beakta

    a. storleken på balansräkningarna hos det värdepappersföretag och dess dotterföretag som omfattas av konsolidering under tillsyn,

b. huruvida värdepappersföretagets tillgångar inom och utanför balansräkningen har ett värde av i genomsnitt högst 100 miljoner euro under den fyraårsperiod som föregår det aktuella räkenskapsåret, enligt de kriterier som anges i artikel 32.4 a i direktiv (EU) 2019/2034,

c. de tillgångar som förvaltas,

d. huruvida värdepappersföretaget har auktorisation att hålla kontanter eller tillgångar för uppdragsgivares räkning,

e. de tillgångar som förvaras och administreras,

f. den mängd kundorder som hanteras,

g. den dagliga handelsflödesvolymen,

h. värdepappersföretagets geografiska närvaro och storleken på dess verksamhet i varje jurisdiktion, inbegripet i tredjeländers jurisdiktioner,

i. värdepappersföretagets juridiska form, inbegripet huruvida värdepappersföretaget ingår i en koncern och, om så är fallet, koncernens proportionalitetsbedömning,

j. huruvida det är ett börsnoterat värdepappersföretag,

k. huruvida värdepappersföretaget har auktorisation att använda interna modeller för att mäta kapitalkrav (t.ex. den interna riskklassificeringsmetoden),

l. den typ av auktoriserad verksamhet och de tjänster som värdepappersföretaget utför (t.ex. avsnitten A och B i bilaga I till direktiv 2014/65/EU) och andra tjänster (t.ex. clearingtjänster) som värdepappersföretaget utför,

m. den underliggande affärsmodellen och affärsstrategin, affärsverksamhetens art och komplexitet samt värdepappersföretagets organisationsstruktur,

n. värdepappersföretagets riskstrategi, riskaptit och faktiska riskprofil, även med beaktande av resultatet av översyns- och utvärderingsprocessens kapital- och likviditetsbedömningar,

o. värdepappersföretagets ägar- och finansieringsstruktur,

p. typen av kunder,

q. de finansiella instrumentens eller kontraktens komplexitet,

r. de funktioner och distributionskanaler som lagts ut på entreprenad,

s. de befintliga it-systemen, inklusive system för driftskontinuitet och utkontrakterade funktioner på detta område.

21. Värdepappersföretag som är juridiska personer som leds av en enda fysisk person ska ha alternativa system som säkerställer en sund och ansvarsfull ledning av värdepappersföretaget och att vederbörlig hänsyn till interna styrningsformer tas.

Avdelning II – ledningsorganets och kommittéernas roll och sammansättning

1 Ledningsorganets roll och ansvarsområden

22. Ledningsorganet måste ha det yttersta och övergripande ansvaret för värdepappersföretaget och det ska definiera, övervaka och ansvara för att inrätta de styrningsformer som anges särskilt i artiklarna 26, 28 och 29 i direktiv (EU) 2019/2034 och som säkerställer en effektiv och ansvarsfull ledning av värdepappersföretaget.

23. Ledningsorganets uppgifter ska vara tydligt definierade och åtskillnad ska göras mellan de uppgifter som åligger ledningsfunktionen (verkställande funktion) respektive tillsynsfunktionen (icke verkställande funktion). Ledningsorganets ansvarsområden och uppgifter ska beskrivas i ett skriftligt dokument och vederbörligen godkännas av ledningsorganet. Alla ledamöter i ledningsorganet ska ha full kännedom om ledningsorganets struktur och ansvarsområden och, i tillämpliga fall, om fördelningen av uppgifter mellan de olika funktionerna inom ledningsorganet och dess kommittéer.

24. Ledningsorganet i dess tillsynsfunktion och i dess ledningsfunktion ska samverka på ett effektivt sätt. Båda funktionerna ska förse varandra med den information som behövs för att de ska kunna fullgöra sina respektive uppgifter. För att säkerställa tillräckliga kontroller och lämplig befogenhetsuppdelning ska beslutsprocessen inom ledningsorganet inte domineras av en enda ledamot eller en liten undergrupp av ledamöter.

25. Utan att det påverkar de uppgifter och ansvarsområden som åläggs ledningsorganet enligt direktiv 2014/65/EU ska ledningsorganets ansvarsområden omfatta att fastställa, godkänna och övervaka genomförandet av följande:

a. Värdepappersföretagets övergripande affärsstrategi och centrala policyer enligt tillämpliga rättsliga ramar, med beaktande av värdepappersföretagets långsiktiga finansiella intressen och solvens.

b. Den övergripande riskstrategin, inbegripet värdepappersföretagets riskaptit och dess riskhanteringsram, inklusive lämpliga policyer och förfaranden, med beaktande av det makroekonomiska klimatet och värdepappersföretagets konjunkturcykel samt

åtgärder för att säkerställa att ledningsorganet ägnar tillräckligt med tid åt riskhanteringsfrågor, tillsammans med en adekvat och effektiv ram för intern styrning och intern kontroll som inbegriper en tydlig organisationsstruktur och välfungerande interna kontrollmekanismer. Sådana mekanismer ska inbegripa en permanent och effektiv funktion för regelefterlevnad och, när så är lämpligt och proportionellt enligt avdelning I, interna riskhanteringsfunktioner och internrevisionsfunktioner som har tillräcklig befogenhet och ställning och tillräckliga resurser för att kunna utföra sina uppgifter på ett oberoende sätt och säkerställa efterlevnad av tillämpliga lagstadgade krav beträffande förebyggande av penningtvätt och finansiering av terrorism, samt när det gäller mål för värdepappersföretagets likviditetshantering.

c. En ersättningspolicy som är förenlig med de ersättningsprinciper som anges i artiklarna 26 och 30–33 i direktiv (EU) 2019/2034 och i EBA:s riktlinjer för en sund ersättningspolicy enligt direktiv (EU) 2019/2034[7].

d. Mekanismer som syftar till att säkerställa att de enskilda och kollektiva lämplighetsbedömningarna av ledningsorganet utförs på ett ändamålsenligt sätt, att ledningsorganets sammansättning och efterträdarplanering är lämplig och att ledningsorganet fullgör sina funktioner på ett effektivt sätt[8].

e. Ett förfarande för urval och lämplighetsbedömning av personer som innehar nyckelfunktioner[9].

f. Mekanismer som syftar till att säkerställa den interna funktionen hos ledningsorganets kommittéer, när sådana har inrättats, med redogörelser för

   i. varje kommittés roll, sammansättning och uppgifter,

   ii. lämpliga informationsflöden, inbegripet dokumentation av rekommendationer och slutsatser, och rapporteringsvägar mellan varje kommitté och ledningsorganet, behöriga myndigheter och andra parter.

g. En riskkultur som är förenlig med avsnitt 8 i dessa riktlinjer och som behandlar värdepappersföretagets riskmedvetenhet och risktagande.

h. En företagskultur och företagsvärden som är förenliga med avsnitt 9 och som främjar ett ansvarsfullt och etiskt beteende, inbegripet en uppförandekod eller ett liknande instrument.

[7] EBA:s riktlinjer för en sund ersättningspolicy enligt direktivet om tillsyn av värdepappersföretag.

[8] Se även Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare.

[9] Se även Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare.

i. En policy om intressekonflikter på värdepappersföretagsnivå som är förenlig med avsnitt 10 och en motsvarande policy på personalnivå som är förenlig med avsnitt 11.

j. Mekanismer som syftar till att säkerställa integriteten hos systemen för redovisning och finansiell rapportering, inbegripet finansiella och operativa kontroller, samt efterlevnad av lagstiftning och relevanta standarder.

26. När ledningsorganet inrättar, godkänner och övervakar genomförandet av de aspekter som anges i punkt 25 ska det sträva efter att säkerställa en affärsmodell och styrningsformer – inbegripet en ram för riskhantering – som tar hänsyn till de risker som värdepappersföretag är eller kan bli exponerade för eller de risker som värdepappersföretag innebär eller kan innebära för andra[10]. Vid beaktandet av samtliga risker ska värdepappersföretag ta hänsyn till alla relevanta riskfaktorer, inbegripet miljömässiga, sociala och styrningsrelaterade (ESG) riskfaktorer. Värdepappersföretag ska även vara medvetna om att de sistnämnda riskfaktorerna kan öka deras tillsynsrelaterade risker[11]. Sådana ESG-riskfaktorer omfattar bland annat rättsliga risker inom avtalsrätt eller arbetsrätt, risker förknippade med potentiella kränkningar av de mänskliga rättigheterna eller andra ESG-riskfaktorer som kan påverka det land där en tjänsteleverantör är etablerad och dess förmåga att tillhandahålla de överenskomna servicenivåerna.

27. Ledningsorganet ska övervaka processerna för informationsgivning och kommunikation med externa intressenter och behöriga myndigheter.

28. Alla ledamöter i ledningsorganet ska ha kännedom om värdepappersföretagets övergripande verksamhet, finansiella situation och risksituation, med beaktande av det ekonomiska klimatet, samt om beslut som fattas som har en betydande inverkan på värdepappersföretagets affärsverksamhet.

29. En ledamot i ledningsorganet får ansvara för en intern kontrollfunktion enligt vad som anges i avdelning V avsnitt 18.1, förutsatt att ledamoten inte har andra uppdrag som skulle kunna äventyra dess interna kontrollarbete och den interna kontrollfunktionens oberoende ställning.

30. Ledningsorganet ska övervaka, regelbundet se över och åtgärda eventuella konstaterade brister i genomförandet av processer, strategier och policyer som rör de ansvarsområden som anges i punkterna 25 och 26. Den interna styrningsramen och dess genomförande ska ses över och uppdateras regelbundet, med beaktande av proportionalitetsprincipen, enligt den närmare beskrivningen i avdelning I. En grundligare översyn ska göras när väsentliga förändringar påverkar värdepappersföretaget.

[10] Se artikel 26 i direktiv (EU) 2019/2034.

[11] Se EBA:s diskussionsunderlag om hantering och tillsyn av ESG-risker, publicerad i enlighet med artikel 98.8 i kapitalkravsdirektivet för att beskriva hur EBA betraktar ESG-risker, överföringskanaler och rekommendationer för system, processer, mekanismer och strategier som institut bör genomföra för att identifiera, bedöma och hantera ESG-risker.

31. I de fall värdepappersföretaget är en juridisk person som leds av en enda fysisk person i enlighet med konstitutionella bestämmelser och nationella lagar, ska hänvisningarna i dessa riktlinjer till ett ledningsorgan tolkas som hänvisningar till den enda person som ansvarar för att införa alternativa system som säkerställer en sund och ansvarsfull ledning av värdepappersföretaget och att vederbörlig hänsyn till interna styrningsformer tas.

2 Ledningsorganets ledningsfunktion

32. Inom ramen för dess ledningsfunktion ska ledningsorganet aktivt arbeta med värdepappersföretagets affärsverksamhet och ska fatta sunda och välgrundade beslut.

33. Ledningsorganet i dess ledningsfunktion ska ansvara för genomförandet av de strategier som fastställs av ledningsorganet och regelbundet diskutera strategiernas genomförande och lämplighet med ledningsorganet i dess tillsynsfunktion. Det operativa genomförandet får utföras av värdepappersföretagets ledning.

34. Ledningsorganet i dess ledningsfunktion ska på ett konstruktivt sätt ifrågasätta och kritiskt granska förslag, förklaringar och information som tas emot när det utövar sitt omdöme och fattar beslut. Ledningsorganet i dess ledningsfunktion ska på ett heltäckande sätt och utan onödigt dröjsmål rapportera till, samt regelbundet och vid behov informera, ledningsorganet i dess tillsynsfunktion om de faktorer som är relevanta för bedömningen av situationer, risker och skeenden som påverkar eller kan påverka värdepappersföretaget, t.ex. beträffande väsentliga beslut som fattas om affärsverksamhet och risker, utvärdering av värdepappersföretagets ekonomiska och affärsmässiga klimat, likviditet och sunda kapitalbas samt bedömning av värdepappersföretagets väsentliga riskexponeringar.

35. Utan att det påverkar det nationella införlivandet av direktiv (EU) 2015/849 om bekämpning av penningtvätt ska ledningsorganet, enligt kraven i artikel 46.4 i direktiv (EU) 2015/849, identifiera den ledamot i ledningsorganet som ska ansvara för genomförandet av de lagar och andra författningar som krävs för att följa direktivet, inbegripet motsvarande riktlinjer och förfaranden för bekämpning av penningtvätt och finansiering av terrorism inom institutet och på ledningsorganets nivå.

3 Ledningsorganets tillsynsfunktion

36. Ledamöternas roll i ledningsorganet i dess tillsynsfunktion ska innefatta övervakning och konstruktivt ifrågasättande av värdepappersföretagets strategi.

37. Utan att det påverkar tillämpningen av nationell rätt ska ledningsorganet i dess tillsynsfunktion inbegripa oberoende ledamöter enligt vad som anges i avsnitt 9.3 i Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare enligt direktiv 2013/36/EU och direktiv 2014/65/EU.

38. Utan att det påverkar de ansvarsområden som föreskrivs i tillämplig nationell bolagsrätt ska uppgifterna för ledningsorganet i dess tillsynsfunktion inbegripa att

a. övervaka och kontrollera ledningens beslutsfattande och åtgärder samt utöva effektiv tillsyn över ledningsorganet i dess ledningsfunktion, inbegripet att övervaka och granska enskilda och kollektiva resultat samt genomförandet av värdepappersföretagets strategi och mål,

b. på ett konstruktivt sätt ifrågasätta och kritiskt granska förslag och information som lämnas av ledamöter i ledningsorganet i dess ledningsfunktion samt ledningsorganets beslut,

c. på lämpligt sätt fullgöra uppgifter och ansvarsområden för riskkommittén och ersättningskommittén, om inga sådana kommittéer har inrättats,

d. säkerställa och regelbundet bedöma ändamålsenligheten i värdepappersföretagets interna styrningsram och vidta lämpliga åtgärder för att hantera eventuella konstaterade brister,

e. övervaka och kontrollera att värdepappersföretagets strategiska mål, organisationsstruktur, riskstrategi, riskaptit, riskhanteringsram samt andra policyer (t.ex. ersättningspolicy) och reglerna för informationslämnande genomförs och tillämpas på ett konsekvent sätt,

f. kontrollera att värdepappersföretagets riskkultur tillämpas på ett konsekvent sätt,

g. övervaka genomförandet och upprätthållandet av en uppförandekod eller liknande regler och effektiva policyer för att identifiera, hantera och mildra faktiska och potentiella intressekonflikter,

h. övervaka integriteten hos finansiell information och rapportering samt ramen för intern kontroll, inbegripet en effektiv och sund riskhanteringsram,

i. säkerställa att cheferna för interna kontrollfunktioner kan agera oberoende och, oaktat ansvaret att rapportera till andra interna organ, affärsområden eller enheter, har möjlighet att ge uttryck för oro och när så krävs varna ledningsorganet i dess tillsynsfunktion om ogynnsamma riskutvecklingar som påverkar eller kan påverka värdepappersföretaget,

j. övervaka genomförandet av internrevisionsplanen efter det att riskkommittén, om en sådan har inrättats, har granskat planen.

4 Rollen för ordföranden i ledningsorganet

39. Ordföranden för ledningsorganet ska leda ledningsorganet, bidra till ett effektivt informationsflöde inom ledningsorganet och mellan ledningsorganet och dess kommittéer, om sådana inrättats, och ansvara för att ledningsorganets övergripande funktion bibehålls.

40. Ordföranden ska uppmuntra och främja öppen och kritisk diskussion och se till att avvikande åsikter och uppfattningar kan uttryckas och diskuteras i beslutsprocessen.

41. Inom företag vari ordföranden får åta sig verkställande uppgifter ska värdepappersföretaget ha fastställda åtgärder för att mildra eventuella negativa effekter på värdepappersföretagets kontroller och befogenhetsuppdelning (exempelvis genom att utse en ledande styrelseledamot eller en överordnad oberoende styrelseledamot, eller genom att ha ett större antal icke verkställande ledamöter i ledningsorganet i dess tillsynsfunktion). Ordföranden för ledningsorganet i dess tillsynsfunktion hos ett värdepappersföretag får inte samtidigt inneha funktionen som verkställande direktör i samma värdepappersföretag, såvida detta inte kan motiveras av värdepappersföretaget och har auktoriserats av de behöriga myndigheterna.

42. Ordföranden ska fastställa dagordningar för möten och se till att diskussioner som rör strategiska frågor prioriteras. Ordföranden ska se till att ledningsorganets beslut fattas på ett sunt sätt och på välinformerade grunder samt att handlingar och information erhålls i tillräckligt god tid före möten.

43. Ledningsorganets ordförande ska säkerställa en tydlig ansvarsfördelning mellan ledamöterna i ledningsorganet och att det finns ett effektivt informationsutbyte mellan dem, så att ledamöterna i ledningsorganet i dess tillsynsfunktion på ett konstruktivt sätt kan bidra till diskussionerna och rösta på sunda och välinformerade grunder.

5 Kommittéer inom ledningsorganet i dess tillsynsfunktion

5.1 Inrättande av kommittéer

44. Enligt artikel 28 i direktivet om tillsyn av värdepappersföretag, och om inte annat anges i nationell rätt[12], måste värdepappersföretag vars tillgångar inom och utanför balansräkningen har ett värde av i genomsnitt mer än 100 miljoner euro under den fyraårsperiod som föregår det aktuella räkenskapsåret inrätta risk- och ersättningskommittéer som fungerar som rådgivare till ledningsorganet i dess tillsynsfunktion och utarbetar de beslut som ska fattas av organet.

45. Om ingen riskkommitté har inrättats ska hänvisningarna i dessa riktlinjer till denna kommitté tolkas som hänvisningar till ledningsorganet i dess tillsynsfunktion.

46. Värdepappersföretag får, med beaktande av de kriterier som anges i avdelning I i dessa riktlinjer, inrätta andra kommittéer (t.ex. kommittéer för bekämpning av penningtvätt och finansiering av terrorism, etikkommittéer, uppförande- och regelefterlevnadskommittéer).

47. Värdepappersföretag ska säkerställa en tydlig ansvars- och uppgiftsfördelning mellan de specialiserade kommittéerna inom ledningsorganet. Varje kommitté ska ha ett dokumenterat

[12] Enligt artikel 28 i direktiv (EU) 2019/2034 måste värdepappersföretag som inte uppfyller kriterierna i artikel 32.4 a inrätta en riskkommitté bestående av ledamöter i ledningsorganet som inte har någon verkställande funktion i det berörda värdepappersföretaget.

uppdrag som inbegriper omfattningen av kommitténs ansvarsområden från ledningsorganet i dess tillsynsfunktion och ska fastställa lämpliga arbetsmetoder.

48. Kommittéerna ska stödja tillsynsfunktionen på specifika områden och bidra till utformningen och genomförandet av en sund intern styrningsram. Delegering till kommittéer ska inte på något sätt befria ledningsorganet i dess tillsynsfunktion från att kollektivt fullgöra sina skyldigheter och ansvarsområden.

5.2 Kommittéernas sammansättning[13]

49. Alla kommittéer ska ledas av en icke verkställande ledamot i ledningsorganet som kan göra objektiva bedömningar.

50. Oberoende ledamöter[14] i ledningsorganet i dess tillsynsfunktion ska vara aktivt delaktiga i kommittéer.

51. I de fall kommittéer måste inrättas i enlighet med direktiv (EU) 2019/2034 eller nationell rätt ska de som en allmän princip bestå av minst tre ledamöter och ha minst en oberoende ledamot, med beaktande av de kriterier som anges i avdelning I i dessa riktlinjer och EBA:s och Esmas gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare. Om det inte finns tillräckligt många ledamöter i ledningsorganet i dess tillsynsfunktion för att säkerställa en sund sammansättning av kommittéerna enligt de kriterier som anges i detta avsnitt, får kommitténs uppgifter delegeras till en ledamot i ledningsorganet i dess tillsynsfunktion som vid behov bistås av personalen. Kommittéerna får bestå av samma grupp av ledamöter, med beaktande av de kriterier som anges i avdelning I och antalet oberoende ledamöter i ledningsorganet i dess tillsynsfunktion samt den särskilda erfarenhet, kunskap och kompetens som är enskilt eller kollektivt nödvändig för kommittéernas arbete. Motiveringen som ligger till grund för kommittéernas sammansättning ska dokumenteras.

52. Riskkommittén ska bestå av icke verkställande ledamöter i ledningsorganet i dess tillsynsfunktion hos det berörda värdepappersföretaget. Ersättningskommitténs sammansättning ska följa bestämmelserna i avsnitt 2.3 i EBA:s riktlinjer för en sund ersättningspolicy[15].

53. Riskkommittén ska om möjligt ledas av en oberoende ledamot. Riskkommitténs ledamöter ska både enskilt och kollektivt ha lämpliga kompetenser, färdigheter och kunskaper beträffande urvalsprocessen och lämplighetskraven samt metoder för hantering och kontroll av risker. I alla värdepappersföretag ska riskkommitténs ordförande varken vara ordförande i ledningsorganet eller ordförande för någon annan kommitté, om så är möjligt.

[13] Detta avsnitt ska läsas mot bakgrund av Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare enligt direktiv 2013/36/EU och direktiv 2014/65/EU.

[14] Enligt definitionen i avsnitt 9.3 i Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare enligt direktiv 2013/36/EU och direktiv 2014/65/EU.

[15] EBA:s riktlinjer för en sund ersättningspolicy enligt artikel 34.3 i direktiv (EU) 2019/2034.

5.3 Kommittéernas förfaranden

54. Kommittéerna ska regelbundet rapportera till ledningsorganet i dess tillsynsfunktion.

55. Kommittéerna ska samverka med varandra när så är lämpligt. Utan att det påverkar tillämpningen av punkt 51 kan sådan samverkan ske i form av korsvist deltagande, dvs. att ordföranden eller en ledamot i en kommitté också kan vara ledamot i en annan kommitté.

56. Kommittéledamöterna ska föra öppna och kritiska diskussioner, och avvikande åsikter ska diskuteras på ett konstruktivt sätt.

57. Kommittéerna ska dokumentera dagordningarna för kommittémöten samt mötenas huvudsakliga resultat och slutsatser.

58. Riskkommittén ska som minst

    a. ha tillgång till all relevant information och alla relevanta data som krävs för att den ska kunna fullgöra sin uppgift, inbegripet information och data från relevanta företags- och kontrollfunktioner (t.ex. juridik, ekonomi, personal, it, internrevision, risk och regelefterlevnad, inklusive information om efterlevnad av reglerna för bekämpning av penningtvätt och finansiering av terrorism och sammanställda uppgifter från rapporter om misstänkta transaktioner och riskfaktorer för penningtvätt och finansiering av terrorism),

    b. erhålla regelbundna rapporter, ad hoc-information, meddelanden och synpunkter från cheferna för de interna kontrollfunktionerna gällande värdepappersföretagets aktuella riskprofil, dess riskkultur och riskgränser, samt alla eventuella väsentliga överträdelser [16] som kan ha inträffat, med detaljerad information och rekommendationer om korrigerande åtgärder som vidtagits, ska vidtas eller som föreslås för att hantera dessa; kommittén ska även periodiskt se över och fatta beslut om innehållet, formatet och frekvensen för den riskinformation som ska rapporteras till den,

    c. se till, när så är nödvändigt, att de interna kontrollfunktionerna och andra relevanta funktioner (personal, juridik och ekonomi) involveras på lämpligt sätt inom deras respektive kompetensområden och/eller söka extern experthjälp.

5.4 Riskkommitténs roll

59. I de fall en riskkommitté inrättats ska den som minst

[16] När det gäller allvarliga överträdelser på området bekämpning av penningtvätt och finansiering av terrorism, se även de kommande riktlinjerna enligt artikel 117.6 i direktiv 2013/36/EU som specificerar hur samarbetet och informationsutbytet ska ske mellan de myndigheter som nämns i punkt 5 i den artikeln, i synnerhet vad gäller gränsöverskridande koncerner och inom ramen för identifiering av allvarliga överträdelser av regler om bekämpning av penningtvätt.

a. ge råd och stöd till ledningsorganet i dess tillsynsfunktion beträffande värdepappersföretagets övergripande aktuella och framtida riskstrategi och riskaptit, och bistå ledningsorganet med att övervaka genomförandet av strategin samt säkerställa att den överensstämmer med värdepappersföretagets affärsmål, företagskultur och företagsvärden,

b. bistå ledningsorganet i dess tillsynsfunktion med att övervaka genomförandet av värdepappersföretagets riskstrategi och fastställa de motsvarande riskgränserna,

c. övervaka genomförandet av strategierna för kapital- och likviditetshantering samt för alla andra relevanta risker som föreligger i ett värdepappersföretag, såsom risker för kunder, marknadsrisker, företagsrisker, operativa risker (inbegripet rättsliga risker och it-risker) och anseenderisker, i syfte att bedöma strategiernas lämplighet i förhållande till den godkända riskstrategin och riskaptiten,

d. ge ledningsorganet i dess tillsynsfunktion rekommendationer om nödvändiga anpassningar av riskstrategin som krävs till följd av bland annat förändringar i värdepappersföretagets affärsmodell, marknadsutvecklingen eller rekommendationer från riskhanteringsfunktionen,

e. ge råd om utnämningen av externa konsulter som tillsynsfunktionen kan komma att anlita för rådgivning eller stöd,

f. se över ett antal möjliga scenarier, inklusive stresscenarier, för att bedöma hur värdepappersföretagets riskprofil skulle reagera på externa och interna händelser,

g. övervaka överensstämmelsen mellan alla väsentliga finansiella instrument och tjänster som erbjuds kunder och värdepappersföretagets affärsmodell och riskstrategi; riskkommittén ska, i de fall en sådan inrättats, bedöma vilka risker som föreligger med de finansiella instrument och tjänster som erbjuds och beakta överensstämmelsen mellan priset på dessa produkter och tjänster och den vinst de inbringar,

h. bedöma rekommendationerna från interna eller externa revisorer och följa upp genomförandet av vidtagna åtgärder.

60. Riskkommittén ska samarbeta med andra kommittéer vars verksamhet kan ha en inverkan på riskstrategin (t.ex. ersättningskommittén, om en sådan inrättats) och regelbundet kommunicera med värdepappersföretagets interna kontrollfunktioner, särskilt riskhanteringsfunktionen.

Avdelning III – styrningsram

6 Organisatorisk ram och struktur

6.1 Organisatorisk ram

61. Ledningsorganet i ett värdepappersföretag ska säkerställa en lämplig och transparent organisatorisk och operativ struktur för värdepappersföretaget och ska ha en skriftlig beskrivning av denna. Strukturen ska främja och påvisa en effektiv och ansvarsfull ledning av värdepappersföretaget på enskild nivå och på gruppnivå.

62. Ledningsorganet ska se till att de interna kontrollfunktionerna har de lämpliga ekonomiska resurserna, personalresurserna och befogenheterna som behövs för att de ska kunna fullgöra sina uppgifter på ett effektivt sätt. Som ett minsta krav ska funktionen för regelefterlevnad fungera oberoende och det ska finnas en lämplig åtskillnad mellan funktioner. Rapporteringsvägarna och ansvarsfördelningen inom värdepappersföretaget, särskilt mellan personer som innehar nyckelfunktioner, ska vara tydliga, väldefinierade, sammanhängande, verkställbara och vederbörligen dokumenterade. Dokumentationen ska uppdateras när så är lämpligt.

63. Värdepappersföretagets struktur ska inte utgöra ett hinder för ledningsorganets förmåga att effektivt övervaka och hantera de risker som värdepappersföretaget eller koncernen ställs inför, eller den behöriga myndighetens förmåga att utöva effektiv tillsyn över värdepappersföretaget.

64. Ledningsorganet ska bedöma om och hur väsentliga förändringar av koncernens struktur (t.ex. inrättande av nya dotterföretag, fusioner och förvärv, försäljning eller likvidation av delar av koncernen eller extern utveckling) påverkar sundheten i värdepappersföretagets organisatoriska ram. Om brister konstateras ska ledningsorganet snabbt göra nödvändiga anpassningar.

6.2 Känna till strukturen

65. Ledningsorganet ska ha full kännedom om och förstå värdepappersföretagets juridiska, organisatoriska och operativa struktur (”känna till strukturen”) och se till att den överensstämmer med företagets godkända affärs- och riskstrategi och riskaptit samt att den innefattas i dess riskhanteringsram.

66. Ledningsorganet ska vara ansvarigt för att godkänna sunda strategier och policyer för inrättandet av nya strukturer. Om ett värdepappersföretag upprättar flera juridiska enheter inom sin koncern ska deras antal och, i synnerhet, sammanlänkningarna och transaktionerna mellan enheterna inte medföra svårigheter för utformningen av den interna styrningen eller för den effektiva hanteringen och tillsynen av riskerna för koncernen som helhet. Ledningsorganet ska säkerställa att värdepappersföretagets struktur och, i tillämpliga fall,

strukturerna inom koncernen, med beaktande av de kriterier som anges i avsnitt 7, är tydliga, effektiva och transparenta för värdepappersföretagets personal, aktieägare och andra intressenter samt för de behöriga myndigheterna.

67. Ledningsorganet ska vägleda värdepappersföretagets struktur, utveckling och begränsningar samt ska säkerställa att strukturen är motiverad och ändamålsenlig och att den inte medför otillbörlig eller olämplig komplexitet.

68. Ledningsorganet i ett moderföretag inom unionen ska inte bara förstå koncernens juridiska, organisatoriska och operativa struktur, utan även dess olika enheters syften och verksamheter samt förbindelserna och förhållandena mellan dem. Detta inbegriper kännedom om koncernspecifika operativa risker och koncerninterna exponeringar samt hur koncernens finansierings-, kapital-, likviditets- och riskprofiler skulle kunna påverkas under såväl normala som ogynnsamma omständigheter. Ledningsorganet ska säkerställa att modervärdepappersföretaget, inom skälig tid, kan ta fram information om koncernen gällande former, egenskaper, organisationsplan, ägarstruktur och verksamhet hos varje juridisk enhet, och om att de värdepappersföretag som ingår i koncernen uppfyller alla krav på tillsynsrapportering på enskild nivå och på gruppnivå.

69. Ledningsorganet i ett moderföretag inom unionen ska säkerställa att de olika koncernenheterna (inbegripet moderföretaget inom unionen självt) får tillräcklig information för att ha en klar uppfattning om koncernens allmänna mål, strategier och riskprofil samt om hur den berörda koncernenheten är integrerad i koncernens struktur och operativa verksamhet. Sådan information, och eventuella revideringar av den, ska dokumenteras och göras tillgänglig för de berörda funktionerna, inbegripet ledningsorganet, affärsområdena och de interna kontrollfunktionerna. Ledamöterna i ledningsorganet i ett moderföretag inom unionen ska hålla sig informerade om de risker som koncernens struktur medför, med beaktande av de kriterier som anges i avsnitt 7 i riktlinjerna. Detta inbegriper att inhämta

    a. information om betydande riskfaktorer,

    b. regelbundna rapporter om bedömning av värdepappersföretagets övergripande struktur och utvärdering av överensstämmelsen mellan enskilda enheters verksamhet och den godkända koncernstrategin,

    c. regelbundna rapporter om frågor där regelverket kräver efterlevnad på enskild nivå och på gruppnivå.

6.3 Komplexa strukturer och icke-standardiserade eller icke-transparenta verksamheter

70. Värdepappersföretag ska undvika att inrätta komplexa strukturer som kan försvåra insynen. Värdepappersföretag ska i sitt beslutsfattande ta hänsyn till resultaten av en riskanalys som utförts för att undersöka huruvida de aktuella strukturerna skulle kunna utnyttjas i samband

med penningtvätt, finansiering av terrorism eller annan ekonomisk brottslighet samt till de kontroller och den lagstiftning som finns på området [17] . I detta avseende ska värdepappersföretagen som minst beakta följande:

a. I vilken utsträckning den jurisdiktion där strukturen ska inrättas effektivt efterlever EU-standarder och internationella standarder för skatteinsyn samt bekämpning av penningtvätt och finansiering av terrorism[18].

b. I vilken utsträckning strukturen har ett tydligt ekonomiskt och lagligt syfte.

c. I vilken utsträckning strukturen skulle kunna användas för att dölja identiteten på den verkliga huvudmannen.

d. I vilken utsträckning den av kundens begäran som leder till ett eventuellt inrättande av en struktur ger upphov till betänkligheter.

e. Huruvida strukturen kan hindra värdepappersföretagets ledningsorgan från att få vederbörlig översyn eller begränsa värdepappersföretagets förmåga att hantera den relaterade risken.

f. Huruvida strukturen utgör ett hinder för de behöriga myndigheternas effektiva tillsyn.

71. Under alla omständigheter ska värdepappersföretag inte inrätta svåröverblickbara eller onödigt komplexa strukturer som saknar tydlig ekonomisk grund eller juridiskt syfte, eller strukturer som kan ge upphov till misstanke om att de inrättas för ändamål som är kopplade till ekonomisk brottslighet.

72. När sådana strukturer inrättas ska ledningsorganet förstå dem och deras syfte samt de särskilda risker som är förknippade med dem, och se till att de interna kontrollfunktionerna är delaktiga på lämpligt sätt. Dessa strukturer ska godkännas och upprätthållas endast när deras syfte har definierats tydligt och förståtts och när ledningsorganet är förvissat om att alla väsentliga risker, inbegripet anseenderisker, har identifierats, att alla risker kan hanteras effektivt och rapporteras korrekt samt att en effektiv tillsyn har säkerställts. Ju mer komplex och svåröverblickbar den organisatoriska och operativa strukturen är, och ju större riskerna är, desto mer ingående ska tillsynen av strukturen vara.

[17] För närmare uppgifter om bedömningen av landspecifik risk och den risk som är förknippad med enskilda produkter och kunder ska värdepappersföretagen även läsa de gemensamma riktlinjerna för riskfaktorer för penningtvätt och finansiering av terrorism (EBA GL JC/2017/37) som för närvarande ses över.

[18] Se även kommissionens delegerade förordning (EU) 2019/758 av den 31 januari 2019 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/849 med avseende på tekniska tillsynsstandarder som fastställer minimiåtgärder och ytterligare åtgärder som kreditinstitut och finansiella institut ska vidta för att minska risken för penningtvätt och finansiering av terrorism i vissa tredjeländer: 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.

73. Värdepappersföretag ska dokumentera sina beslut och ska kunna motivera besluten för de behöriga myndigheterna.

74. Ledningsorganet ska se till att lämpliga åtgärder vidtas för att undvika eller minska de risker som verksamheten inom sådana strukturer medför. I detta ingår att säkerställa följande:

    a. Att värdepappersföretaget har fastställda policyer och förfaranden samt dokumenterade processer (t.ex. tillämpliga gränser och informationsflöden) för beaktandet, regelefterlevnaden, godkännandet och riskhanteringen av sådan verksamhet, och att hänsyn tas till konsekvenserna för koncernens organisatoriska och operativa struktur, riskprofil och anseenderisk.

    b. Att information om denna verksamhet och dess risker är tillgänglig för moderföretaget i unionen samt för interna och externa revisorer och att den rapporteras till ledningsorganet i dess tillsynsfunktion samt till den behöriga myndighet som beviljat auktorisation.

    c. Att värdepappersföretaget regelbundet utvärderar det fortsatta behovet av att upprätthålla sådana strukturer.

75. Dessa strukturer och verksamheter, inbegripet deras efterlevnad av lagstiftning och yrkesstandarder, ska ses över regelbundet. Om en internrevisionsfunktion har inrättats ska den genomföra översynen utifrån en riskbaserad metod.

76. Värdepappersföretag ska vidta effektiva riskhanteringsåtgärder när de utför icke-standardiserade eller icke-transparenta uppgifter åt kunder (t.ex. hjälpa kunder att inrätta instrument i offshore-jurisdiktioner, utveckla komplexa strukturer, underlätta transaktioner eller tillhandahålla förvaltartjänster) som medför snarlika interna styrningsutmaningar och innebär betydande operativa risker och anseenderisker. I synnerhet ska värdepappersföretag analysera varför en kund vill inrätta en viss struktur.

7 Organisatorisk ram i ett koncernsammanhang

77. I enlighet med artikel 25 i direktiv (EU) 2019/2034 och artikel 7 i förordning (EU) 2019/2033, och såvida inte artikel 8 i förordning (EU) 2019/2033 tillämpas av de behöriga myndigheterna, ska moderföretag inom unionen och deras dotterföretag som omfattas av direktiv (EU) 2019/2034 säkerställa att styrningsformer, processer och mekanismer är konsekventa och väl integrerade på gruppnivå. Detta innebär att företag och dotterföretag som omfattas av konsolidering under tillsyn ska genomföra sådana former, processer och mekanismer i de av sina dotterföretag som inte omfattas av direktiv (EU) 2019/2034, inbegripet sådana som är etablerade i tredjeländer, inklusive i finansiella offshore-centrum, för att säkerställa robusta styrningsformer på gruppnivå. Behöriga funktioner i moderföretaget inom unionen och dess dotterföretag ska samverka och utbyta data och information när så är lämpligt. Styrningsformerna, processerna och mekanismerna ska säkerställa att moderföretaget inom

unionen har tillräckliga data och tillräcklig information för att kunna bedöma den koncernövergripande riskprofilen enligt den information som ges i avsnitt 6.2.

78. Ledningsorganet i ett dotterföretag som omfattas av direktiv (EU) 2019/2034 ska på enskild nivå anta och genomföra de koncernövergripande policyer för företagsstyrning som fastställts på gruppnivå på ett sätt som uppfyller alla specifika krav enligt unionsrätt och nationell rätt.

79. På gruppnivå ska moderföretaget inom unionen säkerställa att alla värdepappersföretag och andra enheter som omfattas av konsolidering under tillsyn, inbegripet de dotterföretag som inte omfattas av direktiv (EU) 2019/2034, följer de koncernövergripande policyerna för företagsstyrning och ramen för intern kontroll som avses i avdelning V. När moderföretaget inom unionen införlivar styrningspolicyer ska det se till att det finns robusta styrningsformer hos varje dotterföretag och överväga särskilda styrningsformer, processer och mekanismer för områden där affärsverksamheten inte är organiserad i separata juridiska enheter utan i en uppsättning affärsområden som omfattar flera juridiska enheter.

80. Ett moderföretag inom unionen ska beakta alla dess dotterföretags intressen och hur strategier och policyer inverkar på varje dotterföretags intressen samt den övergripande koncernens intressen på lång sikt.

81. Ett moderföretag inom unionen och dess dotterföretag ska säkerställa att de värdepappersföretag och enheter som ingår i koncernen uppfyller alla specifika lagstadgade krav i de relevanta jurisdiktionerna.

82. Moderföretaget inom unionen ska säkerställa att de dotterföretag som är etablerade i tredjeländer och som omfattas av konsolidering under tillsyn har styrningsformer, processer och mekanismer som är förenliga med de koncernövergripande styrningspolicyerna och uppfyller kraven i artiklarna 25–32 i direktiv (EU) 2019/2034 samt dessa riktlinjer, så länge detta inte strider mot lagen i det berörda tredjelandet.

83. Styrningskraven i direktiv (EU) 2019/2034 och bestämmelserna i dessa riktlinjer gäller för värdepappersföretag som är belägna i EU, oaktat om de är dotterföretag till ett moderföretag i ett tredjeland. I de fall ett EU-dotterföretag till ett moderföretag i ett tredjeland är ett moderföretag inom unionen, omfattar konsolideringen under tillsyn inom EU inte det modervärdepappersföretag som är beläget i ett tredjeland och andra direkta dotterföretag till detta moderföretag. Moderföretaget inom unionen ska säkerställa att de koncernövergripande styrningspolicyerna för modervärdepappersföretaget i ett tredjeland beaktas i dess egna styrningspolicyer, förutsatt att detta inte strider mot kraven i relevant unionsrätt, inbegripet direktiv (EU) 2019/2034 och de ytterligare kraven i dessa riktlinjer.

84. När värdepappersföretag fastställer policyer och dokumenterar styrningsformer ska de ta hänsyn till de aspekter som förtecknas i bilaga I. Policyer och dokumentation får redogöras för i separata dokument, men värdepappersföretagen bör överväga att sammanställa dessa eller hänvisa till dem i ett enhetligt ramdokument för styrning.

Avdelning IV – riskkultur och företagande

8 Riskkultur

85. En sund, omsorgsfull och konsekvent riskkultur ska vara ett väsentligt inslag i värdepappersföretagens effektiva riskhantering och ska göra det möjligt för värdepappersföretagen att fatta sunda och välgrundade beslut.

86. Värdepappersföretag ska utarbeta en integrerad och företagsövergripande riskkultur som bygger på fullständig kännedom om och en helhetssyn på de risker de ställs inför, inbegripet risker för kunder och för marknader, risker för värdepappersföretaget självt och likviditetsrisker, särskilt sådana som kan ha en väsentlig inverkan på eller uttömma de tillgängliga kapitalbaserna och hur de hanteras, med beaktande av värdepappersföretagets riskkapacitet och riskaptit.

87. Värdepappersföretag ska utarbeta en riskkultur genom policyer, kommunikation och personalutbildning som rör värdepappersföretagets verksamhet, strategi och riskprofil, och ska anpassa kommunikationen och personalutbildningen utifrån personalens skyldigheter när det gäller risktagande och riskhantering.

88. Personalen ska ha full kännedom om sina ansvarsområden och skyldigheter avseende riskhantering. Riskhanteringen ska inte skötas av enbart riskspecialister eller interna kontrollfunktioner. Affärsenheter ska, under överinseende av ledningsorganet, ha huvudansvaret för den dagliga hanteringen av risker i enlighet med värdepappersföretagets policyer, förfaranden och kontroller, och hänsyn ska tas till värdepappersföretagets riskaptit och riskkapacitet.

89. En stark riskkultur ska innefatta, men är inte nödvändigtvis begränsad till, följande:

    a. Ledningens exempel: ledningsorganet ska ansvara för att fastställa och förmedla värdepappersföretagets kärnvärden och förväntningar. Ledningsorganets ledamöter ska uppföra sig på ett sätt som återspeglar dessa värden. Värdepappersföretagets ledning, inbegripet personer som innehar nyckelfunktioner, ska bidra till att företagets kärnvärden och förväntningar förmedlas internt till personalen. Personalen ska agera i enlighet med alla tillämpliga lagar och bestämmelser och omgående vidarebefordra information om bristande efterlevnad som konstateras inom eller utanför värdepappersföretaget (t.ex. till den behöriga myndigheten genom ett förfarande för rapportering av överträdelser, så kallad visselblåsning). Ledningsorganet ska fortlöpande främja, övervaka och bedöma värdepappersföretagets riskkultur och beakta riskkulturens inverkan på företagets finansiella stabilitet, riskprofil och robusta styrning samt göra anpassningar när så är nödvändigt.

    b. Ansvarighet: berörd personal på alla nivåer ska känna till och förstå värdepappersföretagets kärnvärden och, i den mån deras roll kräver det, dess riskaptit och riskkapacitet. De ska kunna fullgöra sina uppgifter och vara medvetna om att de

kommer att hållas ansvariga för sina handlingar i förhållande till värdepappersföretagets risktagande och riskbeteende.

c. Effektiv kommunikation och ifrågasättande: en sund riskkultur ska främja ett klimat med öppen kommunikation och effektivt ifrågasättande där beslutsprocesserna gynnar ett brett spektrum av åsikter, ger möjlighet att utmana gällande praxis, uppmuntrar ett konstruktivt och kritiskt förhållningssätt hos personalen och främjar ett klimat präglat av öppet och konstruktivt engagemang i hela organisationen.

d. Incitament: lämpliga incitament ska vara en central del i arbetet med att anpassa risktagande och riskbeteende så att de överensstämmer med värdepappersföretagets riskprofil och dess långsiktiga intressen[19].

9 Företagsvärden och uppförandekod

90. Ledningsorganet ska utveckla, anta, följa och främja höga etiska och yrkesmässiga standarder, med beaktande av värdepappersföretagets särskilda behov och särdrag, och ska se till att sådana standarder införlivas (genom en uppförandekod eller ett liknande instrument). Ledningsorganet ska även övervaka att dessa standarder följs av personalen. När så är tillämpligt får ledningsorganet anta och införliva värdepappersföretagets koncernövergripande standarder eller gemensamma standarder som publiceras av branschföreningar eller andra relevanta yrkesorganisationer.

91. Värdepappersföretag ska säkerställa att det inte förekommer någon diskriminering av personal på grund av kön, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuell läggning.

92. Värdepappersföretagens policyer ska vara könsneutrala. Detta inkluderar men är inte begränsat till ersättning, rekryteringspolicyer, karriärutveckling och efterträdarplanering, tillgång till utbildning och möjligheten att söka interna lediga tjänster. Instituten ska säkerställa lika möjligheter[20] för all personal oavsett kön, bland annat när det gäller karriärmöjligheter, och söka förbättra representationen av det underrepresenterade könet i befattningar inom ledningsorganet samt gruppen av anställda som har ledningsansvar enligt definitionen i kommissionens delegerade förordning (tekniska tillsynsstandarder om identifierad personal). Värdepappersföretag ska övervaka tendenser i löneskillnader mellan könen. I de fall ett värdepappersföretag har 50 eller fler anställda[21] ska övervakningen av löneskillnader mellan könen ske separat för identifierad personal (undantaget ledningsorganets ledamöter), ledamöter i ledningsorganet i dess ledningsfunktion, ledamöter

[19] Se även EBA:s riktlinjer för en sund ersättningspolicy enligt direktiv (EU) 2019/2034.

[20] Se även Europaparlamentets och rådets direktiv 2006/54/EG av den 5 juli 2006 om genomförandet av principen om lika möjligheter och likabehandling av kvinnor och män i arbetslivet.

[21] Se även EBA:s riktlinjer för en sund ersättningspolicy enligt direktiv (EU) 2019/2034.

i ledningsorganet i dess tillsynsfunktion och övrig personal. Värdepappersföretag ska ha policyer som underlättar återintegrering av personal efter föräldraledighet.[22]

93. De standarder som införlivas ska syfta till att förbättra värdepappersföretagets robusta styrningsformer och minska den risk som värdepappersföretaget är exponerat för, särskilt operativa risker och anseenderisker, som kan ha en betydande negativ inverkan på värdepappersföretagets lönsamhet och hållbarhet genom böter, rättegångskostnader, restriktioner som åläggs av behöriga myndigheter, andra ekonomiska och straffrättsliga påföljder samt förlust av varumärkesvärde och konsumenternas förtroende.

94. Ledningsorganet ska ha tydliga och dokumenterade policyer för hur dessa standarder ska uppfyllas. Syftet med dessa ska vara att

    a. påminna personalen om att all verksamhet inom värdepappersföretaget ska bedrivas i enlighet med tillämplig lagstiftning och värdepappersföretagets företagsvärden,

    b. främja riskmedvetenhet genom en stark riskkultur som är förenlig med avsnitt 9 i riktlinjerna och som förmedlar ledningsorganets förväntning om att verksamheten inte ska gå utöver den fastställda riskaptit och de gränser som gäller för värdepappersföretaget och personalens respektive ansvarsområden,

    c. föreskriva principer för och ge exempel på acceptabelt och oacceptabelt beteende, i synnerhet när det gäller felaktig finansiell rapportering och misskötsamhet samt ekonomisk och finansiell brottslighet, inklusive men inte begränsat till bedrägeri, penningtvätt och finansiering av terrorism, metoder för konkurrensbegränsande samverkan, finansiella sanktioner, mutbrott och korruption, otillbörlig marknadspåverkan, vilseledande försäljning och andra överträdelser av konsumentskyddslagstiftning samt skattebrott, oavsett om dessa begås direkt eller indirekt, inbegripet genom olagliga eller förbjudna system för utdelningsarbitrage,

    d. klargöra att personalen utöver att uppfylla de krav som ställs i lagar, förordningar och interna policyer också förväntas uppföra sig med ärlighet och integritet och utföra sina uppgifter med vederbörlig skicklighet, omsorg och aktsamhet,

    e. se till att personalen är medveten om de potentiella interna och externa disciplinära åtgärderna, rättsliga åtgärderna och sanktionerna som kan följa av tjänstefel och oacceptabla beteenden.

95. Värdepappersföretag ska övervaka efterlevnaden av sådana standarder och se till att personalen har kännedom om dem, t.ex. genom att tillhandahålla utbildning. Värdepappersföretag ska ange vilken funktion som är ansvarig för att övervaka efterlevnad och utvärdera överträdelser av uppförandekoden eller liknande instrument och fastställa ett

[22] Se även EBA:s riktlinjer för en sund ersättningspolicy enligt direktiv (EU) 2019/2034.

förfarande för att hantera bristande efterlevnad. Resultaten ska regelbundet rapporteras till ledningsorganet.

10 Policy om intressekonflikter på företagsnivå

96. Ledningsorganet ska vara ansvarigt för att fastställa, godkänna och övervaka genomförandet och upprätthållandet av effektiva policyer som syftar till att identifiera, bedöma, hantera och mildra eller förebygga faktiska och potentiella intressekonflikter på företagsnivå, däribland intressekonflikter som uppstår på grund av värdepappersföretagets olika verksamheter och roller, olika värdepappersföretag som omfattas av konsolidering under tillsyn, olika affärsområden eller enheter inom värdepappersföretaget eller i förhållande till externa intressenter. När värdepappersföretag fastställer dessa policyer ska de vara uppmärksamma på att policyerna också måste vara förenliga med artiklarna 16.3 och 23 i direktiv 2014/65/EU samt artiklarna 33–35 i kommissionens delegerade förordning (EU) 2017/565.

97. Värdepappersföretagens åtgärder för att hantera eller, i tillämpliga fall, mildra intressekonflikter ska dokumenteras och ska bland annat omfatta följande:

    a. En lämplig åtskillnad mellan funktioner, exempelvis genom att ge olika personer ansvaret för oförenliga uppgifter inom hanteringen av transaktioner eller tillhandahållandet av tjänster, eller anförtro tillsyns- och rapporteringsansvar för oförenliga verksamheter till olika personer.

    b. Inrättande av informationshinder, t.ex. genom att fysiskt skilja vissa affärsområden eller enheter åt.

11 Policy om intressekonflikter för personal[23]

98. Utan att det påverkar tillämpningen av artikel 23 i direktiv 2014/65/EU och avsnitt 3 i kapitel 2 i kommissionens delegerade förordning (EU) 2017/565 ska ledningsorganet vara ansvarigt för att fastställa, godkänna och övervaka genomförandet och upprätthållandet av effektiva policyer som syftar till att identifiera, bedöma, hantera och mildra eller förebygga faktiska och potentiella konflikter mellan värdepappersföretagets intressen och personalens privata intressen, inbegripet ledningsorganets ledamöter, som skulle kunna inverka negativt på personalens utförande av sina uppgifter och skyldigheter. Ett moderföretag inom unionen ska beakta intressen inom en koncernövergripande policy om intressekonflikter på gruppnivå.

99. Syftet med policyn ska vara att identifiera intressekonflikter hos personal, inbegripet personalens närmaste familjemedlemmars intressen. Värdepappersföretag ska ta hänsyn till att intressekonflikter inte enbart kan uppstå till följd av nuvarande personliga och yrkesmässiga relationer utan även till följd av tidigare sådana. Om intressekonflikter uppstår

[23] Detta avsnitt ska läsas mot bakgrund av Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare enligt direktiv 2013/36/EU och direktiv 2014/65/EU.

ska värdepappersföretaget bedöma konflikternas väsentlighet och, när så är lämpligt, besluta om och vidta mildrande åtgärder.

100. När det gäller intressekonflikter som kan uppstå till följd av tidigare relationer ska värdepappersföretaget fastställa en lämplig tidsram under vilken personalen måste rapportera sådana intressekonflikter, eftersom dessa fortfarande kan påverka personalens beteende och roll i beslutsfattandet.

101. Policyn ska som minst omfatta följande situationer eller relationer där intressekonflikter kan uppstå:

    a. Ekonomiska intressen (t.ex. aktier, andra äganderätter och medlemskap, finansiella innehav och andra ekonomiska intressen i företagskunder, immateriella rättigheter, medlemskap i ett organ eller ägandeförhållande i ett organ eller en enhet med motstridiga intressen).

    b. Personliga eller yrkesmässiga relationer med ägarna av kvalificerade innehav i värdepappersföretaget.

    c. Personliga eller yrkesmässiga relationer med personal i de värdepappersföretag eller enheter som omfattas av konsolidering under tillsyn (t.ex. familjeband).

    d. Andra anställningar och tidigare anställningar i nära förfluten tid (t.ex. fem år bakåt).

    e. Personliga eller yrkesmässiga relationer med relevanta externa intressenter (t.ex. samröre med betydande leverantörer, konsultföretag eller andra tjänsteleverantörer).

    f. Politiskt inflytande eller politiska förbindelser.

102. Oaktat det som anges ovan, om en anställd är aktieägare i ett värdepappersföretag eller använder sig av andra tjänster som erbjuds av ett sådant företag ska värdepappersföretaget inte betrakta detta som en situation där en intressekonflikt föreligger så länge den anställdas intresse bibehålls inom en lämplig minimigräns.

103. Policyn ska beskriva förfarandena för rapportering och kommunikation till den funktion som ansvarar för frågor om intressekonflikter. Personalen ska vara skyldig att utan dröjsmål rapportera internt om alla situationer som kan leda till, eller redan har lett till, en intressekonflikt.

104. Policyn ska skilja mellan bestående intressekonflikter som måste hanteras permanent och intressekonflikter som uppstår oväntat i samband med en enskild händelse (t.ex. en transaktion eller ett val av en tjänsteleverantör) och som normalt kan hanteras genom en engångsåtgärd. Under alla omständigheter ska värdepappersföretagets intressen stå i centrum för de beslut som fattas.

105. Policyn ska innehålla förfaranden, åtgärder, dokumentationskrav och skyldigheter beträffande identifiering och förebyggande av intressekonflikter, bedömning av deras väsentlighet och vidtagande av mildrande åtgärder. Sådana förfaranden, krav, skyldigheter och åtgärder ska omfatta att

    a. ge olika personer ansvaret för oförenliga uppgifter eller transaktioner,

    b. förhindra att personal som är delaktig i verksamhet utanför värdepappersföretaget har olämpligt inflytande inom värdepappersföretaget när det gäller dessa andra verksamheter,

    c. inrätta en regel som föreskriver att ledningsorganets ledamöter ska avstå från att rösta i alla frågor där ledamoten har eller kan ha en intressekonflikt eller där ledamotens objektivitet eller förmåga att fullgöra sina skyldigheter gentemot värdepappersföretaget på annat sätt kan vara äventyrad,

    d. förhindra att ledamöter i ledningsorganet innehar ledningsfunktioner i konkurrerande värdepappersföretag.

106. Policyn ska särskilt behandla risken för intressekonflikter på ledningsorganets nivå och ge tillräcklig vägledning om identifiering och hantering av intressekonflikter som kan hindra ledningsorganets ledamöter från att fatta objektiva och opartiska beslut vilka syftar till att tillgodose värdepappersföretagets intressen. Värdepappersföretag ska ta i beaktande att intressekonflikter kan påverka oavhängigheten hos ledningsorganets ledamöter[24].

107. När värdepappersföretag mildrar konstaterade intressekonflikter hos ledamöter i ledningsorganet ska de dokumentera de åtgärder som vidtagits samt en motivering för på vilket sätt åtgärderna är effektiva när det gäller att säkerställa objektivt beslutsfattande.

108. Faktiska eller potentiella intressekonflikter som har rapporterats till den ansvariga funktionen inom värdepappersföretaget ska bedömas och hanteras på lämpligt sätt. Om en intressekonflikt hos personalen konstateras ska värdepappersföretaget dokumentera det beslut som fattats, särskilt om intressekonflikten och de risker som den medför har godtagits, samt hur konflikten, om den har godtagits, på ett tillfredsställande sätt har mildrats eller avhjälpts.

109. Alla faktiska och potentiella intressekonflikter på ledningsorganets nivå, både enskilda och kollektiva sådana, ska dokumenteras på lämpligt sätt och förmedlas till ledningsorganet, varpå ledningsorganet ska föra en diskussion och fatta beslut om dem samt hantera dem på vederbörligt sätt.

[24] Se även Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare enligt direktiv 2013/36/EU och direktiv 2014/65/EU.

11.1 Policy om intressekonflikter i samband med lån och andra transaktioner med ledamöter i ledningsorganet och deras närstående parter

110. Som en del av policyn om intressekonflikter för personal (avsnitt 11) och hanteringen av intressekonflikter hos ledamöter i ledningsorganet enligt punkt 107 ska ledningsorganet inrätta en ram för att identifiera och hantera intressekonflikter i samband med beviljandet av lån och genomförandet av andra transaktioner, t.ex. börsintroduktioner, tjänsteavtal eller utkontrakteringsavtal, med ledamöter i ledningsorganet och deras närstående parter.

111. Värdepappersföretag ska överväga ytterligare kategorier av närstående parter som helt eller delvis ska omfattas av ramen för intressekonflikter när det gäller lån och transaktioner.

112. Ramen för intressekonflikter ska säkerställa att beslut som rör lån och genomförandet av andra transaktioner med ledamöter i ledningsorganet och deras närstående parter fattas objektivt och utan otillbörlig inverkan av intressekonflikter, samt att sådan verksamhet i regel sker på rent affärsmässiga villkor.

113. Ledningsorganet ska inrätta tillämpliga beslutsprocesser för beviljandet av lån och genomförandet av andra transaktioner med ledamöter i ledningsorganet och deras närstående parter. Ramen får föreskriva en åtskillnad mellan vanliga affärstransaktioner[25] som genomförs inom ramen för den normala affärsverksamheten enligt sedvanliga marknadsvillkor, och personaltransaktioner som genomförs enligt villkor som är tillgängliga för all personal. Vidare får ramen för intressekonflikter och beslutsprocessen skilja mellan väsentliga och icke-väsentliga lån eller andra väsentliga transaktioner, olika typer av lån och andra transaktioner samt graden av faktiska eller potentiella intressekonflikter som de kan medföra.

114. I ramen för intressekonflikter ska ledningsorganet fastställa lämpliga gränsvärden (t.ex. per produkttyp, volym eller utifrån gällande villkor) över vilka transaktionen med en ledamot i ledningsorganet eller dess närstående parter alltid kräver ledningsorganets godkännande. Beslut som rör väsentliga lån och andra väsentliga transaktioner med ledamöter i ledningsorganet, som inte genomförs enligt sedvanliga marknadsvillkor utan enligt villkor som är tillgängliga för all personal, ska alltid fattas av ledningsorganet.

115. Den ledamot i ledningsorganet som gynnas av ett sådant väsentligt lån eller annan väsentlig transaktion, eller den ledamot som är knuten till motparten, ska inte vara delaktig i beslutsprocessen.

[25] Affärstransaktioner innefattar leasing av lån, factoring, tjänster i samband med börsintroduktioner, fusioner och förvärv samt försäljning och köp av fast egendom.

116. När beslut ska fattas om ett lån eller annan transaktion med en ledamot i ledningsorganet eller dess närstående parter ska värdepappersföretaget, innan det fattar ett beslut, bedöma den risk som värdepappersföretaget kan exponeras för till följd av transaktionen.

117. För att säkerställa efterlevnad av policyerna om intressekonflikter ska värdepappersföretaget se till att alla relevanta interna kontrollförfaranden tillämpas fullt ut på lån och andra transaktioner med ledamöter i ledningsorganet eller deras närstående parter, och att det finns en lämplig tillsynsram hos ledningsorganet i dess tillsynsfunktion.

11.2 Dokumentation av lån till ledamöter i ledningsorganet och deras närstående parter samt ytterligare information

118. Vid tillämpningen av artikel 26 i direktiv (EU) 2019/2034 ska värdepappersföretag dokumentera uppgifter om lån till ledamöter i ledningsorganet och deras närstående parter på ett korrekt sätt. Informationen ska åtminstone inbegripa

a. låntagarens namn och ställning (dvs. ledamot i ledningsorganet eller närstående part) och, när det gäller lån till en närstående part, den ledamot i ledningsorganet till vilken parten är närstående och karaktären av relationen till den närstående parten,

b. lånets typ/form och belopp,

c. villkor som gäller för lånet,

d. datum för godkännande av lånet,

e. namnet på den person, eller det organ och dess sammansättning, som fattat beslutet om att godkänna lånet och de gällande villkoren,

f. huruvida lånet har beviljats enligt marknadsvillkor (ja/nej),

g. huruvida lånet har beviljats enligt villkor som är tillgängliga för all personal (ja/nej).

119. Värdepappersföretag ska se till att dokumentationen av alla lån till ledamöter i ledningsorganet och deras närstående parter är fullständig och aktuell och att värdepappersföretaget på begäran kan göra den fullständiga dokumentationen tillgänglig för de behöriga myndigheterna i ett lämpligt format och utan onödigt dröjsmål.

12 Interna förfaranden för uppgiftslämning

120. Värdepappersföretag ska införa och upprätthålla lämpliga interna policyer och förfaranden för uppgiftslämning så att personalen kan rapportera potentiella eller faktiska överträdelser av förordning (EU) 2019/2033 och nationella bestämmelser som införlivar direktiv (EU) 2019/2034 genom en särskild, oberoende och fristående kanal. Personalen ska inte behöva ha bevis för en överträdelse för att rapportera den, men de bör ha en grad av säkerhet som ger tillräckliga skäl för att inleda en utredning. Värdepappersföretag ska även införa lämpliga processer och förfaranden som säkerställer att de fullgör sina skyldigheter enligt det nationella genomförandet av Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten.

121. För att undvika intressekonflikter ska det vara möjligt för personalen att rapportera överträdelser utanför sedvanliga rapporteringsvägar (t.ex. genom funktionen för regelefterlevnad, internrevisionsfunktionen eller ett oberoende internt förfarande för rapportering av överträdelser). Förfarandena för uppgiftslämning ska säkerställa att personuppgifterna om både den person som rapporterar överträdelsen och den fysiska person som påstås vara ansvarig för överträdelsen skyddas, i enlighet med förordning (EU) 2016/679[26] (allmänna dataskyddsförordningen).

122. Förfarandena för uppgiftslämning ska göras tillgängliga för all personal i ett värdepappersföretag.

123. Information som lämnas av personalen genom förfarandena för uppgiftslämning ska, om så är lämpligt, göras tillgänglig för ledningsorganet och andra ansvariga funktioner som förtecknas i den interna policyn för uppgiftslämning. När så krävs av den anställde som rapporterar en överträdelse ska informationen vidarebefordras till ledningsorganet och andra ansvariga funktioner i anonymiserad form. Värdepappersföretag får också inrätta ett förfarande för rapportering av överträdelser som gör det möjligt att lämna information anonymt.

124. Värdepappersföretag ska se till att den person som rapporterar överträdelsen skyddas på erforderligt sätt från eventuella negativa konsekvenser, t.ex. repressalier, diskriminering eller andra former av missgynnande behandling. Värdepappersföretag ska säkerställa att ingen person som står under värdepappersföretagets kontroll bestraffar en person som har rapporterat en överträdelse, och ska vidta lämpliga åtgärder mot personer som utför sådan bestraffning.

125. Värdepappersföretag ska också skydda personer som har rapporterats från eventuella negativa konsekvenser om utredningen inte finner några bevis som motiverar att åtgärder vidtas mot den personen. Om åtgärder vidtas ska värdepappersföretaget vidta dem på ett sätt som skyddar den berörda personen från oavsiktliga negativa konsekvenser som går utöver syftet med den vidtagna åtgärden.

[26] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

126. I synnerhet ska interna förfaranden för uppgiftslämning

a. dokumenteras (t.ex. i form av personalhandböcker),

b. omfatta tydliga regler som säkerställer att uppgifter om den som rapporterar en överträdelse, den som är föremål för rapporten samt överträdelsen behandlas konfidentiellt i enlighet med förordning (EU) 2016/679, såvida inte röjande av uppgifterna krävs enligt nationell lagstiftning i samband med ytterligare utredningar eller efterföljande rättsliga förfaranden,

c. skydda personal som lämnar uppgifter från att bestraffas till följd av att de har rapporterat överträdelser,

d. säkerställa att de potentiella eller faktiska överträdelser som rapporteras bedöms och vidarebefordras, inbegripet, när så är lämpligt, till den berörda behöriga myndigheten eller det berörda brottsbekämpande organet,

e. säkerställa, när så är möjligt, att bekräftelse på att informationen har mottagits lämnas till personal som har rapporterat potentiella eller faktiska överträdelser,

f. säkerställa att resultaten av utredningar av rapporterade överträdelser följs upp,

g. säkerställa att lämplig registerföring och dokumentation sker.

13 Rapportering av överträdelser till behöriga myndigheter

127. I enlighet med artikel 22 i direktiv (EU) 2019/2034 ska de behöriga myndigheterna inrätta ändamålsenliga och tillförlitliga mekanismer som gör det möjligt för värdepappersföretagens personal att rapportera potentiella eller faktiska överträdelser av förordning (EU) 2019/2033 och nationella bestämmelser som införlivar direktiv (EU) 2019/2034 till de behöriga myndigheterna. Dessa mekanismer ska som minst innefatta

a. särskilda förfaranden för mottagandet av rapporter om överträdelser och uppföljning, exempelvis en särskild avdelning, enhet eller funktion för rapportering av överträdelser,

b. lämpligt skydd enligt avsnitt 13,

c. skydd av personuppgifter om både den fysiska person som rapporterar överträdelsen och den fysiska person som påstås vara ansvarig för överträdelsen, i enlighet med förordning (EU) 2016/679 (allmänna dataskyddsförordningen),

d. tydliga förfaranden enligt avsnitt 12.

128. Utan att det påverkar möjligheten att rapportera överträdelser genom de behöriga myndigheternas mekanismer får de behöriga myndigheterna uppmuntra personalen att först försöka använda sig av värdepappersföretagens interna förfaranden för uppgiftslämning.

Avdelning V – ram och mekanismer för intern kontroll

14 Ram för intern kontroll

129. Värdepappersföretag ska utveckla och bibehålla en kultur som uppmuntrar en positiv inställning till riskkontroll och efterlevnad inom företaget samt en robust och heltäckande ram för intern kontroll. Enligt denna ram ska värdepappersföretagens affärsområden ansvara för att hantera de risker de ådrar sig i sin verksamhet och ha kontroller som syftar till att säkerställa efterlevnad av interna och externa krav. Som ett led i denna ram ska värdepappersföretag ha en permanent och effektiv intern funktion för regelefterlevnad[27] som har lämplig och tillräcklig auktoritet, ställning och tillgång till ledningsorganet för att kunna fullgöra sitt uppdrag, samt en ram för riskhantering. När det är proportionellt med hänsyn till de kriterier som anges i avdelning I ska värdepappersföretag också ha en intern riskhanterings- och revisionsfunktion.

130. Ramen för intern kontroll hos det berörda värdepappersföretaget ska anpassas i varje enskilt fall efter särdragen i företagets verksamhet, dess komplexitet och de förknippade riskerna, med beaktande av koncernens egenskaper. Det berörda värdepappersföretaget ska organisera utbytet av nödvändig information på ett sätt som säkerställer att varje ledningsorgan, affärsområde och intern enhet, inklusive varje intern kontrollfunktion, kan fullgöra sina uppgifter. Detta innebär bland annat ett nödvändigt utbyte av lämplig information mellan affärsområdena och funktionen för regelefterlevnad, och funktionen för bekämpning av penningtvätt och finansiering av terrorism om denna är en separat kontrollfunktion, på gruppnivå, samt mellan cheferna för de interna kontrollfunktionerna på gruppnivå och värdepappersföretagens ledningsorgan.

131. Värdepappersföretag ska införa lämpliga processer och förfaranden för att säkerställa att de fullgör sina skyldigheter när det gäller bekämpning av penningtvätt och finansiering av terrorism. Värdepappersföretag ska bedöma sin exponering för risken att de kan komma att nyttjas för penningtvätt och finansiering av terrorism och, när så är lämpligt, vidta åtgärder för att minska dessa risker samt de operativa risker och anseenderisker som följer därav. Värdepappersföretag ska vidta åtgärder som säkerställer att deras personal är medvetna om riskerna för penningtvätt och finansiering av terrorism samt den inverkan som penningtvätt och finansiering av terrorism har på värdepappersföretaget och det finansiella systemets integritet.

132. Ramen för intern kontroll ska omfatta hela organisationen, inklusive ledningsorganets ansvarsområden och uppgifter, samt verksamheten i alla affärsområden och interna enheter,

[27] Utan att det påverkar tillämpningen av artikel 22 i kommissionens delegerade förordning (EU) 2017/565.

inbegripet interna kontrollfunktioner, utkontrakterade verksamheter och distributionskanaler.

133. Ett värdepappersföretags ram för intern kontroll ska säkerställa

    a. ändamålsenlig och effektiv verksamhet,

    b. tillbörlig identifiering, mätning och reducering av risker,

    c. tillförlitligheten i finansiell och icke-finansiell information som rapporteras både internt och externt,

    d. sunda rutiner för administration och redovisning,

    e. efterlevnad av lagar, förordningar och tillsynskrav samt värdepappersföretagets interna policyer, processer, regler och beslut.

15 Genomförande av en ram för intern kontroll

134. Ledningsorganet ska ansvara för att upprätta och övervaka att ramen, processerna och mekanismerna för intern kontroll är tillräckliga och effektiva, samt övervaka alla affärsområden och interna enheter, inklusive interna kontrollfunktioner (däribland funktionen för regelefterlevnad, inklusive funktionen för bekämpning av penningtvätt och finansiering av terrorism om denna är en separat funktion, samt riskhanterings- och internrevisionsfunktioner i de fall sådana har inrättats). Värdepappersföretag ska införa, upprätthålla och regelbundet uppdatera lämpliga skriftliga policyer, mekanismer och förfaranden för intern kontroll, och dessa ska godkännas av ledningsorganet. Om ingen riskhanteringsfunktion har inrättats ska ledningsorganet ansvara för att upprätta och övervaka lämpliga förfaranden och policyer för riskhantering.

135. Värdepappersföretaget ska ha en tydlig, transparent och dokumenterad beslutsprocess och en tydlig fördelning av ansvarsområden och befogenheter inom ramen för intern kontroll. Detta gäller även företagets affärsområden, interna enheter och interna kontrollfunktioner.

136. Värdepappersföretag ska förmedla dessa policyer, mekanismer och förfaranden till all personal närhelst väsentliga förändringar har införts.

137. De interna kontrollfunktionerna ska kontrollera att de policyer, mekanismer och förfaranden som föreskrivs i ramen för intern kontroll tillämpas på ett korrekt sätt inom deras respektive behörighetsområden.

138. De interna kontrollfunktionerna ska regelbundet lämna skriftliga rapporter till ledningsorganet om allvarliga brister som har konstaterats. Dessa rapporter ska innehålla information om relevanta risker, en konsekvensbedömning, rekommendationer och

korrigerande åtgärder som ska vidtas avseende varje ny allvarlig brist som har konstaterats. Ledningsorganet ska följa upp de interna kontrollfunktionernas iakttagelser i god tid och på ett effektivt sätt och ska utfärda krav om lämpliga korrigerande åtgärder. Ett formellt uppföljningsförfarande för iakttagelser och vidtagna korrigerande åtgärder ska införas.

16 Ram för riskhantering

139. Som ett led i den övergripande ramen för intern kontroll ska värdepappersföretag ha en företagsövergripande och enhetlig riskhanteringsram som omfattar alla affärsområden och interna enheter, inbegripet interna kontrollfunktioner, och som fullt ut erkänner den ekonomiska innebörden i företagets alla riskexponeringar, inklusive de risker som värdepappersföretaget utgör för sig självt, sina kunder och sina marknader samt likviditetsrisker, särskilt sådana som kan ha en väsentlig inverkan på eller uttömma den tillgängliga kapitalbasen. Riskhanteringsramen ska göra det möjligt för värdepappersföretaget att fatta välgrundade beslut om risktagande. Riskhanteringsramen ska omfatta alla risker, såväl faktiska som framtida risker, som värdepappersföretaget kan vara eller kan bli exponerat för. Risker ska utvärderas nedifrån och upp och uppifrån och ned, både inom och mellan affärsområden, och en enhetlig terminologi samt förenliga metoder ska nyttjas i hela värdepappersföretaget och på gruppnivå. Alla relevanta risker ska innefattas i riskhanteringsramen och lämplig hänsyn ska tas till både finansiella och icke-finansiella risker, inbegripet marknadsrisker, likviditetsrisker, koncentrationsrisker, operativa risker, it-risker, anseenderisker, rättsliga risker, beteenderisker, risker förknippade med bekämpning av penningtvätt och finansiering av terrorism och annan ekonomisk brottslighet, ESG-risker och strategiska risker.

140. Ett värdepappersföretags riskhanteringsram ska omfatta policyer, förfaranden, riskgränser och riskkontroller som säkerställer lämplig, punktlig och fortlöpande identifiering, mätning eller bedömning, övervakning, hantering, reducering och rapportering av risker på affärsområdesnivå, värdepappersföretagsnivå och gruppnivå.

141. Ett värdepappersföretags riskhanteringsram ska ge specifik vägledning om genomförandet av företagets strategier. Denna vägledning ska, när så är lämpligt, fastställa och upprätthålla interna gränser som är förenliga med värdepappersföretagets riskaptit och dess verksamhet, finansiella sundhet, kapitalbas och strategiska mål. Värdepappersföretagets riskprofil ska hållas inom dessa fastställda gränser. Riskhanteringsramen ska säkerställa att det finns en fastställd process för att rapportera, vidarebefordra och åtgärda överträdelser av riskgränserna genom ett lämpligt uppföljningsförfarande.

142. Riskhanteringsramen ska vara föremål för oberoende intern översyn utförd av exempelvis internrevisionsfunktionen, och den ska regelbundet omprövas mot värdepappersföretagets riskaptit med beaktande av information från riskhanteringsfunktionen och riskkommittén, i de fall sådana har inrättats. Faktorer som ska beaktas inbegriper interna och externa utvecklingar, däribland förändringar i intäkter, ökad komplexitetsgrad i värdepappersföretagets

affärsverksamhet, riskprofil eller struktur, geografiska expansioner, fusioner och förvärv samt införande av nya produkter eller affärsområden.

143. När ett värdepappersföretag identifierar och mäter eller bedömer risker ska det utarbeta lämpliga metoder som innefattar både framåtblickande och bakåtblickande verktyg. Verktygen ska omfatta bedömning av den faktiska riskprofilen i förhållande till värdepappersföretagets riskaptit samt identifiering och bedömning av potentiella och stressdrivna riskexponeringar under en rad förmodade ogynnsamma omständigheter i förhållande till värdepappersföretagets riskkapacitet. Verktygen ska syfta till att ge information om eventuella anpassningar av riskprofilen som kan vara nödvändiga. Värdepappersföretag ska göra tillräckligt försiktiga antaganden när de utformar modeller med stresscenarier.

144. Värdepappersföretag ska ta hänsyn till att resultaten av kvantitativa bedömningsmetoder, inbegripet stresstester, i hög grad är beroende av modellernas begränsningar och antaganden (inbegripet den stressdrivna påfrestningens allvarlighetsgrad och varaktighet samt de underliggande riskerna). Exempelvis kan modeller som uppvisar mycket hög avkastning på det ekonomiska kapitalet tyda på en svaghet i modellerna (t.ex. att vissa relevanta risker har uteslutits) snarare än att värdepappersföretaget har en överordnad strategi eller att det genomför strategin på ett utmärkt sätt. Risknivån ska därför inte fastställas enbart på grundval av kvantitativ information eller modellresultat, utan ska även omfatta en kvalitativ bedömning (genom bland annat expertutlåtanden och kritisk analys). Relevanta tendenser och uppgifter i det makroekonomiska området ska särskilt beaktas för att identifiera deras potentiella inverkan på exponeringar och portföljer.

145. Det yttersta ansvaret för riskbedömning ligger helt och hållet hos värdepappersföretaget, som följaktligen ska utvärdera sina risker kritiskt och inte uteslutande förlita sig på externa bedömningar.

146. Värdepappersföretag ska vara fullt medvetna om modellernas och mätmetodernas begränsningar och inte bara använda sig av kvantitativa riskbedömningsverktyg, utan även kvalitativa sådana (däribland expertutlåtanden och kritisk analys).

147. Utöver de egna bedömningarna får värdepappersföretag även använda sig av externa riskbedömningar (inklusive externa kreditutvärderingar eller externt förvärvade riskmodeller). Värdepappersföretag ska ha full kännedom om den exakta omfattningen av sådana bedömningar och deras begränsningar.

148. Mekanismer för regelbunden och öppen rapportering ska inrättas så att ledningsorganet, dess riskkommitté, om en sådan har inrättats, och alla relevanta enheter i värdepappersföretaget får rapporter på ett punktligt, korrekt, koncist, begripligt och meningsfullt sätt samt har möjlighet att utbyta relevant information om identifiering, mätning eller bedömning, övervakning och hantering av risker. Rapporteringsramen ska vara tydligt definierad och dokumenterad.

149. Effektiv kommunikation och medvetenhet om risker och riskstrategin är avgörande för hela riskhanteringsprocessen, inbegripet översyns- och beslutsprocesserna, och bidrar till att förhindra beslut som oavsiktligt kan öka riskerna. Effektiv riskrapportering förutsätter en god intern kännedom om och förmedling av riskstrategin och relevanta riskdata (t.ex. exponeringar och centrala riskindikatorer), både horisontellt inom värdepappersföretaget samt uppåt och nedåt i ledningskedjan.

17 Interna kontrollfunktioner

150. De interna kontrollfunktionerna ska inbegripa en ändamålsenlig och permanent intern funktion för regelefterlevnad och, när så är lämpligt och proportionellt med beaktande av de kriterier som anges i avdelning I, en riskhanteringsfunktion samt en internrevisionsfunktion. I kontrollfunktionernas ansvarsområden ingår även att säkerställa att kraven gällande bekämpning av penningtvätt och finansiering av terrorism efterlevs. I de fall värdepappersföretaget inte inrättar och upprätthåller en riskhanteringsfunktion och en internrevisionsfunktion ska de på begäran kunna visa att de policyer och förfaranden som antagits och införts i ramen för intern kontroll uppnår samma resultat som åsyftas i riktlinjerna i denna avdelning V.

151. Om värdepappersföretaget inte inrättar en intern riskhanteringsfunktion eller en internrevisionsfunktion ska ansvaret för dessa funktioner, enligt de föreskrifter som anges i dessa riktlinjer, åläggas den personal som har ansvaret för de fastställda förfarandena, och det yttersta ansvaret ska ligga hos ledningsorganet som får delegera de berörda verksamhetsuppgifterna internt eller externt.

152. Utan att det påverkar tillämpningen av den nationella lagstiftning som införlivar direktiv (EU) 2015/849 ska värdepappersföretag ålägga en anställd (t.ex. chefen för regelefterlevnad) ansvaret för att säkerställa att värdepappersföretaget uppfyller kraven i direktivet samt efterlever företagets policyer och förfaranden. Värdepappersföretag får inrätta en separat funktion för efterlevnad av reglerna för bekämpning av penningtvätt och finansiering av terrorism som en oberoende kontrollfunktion. Den person som ansvarar för funktionen för bekämpning av penningtvätt och finansiering av terrorism ska vid behov kunna rapportera direkt till ledningsorganet i dess ledningsfunktion respektive i dess tillsynsfunktion.

17.1 Chefer för de interna kontrollfunktionerna

153. Chefer för interna kontrollfunktioner ska tillsättas på en nivå i hierarkin som är tillräcklig för att dessa chefer ska ha den befogenhet och ställning som krävs för att kunna fullgöra sina skyldigheter. Chefen för regelefterlevnad och, i förekommande fall, cheferna för riskhanterings- och internrevisionsfunktionerna ska rapportera till och vara direkt ansvariga inför ledningsorganet, och chefernas resultat och prestationer ska granskas av ledningsorganet.

154. Cheferna för interna kontrollfunktioner ska i tillämpliga fall ha tillgång till, samt rapportera direkt till, ledningsorganet i dess tillsynsfunktion så att cheferna har möjlighet att lyfta frågor och problem samt varna tillsynsfunktionen när specifika skeenden påverkar eller kan komma

att påverka värdepappersföretaget. Detta ska inte hindra cheferna för de interna kontrollfunktionerna från att även kunna rapportera via de vanliga rapporteringsvägarna.

155. Värdepappersföretag ska ha dokumenterade förfaranden för att tillsätta chefer för interna kontrollfunktioner samt för att frånta chefer deras ansvar. Under alla omständigheter ska chefer för interna kontrollfunktioner inte avsättas utan att detta på förhand godkänns av ledningsorganet i dess tillsynsfunktion.

17.2 De interna kontrollfunktionernas oberoende ställning

156. För att de interna kontrollfunktionerna ska anses vara oberoende ska följande villkor vara uppfyllda:

a. Deras personal utför inte några verksamhetsuppgifter som faller inom ramen för den verksamhet som de interna kontrollfunktionerna är avsedda att övervaka och kontrollera, såvida det inte kan påvisas att de interna kontrollfunktionerna förblir effektiva mot bakgrund av de kriterier som anges i avdelning I för tillämpningen av proportionalitetsprincipen. I detta fall ska värdepappersföretaget bedöma om de interna kontrollfunktionernas effektivitet är äventyrad.

b. De är, när så är lämpligt, organisatoriskt åtskilda från den verksamhet som de ska övervaka och kontrollera.

c. Ersättningen till de interna kontrollfunktionernas personal ska inte vara kopplad till den verksamhet som respektive kontrollfunktion ska övervaka och kontrollera och ska inte heller på annat sätt kunna äventyra personalens objektivitet[28].

17.3 De interna kontrollfunktionernas resurser

157. De interna kontrollfunktionerna ska ha tillräckliga resurser. Med beaktande av tillämpningen av den proportionalitetsprincip som föreskrivs i avdelning I ska de ha tillräckligt med kvalificerad personal (både på moder- och dotterföretagsnivå). Personalen ska förbli kvalificerad och få fortutbildning när så behövs.

158. Interna kontrollfunktioner ska ha lämpliga it-system och stöd till sitt förfogande samt ha tillgång till den interna och externa information som är nödvändig för att de ska kunna fullgöra sina skyldigheter. De ska ha tillgång till all nödvändig information om alla affärsområden och relevanta riskbärande dotterföretag, särskilt sådana som potentiellt kan medföra väsentliga risker för värdepappersföretaget.

[28] Se även EBA:s riktlinjer för en sund ersättningspolicy som finns på https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

18 Riskhanteringsfunktion

159. Riskhanteringsfunktionen ska omfatta hela värdepappersföretaget. Riskhanteringsfunktionen ska, med beaktande av de proportionalitetskriterier som anges i avdelning I, ha de befogenheter och resurser samt den ställning som krävs för att kunna genomföra riskpolicyer och inrätta den riskhanteringsram som beskrivs i avsnitt 17.

160. Riskhanteringsfunktionen ska, när så krävs, ha direkt tillgång till ledningsorganet i dess tillsynsfunktion och ledningsorganets kommittéer, om sådana har inrättats, inklusive och i synnerhet riskkommittén.

161. Riskhanteringsfunktionen ska ha tillgång till alla affärsområden och andra interna enheter som kan medföra risker samt till relevanta dotterföretag och närstående företag.

162. Personalen vid riskhanteringsfunktionen ska ha tillräckliga kunskaper, färdigheter och erfarenheter när det gäller riskhanteringsmetoder och riskhanteringsförfaranden samt marknader och produkter, och ska ha tillgång till regelbunden fortbildning.

163. Riskhanteringsfunktionen ska vara ett centralt organisatoriskt inslag i värdepappersföretaget och ska vara strukturerat på ett sätt som gör det möjligt för funktionen att genomföra riskpolicyer och styra riskhanteringsramen. Riskhanteringsfunktionen ska ha en väsentlig roll i att säkerställa att värdepappersföretaget har effektiva riskhanteringsprocesser. Riskhanteringsfunktionen ska vara delaktig i alla väsentliga beslut som rör riskhantering.

164. I en koncern ska riskhanteringsfunktionen i moderföretaget inom unionen kunna ge en koncernövergripande helhetssyn på alla risker och säkerställa att riskstrategin följs.

165. Riskhanteringsfunktionen ska tillhandahålla relevanta och oberoende uppgifter, analyser och expertbedömningar om riskexponeringar samt ge råd om förslag och riskbeslut som fattas av affärsområden eller interna enheter, och ska informera ledningsorganet om huruvida sådana uppgifter och sådana råd är förenliga med värdepappersföretagets riskstrategi och riskaptit. Riskhanteringsfunktionen får rekommendera förbättringar av riskhanteringsramen och korrigerande åtgärder för att åtgärda överträdelser av riskrelaterade policyer, förfaranden och gränser.

18.1 Riskhanteringsfunktionens roll i riskstrategi och riskbeslut

166. Riskhanteringsfunktionen ska på ett tidigt stadium vara delaktig i utarbetandet av värdepappersföretagets riskstrategi och i att säkerställa att värdepappersföretaget har effektiva riskhanteringsprocesser. Riskhanteringsfunktionen ska förse ledningsorganet med all relevant riskrelaterad information så att ledningen kan fastställa en nivå för värdepappersföretagets riskaptit. Riskhanteringsfunktionen ska bedöma riskstrategins och riskaptitens stabilitet och hållbarhet. Den ska säkerställa att riskaptiten på lämpligt sätt

omsätts i specifika riskgränser. Riskhanteringsfunktionen ska även bedöma affärsenheternas riskstrategier, inbegripet de mål som föreslås av affärsenheterna, och ska involveras innan ledningsorganet fattar ett beslut om riskstrategier och riskaptit. Målen ska vara rimliga och förenliga med värdepappersföretagets riskstrategi och riskaptit.

167. Riskhanteringsfunktionens involvering i beslutsprocesser ska säkerställa att riskövervägande beaktas på lämpligt sätt. Ansvarighet för de beslut som fattas ska emellertid ligga kvar hos affärsenheterna och de interna enheterna, och det yttersta ansvaret ska ligga hos ledningsorganet.

18.2 Riskhanteringsfunktionens roll vid väsentliga förändringar

168. Innan beslut om väsentliga förändringar av processer eller system, eller exceptionella transaktioner, fattas ska riskhanteringsfunktionen vara delaktig i utvärderingen av effekterna av sådana förändringar och exceptionella transaktioner på värdepappersföretagets och koncernens övergripande risk, och ska rapportera sina slutsatser direkt till ledningsorganet innan ett beslut fattas.

169. Riskhanteringsfunktionen ska utvärdera på vilka sätt de risker som identifierats kan påverka värdepappersföretagets eller koncernens förmåga att hantera sin riskprofil, likviditet och sunda kapitalbas under normala och ogynnsamma omständigheter.

18.3 Riskhanteringsfunktionens roll när det gäller att identifiera, mäta, bedöma, hantera, reducera, övervaka och rapportera risker

170. Riskhanteringsfunktionen ska säkerställa att det finns en lämplig riskhanteringsram och att alla risker identifieras, bedöms, mäts, övervakas, hanteras och rapporteras på korrekt sätt av de berörda enheterna inom värdepappersföretaget.

171. Riskhanteringsfunktionen ska säkerställa att identifieringen och bedömningen av risker inte enbart utgår från kvantitativ information eller modellresultat, utan även grundas på kvalitativa metoder. Riskhanteringsfunktionen ska hålla ledningsorganet informerat om de antaganden som används i, och de potentiella bristerna hos, riskmodellerna och riskanalysen.

172. Riskhanteringsfunktionen ska säkerställa att transaktioner med närstående parter ses över och att de risker som dessa medför för värdepappersföretaget identifieras och bedöms på lämpligt sätt.

173. Riskhanteringsfunktionen ska se till att alla identifierade risker övervakas på ett effektivt sätt av affärsenheterna.

174. Riskhanteringsfunktionen ska regelbundet övervaka värdepappersföretagets faktiska riskprofil och granska den i förhållande till värdepappersföretagets strategiska mål och riskaptit för att göra det möjligt för ledningsorganet i dess ledningsfunktion att fatta beslut samt för ledningsorganet i dess tillsynsfunktion att göra invändningar.

175. Riskhanteringsfunktionen ska analysera tendenser och erkänna nya eller framväxande risker och riskökningar som uppstår till följd av förändrade omständigheter och förhållanden. Den ska också regelbundet se över faktiska riskutfall i förhållande till tidigare uppskattningar (dvs. utföra utfallstester) för att bedöma och förbättra riskhanteringsprocessens tillförlitlighet och effektivitet.

176. Riskhanteringsfunktionen ska utvärdera tänkbara sätt att minska risker. Rapporteringen till ledningsorganet ska inbegripa förslag på lämpliga riskreducerande åtgärder.

18.4 Riskhanteringsfunktionens roll när det gäller gränser

177. Riskhanteringsfunktionen ska göra oberoende bedömningar av överträdelser av riskaptit eller riskgränser (dvs. bland annat fastställa orsaken till överträdelsen och genomföra en juridisk och ekonomisk analys av den faktiska kostnaden för att avsluta, minska eller säkra exponeringen i förhållande till den potentiella kostnaden för att behålla den). Riskhanteringsfunktionen ska förse de berörda affärsenheterna och ledningsorganet med information och ska rekommendera möjliga åtgärder. Riskhanteringsfunktionen ska rapportera direkt till ledningsorganet i dess tillsynsfunktion när överträdelsen är väsentlig, utan att det påverkar riskhanteringsfunktionens möjlighet att även rapportera till andra interna funktioner och kommittéer.

178. Riskhanteringsfunktionen ska ha en central roll i att säkerställa att ett beslut beträffande dess rekommendation fattas på relevant nivå och att beslutet efterlevs av de relevanta affärsenheterna samt rapporteras på lämpligt sätt till ledningsorganet och, i förekommande fall, riskkommittén.

18.5 Chef för riskhanteringsfunktionen

179. I de fall en chef för riskhanteringsfunktionen har tillsatts ska denne ansvara för att förse ledningsorganet med omfattande och tydlig information om risker samt ge råd till ledningsorganet, så att ledningen kan skaffa sig en uppfattning om värdepappersföretagets övergripande riskprofil. Detsamma gäller chefen för riskhanteringsfunktionen i ett modervärdepappersföretag avseende den konsoliderade situationen. I de fall ingen oberoende funktion har inrättats ligger de ansvarsområden som tilldelas chefen för riskhanteringsfunktionen hos den personal som ansvarar för riskhanteringsförfarandena eller hos ledamöterna i ledningsorganet.

180. Chefen för riskhanteringsfunktionen ska ha den sakkunskap och den oberoende och ledande ställning som är nödvändig för att kunna ifrågasätta beslut som påverkar

värdepappersföretagets riskexponering. I de fall chefen för riskhanteringsfunktionen inte är en ledamot i ledningsorganet ska värdepappersföretaget, med beaktande av proportionalitetsprincipen i avdelning I, utse en oberoende person till rollen som chef för riskhanteringsfunktionen som inte har ansvar för några andra funktioner och som rapporterar direkt till ledningsorganet. Om det inte är proportionerligt att utse en person som enbart ägnar sig åt rollen som chef för riskhanteringsfunktionen mot bakgrund av proportionalitetsprincipen i avdelning I, kan denna roll kombineras med rollen som chef för funktionen för regelefterlevnad eller utföras av en annan person i ledande ställning, förutsatt att det inte föreligger någon intressekonflikt mellan de uppgifter som utförs. Under alla omständigheter ska denna person ha tillräcklig auktoritet och ställning samt vara oberoende (t.ex. chef för rättsliga frågor).

181. Chefen för riskhanteringsfunktionen ska kunna invända mot beslut som fattats av värdepappersföretagets ledning och ledningsorgan, och grunderna till invändningarna ska dokumenteras formellt. Om ett värdepappersföretag vill ge chefen för riskhanteringsfunktionen rätten att inlägga veto mot beslut (t.ex. ett kredit- eller investeringsbeslut eller fastställandet av en gräns) på nivåer under ledningsorganet, ska det ange omfattningen av en sådan vetorätt, förfaranden för eskalering eller överklagande och på vilket sätt ledningsorganet ska involveras i processen.

182. Värdepappersföretag ska inrätta skärpta förfaranden för godkännandet av beslut om vilka chefen för riskhanteringsfunktionen har uttryckt en negativ ståndpunkt. I dess tillsynsfunktion ska ledningsorganet kunna kommunicera direkt med chefen för riskhanteringsfunktionen om väsentliga riskfrågor, inklusive när det gäller skeenden som kan vara oförenliga med värdepappersföretagets riskstrategi och riskaptit.

19 Funktion för regelefterlevnad[29]

183. Värdepappersföretag ska inrätta en permanent och ändamålsenlig funktion för regelefterlevnad för att hantera efterlevnadsrisker, och ska utse en person som ska ansvara för denna funktion i hela värdepappersföretaget (en regelefterlevnadsansvarig). Funktionen, policyerna och förfarandena för regelefterlevnad ska vara förenliga med artikel 22 i kommissionens delegerade förordning (EU) 2017/565 och Esmas riktlinjer för funktionen för regelefterlevnad.

184. Den regelefterlevnadsansvariges roll kan, med beaktande av proportionalitetsprincipen i avdelning I, kombineras med rollen som chef för riskhanteringsfunktionen eller, om det inte är proportionellt att utse en person som enbart ägnar sig åt denna roll, utföras av en annan person i ledande ställning (t.ex. chef för rättsliga frågor), förutsatt att det inte föreligger någon intressekonflikt mellan de uppgifter som utförs.

[29] Detta avsnitt ska läsas utan att det påverkar tillämpningen av, samt mot bakgrund av, Esmas riktlinjer för funktionen för regelefterlevnad.

185. Personalen vid funktionen för regelefterlevnad ska ha tillräckliga kunskaper, färdigheter och erfarenheter när det gäller regelefterlevnad och relevanta förfaranden, och ska ha tillgång till regelbunden fortbildning.

186. Ledningsorganet i dess tillsynsfunktion ska övervaka genomförandet av en väldokumenterad policy för regelefterlevnad, och denna ska förmedlas till all personal. Värdepappersföretag ska inrätta ett förfarande för att regelbundet bedöma ändringar av de lagar och förordningar som är tillämpliga på verksamheten.

187. Funktionen för regelefterlevnad ska ge ledningsorganet råd om åtgärder som ska vidtas för att säkerställa efterlevnad av tillämpliga lagar, regler, förordningar och standarder, och ska bedöma de potentiella följder som ändringar av lagstiftningen eller regelverket kan ha på värdepappersföretagets verksamhet och regelefterlevnadsram.

188. Funktionen för regelefterlevnad ska se till att övervakning av regelefterlevnad utförs genom ett strukturerat och väldefinierat övervakningsprogram och att policyn för regelefterlevnad följs. Funktionen för regelefterlevnad ska rapportera till ledningsorganet och, när så är lämpligt, kommunicera med riskhanteringsfunktionen om värdepappersföretagets efterlevnadsrisk och hur denna hanteras. Funktionen för regelefterlevnad och riskhanteringsfunktionen ska samarbeta och utbyta information på lämpligt sätt för att fullgöra sina respektive uppgifter. Iakttagelser som görs av funktionen för regelefterlevnad ska beaktas av ledningsorganet och riskhanteringsfunktionen när dessa fattar beslut.

189. Värdepappersföretag ska vidta lämpliga åtgärder mot interna eller externa beteenden som skulle kunna underlätta eller möjliggöra bedrägeri, penningtvätt/finansiering av terrorism eller annan ekonomisk brottslighet samt disciplinbrott (t.ex. överträdelser av interna förfaranden eller överskridande av gränser).

190. Värdepappersföretag ska se till att deras dotterföretag och filialer vidtar åtgärder för att säkerställa att deras verksamhet är förenlig med lokala lagar och förordningar. Om lokala lagar och förordningar hindrar att de strikta förfaranden och system för regelefterlevnad som införlivats i koncernen tillämpas, särskilt om de förhindrar utlämnande och utbyte av nödvändig information mellan enheter inom koncernen, ska dotterföretag och filialer informera den regelefterlevnadsansvarige eller chefen för regelefterlevnad vid moderföretaget inom unionen om detta.

20 Internrevisionsfunktion

191. I de fall en internrevisionsfunktion har inrättats ska den vara oberoende och ha tillräcklig auktoritet och ställning samt tillräckliga resurser. Värdepappersföretag ska i synnerhet se till att kompetensen hos internrevisionsfunktionens personal och funktionens resurser, särskilt dess revisionsverktyg och riskanalysmetoder, är tillräckliga i förhållande till värdepappersföretagets storlek och belägenhet, samt till karaktären, omfattningen och

komplexiteten hos de risker som är förknippade med värdepappersföretagets affärsmodell, verksamhet, riskkultur och riskaptit.

192. Internrevisionsfunktionen ska vara oberoende av den verksamhet som den granskar. Den ska därför inte kombineras med andra funktioner.

193. Internrevisionsfunktionen ska, utifrån en riskbaserad metod, oberoende granska och objektivt garantera att alla verksamheter och enheter i ett värdepappersföretag, inklusive utkontrakterad verksamhet, efterlever värdepappersföretagets policyer och förfaranden samt lagstadgade krav. Samtliga enheter inom koncernen ska omfattas av internrevisionsfunktionens verksamhetsområde.

194. Internrevisionsfunktionen ska inte vara delaktig i utformningen, urvalet, fastställandet eller genomförandet av specifika policyer, mekanismer, förfaranden och riskgränser för intern kontroll. Detta ska dock inte hindra ledningsorganet i dess ledningsfunktion från att begära in synpunkter från internrevisionsfunktionen i frågor som rör risker, interna kontroller och efterlevnad av tillämpliga regler.

195. Internrevisionsfunktionen ska bedöma om värdepappersföretagets ram för intern kontroll, som föreskrivs i avsnitt 15, är både ändamålsenlig och verkningsfull. Internrevisionsfunktionen ska särskilt bedöma

    a. lämpligheten i värdepappersföretagets styrningsram,

    b. huruvida befintliga policyer och förfaranden är tillräckliga och uppfyller kraven i lagar och förordningar samt överensstämmer med värdepappersföretagets riskstrategi och riskaptit,

    c. att förfarandena är förenliga med tillämpliga lagar och förordningar och med ledningsorganets beslut,

    d. huruvida förfarandena genomförs på ett korrekt och ändamålsenligt sätt (t.ex. efterlevnad i samband med transaktioner och den faktiska risknivå som föreligger),

    e. ändamålsenligheten, kvaliteten och effektiviteten i de kontroller som utförs och den rapportering som görs av affärsenheterna (första försvarslinjen) och av funktionerna för riskhantering och regelefterlevnad.

196. Internrevisionsfunktionen ska i synnerhet kontrollera integriteten hos de processer som säkerställer tillförlitligheten i värdepappersföretagets metoder och tekniker samt de antaganden och informationskällor som används i dess interna modeller (t.ex. riskmodellering och värderingar i redovisning). Den ska också utvärdera kvaliteten på och användningen av verktyg för identifiering och bedömning av kvalitativa risker och de riskreducerande åtgärder som vidtagits.

197. Internrevisionsfunktionen ska ha obegränsad tillgång till värdepappersföretagens samtliga register, handlingar, uppgifter och byggnader. Detta ska innefatta tillgång till förvaltningsinformationssystem och protokoll från alla kommittéer och beslutsfattande organ.

198. Internrevisionsfunktionen ska följa nationella och internationella yrkesstandarder. Ett exempel på sådana yrkesstandarder är de normer som föreskrivs av Institute of Internal Auditors.

199. Internrevisionsarbetet ska utföras enligt en revisionsplan och ett detaljerat revisionsprogram som utgår från en riskbaserad metod.

200. En internrevisionsplan ska utarbetas minst en gång per år på grundval av de årliga målen för internrevisionskontroll. Internrevisionsplanen ska godkännas av ledningsorganet.

201. Alla revisionsrekommendationer ska vara föremål för ett formellt uppföljningsförfarande på lämplig ledningsnivå som syftar till att säkerställa och upprätta rapporter om det effektiva uppfyllandet av rekommendationerna.

Avdelning VI – hantering av driftskontinuitet

202. Värdepappersföretag ska upprätta en sund hanterings- och återhämtningsplan för driftskontinuitet i syfte att säkerställa sin förmåga att bedriva löpande verksamhet och begränsa förluster i händelse av allvarliga avbrott i affärsverksamheten.

203. Värdepappersföretag får inrätta en särskild och oberoende driftskontinuitetsfunktion.

204. Ett värdepappersföretags verksamhet är beroende av flera kritiska resurser (däribland it-system inklusive molntjänster, kommunikationssystem, personal och byggnader). Syftet med driftskontinuitetshantering är att minska operativa, ekonomiska, rättsliga, anseendemässiga och andra väsentliga konsekvenser som kan följa av en katastrof eller långa avbrott eller störningar hos dessa resurser samt de därav följande avbrotten i värdepappersföretagets ordinarie affärsverksamhet. Andra riskhanteringsåtgärder kan syfta till att minska sannolikheten att sådana incidenter inträffar eller att överföra deras ekonomiska konsekvenser till tredje parter (t.ex. genom försäkringar).

205. För att upprätta en sund plan för driftskontinuitetshantering ska värdepappersföretaget noggrant analysera riskfaktorer som rör, och dess exponering för, allvarliga avbrott i verksamheten samt (kvantitativt och kvalitativt) bedöma de potentiella effekterna av sådan avbrott med hjälp av interna och/eller externa data samt scenarioanalyser. Sådana analyser ska omfatta alla affärsområden och interna enheter, inklusive riskhanteringsfunktionen eller riskhanteringsförfarandena, och ska ta hänsyn till deras inbördes beroende. Resultaten av analyserna ska utgöra en av grunderna för värdepappersföretagets återhämtningsprioriteringar och återhämtningsmål.

206. På grundval av ovannämnda analyser ska värdepappersföretaget inrätta följande:

    a. Beredskaps- och driftskontinuitetsplaner som säkerställer att värdepappersföretaget reagerar på nödsituationer på lämpligt sätt och kan upprätthålla sin viktigaste verksamhet i händelse av avbrott i den ordinarie affärsverksamheten.

    b. Återhämtningsplaner för kritiska resurser som gör det möjligt för värdepappersföretaget att återgå till den ordinarie affärsverksamheten inom en lämplig tidsram. Eventuella kvarstående risker till följd av avbrott i verksamheten ska vara förenliga med värdepappersföretagets riskaptit.

207. Beredskapsplaner, driftskontinuitetsplaner och återhämtningsplaner ska dokumenteras och genomföras noggrant. Dokumentationen ska finnas tillgänglig inom affärsområdena, de interna enheterna och riskhanteringsfunktionen för den personal som ansvar för riskhanteringsförfaranden, och ska finnas bevarad i system som är fysiskt åtskilda och lättillgängliga i händelse av oförutsedda situationer. Lämplig utbildning på detta område ska tillhandahållas. Planerna ska testas och uppdateras regelbundet. Problem eller brister som konstateras när dessa tester genomförs ska dokumenteras och analyseras, och planerna ska ses över i enlighet med detta.

Avdelning VII – transparens

208. Strategier, policyer och förfaranden ska förmedlas till all relevant personal i hela värdepappersföretaget. Värdepappersföretagets personal ska förstå och följa de policyer och förfaranden som gäller för deras uppgifter och ansvarsområden.

209. Ledningsorganet ska således på ett tydligt och konsekvent sätt informera och uppdatera den berörda personalen om värdepappersföretagets strategier och policyer, åtminstone i den utsträckning som krävs för att personalen ska kunna utföra sina uppgifter. Detta kan ske genom skriftliga riktlinjer, handböcker eller på annat sätt.

210. I de fall de behöriga myndigheterna, i enlighet med artikel 44 i direktiv (EU) 2019/2034, kräver att moderföretag årligen offentliggör en beskrivning av sin rättsliga struktur samt värdepappersföretagskoncernens lednings- och organisationsstruktur ska denna information omfatta alla enheter i koncernstrukturen enligt definitionen i direktiv 2013/34/EU [30], förtecknade per land.

211. Offentliggörandet ska som minst innehålla

[30] Europaparlamentets och rådets direktiv 2013/34/EU av den 26 juni 2013 om årsbokslut, koncernredovisning och rapporter i vissa typer av företag, om ändring av Europaparlamentets och rådets direktiv 2006/43/EG och om upphävande av rådets direktiv 78/660/EEG och 83/349/EEG (EUT L 182, 29.6.2013, s. 19).

a. en översikt över värdepappersföretagets och koncernstrukturens interna organisation enligt definitionen i direktiv 2013/34/EU, och ändringar därav, inklusive de huvudsakliga rapporteringsvägarna och ansvarsområdena,

b. alla väsentliga förändringar sedan det föregående offentliggörandet och datum för den väsentliga förändringen,

c. nya rättsliga strukturer, styrningsstrukturer eller organisationsstrukturer,

d. information om ledningsorganets struktur, organisation och ledamöter, inklusive antalet ledamöter samt antalet av dessa som betecknas som oberoende, med angivande av kön och uppdragsperiod för varje ledamot i ledningsorganet,

e. ledningsorganets huvudsakliga ansvarsområden,

f. en förteckning över kommittéerna i ledningsorganet i dess tillsynsfunktion och kommittéernas sammansättning,

g. en översikt över den policy om intressekonflikter som gäller för värdepappersföretaget och ledningsorganet,

h. en översikt över ramen för intern kontroll,

i. en översikt över ramen för driftskontinuitetshantering.

Bilaga I – aspekter som ska beaktas vid utarbetandet av en intern styrningspolicy

I enlighet med avdelning III ska värdepappersföretag beakta följande aspekter vid dokumentationen av interna styrningspolicyer och styrningsformer:

1. Aktieägarstruktur
2. Koncernstruktur, i tillämpliga fall (rättslig och funktionell struktur)
3. Ledningsorganets sammansättning och funktionssätt
   a) urvalskriterier, inklusive på vilka sätt mångfald beaktas
   b) antal, uppdragsperiod, rotation, ålder
   c) oberoende ledamöter i ledningsorganet
   d) verkställande ledamöter i ledningsorganet
   e) icke verkställande ledamöter i ledningsorganet
   f) intern ansvarsfördelning, i tillämpliga fall
4. Styrningsstruktur och organisationsplan (med inverkan på koncernen, i tillämpliga fall)
   a) specialiserade kommittéer
      i. sammansättning
      ii. funktion
   b) verkställande kommitté, i förekommande fall
      i. sammansättning
      ii. funktion
5. Personer som innehar nyckelfunktioner
   a) chef för riskhanteringsfunktionen
   b) chef för funktionen för regelefterlevnad
   c) chef för internrevisionsfunktionen
   d) finansdirektör
   e) andra personer som innehar nyckelfunktioner
6. Ram för intern kontroll
   a) beskrivning av varje funktion, inklusive dess organisation, resurser, ställning och befogenheter
7. Beskrivning av riskstrategin och ramen för riskhantering

8. Organisationsstruktur (med inverkan på koncernen, i tillämpliga fall)
    a) operativ struktur, affärsområden och fördelning av befogenheter och ansvarsområden
    b) utkontraktering
    c) produkt- och tjänsteutbud
    d) verksamhetens geografiska omfattning
    e) tillhandahållande av tjänster enligt principen om fritt tillhandahållande av tjänster
    f) filialer
    g) dotterföretag, samriskföretag osv.
    h) användning av offshore-centrum
9. Uppförandekod (med inverkan på koncernen, i tillämpliga fall)
    a) strategiska mål och företagsvärden
    b) interna koder och föreskrifter, inbegripet riktlinjer för bekämpning av penningtvätt och finansiering av terrorism
    c) policy om intressekonflikter
    d) uppgiftslämning (visselblåsning)
10. Den interna styrningspolicyns status, med datum
    a) utarbetande
    b) senaste ändring
    c) senaste bedömning
    d) godkännande av ledningsorganet.