EBA/GL/2021/05

2. juli 2021

Udkast til retningslinjer

vedrørende intern ledelse

1. Compliance og indberetningsforpligtelser

Status for disse retningslinjer

1. Disse retningslinjer er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010[1]. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle virksomheder, herunder institutter, bestræbe sig på at efterleve disse retningslinjer bedst muligt.

2. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis inden for det europæiske finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. Den kompetente myndighed, som er omhandlet i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, og som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsprocesser), også hvor retningslinjerne primært er rettet mod institutter.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den (05.12.2021) underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller begrunde en eventuel manglende efterlevelse. Hvis EBA ikke er blevet underrettet inden denne dato, anser EBA den kompetente myndighed for ikke at efterleve retningslinjerne. Underretninger bør fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, til compliance@eba.europa.eu med referencen "EBA/GL/2021/05". Underretninger bør fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndighed. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.

4. Underretninger offentliggøres på EBA's websted i henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010.

[1] Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

2. Emne, anvendelsesområde og definitioner

Emne

5. Disse retningslinjer præciserer de interne ledelsesordninger, -processer og -mekanismer, som kreditinstitutter, der er omfattet af direktiv 2013/36/EU[2], og investeringsselskaber, der er omfattet af afsnit VII i direktiv 2013/36/EU i medfør af artikel 1, stk. 2, og stk. 5, i forordning (EU) 2019/2033, bør gennemføre i henhold til artikel 74, stk. 1, i direktiv 2013/36/EU for at sikre en effektiv og forsigtig ledelse heraf.

Målgrupper

6. Disse retningslinjer henvender sig til kompetente myndigheder som defineret i artikel 4, stk. 2, litra i), i forordning (EU) nr. 1093/2010 og til finansieringsinstitutter som defineret i artikel 4, stk. 1, i forordning (EU) nr. 1093/2010, som er enten institutter med henblik på anvendelsen af direktiv 2013/36/EU som defineret i artikel 3, stk. 1, nr. 3), i direktiv 2013/36/EU, også under hensyntagen til artikel 3, stk. 3, i nævnte direktiv, eller investeringsselskaber, der er omfattet af afsnit VII i direktiv 2013/36/EU i medfør af artikel 1, stk. 2 og stk. 5,i forordning (EU) 2019/2033 ("institutter").

Anvendelsesområde

7. Disse retningslinjer gælder i forhold til institutternes ledelsesordninger, herunder deres organisatoriske struktur og den tilsvarende ansvarsfordeling, procedurer til at identificere, håndtere, overvåge og indberette alle de risici[3], som institutterne er eller kan blive eksponeret for, samt rammer for intern kontrol.

8. Retningslinjerne tager sigte på at omfatte alle eksisterende ledelsesstrukturer og anbefaler ikke nogen bestemt struktur. Retningslinjerne griber ikke ind i den almindelige kompetencetildeling i overensstemmelse med national selskabsret. De bør derfor anvendes uanset den anvendte ledelsesstruktur (en- og/eller tostrenget ledelsesstruktur og/eller anden struktur) i medlemsstaterne. Ledelsesorganet, jf. artikel 3, stk. 1, nr. 7) og 8), i direktiv 2013/36/EU, bør forstås som et organ med en ledelsesfunktion (direktionen) og en tilsynsfunktion (bestyrelsen)[4].

[2] Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).
[3] Enhver henvisning til risici i disse retningslinjer bør omfatte risici for hvidvaskning af penge og finansiering af terrorisme.
[4] Jf. også betragtning 56 til direktiv 2013/36/EU.

9. Udtrykkene "ledelsesorgan med ledelsesfunktion" og "ledelsesorgan med tilsynsfunktion" bruges i disse retningslinjer, uden at der henvises til en specifik ledelsesstruktur, og henvisninger til ledelsesfunktionen (direktionen) eller tilsynsfunktionen (bestyrelsen) bør forstås som henvisninger til de organer eller medlemmer af ledelsesorganet, der er ansvarlige for den pågældende funktion i henhold til national lovgivning. Når de kompetente myndigheder implementerer disse retningslinjer, bør de tage hensyn til deres nationale selskabsret og om nødvendigt præcisere, hvilket organ eller hvilke medlemmer af ledelsesorganet disse funktioner bør gælde for.

10. I medlemsstater, hvor ledelsesorganet helt eller delvist delegerer ledelsesfunktionerne til en person eller et internt ledende organ (f.eks. en administrerende direktør, et ledelsesteam eller et forretningsudvalg), bør de personer, der varetager disse ledelsesfunktioner på grundlag af denne delegering, forstås som ledelsesorganets ledelsesfunktion. I disse retningslinjer bør enhver henvisning til ledelsesorganet i dets ledelsesfunktion forstås således, at det også omfatter medlemmerne af det ledende organ eller den administrerende direktør, som defineret i disse retningslinjer, selv hvis de ikke er blevet indstillet eller udnævnt som formelle medlemmer af instituttets ledelsesorgan eller -organer i henhold til national ret.

11. I medlemsstater, hvor noget ansvar udøves direkte af aktionærer, medlemmer eller ejere af instituttet i stedet for ledelsesorganet, bør institutterne sikre, at dette ansvar og beslutninger i denne forbindelse så vidt muligt er i overensstemmelse med de retningslinjer, der gælder for ledelsesorganet.

12. Definitionerne af administrerende direktør, økonomidirektør og personer med nøglefunktioner, der anvendes i disse retningslinjer, er rent funktionelle og har ikke til formål at indføre udnævnelse af disse medarbejdere eller oprettelse af sådanne stillinger, medmindre det er foreskrevet i den relevante EU-lovgivning eller national lovgivning.

13. Institutterne bør overholde disse retningslinjer — og de kompetente myndigheder bør føre tilsyn hermed — på individuelt, delkonsolideret og konsolideret niveau i overensstemmelse med det anvendelsesområde, der er fastsat i artikel 109 i direktiv 2013/36/EU.

Definitioner

14. Medmindre andet er bestemt, har de udtryk, der er anvendt og defineret i direktiv 2013/36/EU og i forordning (EU) nr. 575/2013, den samme betydning i retningslinjerne. I disse retningslinjer gælder derudover følgende definitioner:

Administrerende direktør	Den person, som har ansvar for at forvalte og styre et instituts samlede forretningsmæssige aktiviteter.
Aktionær	En person, der ejer aktier i et institut, eller, afhængigt af instituttets selskabsform, andre ejere eller medlemmer af instituttet.
Børsnoteret institut	Institutter, hvis finansielle instrumenter er optaget til handel på et reguleret marked eller i en multilateral handelsfacilitet, jf. artikel 4, nr. 21) og artikel 4, nr. 22), i direktiv 2014/65/EU, i en eller flere medlemsstater[5].
Direktør- og bestyrelsespost	En stilling som medlem af et instituts eller en anden juridisk enheds ledelsesorgan.
Konsoliderende institut	Et institut, der skal overholde tilsynskravene på grundlag af den konsoliderede situation i overensstemmelse med første del, afsnit II, kapitel 2, i forordning (EU) nr. 575/2013.
Konsolideringsregler	Anvendelsen af de tilsynsmæssige krav, der er fastsat i direktiv 2013/36/EU og forordning (EU) nr. 575/2013, på konsolideret eller delkonsolideret grundlag i overensstemmelse med første del, afsnit II, kapitel 2, i forordning (EU) nr. 575/2013.[6]
Kønsbestemte lønforskelle	Forskellen mellem den gennemsnitlige bruttotimeløn for mænd og kvinder udtrykt i procent af mænds gennemsnitlige bruttotimeløn.
Ledere af interne kontrolfunktioner	Personerne med øverste ansvar for den faktiske daglige ledelse af den uafhængige risikostyringsfunktion, compliancefunktion og interne revisionsfunktion.
Medarbejdere	Alle medarbejdere i et institut og dets datterselskaber, som indgår i dets konsolidering, herunder datterselskaber, som ikke er omfattet af direktiv 2013/36/EU, og alle medlemmer af ledelsesorganet i dets ledelsesfunktion og i dets tilsynsfunktion.
Økonomidirektør	Den person, der bærer det overordnede ansvar for ledelsen af alle følgende aktiviteter: forvaltning af finansielle ressourcer, finansiel planlægning og finansiel rapportering.
Personer med nøglefunktioner	Personer, som har betydelig indflydelse på instituttets ledelsesprincipper, men som hverken er medlem af ledelsesorganet eller er administrerende direktør. De omfatter lederne af interne kontrolfunktioner og økonomidirektøren, når de ikke er medlem af ledelsesorganet, og andre personer med

[5] Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

[6] Se også RTS om konsolideringsregler under: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

	nøglefunktioner, når de er identificeret af institutter på grundlag af en risikobaseret tilgang. Andre nøglepersoner kunne omfatte ledere af vigtige forretningsområder, filialer i Det Europæiske Økonomiske Samarbejdsområde/Den Europæiske Frihandelssammenslutning, datterselskaber i tredjelande og andre interne funktioner.
Risikokapacitet	Den maksimale risiko, som et institut kan påtage sig i betragtning af dets kapitalgrundlag, dets risikostyrings- og kontrolkapacitet og dets reguleringsmæssige restriktioner.
Risikoappetit	Det samlede risikoniveau og de typer risici, som et institut er villigt til at påtage sig for at nå sine strategiske mål inden for rammerne af sin risikokapacitet og i overensstemmelse med sin forretningsmodel.
Risikokultur	Et instituts normer, holdninger og adfærd i relation til risikobevidsthed, risikotagning og risikostyring og de kontrolforanstaltninger, der former beslutninger vedrørende risici. Risikokulturen påvirker ledelsens og medarbejdernes beslutninger i forbindelse med det daglige arbejde og indvirker på de risici, de påtager sig.
Væsentlige institutter	Institutter, der er nævnt i artikel 131 i direktiv 2013/36/EU (globale systemisk vigtige institutter (G-SII'er) og andre systemisk vigtige institutter (O-SII'er)), og, hvor det er hensigtsmæssigt, andre institutter, der identificeres af de kompetente myndigheder eller national ret, baseret på en vurdering af instituttets størrelse og interne organisation og på arten, omfanget og kompleksiteten af dets aktiviteter.

3. Gennemførelse

Ikrafttrædelsestidspunkt

15. Disse opdaterede retningslinjer finder anvendelse fra den 31. december 2021.

Ophævelse

16. EBA-retningslinjerne vedrørende intern ledelse (EBA/GL/2017/11) af 26. september 2017 ophæves med virkning fra den 31. december 2021.

4. Retningslinjer

Del I — Proportionalitet

17. Proportionalitetsprincippet, som er nedfældet i artikel 74, stk. 2, i direktiv 2013/36/EU, har til formål at sikre, at de interne ledelsesordninger er i overensstemmelse med instituttets individuelle risikoprofil og forretningsmodel, således at målene med de reguleringsmæssige krav og bestemmelser opfyldes effektivt.

18. Institutterne bør tage hensyn til deres størrelse og interne organisation samt arten, omfanget og kompleksiteten af deres aktiviteter, når de udvikler og gennemfører interne ledelsesordninger. Væsentlige institutter bør have mere avancerede ledelsesordninger, mens små og mindre komplekse institutter kan gennemføre simplere ledelsesordninger. Institutterne bør dog bemærke, at et instituts størrelse eller systemiske betydning ikke i sig selv behøver at være en indikator for, i hvilket omfang et institut er eksponeret for risici.

19. Med henblik på anvendelse af proportionalitetsprincippet og for at sikre en korrekt gennemførelse af myndighedskravene og disse retningslinjer bør institutterne og de kompetente myndigheder tage hensyn til alle følgende aspekter:

    a. størrelsen med hensyn til balancesummen for instituttet og dets datterselskaber inden for konsolideringsreglernes anvendelsesområde

    b. instituttets geografiske tilstedeværelse og størrelsen af dets aktiviteter i hver jurisdiktion

    c. instituttets retlige form, herunder om instituttet er en del af en koncern og i så fald proportionalitetsvurderingen for koncernen

    d. hvorvidt instituttet er børsnoteret

    e. om instituttet har tilladelse til at anvende interne modeller til beregning af kapitalkrav (f.eks. metoden med interne ratings)

    f. typen af godkendte aktiviteter og tjenester, der udføres af instituttet (jf. f.eks. også bilag 1 til direktiv 2013/36/EU og bilag 1 til direktiv 2014/65/EU)

    g. den underliggende forretningsmodel og -strategi, forretningsaktiviteternes art og kompleksitet og instituttets organisatoriske struktur

    h. instituttets risikostrategi, risikoappetit og faktiske risikoprofil, også under hensyntagen til resultatet af SREP-kapitalvurderingen og SREP-likviditetsvurderingen

i. instituttets ejerskabs- og finansieringsstruktur

j. kundetypen (f.eks. detailkunder, virksomhedskunder, institutionelle kunder, små virksomheder eller offentlige enheder) og produkternes eller kontrakternes kompleksitet

k. de outsourcede aktiviteter og distributionskanaler

l. de eksisterende IT-systemer, herunder systemer til driftskontinuitet og outsourcingaktiviteter på dette område, og

m. hvorvidt instituttet er omfattet af definitionen i artikel 4, stk. 1, nr. 145) og 146), i forordning (EU) nr. 575/2013 på et lille og ikke-komplekst institut eller et stort institut.

Del II — Ledelsesorganets og udvalgenes rolle og sammensætning

1 Ledelsesorganets rolle og ansvar

20. I henhold til artikel 88, stk. 1, i direktiv 2013/36/EU skal ledelsesorganet have det endelige og overordnede ansvar for instituttet og fastlægger, fører tilsyn med og er ansvarligt for gennemførelsen af ledelsesordningerne inden for instituttet, som sikrer effektiv og forsigtig ledelse af instituttet.

21. Ledelsesorganets opgaver bør defineres klart, idet der sondres mellem de opgaver, der henhører under ledelsesfunktionen (direktionen) og tilsynsfunktionen (bestyrelsen). Ledelsesorganets ansvar og opgaver bør beskrives i et skriftligt dokument og godkendes behørigt af ledelsesorganet. Alle medlemmer af ledelsesorganet bør have fuldt kendskab til ledelsesorganets struktur og ansvar og til opgavefordelingen mellem forskellige funktioner i ledelsesorganet og dets udvalg.

22. Ledelsesorganet i dets tilsynsfunktion eller i dets ledelsesfunktion bør fungere effektivt i samspil med hinanden. Begge funktioner bør give hinanden tilstrækkelige oplysninger for at gøre det muligt for dem at varetage deres respektive roller. Med henblik på at indføre hensigtsmæssige kontrolforanstaltninger bør beslutningsprocessen i ledelsesorganet ikke være domineret af et enkelt medlem eller en lille delmængde af dets medlemmer.

23. Ledelsesorganets ansvar bør omfatte fastsættelse og godkendelse af og tilsyn med gennemførelsen af:

a. instituttets generelle forretningsstrategi og væsentlige politikker inden for rammerne af gældende love og bestemmelser under hensyntagen til instituttets langsigtede finansielle interesser og solvens

b. den generelle risikostrategi, instituttets risikoappetit og rammerne for dets risikostyring og foranstaltninger til at sikre, at ledelsesorganet afsætter tilstrækkelig tid til risiko- og risikostyringsspørgsmål

c. en tilstrækkelig og effektiv ramme for intern ledelse og intern kontrol som defineret i afsnit V, der:

    i. omfatter en klar organisatorisk struktur og velfungerende uafhængige interne risikostyrings-, compliance- og revisionsfunktioner, som i tilstrækkeligt omfang har autoritet, vægt og ressourcer til at varetage deres funktioner

    ii. sikrer overholdelse af gældende myndighedskrav i forbindelse med forebyggelse af hvidvaskning af penge og finansiering af terrorisme

d. størrelse, type og fordeling af både intern kapital og lovpligtig kapital til i tilstrækkelig grad at afdække instituttets risici

e. mål for instituttets likviditetsstyring

f. en aflønningspolitik, der er i overensstemmelse med de aflønningsprincipper, der er fastsat i artikel 92-95 i direktiv 2013/36/EU, og EBA's retningslinjer vedrørende forsvarlige aflønningspolitikker i henhold til artikel 74, stk. 3, og artikel 75, stk. 2, i direktiv 2013/36/EU[7]

g. ordninger, der har til formål at sikre, at de individuelle og kollektive egnethedsvurderinger af ledelsesorganet gennemføres effektivt, at ledelsesorganets sammensætning og successionsplanlægning er hensigtsmæssig, og at ledelsesorganet varetager sine funktioner effektivt[8]

h. en udvælgelses- og egnethedsvurderingsproces for personer med nøglefunktioner[9]

i. ordninger, der har til formål at sikre den interne funktion af hvert af ledelsesorganets udvalg, hvis et sådant er nedsat, med nærmere oplysninger om:

    i. hver enkelt udvalgs rolle, sammensætning og opgaver

    ii. passende informationsstrøm, herunder dokumentation af anbefalinger og konklusioner, og rapporteringslinjer mellem hvert udvalg og ledelsesorganet, de kompetente myndigheder og andre parter

[7] EBA's retningslinjer vedrørende forsvarlige aflønningspolitikker
[8] Se ligeledes ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner.
[9] Jf. også ESMA's og EBA's retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner

j. en risikokultur i overensstemmelse med afsnit 9 i disse retningslinjer, som omfatter instituttets risikobevidsthed og risikoadfærd

k. en virksomhedskultur og værdier i overensstemmelse med afsnit 10, som fremmer en ansvarlig og etisk adfærd, herunder en adfærdskodeks eller et lignende instrument

l. en politik for interessekonflikter på institutionelt plan i overensstemmelse med afsnit 11 og for medarbejdere i overensstemmelse med afsnit 12 og

m. ordninger, der har til formål at sikre integriteten af systemerne til regnskabsføring og finansiel rapportering, herunder hvad angår finansiel og operationel kontrol og overholdelse af love og relevante standarder.

24. Når ledelsesorganet fastsætter, godkender og fører tilsyn med gennemførelsen af de aspekter, der er anført i punkt 22, bør det tilstræbe at sikre en forretningsmodel og ledelsesordning, herunder en risikostyringsramme, der tager højde for alle risici. Når institutterne tager højde for alle risici, bør de tage hensyn til alle relevante risikofaktorer, herunder miljømæssige, sociale og ledelsesmæssige risikofaktorer. Institutterne bør tage hensyn til, at sidstnævnte kan være drivkraften bag deres tilsynsmæssige risici, herunder kreditrisici, f.eks. via risikofaktorer i forbindelse med omstillingen til en bæredygtig økonomi eller eksterne fysiske klimarelaterede hændelser, der kan påvirke debitorer, markeder, likviditet, operationelle risici og også omdømmemæssige risici, bl.a. via sociale og ledelsesmæssige risikofaktorer, f.eks. i forbindelse med outsourcingaftaler[10]. Sådanne risici omfatter f.eks. juridiske risici inden for aftale- eller arbejdsret, risici i forbindelse med potentielle krænkelser af menneskerettighederne eller andre ESG-risikofaktorer, der kan påvirke det land, hvor en tjenesteyder er etableret, og dennes evne til at levere de aftalte serviceniveauer.

25. Ledelsesorganet skal føre tilsyn med offentliggørelses- og kommunikationsprocessen i forhold til eksterne interessenter og kompetente myndigheder.

26. Alle medlemmer af ledelsesorganet bør informeres om instituttets generelle aktiviteter, finansielle situation og risikosituation under hensyntagen til det økonomiske miljø samt om trufne beslutninger, der i høj grad indvirker på instituttets virksomhed.

27. Et medlem af ledelsesorganet kan være ansvarligt for en intern kontrolfunktion, jf. del V, afsnit 19.1, forudsat at medlemmet ikke har andre mandater, der ville bringe medlemmets interne kontrolaktiviteter og den interne kontrolfunktions uafhængighed i fare.

28. Ledelsesorganet bør overvåge, regelmæssigt gennemgå og afhjælpe svagheder, der er identificeret vedrørende gennemførelsen af processer, strategier og politikker i forbindelse med de ansvarsområder, der er omhandlet i punkt 22 og 23. Rammen for intern ledelse og

[10] Se EBA's rapport om ESG-risikostyring og -tilsyn offentliggjort i henhold til artikel 98, stk. 8, i kapitalkravsdirektivet for en beskrivelse af EBA's forståelse af ESG-risici, transmissionskanaler og anbefalinger til ordninger, processer, mekanismer og strategier, som institutterne skal gennemføre for at identificere, vurdere og styre ESG-risici.

gennemførelsen heraf bør gennemgås og opdateres jævnligt under hensyntagen til proportionalitetsprincippet, som yderligere forklaret i del I. En mere indgående gennemgang bør foretages, når væsentlige ændringer påvirker instituttet.

2 Ledelsesorganets ledelsesfunktion

29. Ledelsesorganet i dets ledelsesfunktion bør engagere sig aktivt i et instituts drift og træffe beslutninger på et betryggende og velinformeret grundlag.

30. Ledelsesorganet i dets ledelsesfunktion bør være ansvarlig for gennemførelsen af de af ledelsesorganet fastlagte strategier og løbende diskutere gennemførelsen og hensigtsmæssigheden af disse strategier med ledelsesorganet i dets tilsynsfunktion. Den operationelle gennemførelse kan udføres af instituttets ledelse.

31. Ledelsesorganet i dets ledelsesfunktion bør konstruktivt udfordre og kritisk gennemgå forslag, redegørelser og oplysninger, der modtages, når det udøver sit skøn og træffer beslutninger. Ledelsesorganet i dets ledelsesfunktion bør rapportere fyldestgørende til og løbende — og om nødvendigt hurtigst muligt — give ledelsesorganet i dets tilsynsfunktion information om de elementer, der er relevante for vurderingen af en situation, de risici og udviklinger, der påvirker eller kan påvirke instituttet, f.eks. væsentlige beslutninger om forretningsaktiviteter og de risici, der er taget, evalueringen af instituttets økonomiske miljø og forretningsmiljø, likviditet og sundt kapitalgrundlag og vurdering af dets væsentlige risikoeksponeringer.

32. Med forbehold af gennemførelsen af direktiv (EU) 2015/849 i national lovgivning bør ledelsesorganet udpege et af sine medlemmer i overensstemmelse med kravene i artikel 46, stk. 4, i direktiv (EU) 2015/849 om bekæmpelse af hvidvaskning af penge, som er ansvarligt for gennemførelsen af de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv, herunder de tilsvarende politikker og procedurer for bekæmpelse af hvidvask af penge og finansiering af terrorisme (AML/CFT) i instituttet og på ledelsesorganniveau[11].

3 Ledelsesorganets tilsynsfunktion

33. Medlemmerne af ledelsesorganet i dets tilsynsfunktion bør have til opgave bl.a. at overvåge og konstruktivt udfordre instituttets strategi.

34. Med forbehold af national ret bør ledelsesorganet i dets tilsynsfunktion omfatte uafhængige medlemmer som omhandlet i afsnit 9.3 i ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

35. Med forbehold af ansvarsområderne i henhold til gældende national selskabsret bør ledelsesorganet i dets tilsynsfunktion:

[11] Ledelsesorganet som kollegialt organ er fortsat ansvarligt som helhed.

a. føre tilsyn med og overvåge ledelsens beslutningstagning og handlinger og føre effektivt tilsyn med ledelsesorganet i dets ledelsesfunktion, herunder overvågning og undersøgelse af dets individuelle og kollektive resultater og gennemførelsen af instituttets strategi og mål

b. konstruktivt udfordre og kritisk gennemgå forslag og oplysninger, som stilles til rådighed af medlemmer af ledelsesorganet i dets ledelsesfunktion, samt dets beslutninger

c. under hensyntagen til proportionalitetsprincippet som omhandlet i del I, varetage risikoudvalgets, aflønningsudvalgets og nomineringsudvalgets opgaver og rolle, hvis der ikke er nedsat sådanne udvalg

d. sikre og regelmæssigt vurdere effektiviteten af instituttets ramme for intern ledelse og træffe passende foranstaltninger med henblik på at afhjælpe eventuelle konstaterede mangler

e. føre tilsyn med og overvåge, at instituttets strategiske mål, organisatoriske struktur og risikostrategi, dets risikoappetit og rammer for risikostyring, samt andre politikker (f.eks. aflønningspolitik) og offentliggørelsesramme gennemføres konsekvent

f. overvåge, at instituttets risikokultur gennemføres konsekvent

g. føre tilsyn med gennemførelsen og opretholdelsen af et adfærdskodeks eller lignende og effektive politikker til identifikation, håndtering og afhjælpning af faktiske og potentielle interessekonflikter

h. føre tilsyn med integriteten af finansielle oplysninger og finansiel rapportering og rammen for intern kontrol, herunder en effektiv og solid ramme for risikostyring

i. sikre, at lederne af interne kontrolfunktioner er i stand til at handle uafhængigt og — uanset ansvaret for at rapportere til andre interne organer, forretningsområder eller enheder — kan give udtryk for betænkeligheder og advare ledelsesorganet i dets tilsynsfunktion direkte, når det er nødvendigt, hvis ugunstige risikoudviklinger påvirker eller kan påvirke instituttet, og

j. overvåge gennemførelsen af den interne revisionsplan, efter forudgående inddragelse af risikoudvalget og revisionsudvalget, hvis sådanne udvalg er nedsat.

4 Ledelsesorganets formands rolle

36. Ledelsesorganets formand bør stå for ledelsen af ledelsesorganet, bidrage til en effektiv informationsstrøm inden for ledelsesorganet og mellem ledelsesorganet og dets udvalg, hvis sådanne er nedsat, og være ansvarlig for, at det generelt fungerer effektivt.

37. Formanden bør tilskynde til og fremme en åben og kritisk diskussion og sikre, at afvigende synspunkter kan komme til orde og diskuteres i forbindelse med beslutningsprocessen.

38. Som et generelt princip bør ledelsesorganets formand være et ikke-ledende medlem. Hvis formanden har tilladelse til at påtage sig ledende opgaver, bør instituttet have indført foranstaltninger til at afhjælpe en eventuel negativ indvirkning på instituttets kontrolforanstaltninger (f.eks. ved at udpege et ledende bestyrelsesmedlem eller et højtstående uafhængigt bestyrelsesmedlem eller ved at have et større antal ikke-ledende medlemmer i ledelsesorganet i dets tilsynsfunktion). I henhold til artikel 88, stk. 1, litra e), i direktiv 2013/36/EU må formanden for ledelsesorganet i dets tilsynsfunktion i et institut navnlig ikke samtidig udøve de funktioner, der påhviler en administrerende direktør i samme institut, medmindre instituttet begrunder dette, og de kompetente myndigheder har givet deres tilladelse hertil.

39. Formanden bør fastlægge mødedagsordener og sikre, at strategiske spørgsmål drøftes med prioritet. Formanden bør sikre, at ledelsesorganets beslutninger træffes på et betryggende og velinformeret grundlag, og at dokumenter modtages i tilstrækkelig god tid inden mødet.

40. Ledelsesorganets formand bør bidrage til en klar opgavefordeling mellem ledelsesorganets medlemmer og eksistensen af en effektiv informationsstrøm mellem dem, for at gøre det muligt for medlemmerne af ledelsesorganet i dets tilsynsfunktion at bidrage konstruktivt til drøftelser og afgive deres stemmer på et betryggende og velinformeret grundlag.

5 Udvalg under ledelsesorganet i dets tilsynsfunktion

5.1 Nedsættelse af udvalg

41. I henhold til artikel 109, stk. 1, i direktiv 2013/36/EU sammenholdt med artikel 76, stk. 3, artikel 88, stk. 2, og artikel 95, stk. 1, i direktiv 2013/36/EU skal alle institutter, der selv er væsentlige på grundlag af det individuelle, delkonsoliderede og konsoliderede niveau, nedsætte risiko-, nominerings- [12] og aflønningsudvalg [13] med henblik på at rådgive ledelsesorganet i dets tilsynsfunktion og forberede de beslutninger, der skal træffes af dette organ. Ikke-væsentlige institutter, herunder når de er inden for anvendelsesområdet for den tilsynsmæssige konsolidering af et institut, der er væsentligt i en delkonsolideret eller konsolideret situation, er ikke forpligtet til at nedsætte disse udvalg.

42. Hvis et risiko- eller nomineringsudvalg ikke er nedsat, bør henvisningerne i disse retningslinjer til disse udvalg anses for at gælde for ledelsesorganet i dets tilsynsfunktion under hensyntagen til proportionalitetsprincippet som omhandlet i del I.

[12] Jf. også ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.
[13] Med hensyn til aflønningsudvalget henvises til EBA's retningslinjer vedrørende forsvarlig aflønningspraksis.

43. Institutterne kan under hensyntagen til kriterierne i del I i disse retningslinjer nedsætte andre udvalg (f.eks. udvalg til bekæmpelse af hvidvaskning af penge og finansiering af terrorisme (AML/CTF), etisk udvalg, adfærds- og complianceudvalg).

44. Institutterne bør sikre en klar tildeling og fordeling af pligter og opgaver mellem ledelsesorganets specialiserede udvalg.

45. Hvert udvalg bør have et dokumenteret mandat, herunder dets ansvarsområder, fra ledelsesorganet i dets tilsynsfunktion og etablere hensigtsmæssige arbejdsprocedurer.

46. Udvalgene bør understøtte tilsynsfunktionen på specifikke områder og fremme udviklingen og gennemførelsen af en solid ramme for intern ledelse. En uddelegering til udvalg friholder på ingen måde ledelsesorganet i dets tilsynsfunktion fra kollektivt at opfylde sine pligter og sit ansvar.

5.2 Udvalgenes sammensætning[14]

47. Alle udvalg bør som formand have et ikke-ledende medlem af ledelsesorganet, som kan udøve et objektivt skøn.

48. Uafhængige medlemmer[15] af ledelsesorganet i dets tilsynsfunktion bør deltage aktivt i et udvalg.

49. Hvis der skal nedsættes udvalg i henhold til direktiv 2013/36/EU eller national ret, bør de bestå af mindst tre medlemmer.

50. Institutterne bør under hensyntagen til ledelsesorganets størrelse og antallet af uafhængige medlemmer af ledelsesorganet i dets tilsynsfunktion sikre, at udvalgene ikke er sammensat af den samme gruppe af medlemmer, der udgør et andet udvalg.

51. Institutterne bør overveje lejlighedsvis rotation af formænd og udvalgsmedlemmer under hensyntagen til den specifikke erfaring, viden og kompetence, der individuelt eller kollektivt kræves til disse udvalg.

52. Risiko- og nomineringsudvalget bør være sammensat af ikke-ledende medlemmer af det pågældende instituts ledelsesorgan i dets tilsynsfunktion. Revisionsudvalget bør være sammensat i overensstemmelse med artikel 41 i direktiv 2006/43/EF[16]. Aflønningsudvalget

[14] Dette afsnit bør sammenholdes med ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.
[15] Som defineret i afsnit 9.3 i ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.
[16] Europa-Parlamentets og Rådets direktiv 2006/43/EF af 17. maj 2006 om lovpligtig revision af årsregnskaber og konsoliderede regnskaber, om ændring af Rådets direktiv 78/660/EØF og 83/349/EØF og om ophævelse af Rådets direktiv 84/253/EØF (EUT L 157 af 9.6.2006, s. 87), senest ændret ved Europa-Parlamentets og Rådets direktiv 2014/56/EU af 16. april 2014.

bør være sammensat i overensstemmelse med afsnit 2.4.1 i EBA's retningslinjer vedrørende forsvarlige aflønningspolitikker[17].

53. I G-SII'er og O-SII'er bør nomineringsudvalget omfatte et flertal af medlemmer, der er uafhængige, og formanden bør være et uafhængigt medlem. I andre væsentlige institutter, der identificeres af de kompetente myndigheder eller national ret, bør nomineringsudvalget omfatte et tilstrækkeligt antal medlemmer, som er uafhængige; sådanne institutter kan også anse det som god praksis, at nomineringsudvalgets formand er uafhængig.

54. Medlemmerne af nomineringsudvalget bør individuelt eller kollektivt have tilstrækkelig viden, kompetence og ekspertise vedrørende udvælgelsesprocessen og egnethedskravene som fastsat i direktiv 2013/36/EU.

55. I G-SII'er og O-SII'er bør risikoudvalget omfatte et flertal af medlemmer, der er uafhængige. I G-SII'er og O-SII'er bør risikoudvalgets formand være et uafhængigt medlem. I andre væsentlige institutter, der identificeres af de kompetente myndigheder eller national ret, bør risikoudvalget omfatte et tilstrækkeligt antal medlemmer, som er uafhængige, og risikoudvalgets formand bør om muligt være et uafhængigt medlem. I alle institutter bør risikoudvalgets formand hverken være formand for ledelsesorganet eller formand for noget andet udvalg.

56. Medlemmerne af risikoudvalget bør individuelt eller kollektivt have tilstrækkelig viden, kompetence og ekspertise vedrørende risikostyring og kontrolpraksis.

5.3 Udvalgsprocesser

57. Udvalgene bør regelmæssigt aflægge rapport til ledelsesorganet i dets tilsynsfunktion.

58. Udvalgene bør fungere i samspil med hinanden i det omfang, det er relevant. Med forbehold af punkt 49 kunne et sådant samspil være i form at krydsdeltagelse, således at formanden eller et medlem af et udvalg ligeledes kan være medlem af et andet udvalg.

59. Udvalgsmedlemmerne bør indgå i åbne og kritiske diskussioner, hvor afvigende synspunkter drøftes på en konstruktiv måde.

60. Udvalgene bør dokumentere dagsordenerne for udvalgsmøderne og de vigtigste resultater og konklusioner heraf.

61. Risiko- og nomineringsudvalgene bør som minimum:

    a. have adgang til alle relevante oplysninger og data, der er nødvendige for at varetage deres rolle, herunder oplysninger og data fra relevante stabs- og kontrolfunktioner (f.eks. i henseende til retlige anliggender, økonomi, menneskelige ressourcer, IT, intern revision, risiko, compliance, herunder oplysninger om efterkommelse af

[17] EBA's retningslinjer vedrørende forsvarlige aflønningspolitikker i henhold til artikel 74, stk. 3, og artikel 75, stk. 2, i direktiv 2013/36/EU og oplysninger i henhold til artikel 450 i forordning (EU) nr. 575/2013 (EBA/GL/2015/22).

procedurer for AML/CTF og aggregerede oplysninger om indberetninger af mistænkelige transaktioner og ML/TF-risikofaktorer

b. modtage regelmæssige rapporter, ad hoc-oplysninger, meddelelser og udtalelser fra ledere af interne kontrolfunktioner vedrørende instituttets nuværende risikoprofil, dets risikokultur og risikogrænser samt om eventuelle væsentlige overtrædelser[18], der måtte have fundet sted, med detaljerede oplysninger om og anbefalinger til korrigerende foranstaltninger, der er truffet, skal træffes eller er foreslået med henblik på at afhjælpe dem, regelmæssigt gennemgå og træffe beslutning om indholdet, formatet og hyppigheden af de oplysninger om risici, der skal indberettes til dem, og

c. når det er nødvendigt, sikre passende inddragelse af de interne kontrolfunktioner og andre relevante funktioner (menneskelige ressourcer, retlige anliggender, økonomi) inden for deres respektive ekspertiseområder og/eller søge ekstern ekspertrådgivning.

5.4 Risikoudvalgets rolle

62. Hvis et risikoudvalg er nedsat, bør det som minimum:

a. rådgive og støtte ledelsesorganet i dets tilsynsfunktion vedrørende overvågningen af instituttets overordnede nuværende og fremtidige risikostrategi og risikoappetit, under hensyntagen til alle former for risici, for at sikre, at de er i overensstemmelse med instituttets forretningsstrategi, mål, virksomhedskultur og værdier

b. bistå ledelsesorganet i dets tilsynsfunktion med at overvåge gennemførelsen af instituttets risikostrategi og de tilsvarende grænser, der er fastsat

c. føre tilsyn med gennemførelsen af strategierne for kapital- og likviditetsstyring samt for alle andre relevante risici for et institut, såsom markeds- og kreditrisici, operationelle risici (herunder retlige risici og IT-risici) og omdømmemæssige risici, for at vurdere deres tilstrækkelighed i forhold til den godkendte risikostrategi og risikoappetit

d. fremsætte anbefalinger til ledelsesorganet i dets tilsynsfunktion om nødvendige tilpasninger af risikostrategien som følge af bl.a. ændringer af instituttets forretningsmodel, markedsudviklinger eller anbefalinger fra risikostyringsfunktionen

e. rådgive om udpegelsen af eksterne konsulenter, som tilsynsfunktionen måtte beslutte at ansætte med henblik på rådgivning eller støtte

[18] Med hensyn til alvorlige overtrædelser på AML/TF-området. Der henvises også til de retningslinjer, der skal udstedes i henhold til artikel 117, stk. 6, i direktiv 2013/36/EU, hvori det præciseres, hvordan samarbejdet og informationsudvekslingen mellem de myndigheder, der er omhandlet i stk. 5 i denne artikel, skal foregå, navnlig i forbindelse med grænseoverskridende koncerner og i forbindelse med identifikation af grove overtrædelser af reglerne om bekæmpelse af hvidvaskning af penge.

f. afdække en række mulige scenarier, herunder stressscenarier, med henblik på at vurdere, hvordan instituttets risikoprofil ville reagere på eksterne og interne begivenheder

g. føre tilsyn med overensstemmelsen mellem alle væsentlige finansielle produkter og tjenesteydelser, der tilbydes kunderne, og instituttets forretningsmodel og risikostrategi[19]. Risikoudvalget bør vurdere de risici, der er forbundet med de tilbudte finansielle produkter og tjenesteydelser, og tage hensyn til overensstemmelsen mellem priserne for og gevinsterne ved disse produkter og tjenesteydelser, og

h. vurdere anbefalingerne fra interne eller eksterne revisorer og følge op på, om de trufne foranstaltninger er gennemført korrekt.

63. Risikoudvalget bør samarbejde med andre udvalg, hvis aktiviteter kan have indvirkning på risikostrategien (f.eks. revisions- og aflønningsudvalg) og løbende kommunikere med instituttets interne kontrolfunktioner, navnlig risikostyringsfunktionen.

64. Hvis et risikoudvalg er nedsat, skal det — uden dermed at gribe ind i aflønningsudvalgets opgaver — undersøge, om incitamenterne i aflønningspolitikken og -praksissen tager hensyn til instituttets risiko, kapital og likviditet samt sandsynligheden og tidspunkterne for fortjeneste.

5.5 Revisionsudvalgets rolle

65. I henhold til direktiv 2006/43/EF[20] bør revisionsudvalget, hvis et sådant er nedsat, bl.a.:

a. overvåge, om instituttets interne kvalitetskontrol- og risikostyringssystemer, og i givet fald dets interne revisionsfunktion, fungerer effektivt med hensyn til regnskabsaflæggelsen i det reviderede institut, uden at krænke dets uafhængighed

b. føre tilsyn med instituttets fastlæggelse af regnskabspolitikker

c. overvåge den finansielle rapporteringsproces og fremsætte henstillinger med henblik på at sikre integriteten

d. kontrollere og overvåge revisorernes eller revisionsfirmaernes uafhængighed i overensstemmelse med artikel 22, 22a, 22b, 24a og 24b i direktiv 2006/43/EF og artikel

[19] Jf. også EBA's retningslinjer vedrørende produktudviklings- og produktstyringsprocesser for detailbankprodukter, findes på http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

[20] Europa-Parlamentets og Rådets direktiv 2006/43/EF af 17. maj 2006 om lovpligtig revision af årsregnskaber og konsoliderede regnskaber, om ændring af Rådets direktiv 78/660/EØF og 83/349/EØF og om ophævelse af Rådets direktiv 84/253/EØF (EUT L 157 af 9.6.2006, s. 87), senest ændret ved Europa-Parlamentets og Rådets direktiv 2014/56/EU af 16. april 2014.

6 i forordning (EU) nr. 537/2014[21], og navnlig hensigtsmæssigheden ved udførelsen af ikke-revisionsydelser for det reviderede institut, jf. artikel 5 i nævnte forordning

e. overvåge den lovpligtige revision af årsregnskabet og det konsoliderede regnskab, navnlig udførelsen heraf, under hensyntagen til den kompetente myndigheds resultater og konklusioner i henhold til artikel 26, stk. 6, i forordning (EU) nr. 537/2014

f. være ansvarligt for proceduren for udvælgelse af eksterne revisorer eller revisionsfirmaer og indstille til instituttets kompetente organs godkendelse angående deres udnævnelse (i overensstemmelse med artikel 16 i forordning (EU) nr. 537/2014, medmindre artikel 16, stk. 8, i forordning (EU) nr. 537/2014 finder anvendelse), honorering og afskedigelse

g. gennemgå revisionens omfang og hyppigheden af den lovpligtige revision af årsregnskaber og konsoliderede regnskaber

h. i overensstemmelse med artikel 39, stk. 6, litra a), i direktiv 2006/43/EF underrette bestyrelsen eller tilsynsorganet i den reviderede virksomhed om resultatet af den lovpligtige revision og forklare, hvordan den lovpligtige revision bidrog til regnskabsaflæggelsens integritet, og hvad revisionsudvalgets rolle var i den proces, og

i. modtage og tage hensyn til revisionsrapporter.

5.6 Kombinerede udvalg

66. I henhold til artikel 76, stk. 3, i direktiv 2013/36/EU kan de kompetente myndigheder tillade, at institutter, der ikke anses for at være væsentlige, kombinerer risikoudvalget med det revisionsudvalg — hvis et sådant er nedsat — der er omhandlet i artikel 39 i direktiv 2006/43/EF.

67. Hvis risiko- og nomineringsudvalg er nedsat i ikke-væsentlige institutter, kan de kombinere udvalgene. Hvis de gør dette, bør disse institutter dokumentere, hvorfor de har valgt at kombinere udvalgene, og hvordan tilgangen opnår udvalgenes mål.

68. Institutterne bør til enhver tid sikre, at medlemmerne af et kombineret udvalg individuelt og kollektivt besidder den nødvendige viden, kompetence og ekspertise til fuldt ud at forstå de opgaver, der skal varetages af det kombinerede udvalg[22].

[21] Europa-Parlamentets og Rådets forordning (EU) nr. 537/2014 af 16. april 2014 om specifikke krav til lovpligtig revision af virksomheder af interesse for offentligheden og om ophævelse af Kommissionens afgørelse 2005/909/EF (EUT L 158 af 27.5.2014, s. 77).

[22] Jf. også ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

Del III — Ledelsesramme

6 Organisatorisk ramme og struktur

6.1 Organisatorisk ramme

69. Ledelsesorganet i et institut bør sikre en passende og gennemsigtig organisatorisk og operationel struktur for dette institut og have en skriftlig beskrivelse heraf. Strukturen bør fremme og afspejle et instituts effektive og forsigtige forvaltning på individuelt, delkonsolideret og konsolideret niveau. Ledelsesorganet bør sikre, at de interne kontrolfunktioner er uafhængige af de forretningsområder, de kontrollerer, herunder at der er en tilstrækkelig funktionsadskillelse, og at de har de nødvendige finansielle og menneskelige ressourcer samt beføjelser til at varetage deres rolle effektivt. Rapporteringslinjerne og fordelingen af ansvar, navnlig blandt personer med nøglefunktioner, i et institut bør være klare, veldefinerede og sammenhængende, kunne håndhæves og være behørigt dokumenteret. Dokumentationen bør opdateres efter behov.

70. Instituttets struktur bør ikke hindre ledelsesorganets mulighed for at overvåge og håndtere de risici effektivt, som instituttet eller koncernen står over for, eller den kompetente myndigheds mulighed for at føre effektivt tilsyn med instituttet.

71. Ledelsesorganet bør vurdere, om og hvordan væsentlige ændringer i koncernstrukturen (f.eks. oprettelsen af nye datterselskaber, fusioner og overtagelser, frasalg eller opløsning af dele af koncernen eller eksterne udviklinger) påvirker soliditeten af instituttets organisatoriske ramme. Hvis der identificeres svagheder, bør ledelsesorganet gennemføre alle nødvendige justeringer hurtigt.

6.2 Kendskab til strukturen ("know your structure")

72. Ledelsesorganet bør fuldt ud kende og forstå instituttets retlige, organisatoriske og operationelle struktur ("know your structure") og sikre, at denne stemmer overens med instituttets godkendte forretnings- og risikostrategi og risikoappetit og er omfattet af dets risikostyringsramme.

73. Ledelsesorganet bør være ansvarligt for vedtagelsen af forsvarlige strategier og politikker for etablering af nye strukturer. Hvis et institut opretter mange juridiske enheder i sin koncern, bør deres antal, og især de indbyrdes forbindelser og transaktioner mellem dem, ikke give anledning til problemer for udformningen af dets interne ledelse og for en effektiv styring af og et effektivt tilsyn med risiciene for koncernen som helhed. Ledelsesorganet bør sikre, at et instituts struktur, og i givet fald strukturerne i en koncern, under hensyntagen til kriterierne i afsnit 7, er klare, effektive og gennemsigtige for instituttets medarbejdere, aktionærer og andre interessenter og for den kompetente myndighed.

74. Ledelsesorganet bør lede instituttets struktur, dets udvikling og begrænsninger og bør sikre, at strukturen er begrundet og effektiv og ikke medfører unødig eller uhensigtsmæssig kompleksitet.

75. Ledelsesorganet i et konsoliderende institut bør ikke alene forstå koncernens retlige, organisatoriske og operationelle struktur, men også formålet med og aktiviteterne i dens forskellige enheder og sammenhængen og forbindelserne mellem dem. Hertil hører en forståelse af koncernspecifikke operationelle risici og engagementer inden for koncernen samt af, hvordan koncernens finansiering, kapital, likviditet og risikoprofiler vil kunne blive påvirket under normale og under negative omstændigheder. Ledelsesorganet bør sikre, at instituttet er i stand til at udarbejde rettidig information om koncernen vedrørende den enkelte retlige enheds type, karakteristika, organisationsplan, ejerstruktur og aktivitetsområder, og at institutterne inden for koncernen overholder alle tilsynsmæssige rapporteringskrav på individuelt, delkonsolideret og konsolideret grundlag.

76. Ledelsesorganet i et konsoliderende institut bør sikre, at de forskellige enheder i koncernen (herunder det konsoliderende institut selv) modtager tilstrækkelig information til at få en klar opfattelse af koncernens generelle mål, strategier og risikoprofil og af, hvordan den pågældende koncernenhed er indlejret i koncernens struktur og operationelle funktion. En sådan information og revisioner heraf bør dokumenteres og stilles til rådighed for de pågældende relevante funktioner, herunder ledelsesorganet, forretningsområder og interne kontrolfunktioner. Medlemmerne af ledelsesorganet i et konsoliderende institut bør holde sig selv informeret om de risici, som koncernens struktur giver anledning til, under hensyntagen til kriterierne i afsnit 7 i retningslinjerne. Hertil hører modtagelse af:

    a. information om væsentlige risikofaktorer

    b. regelmæssige rapporter, der vurderer instituttets generelle struktur og vurderer, om aktiviteterne i de enkelte enheder overholder den godkendte koncernstrategi, og

    c. regelmæssige rapporter om emner, hvor regelsættet kræver overholdelse på individuelt, delkonsolideret og konsolideret niveau.

6.3 Komplekse strukturer og ikke-standardiserede eller uigennemsigtige aktiviteter

77. Institutterne bør undgå at oprette komplekse og potentielt uigennemsigtige strukturer. Institutterne bør i deres beslutningstagning tage hensyn til resultaterne af en risikovurdering, der er foretaget for at afdække, om sådanne strukturer kunne anvendes til et formål i tilknytning til hvidvaskning af penge, finansiering af terrorisme eller anden økonomisk

kriminalitet, og de respektive kontrolforanstaltninger og retlige rammer, der er indført[23]. Med henblik herpå bør institutterne som minimum tage hensyn til følgende:

a. i hvilket omfang den jurisdiktion, hvor strukturen vil blive etableret, effektivt overholder EU-standarder og internationale standarder om gennemsigtighed på skatteområdet, bekæmpelse af hvidvaskning af penge og finansiering af terrorisme[24]

b. i hvilket omfang strukturen tjener et åbenbart økonomisk og lovligt formål

c. i hvilket omfang strukturen kunne anvendes til at skjule identiteten af den ultimative reelle ejer

d. i hvilket omfang kundens anmodning, som fører til den eventuelle etablering af en struktur, giver anledning til bekymring

e. om strukturen kunne hindre et effektivt tilsyn fra instituttets ledelsesorgan eller instituttets mulighed for håndtere den dermed forbundne risiko, og

f. om strukturen udgør hindringer for de kompetente myndigheders effektive tilsyn.

78. Under alle omstændigheder bør institutterne ikke etablere uigennemsigtige og unødvendigt komplekse strukturer, som ikke har nogen klar økonomisk begrundelse eller noget klart retligt formål, eller strukturer, der kan give anledning til bekymring over, om de oprettes med henblik på økonomisk kriminalitet.

79. Ved etableringen af sådanne strukturer bør ledelsesorganet forstå dem og deres formål og de særlige risici, der er forbundet med dem, og sikre, at de interne kontrolfunktioner er tilstrækkeligt involveret. Sådanne strukturer bør kun godkendes og bibeholdes, når deres formål er blevet klart defineret og forstået, og når ledelsesorganet finder det godtgjort, at alle væsentlige risici, herunder omdømmemæssige risici, er blevet identificeret, at alle risici kan håndteres effektivt og rapporteres i tilstrækkeligt omfang, og at et effektivt tilsyn er sikret. Jo mere kompleks og uigennemsigtig den organisatoriske og operationelle struktur er og jo større risici, jo mere intensiv bør tilsynet med strukturen være.

80. Institutterne bør dokumentere deres beslutninger og kunne begrunde deres beslutninger over for de kompetente myndigheder.

81. Ledelsesorganet bør sikre, at der træffes passende foranstaltninger for at undgå eller afhjælpe risiciene ved aktiviteter inden for sådanne strukturer. Herunder sikres det bl.a., at:

[23] For yderligere oplysninger om vurderingen af landerisiko og den risiko, der er forbundet med individuelle produkter og kunder, bør institutterne også henvise til de fælles retningslinjer vedrørende ML/TF-risikofaktorer (EBA GL JC/2017/37), der er under revision.

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

a. instituttet har indført passende politikker og procedurer samt dokumenterede processer (f.eks. gældende grænser, informationsstrømme), der gør det muligt at overveje, overholde og godkende sådanne aktiviteter og håndtere risiciene i forbindelse hermed, samtidig med at der tages hensyn til konsekvenserne for koncernens organisatoriske og operationelle struktur, dens risikoprofil og omdømmemæssige risiko

b. information om disse aktiviteter og risiciene i forbindelse hermed er tilgængelig for det konsoliderende institut og interne og eksterne revisorer og rapporteres til ledelsesorganet i dets tilsynsfunktion og til den kompetente myndighed, der meddelte tilladelse, og

c. instituttet med jævne mellemrum vurderer det fortsatte behov for at bibeholde sådanne strukturer.

82. Disse strukturer og aktiviteter, herunder deres overholdelse af lovgivning og faglige standarder, bør være underkastet regelmæssig revision udført af den interne revisionsfunktion på grundlag af en risikobaseret tilgang.

83. Institutterne bør træffe de samme risikostyringsforanstaltninger som i forbindelse med instituttets egne forretningsaktiviteter, når de udfører kundeaktiviteter, der ikke er standard eller ikke er gennemsigtige (f.eks. hjælp til kunder med at oprette enheder i offshorecentre, udvikling af komplekse strukturer, finansiering af transaktioner for dem eller tilbud om formueforvaltning), og som stiller den interne ledelse over for lignende udfordringer og giver anledning til betydelige operationelle og omdømmemæssige risici. Institutterne bør navnlig analysere baggrunden for, at en kunde ønsker at etablere en særlig struktur.

7 Organisatorisk ramme i koncernsammenhæng

84. I henhold til artikel 109, stk. 2, i direktiv 2013/36/EU bør moderselskaber og datterselskaber, der er omfattet af det pågældende direktiv, sikre, at ledelsesordninger, -processer og -mekanismer er konsekvente og velintegrerede på et konsolideret og delkonsolideret grundlag. Med henblik herpå bør moderselskaber og datterselskaber inden for konsolideringsreglernes anvendelsesområde gennemføre sådanne ordninger, processer og mekanismer i deres datterselskaber, som ikke er omfattet af direktiv 2013/36/EU, herunder dem, som er etableret i tredjelande, bl.a. i offshore-finanscentre, for at sikre robuste ledelsesordninger på konsolideret og delkonsolideret grundlag. For så vidt angår aflønningskravene, finder visse undtagelser i overensstemmelse med artikel 109, stk. 4 og stk. 5 anvendelse [25]. De kompetente funktioner i det konsoliderende institut og dets datterselskaber bør samarbejde og udveksle data og informationer efter behov. Ledelsesordningerne, -processerne og -mekanismerne bør sikre, at det konsoliderende institut har tilstrækkelige data og informationer og er i stand til at vurdere koncernens risikoprofil, som nærmere beskrevet i afsnit 6.2.

[25] Der henvises ligeledes til EBA's retningslinjer vedrørende forsvarlige aflønningspolitikker.

85. Ledelsesorganet i et datterselskab, som er omfattet af direktiv 2013/36/EU, bør på individuelt niveau vedtage og gennemføre koncernledelsespolitikker, der er fastsat på konsolideret eller delkonsolideret niveau, på en måde, der overholder alle specifikke krav i henhold til EU-retten og national ret.

86. På konsolideret og delkonsolideret niveau bør det konsoliderende institut sikre, at alle institutter og andre enheder, der er omfattet af konsolideringsreglernes anvendelsesområde, herunder deres datterselskaber, der ikke selv er omfattet af direktiv 2013/36/EU, overholder de koncerndækkende ledelsespolitikker og interne kontrolrammer, der er omhandlet i afsnit V. Ved gennemførelsen af ledelsespolitikker bør det konsoliderende institut sikre, at der er indført robuste ledelsesordninger for hvert datterselskab, og overveje specifikke ordninger, processer og mekanismer, hvis forretningsaktiviteterne ikke er organiseret i separate juridiske enheder, men inden for en matrix af forretningsområder, der omfatter flere juridiske enheder.

87. Et konsoliderende institut bør tage hensyn til alle dets datterselskabers interesser, og hvordan strategier og politikker bidrager til hvert enkelt datterselskabs interesse og koncernen som helheds interesse på lang sigt.

88. Moderselskaber og deres datterselskaber bør sikre, at institutterne og enhederne inden for koncernen overholder alle specifikke myndighedskrav i en relevant jurisdiktion.

89. Det konsoliderende institut bør sikre, at datterselskaber, der er etableret i tredjelande, og som er omfattet af konsolideringsreglernes anvendelsesområde, har indført ledelsesordninger, -processer og -mekanismer, som er i overensstemmelse med koncernledelsespolitikker og overholder kravene i artikel 74-96 i direktiv 2013/36/EU og disse retningslinjer, så længe dette ikke strider mod lovgivningen i tredjelandet.

90. Ledelseskravene i direktiv 2013/36/EU og bestemmelserne i disse retningslinjer gælder for institutter uden hensyntagen til, om de er datterselskaber af et moderselskab i et tredjeland. Hvis et EU-datterselskab af et moderselskab i et tredjeland er et konsoliderende institut, omfatter konsolideringsreglernes anvendelsesområde ikke niveauet for det moderselskab, der er beliggende i et tredjeland, og andre direkte datterselskaber af dette moderselskab. Det konsoliderende institut bør sikre, at koncernledelsespolitikken for moderinstituttet i et tredjeland tages i betragtning i dets egne ledelsespolitikker, for så vidt som denne politik ikke er i strid med kravene i den relevante EU-ret, herunder direktiv 2013/36/EU og de yderligere betingelser i disse retningslinjer.

91. Når institutterne fastsætter politikker og dokumenterer ledelsesordninger, bør de tage hensyn til de aspekter, der er anført i bilag I til retningslinjerne. Selv om politikker og dokumentation kan omfattes af separate dokumenter, bør institutterne overveje at kombinere dem eller henvise til dem i et enkelt ledelsesrammedokument.

8 Outsourcingpolitik[26]

92. Ledelsesorganet bør godkende og løbende revidere og opdatere et instituts outsourcingpolitik og sikre, at relevante ændringer gennemføres rettidigt.

93. Outsourcingpolitikken bør beskæftige sig med konsekvenserne af outsourcing for et instituts virksomhed og de risici, det står over for (f.eks. operationelle risici, herunder retlige risici og IT-risici, omdømmemæssige risici og koncentrationsrisici). Politikken bør omfatte de ordninger for indberetning og overvågning, der skal gennemføres fra en outsourcingaftales start til dens ophør (herunder udarbejdelsen af en business case for outsourcing, indgåelsen af en outsourcingkontrakt, gennemførelsen af kontrakten frem til dens udløb, nødplaner og exitstrategier). Et institut vil fortsat være fuldt ansvarligt for alle outsourcede ydelser og aktiviteter samt for ledelsesbeslutninger, der udspringer heraf. I overensstemmelse hermed bør outsourcingpolitikken præcisere, at outsourcing ikke fritager instituttet fra dets reguleringsforpligtelser og dets ansvar over for kunderne.

94. Politikken bør præcisere, at outsourcingordninger ikke bør være nogen hindring for et effektivt stedligt og ikke-stedligt tilsyn med instituttet og må ikke stride mod eventuelle tilsynsmæssige begrænsninger af tjenesteydelser og aktiviteter. Politikken bør ligeledes omfatte koncernintern outsourcing (dvs. tjenesteydelser leveret af separat juridisk enhed inden for et instituts koncern) og tage hensyn til alle specifikke koncernforhold.

Del IV — Risikokultur og forretningsadfærd

9 Risikokultur

95. En sund, omhyggelig og konsekvent risikokultur bør være et afgørende element i institutternes effektive risikostyring og bør sætte institutterne i stand til at træffe hensigtsmæssige og kvalificerede beslutninger.

96. Institutterne bør udvikle en integreret risikokultur for hele instituttet baseret på en fuld forståelse og et holistisk billede af de risici, de står over for, og af styringen heraf, under hensyntagen til instituttets risikoappetit.

97. Institutterne bør udvikle en risikokultur gennem politikker, kommunikation og uddannelse af medarbejderne med hensyn til institutternes aktiviteter, strategi og risikoprofil og bør tilpasse kommunikation og uddannelse af medarbejdere for at tage højde for medarbejdernes ansvar med hensyn til risikotagning og risikostyring.

98. Medarbejderne bør være fuldt ud klar over deres ansvar i forbindelse med risikostyring. Risikostyring bør ikke være begrænset til risikospecialister eller interne kontrolfunktioner. Forretningsområderne bør, under ledelsesorganets tilsyn, primært være ansvarlige for den

[26] Se også: EBA's retningslinjer vedrørende outsourcingaftaler findes på: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

daglige styring af risici i overensstemmelse med instituttets politikker, procedurer og kontrolforanstaltninger, under hensyntagen til instituttets risikoappetit og risikokapacitet.

99. En stærk risikokultur bør omfatte, men er ikke nødvendigvis begrænset til:

a. Ledelsesstyring: Ledelsesorganet bør være ansvarligt for at fastsætte og kommunikere instituttets kerneværdier og forventninger. Dets medlemmers adfærd bør afspejle de værdier, der forfægtes. Institutternes ledelse, herunder personer med nøglefunktioner, bør bidrage til den interne kommunikation af kerneværdier og forventninger til medarbejdere. Medarbejderne bør handle i overensstemmelse med alle gældende love og bestemmelser og straks videreformidle en konstateret manglende overholdelse inden eller uden for instituttet (f.eks. til den kompetente myndighed gennem en whistleblowerproces). Ledelsesorganet bør løbende fremme, overvåge og vurdere instituttets risikokultur og overveje, hvilken indvirkning risikokulturen har på instituttets finansielle stabilitet, risikoprofil og robuste ledelse, samt foretage ændringer, når det er nødvendigt.

b. Ansvarlighed: Relevante medarbejdere på alle niveauer bør vide og forstå instituttets kerneværdier og i det omfang, det er nødvendigt for deres rolle, dets risikoappetit og risikokapacitet. De bør være i stand til at varetage deres roller og være opmærksomme på, at de vil blive holdt ansvarlige for deres handlinger i relation til instituttets risikoadfærd.

c. Effektiv kommunikation og udfordring: En forsvarlig risikokultur bør fremme et miljø med åben kommunikation og effektive udfordringer, hvor beslutningsprocesser tilskynder til en bred vifte af synspunkter, giver mulighed for at afprøve den nuværende praksis, stimulerer en konstruktiv kritisk holdning blandt medarbejderne og fremmer et miljø med et åbent og konstruktivt engagement i hele organisationen.

d. Incitamenter: Passende incitamenter bør spille en central rolle med hensyn til at tilpasse risikoadfærden til instituttets risikoprofil og dets langsigtede interesse[27].

10 Virksomhedsværdier og adfærdskodeks

100. Ledelsesorganet bør udvikle, indføre, overholde og fremme høje etiske og faglige standarder, under hensyntagen til instituttets specifikke behov og karakteristika, og bør sikre gennemførelsen af sådanne standarder (gennem en adfærdskodeks eller et lignende instrument). Det bør ligeledes føre tilsyn med, at disse standarder efterleves af medarbejderne. Ledelsesorganet kan i givet fald indføre og gennemføre instituttets koncernstandarder eller fælles standarder udgivet af sammenslutninger eller andre relevante organisationer.

[27] Jf. også EMA's retningslinjer vedrørende forsvarlige aflønningspolitikker i henhold til artikel 74, stk. 3, og artikel 75, stk. 2, i direktiv 2013/36/EU og offentliggørelse af oplysninger i henhold til artikel 450 i forordning (EU) nr. 575/2013 (EBA/GL/2015/22), findes på https://www.eba.europa.eu/regulation-and-policy/remuneration.

101. Institutterne bør sikre, at personalet ikke forskelsbehandles på grund af køn, race, hudfarve, etnisk eller social oprindelse, genetiske anlæg, sprog, religion eller tro, politiske eller andre anskuelser, tilhørsforhold til et nationalt mindretal, formueforhold, fødsel, handicap, alder eller seksuel orientering.

102. Institutternes politikker bør være kønsneutrale. Dette omfatter, men er ikke begrænset til, aflønning, ansættelsespolitik, karriereudvikling og planer for generationsskifte, adgang til uddannelse og mulighed for at søge interne ledige stillinger. Institutterne bør sikre lige muligheder[28] for alle medarbejdere uanset køn, herunder med hensyn til karriereudsigter, og sigte mod at forbedre det underrepræsenterede køns repræsentation i stillinger i ledelsesorganet samt i den gruppe af medarbejdere, der har ledelsesansvar som defineret i Kommissionens delegerede forordning (reguleringsmæssige tekniske standarder for identificerede medarbejdere).[29] Institutterne bør overvåge udviklingen i den kønsbestemte lønforskel separat for identificerede medarbejdere (undtagen medlemmer af ledelsesorganet), medlemmer af ledelsesorganet i dets ledelsesfunktion, medlemmer af ledelsesorganet i tilsynsfunktionen og andet personale. Institutterne bør have politikker, der gør det lettere for medarbejderne at vende tilbage til arbejdsmarkedet efter barsels-, fædre- eller forældreorlov.

103. De gennemførte standarder bør sigte mod at forbedre instituttets robuste ledelsesordninger og reducere de risici, som instituttet er eksponeret for, navnlig de operationelle og omdømmemæssige risici, som kan have en betydelig negativ indvirkning på et instituts rentabilitet og bæredygtighed gennem bøder, sagsomkostninger, restriktioner pålagt af kompetente myndigheder, andre finansielle og strafferetlige sanktioner samt tab af mærkeværdi og forbrugertillid.

104. Ledelsesorganet bør have klare og dokumenterede politikker for, hvordan disse standarder skal efterleves. Disse politikker bør:

a. minde medarbejderne om, at alle instituttets aktiviteter bør gennemføres i overensstemmelse med gældende ret og med instituttets virksomhedsværdier

b. fremme risikobevidsthed gennem en stærk risikokultur i overensstemmelse med afsnit 9 i retningslinjerne og formidle ledelsesorganets forventning om, at aktiviteterne ikke vil gå ud over den fastsatte risikoappetit og de grænser, der er fastsat af instituttet, og medarbejdernes respektive ansvar

c. fastsætte principper for og give eksempler på acceptabel og uacceptabel adfærd, navnlig i tilknytning til finansiel fejlindberetning og forseelser, økonomisk og finansiel kriminalitet (herunder, men ikke begrænset til, svig, hvidvaskning af penge og finansiering af terrorisme (ML/TF), kartelpraksis, finansielle sanktioner, bestikkelse og korruption, markedsmanipulation, fejlsalg og andre overtrædelser af

[28] Se også Europa-Parlamentets og Rådets direktiv 2006/54/EF af 5. juli 2006 om gennemførelse af princippet om lige muligheder for og ligebehandling af mænd og kvinder i forbindelse med beskæftigelse og erhverv
[29] Se også EBA's retningslinjer vedrørende kønsneutrale aflønningspolitikker.

forbrugerbeskyttelseslovgivningen, skatteovertrædelser, uanset om de begås direkte eller indirekte, herunder gennem ulovlige eller forbudte udbyttearbitrageordninger

d. præcisere, at foruden at overholde lov- og myndighedskrav og interne politikker forventes det, at medarbejderne udviser ærlighed og integritet og varetager deres opgaver med fornøden dygtighed, omtanke og omhu, og

e. sikre, at medarbejderne har kendskab til de potentielle interne og eksterne disciplinære foranstaltninger, retssager og sanktioner, der kan være en følge af forseelser og uacceptabel adfærd.

105. Institutterne bør overvåge overholdelsen af sådanne standarder og sikre, at medarbejderne har kendskab hertil, f.eks. ved at tilbyde uddannelse. Institutterne bør definere den funktion, der er ansvarlig for at overvåge overholdelsen af og evaluere overtrædelser af adfærdskodeksen eller et lignende instrument og en procedure til behandling af spørgsmål om manglende overholdelse. Resultaterne bør regelmæssigt rapporteres til ledelsesorganet.

11 Politik for interessekonflikter på institutionelt plan

106. Ledelsesorganet bør være ansvarligt for at fastsætte, godkende og føre tilsyn med gennemførelsen og opretholdelsen af effektive politikker til at identificere, vurdere, håndtere og afhjælpe eller forebygge faktiske og potentielle interessekonflikter på institutionelt plan, f.eks. som et resultat af de forskellige aktiviteter og roller, som varetages af instituttet, af forskellige institutter inden for konsolideringsreglernes anvendelsesområde eller af forskellige forretningsområder eller enheder inden for et institut eller med hensyn til eksterne interessenter.

107. Institutterne bør inden for deres organisatoriske og administrative ordninger træffe hensigtsmæssige foranstaltninger til at forebygge, at interessekonflikter indvirker negativt på kundernes interesser.

108. Institutternes foranstaltninger til at håndtere eller i givet fald afhjælpe interessekonflikter bør dokumenteres og bl.a. omfatte:

a. en hensigtsmæssig funktionsadskillelse, f.eks. ved at overlade modstridende aktiviteter inden for behandlingen af transaktioner eller ved levering af tjenesteydelser til forskellige personer eller overdrage tilsyns- eller indberetningsansvar for modstridende aktiviteter til forskellige personer

b. etablering af informationsbarrierer, f.eks. gennem fysisk adskillelse af visse forretningsområder eller enheder.

12 Politik for interessekonflikter blandt medarbejdere[30]

109. Ledelsesorganet bør være ansvarligt for at fastsætte, godkende og føre tilsyn med gennemførelsen og opretholdelsen af effektive politikker til at identificere, vurdere, håndtere og afhjælpe eller forebygge faktiske og potentielle konflikter mellem instituttets interesser og medarbejdernes private interesser, herunder medlemmer af ledelsesorganet, som kunne indvirke negativt på varetagelsen af deres opgaver og ansvar. Et konsoliderende institut bør tage hensyn til interesser inden for en koncernpolitik for interessekonflikter på konsolideret og delkonsolideret grundlag.

110. Politikken bør tilsigte at identificere interessekonflikter blandt medarbejdere, herunder deres nærmeste familiemedlemmers interesser. Institutterne bør tage højde for, at interessekonflikter ikke kun kan opstå i forbindelse med nuværende, men også tidligere personlige eller faglige relationer. Hvis der opstår interessekonflikter, bør institutterne vurdere, hvor væsentlige de er, og efter behov vedtage og gennemføre afhjælpende foranstaltninger.

111. Med hensyn til interessekonflikter, der kan opstå som følge af tidligere forbindelser, bør institutterne fastsætte en passende tidsramme, for hvilken de ønsker, at medarbejderne skal rapportere sådanne interessekonflikter, på grundlag af, at disse stadig kan have indvirkning på medarbejdernes adfærd og deltagelse i beslutningstagningen.

112. Politikken bør som minimum omfatte følgende situationer eller forbindelser, hvor der kan opstå interessekonflikter:

a. økonomiske interesser (f.eks. aktier, andre ejerskabsinteresser og medlemskaber, kapitalinteresser og andre økonomiske interesser i erhvervskunder, intellektuelle ejendomsrettigheder, lån ydet af instituttet til en virksomhed ejet af en medarbejder, medlemskab af et organ eller ejerskab af et organ eller en enhed med modstridende interesser)

b. personlige eller professionelle forbindelser til ejerne af kvalificerede andele i instituttet

c. personlige eller faglige relationer til medarbejdere i instituttet eller enheder inden for konsolideringsreglernes anvendelsesområde (f.eks. familierelationer)

d. anden ansættelse og tidligere ansættelse inden for den senere tid (f.eks. fem år)

e. personlige eller faglige relationer til relevante eksterne interessenter (f.eks. tilknytning til væsentlige leverandører, konsulentvirksomheder eller andre tjenesteudbydere) og

[30] Dette afsnit bør sammenholdes med ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

f. politisk indflydelse eller politiske forbindelser.

113. Uanset ovenstående bør institutterne tage højde for, at det forhold, at medarbejdere er aktionær i et institut eller har private konti eller lån hos et institut eller anvender andre af instituttets tjenester, bør ikke føre til en situation, hvor medarbejderne anses for at have en interessekonflikt, hvis de holder sig inden for en passende minimumstærskel.

114. Politikken bør fastsætte processerne for rapportering og kommunikation til den funktion, der er ansvarlig på grundlag af politikken. Medarbejderne bør være forpligtet til internt straks at oplyse om et hvilket som helst forhold, der kan give, eller har givet, anledning til en interessekonflikt.

115. Politikken bør sondre mellem interessekonflikter, der varer ved og skal håndteres permanent, og interessekonflikter, der opstår uventet med hensyn til en enkelt begivenhed (f.eks. en transaktion, udvælgelse af tjenesteudbyder osv.) og normalt kan afhjælpes ved hjælp af en engangsforanstaltning. Under alle omstændigheder bør instituttets interesse være af central betydning for de beslutninger, der træffes.

116. Politikken bør fastsætte procedurer, foranstaltninger, dokumentationskrav og ansvarsområder med hensyn til identifikation og forebyggelse af interessekonflikter, vurdering af, om de er væsentlige, og med henblik på at træffe afhjælpende foranstaltninger. Sådanne procedurer, elementer, ansvarsområder og foranstaltninger bør omfatte:

a. overladelse af modstridende aktiviteter eller transaktioner til forskellige personer

b. forhindring af, at medarbejdere, der også er aktive uden for instituttet, får uhensigtsmæssig indflydelse inden for instituttet vedrørende disse andre aktiviteter

c. godtgørelse af ansvaret for ledelsesorganets medlemmer for at afholde sig fra at deltage i en afstemning om noget forhold, hvor et medlem har eller kan have en interessekonflikt, eller hvor medlemmets objektivitet eller evne til fuldt ud at varetage sine opgaver over for instituttet på anden måde kan blive kompromitteret

d. forhindring af, at medlemmer af ledelsesorganet har direktør- og bestyrelsesposter i konkurrerende institutter, medmindre de er inden for institutter, der tilhører samme institutsikringsordning, jf. artikel 113, stk. 7, i forordning (EU) nr. 575/2013, institutter, som er fast tilknyttet et centralt organ, jf. artikel 10 i forordning (EU) nr. 575/2013, eller institutter inden for konsolideringsreglernes anvendelsesområde.

117. Politikken bør specifikt omfatte risikoen for interessekonflikter i ledelsesorganet og indeholde tilstrækkelig vejledning vedrørende identifikation og håndtering af interessekonflikter, som kan hindre ledelsesorganets medlemmers mulighed for at træffe objektive og upartiske beslutninger, der tager sigte på at varetage instituttets bedste

interesser. Institutterne bør tage højde for, at interessekonflikter kan have indvirkning på ledelsesorganets medlemmers uafhængighed[31].

118. Når institutter afbøder identificerede interessekonflikter hos medlemmer af ledelsesorganet, bør de dokumentere de trufne foranstaltninger, herunder begrundelsen for, hvordan disse er effektive med hensyn til at sikre objektiv beslutningstagning.

119. Faktiske eller potentielle interessekonflikter, som den ansvarlige funktion inden for instituttet har fået underretning om, bør vurderes og håndteres hensigtsmæssigt. Hvis en interessekonflikt identificeres i forbindelse med en medarbejder, bør instituttet dokumentere den trufne beslutning, navnlig om interessekonflikten og de dermed forbundne risici er blevet anerkendt, og hvis den er blevet anerkendt, hvordan denne interessekonflikt er blevet mindsket eller afhjulpet på tilfredsstillende vis.

120. Alle faktiske og potentielle interessekonflikter i ledelsesorganet, individuelt og kollektivt, bør dokumenteres i tilstrækkeligt omfang, kommunikeres til ledelsesorganet og drøftes, vedtages og håndteres behørigt af ledelsesorganet.

12.1 Politik for interessekonflikter i forbindelse med lån og andre transaktioner med medlemmer af ledelsesorganet og deres nærtstående parter

121. Som led i deres politik for interessekonflikter for medarbejdere (afsnit 12) og håndteringen af interessekonflikter blandt medlemmer af ledelsesorganet, jf. punkt 117, bør ledelsesorganet opstille en ramme for identifikation og håndtering af interessekonflikter i forbindelse med ydelse af lån og indgåelse af andre transaktioner (f.eks. factoring, leasing, ejendomstransaktioner osv.) med medlemmer af ledelsesorganet og deres nærtstående parter.

122. Med forbehold for gennemførelsen af direktiv 2013/36/EU[32] i national lovgivning kan institutterne overveje yderligere kategorier af nærtstående parter, som de helt eller delvist finder anvendelse på, for så vidt angår lån og andre transaktioner.

123. Rammen for interessekonflikter bør sikre, at beslutninger om ydelse af lån og indgåelse af andre transaktioner med medlemmer af ledelsesorganet og deres nærtstående parter træffes objektivt, uden utilbørlig påvirkning fra interessekonflikter og som et generelt princip på armslængdevilkår.

124. Ledelsesorganet bør fastlægge de gældende beslutningsprocesser for ydelse af lån til og indgåelse af andre transaktioner med medlemmer af ledelsesorganet og deres nærtstående parter. Denne ramme kan give mulighed for at skelne mellem almindelige

[31] Jf. også ESMA's og EBA's fælles retningslinjer vedrørende vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.
[32] Se også Basel-kerneprincip 20

forretningstransaktioner[33], der indgås som led i den normale drift og indgås på normale markedsvilkår, og personalelån og -transaktioner, som indgås på vilkår, der er til rådighed for alle medarbejdere. Desuden kan rammerne for interessekonflikter og beslutningsprocessen skelne mellem væsentlige og ikke-væsentlige lån og andre transaktioner, forskellige typer af lån og andre transaktioner og omfanget af faktiske eller potentielle interessekonflikter, som de måtte skabe.

125. Som led i rammen for interessekonflikter bør ledelsesorganet fastsætte passende tærskler (f.eks. pr. produkttype eller alt efter forholdene), over hvilke lån eller andre transaktioner med et medlem af ledelsesorganet eller vedkommendes nærtstående parter altid kræver godkendelse af ledelsesorganet. Beslutninger om væsentlige lån eller andre væsentlige transaktioner med medlemmer af ledelsesorganet, som ikke indgås på normale markedsvilkår, men på vilkår der gælder for alle medarbejdere, bør altid træffes af ledelsesorganet.

126. Det medlem af ledelsesorganet, der drager fordel af et sådant væsentligt lån eller en sådan væsentlig transaktion, eller det medlem, der står modparten nær, bør ikke inddrages i beslutningstagningen.

127. Når institutterne træffer beslutning om et lån eller en anden transaktion med et medlem af ledelsesorganet eller vedkommendes nærtstående parter, bør de, inden de træffer en beslutning, vurdere den risiko, som instituttet kan blive eksponeret for som følge af transaktionen.

128. Hvis lån er udformet som en kreditlinje (f.eks. overtræk), bør den oprindelige beslutning og ændringer heraf dokumenteres. Enhver anvendelse af sådanne aftalte kreditfaciliteter inden for de aftalte grænser bør ikke betragtes som en ny beslutning om et lån til et medlem af ledelsesorganet eller vedkommendes nærtstående part. Hvis en ændring af en kreditlinje er væsentlig i overensstemmelse med instituttets politik, bør der foretages en ny vurdering og træffes en ny afgørelse.

129. For at sikre, at deres politikker vedrørende interessekonflikter overholdes, bør institutterne sikre, at alle relevante interne kontrolprocedurer fuldt ud finder anvendelse på lån og andre transaktioner med medlemmer af ledelsesorganet eller deres nærtstående parter, og at der findes en passende tilsynsramme for ledelsesorganet i dets tilsynsfunktion.

[33] Forretningstransaktioner omfatter lån og andre transaktioner (f.eks. leasing, factoring, tjenester i forbindelse med børsintroduktioner, fusioner og overtagelser, salg og køb af fast ejendom).

12.2 Dokumentation for lån til medlemmer af ledelsesorganet og deres nærtstående parter og yderligere oplysninger

130. Med henblik på artikel 88, stk. 1, i direktiv 2013/36/EU bør institutterne dokumentere data om lån[34] til medlemmer af ledelsesorganet og deres nærtstående parter korrekt, herunder mindst:

a. debitors navn og status (dvs. medlem af ledelsesorganet eller den nærtstående part) og, vedrørende lån til en nærtstående part, det medlem af ledelsesorganet, som parten er tilknyttet, og arten af forholdet til den nærtstående part

b. lånets type/art og beløbet

c. de vilkår og betingelser, der gælder for lånet

d. datoen for godkendelse af lånet

e. navnet på den person eller det organ og dets sammensætning, der træffer beslutningen om at godkende lånet, og de gældende betingelser

f. det forhold (ja/nej), om lånet er ydet på markedsvilkår eller ej

g. det forhold (ja/nej), om lånet er ydet på vilkår, der er til rådighed for alle medarbejdere.

131. Institutterne bør sikre, at dokumentationen for alle lån til medlemmerne af ledelsesorganet og deres nærtstående parter er fuldstændig og ajourført, og at instituttet efter anmodning uden unødig forsinkelse kan stille den fuldstændige dokumentation til rådighed for de kompetente myndigheder i et passende format.

132. I forbindelse med et lån på over 200 000 EUR til et medlem af ledelsesorganet eller dets nærtstående parter bør institutterne efter anmodning kunne give den kompetente myndighed følgende yderligere oplysninger:

a. lånets procentvise andel og den procentvise andel af summen af alle udestående lånebeløb til samme debitor i forhold til:

i. summen af kernekapital og supplerende kapital og

ii. egentlig kernekapital i instituttet

b. hvorvidt lånet er en del af en stor eksponering[35], og

c. den relative vægt af den samlede sum af alle udestående lånebeløb til samme skyldner, beregnet som en procentdel ved at dividere det samlede udestående

[34] Se også EBA's retningslinjer vedrørende lånoptagelse, som findes på: https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

[35] Se også del IV i forordning (EU) nr. 575/2013, særlig artikel 392.

beløb med det samlede beløb for alle udestående lån til medlemmer af ledelsesorganet og deres nærtstående parter.

13 Interne advarselsprocedurer

133. Institutterne bør etablere og opretholde passende interne advarselspolitikker og -procedurer, som gør det muligt for medarbejderne at indberette potentielle eller faktiske overtrædelser af lovgivningsmæssige eller interne krav, herunder, men ikke begrænset til, kravene i forordning (EU) nr. 575/2013 og nationale bestemmelser til gennemførelse af direktiv 2013/36/EU, eller af interne ledelsesordninger, gennem en særlig, uafhængig og selvstændig kanal. Det bør ikke være nødvendigt for medarbejdere, der foretager en indberetning, at have bevis for en overtrædelse; de bør imidlertid have en tilstrækkelig grad af sikkerhed, som giver tilstrækkelig grund til at iværksætte en undersøgelse. Institutterne bør ligeledes indføre passende processer og procedurer, der sikrer, at de opfylder deres forpligtelser i henhold til den nationale gennemførelse af Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten.

134. For at undgå interessekonflikter bør det være muligt for medarbejderne at indberette overtrædelser uden for de normale rapporteringslinjer (f.eks. via compliancefunktionen, den interne revisionsfunktion eller en uafhængig intern whistleblowerprocedure). Advarselsprocedurerne bør sikre beskyttelse af personoplysninger, både hvad angår den person, som indberetter overtrædelsen, og den fysiske person, som formodes at være ansvarlig for overtrædelsen, i overensstemmelse med forordning (EU) 2016/679[36] (GDPR).

135. Advarselsprocedurerne bør kunne benyttes af alle instituttets medarbejdere.

136. Alle relevante oplysninger, som medarbejdere videregiver via advarselsprocedurerne, bør i givet fald videreformidles til ledelsesorganet og andre ansvarlige funktioner, der er fastsat i den interne advarselspolitik. Når det kræves af den medarbejder, der indberetter en overtrædelse, bør oplysningerne videregives til ledelsesorganet og andre ansvarlige funktioner i anonymiseret form. Institutterne kan også fastsætte en whistleblowerproces, som gør det muligt at videregive oplysninger i anonymiseret form.

137. Institutterne bør sikre, at den person, der indberetter overtrædelsen, er behørigt beskyttet mod enhver negativ indvirkning, f.eks. gengældelse, forskelsbehandling eller andre former for uretfærdig behandling. Instituttet bør sikre, at ingen personer under instituttets kontrol udøver repressalier mod en person, der har indberettet en overtrædelse, og bør træffe passende foranstaltninger mod de ansvarlige for sådanne repressalier.

138. Institutterne bør ligeledes beskytte personer, der er blevet indberettet, mod eventuelle negative virkninger i tilfælde af, at der på grundlag af undersøgelsen ikke er nogen

[36] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

dokumentation, der berettiger, at der træffes foranstaltninger over for den pågældende person. Hvis der træffes foranstaltninger, bør instituttet træffe dem på en måde, der tager sigte på at beskytte den pågældende person mod utilsigtede negative virkninger, som går videre end målet med den trufne foranstaltning.

139. Navnlig bør interne advarselsprocedurer:

a. være dokumenteret (f.eks. personalehåndbøger)

b. fastlægge klare regler, der sikrer, at oplysninger om indberetningen, de indberettede og overtrædelsen behandles fortroligt, i overensstemmelse med forordning (EU) 2016/679, medmindre offentliggørelse kræves i national ret som led i yderligere undersøgelser eller efterfølgende retssager

c. beskytte medarbejdere, der gør opmærksom på problemer, mod at blive udsat for repressalier, fordi de har videregivet oplysninger om overtrædelser, der kan indberettes

d. sikre, at de potentielle eller faktiske overtrædelser, der gøres opmærksom på, vurderes og videreformidles, herunder efter behov til den relevante kompetente myndighed eller retshåndhævende myndighed

e. om muligt sikre, at medarbejdere, der har gjort opmærksom på potentielle eller faktiske overtrædelser, får en bekræftelse af modtagelsen af oplysningerne

f. sikre sporing af resultatet af en undersøgelse af en indberettet overtrædelse og

g. sikre hensigtsmæssig registrering.

14 Indberetning af overtrædelser til de kompetente myndigheder

140. De kompetente myndigheder bør indføre effektive og pålidelige mekanismer, som gør det muligt for institutternes medarbejdere at indberette relevante potentielle eller faktiske overtrædelser af lovgivningsmæssige krav, herunder, men ikke begrænset til, kravene i forordning (EU) nr. 575/2013 og nationale bestemmelser til gennemførelse af direktiv 2013/36/EU, til de kompetente myndigheder. Disse mekanismer bør som minimum omfatte:

a. særlige procedurer for modtagelse af indberetninger om overtrædelser og opfølgning heraf, f.eks. en dedikeret whistleblowerafdeling, -enhed eller -funktion

b. passende beskyttelse, jf. afsnit 13

c. beskyttelse af personoplysninger både hvad angår den fysiske person, som indberetter overtrædelsen, og den fysiske person, som formodes at være ansvarlig for overtrædelsen, i overensstemmelse med direktiv 2016/679/EF (GDPR) og

d. klare procedurer, jf. afsnit 13.

141. Uden at berøre muligheden for at indberette overtrædelser gennem de kompetente myndigheders mekanismer kan de kompetente myndigheder tilskynde medarbejdere til først at forsøge at anvende deres institutters interne advarselsprocedurer.

Del V — Rammerne og mekanismerne for intern kontrol

15 Rammerne for intern kontrol

142. Institutterne bør udvikle og opretholde en kultur, der tilskynder en positiv holdning til risikostyring og compliance inden for instituttet og en stærk og omfattende ramme for intern kontrol. Inden for denne ramme bør institutternes forretningsområder være ansvarlige for at forvalte de risici, de påtager sig under udøvelsen af deres aktiviteter og have kontrolforanstaltninger, der har til formål at sikre overholdelse af interne og eksterne krav. Som en del af denne ramme bør institutterne have interne kontrolfunktioner, som i behørigt og tilstrækkeligt omfang har autoritet, vægt og adgang til ledelsesorganet til at udføre deres mission, og en ramme for risikostyring.

143. Institutternes interne kontrol bør tilpasses på individuelt grundlag til virksomhedens særlige karakter, dens kompleksitet og de dermed forbundne risici, under hensyntagen til koncernsammenhængen. Institutterne bør tilrettelægge udvekslingen af de nødvendige oplysninger på en måde, der sikrer, at hvert ledelsesorgan,forretningsområde og hver intern enhed, herunder den enkelte kontrolfunktion, kan varetage sine opgaver. Dette indebærer eksempelvis en nødvendig udveksling af tilstrækkelige oplysninger mellem forretningsområderne og compliancefunktionen og AML/CFT-compliancefunktionen, hvor den er en separat kontrolfunktion, på koncernniveau og mellem lederne af de interne kontrolfunktioner på koncernniveau og instituttets ledelsesorgan.

144. Institutterne bør indføre passende processer og procedurer, der sikrer, at de opfylder deres forpligtelser i forbindelse med bekæmpelse af hvidvaskning af penge og finansiering af terrorisme. Institutterne bør vurdere deres risiko for, at de kan misbruges med henblik på ML/TF, og om nødvendigt træffe afbødende foranstaltninger for at reducere disse risici samt deres operationelle og omdømmemæssige risici i forbindelse hermed. Institutterne bør træffe foranstaltninger til at sikre, at deres medarbejdere er opmærksomme på sådanne ML/TF-risici og den indvirkning, som ML/TF har på instituttet og det finansielle systems integritet.

145. Den interne kontrolramme bør omfatte hele organisationen, herunder ledelsesorganets ansvarsområder og opgaver, og aktiviteterne i alle forretningsområder og interne enheder, herunder interne kontrolfunktioner, outsourcede aktiviteter og distributionskanaler.

146. Et instituts ramme for intern kontrol bør sikre:

a. effektive operationer

b. forsigtig forretningsadfærd

c. tilstrækkelig identifikation, måling og afhjælpning af risici

d. pålideligheden af indberettede finansielle og ikke-finansielle oplysninger, både internt og eksternt

e. en forsvarlig administrativ og regnskabsmæssig praksis og

f. overholdelse af love, forskrifter, tilsynskrav og instituttets interne politikker, processer, regler og beslutninger.

16 Gennemførelse af rammerne for intern kontrol

147. Ledelsesorganet bør være ansvarligt for at fastslå og overvåge, om rammen for og processerne og mekanismerne i forbindelse med den interne kontrol er hensigtsmæssige og effektive, og for at føre tilsyn med alle forretningsområder og interne enheder, herunder interne kontrolfunktioner (såsom risikostyring, compliance, AML/CFT-compliance, hvis disse er adskilt fra compliancefunktionen, og den interne revisionsfunktion). Institutterne bør fastlægge, opretholde og regelmæssigt ajourføre hensigtsmæssige skriftlige politikker, mekanismer og procedurer for den interne kontrol, som bør godkendes af ledelsesorganet.

148. Et institut bør have en klar, gennemsigtig og dokumenteret beslutningsproces og en klar fordeling af ansvar og beføjelser inden for sin ramme for intern kontrol, herunder dets forretningsområder, interne enheder og interne kontrolfunktioner.

149. Institutterne bør kommunikere disse politikker, mekanismer og procedurer til alle medarbejdere og hver gang, der er foretaget væsentlige ændringer.

150. Ved gennemførelsen af rammen for intern kontrol bør institutterne sørge for en tilstrækkelig funktionsadskillelse — f.eks. ved at overlade modstridende aktiviteter inden for behandlingen af transaktioner eller ved levering af tjenesteydelser til forskellige personer eller overdrage tilsyns- og indberetningsansvar for modstridende aktiviteter til forskellige personer — og etablere informationsbarrierer, f.eks. gennem fysisk adskillelse af visse afdelinger.

151. De interne kontrolfunktioner bør kontrollere, at de politikker, mekanismer og procedurer, der er fastsat i rammen for intern kontrol, gennemføres korrekt på deres respektive kompetenceområder.

152. De interne kontrolfunktioner bør regelmæssigt fremsende skriftlige rapporter om større identificerede mangler til ledelsesorganet. Disse rapporter bør for hver ny identificeret alvorlig mangel indeholde oplysninger om de pågældende relevante risici, en konsekvensanalyse, henstillinger og nødvendige korrigerende tiltag. Ledelsesorganet bør følge rettidigt og effektivt op på resultaterne af de interne kontrolfunktioner og kræve passende, afhjælpende tiltag gennemført. Der bør indføres en formel opfølgningsprocedure for resultater og korrigerende tiltag.

17 Rammerne for risikostyring

153. Som en del af den overordnede ramme for intern kontrol bør institutterne have en holistisk ramme for risikostyring for hele instituttet, der rækker på tværs af alle dets forretningsområder og interne enheder, herunder interne kontrolfunktioner, under fuld anerkendelse af den økonomiske substans af alle dets risikoeksponeringer. Rammen for risikostyring bør sætte instituttet i stand til at træffe fuldt informerede beslutninger om risikotagning. Rammen for risikostyring bør omfatte risici i og uden for balancen samt faktiske risici og fremtidige risici, som instituttet kan være eksponeret for. Risici bør vurderes efter "bottom up"- og "top down"-princippet, inden for og på tværs af forretningsområder, under anvendelse af konsekvent terminologi og kompatible metoder i hele instituttet og på konsolideret eller delkonsolideret niveau. Alle relevante risici bør være omfattet af rammen for risikostyring med passende hensyntagen til både finansielle og ikke-finansielle risici, herunder kredit-, markeds-, likviditets- og koncentrationsrisici, operationelle risici, IT-risici, omdømmemæssige, juridiske og adfærdsmæssige risici, risici i forhold til overholdelse af AML/CTF, risici forbundet med anden økonomisk kriminalitet, ESG-risici og strategiske risici.

154. Et instituts ramme for risikostyring bør omfatte politikker, procedurer, risikogrænser og risikokontrolforanstaltninger, der sikrer passende, rettidig og vedvarende identifikation, måling eller vurdering, overvågning, styring, afhjælpning og rapportering af risiciene i forretningsområderne, på institutniveau og konsolideret eller delkonsolideret niveau.

155. Et instituts ramme for risikostyring bør opstille specifikke retningslinjer for implementeringen af dets strategier. Disse retningslinjer bør i det relevante omfang fastlægge og opretholde interne grænser, der er i overensstemmelse med instituttets risikoappetit og står i forhold til dets forsvarlige funktion, finansielle styrke, kapitalgrundlag og strategiske mål. Et instituts risikoprofil bør holdes inden for disse fastsatte grænser. Rammen for risikostyring bør sikre, at der, når der opstår overtrædelser af risikogrænser, er en fastsat proces til at videreformidle og håndtere dem med en passende opfølgningsprocedure.

156. Rammen for risikostyring bør være omfattet af en uafhængig intern kontrol, f.eks. udført af den interne revisionsfunktion, og bør revurderes løbende i forhold til instituttets

risikoappetit, under hensyntagen til oplysninger fra risikostyringsfunktionen og fra risikoudvalget, hvis et sådant er nedsat. Faktorer, der bør tages hensyn til, omfatter interne eller eksterne udviklinger, herunder ændringer i balance og indtægter, en eventuel stigning i kompleksiteten af instituttets virksomhed, risikoprofil eller driftsstruktur, geografisk ekspansion, fusioner og overtagelser samt indførelse af nye produkter eller forretningsområder.

157. Når et institut identificerer og måler eller vurderer risici, bør det udvikle passende metoder, herunder både fremad- og bagudrettede værktøjer. Disse metoder bør gøre det muligt at aggregere risikoeksponeringer på tværs af forretningsområder og støtte identifikationen af risikokoncentrationer. Værktøjerne bør omfatte en vurdering af den faktiske risikoprofil i forhold til instituttets risikoappetit samt afdækning og vurdering af potentielle og stressede risikoeksponeringer under en række forskellige formodede negative omstændigheder i forhold til instituttets risikokapacitet. Værktøjerne bør give oplysninger om enhver justering af risikoprofilen, som måtte være nødvendig. Institutterne bør foretage passende konservative skøn, når de opstiller stressscenarier.

158. Institutterne bør tage i betragtning, at resultaterne af kvantitative vurderingsmetoder, herunder stresstest, er stærkt afhængige af modellernes begrænsninger og antagelser (herunder alvoren og varigheden af chokket og de underliggende risici). Hvis f.eks. modeller viser meget høje afkast af økonomisk kapital, kan det skyldes en svaghed i modellerne (f.eks. at visse relevante risici ikke er medtaget) snarere end det forhold, at instituttet har en overlegen strategi eller har gennemført en strategi på fremragende vis. Bestemmelsen af graden af den risiko, der tages, bør derfor ikke alene være baseret på kvantitative oplysninger eller modeloutput, men bør også omfatte en kvalitativ metode (herunder ekspertvurdering og kritisk analyse). Relevante makroøkonomiske tendenser og data bør eksplicit være rettet mod at identificere deres mulige virkning på eksponeringer og porteføljer.

159. Det endelige ansvar for risikovurdering ligger udelukkende hos instituttet, som i overensstemmelse hermed bør evaluere sine risici kritisk og ikke udelukkende forlade sig på eksterne vurderinger. F.eks. bør et institut validere en indkøbt risikomodel og tilpasse den til sine egne omstændigheder for at sikre, at modellen måler og analyserer risikoen præcist og omfattende.

160. Institutterne bør være fuldt ud opmærksomme på modellernes og parametrenes begrænsninger og ikke kun anvende kvantitative, men også kvalitative risikovurderingsværktøjer (herunder ekspertvurdering og kritisk analyse).

161. Ud over institutternes egne vurderinger kan de anvende eksterne risikovurderinger (herunder eksterne kreditvurderinger eller eksternt indkøbte risikomodeller). Institutterne bør være helt klar over det præcise anvendelsesområde for sådanne vurderinger og deres begrænsninger.

162. Der bør etableres regelmæssige og gennemsigtige mekanismer, således at ledelsesorganet, dets risikoudvalg, hvis et sådant er nedsat, og alle relevante enheder i et institut rettidigt får adgang til rapporter på en forståelig og hensigtsmæssig måde, og at de kan dele relevante oplysninger om identifikation, måling eller vurdering samt overvågning og styring af risici. Rapporteringsrammen bør være veldefineret og dokumenteret.

163. En effektiv kommunikation og bevidsthed om risici og risikostrategien er afgørende for hele risikostyringsprocessen, herunder evaluerings- og beslutningsprocesserne, og er med til at forhindre, at der bliver taget beslutninger, der uforvarende kan forøge risikoen. En effektiv risikorapportering indebærer passende interne overvejelser og kommunikation af risikostrategi og relevante risikodata (f.eks. eksponeringer og indikatorer for nøglerisici), både horisontalt gennem instituttet og vertikalt i ledelseskæden.

18 Nye produkter og væsentlige ændringer[37]

164. Et institut bør have indført en veldokumenteret politik for godkendelse af nye produkter, der er godkendt af ledelsesorganet, og som omfatter udviklingen af nye markeder, produkter og tjenesteydelser og væsentlige ændringer af de eksisterende samt ekstraordinære transaktioner. Politikken bør endvidere omfatte væsentlige ændringer af tilhørende processer (f.eks. nye outsourcingordninger) og systemer (f.eks. IT-forandringsprocesser). Politikken for godkendelse af nye produkter bør sikre, at godkendte produkter og ændringer er i overensstemmelse med instituttets risikostrategi og risikoappetit og instituttets tilsvarende grænser, eller at de nødvendige revisioner foretages.

165. Væsentlige ændringer eller ekstraordinære transaktioner kan være fusioner og overtagelser, herunder de mulige konsekvenser af at gennemføre utilstrækkelig due diligence, der undlader at identificere risici og forpligtelser efter en fusion, oprettelse af strukturer (f.eks. nye datterselskaber eller selskaber med et enkelt formål), nye produkter, ændringer af systemer eller risikostyringsramme eller -procedurer og ændringer i instituttets organisation.

166. Et institut bør indføre specifikke procedurer til vurdering af overholdelse af disse politikker, under hensyntagen til input fra risikostyringsfunktionen. Dette bør omfatte en systemisk forhåndsvurdering og dokumenteret udtalelse fra compliancefunktionen vedrørende nye produkter eller væsentlige ændringer af eksisterende produkter.

167. Et instituts politik for godkendelse af nye produkter bør omfatte enhver overvejelse, der skal gøres, inden der træffes beslutning om at trænge ind på nye markeder, beskæftige sig med nye produkter, lancere en ny tjenesteydelse eller foretage væsentlige ændringer af eksisterende produkter eller tjenesteydelser. Politikken for godkendelse af nye produkter bør også omfatte definitioner af "nyt produkt/marked/forretningsområde" og "væsentlige

[37] Jf. også EBA's retningslinjer vedrørende produktudviklings- og produktstyringsprocesser for udviklere og distributører af detailbankprodukter, findes på https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

ændringer", der skal anvendes i organisationen samt de interne funktioner, der skal inddrages i beslutningsprocessen.

168. Politikken for godkendelse af nye produkter bør fastlægge de væsentligste spørgsmål, der skal besvares, før der træffes en beslutning. Hertil hører spørgsmålet om overholdelse af lovgivningen, regnskabsføring, prisfastsættelsesmodeller, konsekvensen for risikoprofilen, kapitaldækning og lønsomhed, adgangen til tilstrækkelige frontoffice-, backoffice- og middleoffice-ressourcer og adgangen til tilstrækkelige interne værktøjer og ekspertise til at forstå og overvåge de dermed forbundne risici. For at opfylde forpligtelserne i henhold til direktiv (EU) 2015/849 bør institutterne desuden identificere og vurdere den ML/TF-risiko, der er forbundet med det nye produkt eller den nye forretningspraksis, og fastsætte de foranstaltninger, der skal træffes for at afhjælpe disse risici. Beslutningen om at påbegynde en ny aktivitet bør klart angive det forretningsområde og de enkeltpersoner, der er ansvarlige for denne aktivitet. En ny aktivitet bør ikke gennemføres, før de fornødne ressourcer til at forstå og håndtere de dermed forbundne risici er til stede.

169. Risikostyringsfunktionen og compliancefunktionen bør involveres i godkendelsen af nye produkter eller væsentlige ændringer af eksisterende produkter, processer og systemer. Deres input bør omfatte en fuldstændig og objektiv vurdering af risiciene ved nye aktiviteter under en række forskellige scenarier, af potentielle mangler i instituttets risikostyring og interne kontrolrammer samt instituttets evne til at håndtere nye risici effektivt. Risikostyringsfunktionen bør ligeledes have et klart overblik over indførelsen af nye produkter (eller væsentlige ændringer af eksisterende produkter, processer og systemer) på tværs af forretningsområder og porteføljer og bør have beføjelse til at kræve, at ændringer af eksisterende produkter gennemløber den formelle proces for godkendelse af nye produkter.

19 Interne kontrolfunktioner

170. De interne kontrolfunktioner bør omfatte en risikostyringsfunktion (jf. afsnit 20), en compliancefunktion (jf. afsnit 21) og en intern revisionsfunktion (jf. afsnit 22). Risikostyrings- og compliancefunktionen bør være underkastet revision udført af den interne revisionsfunktion. Kontrolfunktionerne har også ansvaret for at sikre overholdelse af AML/CTF-kravene.

171. De interne kontrolfunktioners operationelle opgaver kan blive outsourcet, under hensyntagen til de i del I anførte proportionalitetskriterier, til det konsoliderende institut eller en anden enhed inden eller uden for koncernen med samtykke fra de pågældende institutters ledelsesorganer. Selv hvis de operationelle opgaver i forbindelse med den interne kontrol er helt eller delvist outsourcet, er lederen af den pågældende interne kontrolfunktion og ledelsesorganet stadig ansvarlige for disse aktiviteter og for at opretholde en intern kontrolfunktion inden for instituttet.

172. Med forbehold af gennemførelsen af direktiv (EU) 2015/849 i national lovgivning bør institutterne overdrage ansvaret for at sikre instituttets overholdelse af kravene i nævnte

direktiv og instituttets politikker og procedurer til en medarbejder (f.eks. lederen af complianceafdelingen). Institutterne kan oprette en særskilt AML/CTF-compliancefunktion som en uafhængig kontrolfunktion.[38] Den person, der er ansvarlig for AML/CTF, bør om nødvendigt kunne rapportere direkte til ledelsesorganet i dets ledelses- og tilsynsfunktion.

19.1 Ledere af de interne kontrolfunktioner

173. Der bør udpeges ledere af interne kontrolfunktioner på et hierarkisk passende niveau, sådan at de har den nødvendige autoritet og vægt til at opfylde deres forpligtelser. Uanset ledelsesorganets overordnede ansvar bør lederne af interne kontrolfunktioner være uafhængige af de forretningsområder eller enheder, de kontrollerer. Med henblik herpå bør lederne af risikostyrings-, compliance- og den interne revisionsfunktion rapportere direkte til og være direkte ansvarlige over for ledelsesorganet, og deres resultater bør revideres af ledelsesorganet.

174. Lederne af de interne kontrolfunktioner bør om nødvendigt kunne få adgang til og rapportere direkte til ledelsesorganet i dets tilsynsfunktion for at rejse problemstillinger og advare overvågningsfunktionen, hvis relevant, når specifikke udviklinger påvirker eller kan påvirke instituttet. Dette bør ikke hindre lederne af interne kontrolfunktioner i ligeledes at rapportere inden for de normale rapporteringslinjer.

175. Institutterne bør have indført dokumenterede processer for besættelse af stillingen som leder af en intern kontrolfunktion og for fratagelse af dennes ansvarsområder. Under alle omstændigheder bør lederne af interne kontrolfunktioner — og i henhold til artikel 76, stk. 5, i direktiv 2013/36/EU må lederen af risikostyringsfunktionen — ikke fratages denne opgave uden forudgående godkendelse fra ledelsesorganet i dets tilsynsfunktion. I væsentlige institutter bør de kompetente myndigheder straks informeres om godkendelsen og hovedårsagerne til, at en leder af en intern kontrolfunktion har fået frataget denne opgave.

19.2 Interne kontrolfunktioners uafhængighed

176. For at de interne kontrolfunktioner kan betragtes som uafhængige, bør følgende betingelser være opfyldt:

a. Deres medarbejdere udfører ikke operationelle opgaver, der falder inden for anvendelsesområdet for de aktiviteter, som de interne kontrolfunktioner forventes at overvåge og kontrollere.

b. De er organisatorisk adskilt fra de aktiviteter, som det påhviler dem at overvåge og kontrollere.

c. Uanset det overordnede ansvar, som ledelsesorganets medlemmer har for instituttet, bør lederen af en intern kontrolfunktion ikke være underordnet en person, der har

[38] Der henvises også til EBA's retningslinjer vedrørende AML/CTF's compliancefunktion (under udarbejdelse).

ansvar for at håndtere de aktiviteter, som den interne kontrolfunktion overvåger og kontrollerer.

d. Aflønningen af de interne kontrolfunktioners medarbejdere bør ikke være knyttet til udøvelsen af de aktiviteter, som den interne kontrolfunktion overvåger og kontrollerer, og bør ikke på anden måde påvirke deres objektivitet[39].

19.3 Kombination af interne kontrolfunktioner

177. Under hensyntagen til de i del I anførte proportionalitetskriterier kan risikostyringsfunktionen og compliancefunktionen kombineres. Den interne revisionsfunktion bør ikke kombineres med en anden intern kontrolfunktion.

19.4 Interne kontrolfunktioners ressourcer

178. De interne kontrolfunktioner bør have tilstrækkelige ressourcer. De bør have et tilstrækkeligt antal kvalificerede medarbejdere (både i moder- og datterselskaber). Medarbejderne bør opkvalificeres løbende og modtage uddannelse efter behov.

179. De interne kontrolfunktioner bør have tilstrækkelige IT-systemer og støtte til deres rådighed, med adgang til de interne og eksterne oplysninger, der er nødvendige for at leve op til deres ansvar. De bør have adgang til alle nødvendige oplysninger vedrørende alle forretningsområder og relevante datterselskaber, der indebærer en risiko, navnlig hvis de potentielt kan medføre væsentlige risici for institutterne.

20 Risikostyringsfunktion

180. Institutterne bør oprette en risikostyringsfunktion, der omfatter hele instituttet. Risikostyringsfunktionen bør i tilstrækkeligt omfang have autoritet, vægt og ressourcer, under hensyntagen til de i del I anførte proportionalitetskriterier, til at gennemføre risikopolitikker og rammen for risikostyring, jf. afsnit 17.

181. Risikostyringsfunktionen bør om nødvendigt have direkte adgang til ledelsesorganet i dets tilsynsfunktion og dets udvalg, hvis sådanne er nedsat, herunder navnlig risikoudvalget.

182. Risikostyringsfunktionen bør have adgang til alle forretningsområder og andre interne enheder, der har potentiale til at medføre risici, samt til relevante datterselskaber og tilknyttede selskaber.

183. Medarbejdere inden for risikostyringsfunktionen bør være i besiddelse af tilstrækkelig viden, kompetence og ekspertise med hensyn til risikostyringsteknikker og -procedurer samt markeder og produkter og have adgang til regelmæssig uddannelse.

[39] Jf. også EBA's retningslinjer vedrørende forsvarlige aflønningspolitikker, der findes på https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

184. Risikostyringsfunktionen bør være uafhængig af de forretningsområder og enheder, hvis risici den kontrollerer, men bør ikke hindres i at indgå i samspil med dem. Et samspil mellem de operationelle funktioner og risikostyringsfunktionen bør bidrage til at nå målsætningen om, at alle instituttets medarbejdere har ansvar for at håndtere risici.

185. Risikostyringsfunktionen bør være en central organisatorisk funktion, der er struktureret, så den kan gennemføre risikopolitikker og kontrollere rammen for risikostyring. Risikostyringsfunktionen bør spille en central rolle i at sikre, at instituttet har indført effektive risikostyringsprocesser. Risikostyringsfunktionen bør være aktivt involveret i alle væsentlige risikostyringsbeslutninger.

186. Væsentlige institutter kan overveje at oprette specifikke risikostyringsfunktioner for hvert væsentligt forretningsområde. Der bør imidlertid være en central risikostyringsfunktion, herunder en koncernrisikostyringsfunktion i det konsoliderende institut, der for hele instituttet og koncernen tegner et holistisk billede af hele risikospektret og sikrer, at risikostrategien efterleves.

187. Risikostyringsfunktionen bør levere relevante uafhængige oplysninger, analyser og ekspertvurdering om risikoeksponeringer, samt rådgivning om forslag og risikobeslutninger truffet af forretningsområder eller interne enheder, og bør informere ledelsesorganet om, hvorvidt de er i overensstemmelse med instituttets risikostrategi og risikoappetit. Risikostyringsfunktionen kan foreslå forbedringer af rammen for risikostyring og korrigerende foranstaltninger til at afhjælpe overtrædelser af risikopolitikker, -procedurer og -grænser.

20.1 Risikostyringsfunktionens rolle med hensyn til risikostrategi og beslutninger

188. Risikostyringsfunktionen bør på et tidligt tidspunkt være aktivt involveret i udformningen af instituttets risikostrategi og i at sikre, at instituttet har indført effektive risikostyringsprocesser. Risikostyringsfunktionen bør fremsende alle relevante risikorelaterede oplysninger til ledelsesorganet, så det bliver i stand til at fastlægge niveauet for instituttets risikoappetit. Risikostyringsfunktionen bør vurdere soliditeten og bæredygtigheden af risikostrategien og -villigheden. Den bør sikre, at risikoappetitten på passende vis omsættes til specifikke risikogrænser. Risikostyringsfunktionen bør ligeledes vurdere risikostrategierne og risikoappetitten i forretningsenheder, herunder målsætninger foreslået af forretningsenhederne, og bør involveres, inden ledelsesorganet træffer beslutning vedrørende risikostrategierne og risikoappetitten. Målsætningerne bør være plausible og konsistente med instituttets risikostrategi.

189. Risikostyringsfunktionens inddragelse bør sikre, at der i tilstrækkeligt omfang kommer til at indgå risikoovervejelser i beslutningsprocesser. Imidlertid bør ansvaret for de beslutninger, der træffes, fortsat ligge hos forretningsenhederne og de interne enheder og i sidste instans hos ledelsesorganet.

20.2 Risikostyringsfunktionens rolle med hensyn til væsentlige ændringer

190. I overensstemmelse med afsnit 18 bør risikostyringsfunktionen, inden der træffes beslutninger om væsentlige ændringer eller ekstraordinære transaktioner, inddrages i vurderingen af virkningen af sådanne ændringer og ekstraordinære transaktioner på instituttets og koncernens samlede risiko og rapportere om sine konklusioner direkte til ledelsesorganet, inden der træffes beslutning.

191. Risikostyringsfunktionen bør vurdere, på hvilken måde identificerede risici kunne påvirke instituttets eller koncernens evne til at håndtere sin risikoprofil, sin likviditet og et sundt kapitalgrundlag under normale og negative omstændigheder.

20.3 Risikostyringsfunktionens rolle med hensyn til identifikation, måling, vurdering, håndtering, afhjælpning, overvågning og rapportering af risici

192. Risikostyringsfunktionen bør sikre, at der findes en passende risikostyringsramme, og at alle risici identificeres, vurderes, måles, overvåges, håndteres og rapporteres korrekt af de relevante enheder i instituttet.

193. Risikostyringsfunktionen bør sikre, at identifikationen og vurderingen ikke kun er baseret på kvantitative oplysninger eller modeloutput, men også tager hensyn til kvalitative metoder. Risikostyringsfunktionen bør holde ledelsesorganet underrettet om de anvendte antagelser og potentielle mangler i forbindelse med risikomodellerne og -analyserne.

194. Risikostyringsfunktionen bør sikre, at transaktioner med nærtstående parter kontrolleres, og at de risici, de udgør for instituttet, identificeres og vurderes korrekt.

195. Risikostyringsfunktionen bør sikre, at alle identificerede risici overvåges effektivt af forretningsenhederne.

196. Risikostyringsfunktionen bør regelmæssigt overvåge instituttets faktiske risikoprofil og holde den op mod instituttets strategiske mål og risikoappetit, således at ledelsesorganet i dets ledelsesfunktion kan træffe beslutninger, der kan anfægtes af ledelsesorganet i dets tilsynsfunktion.

197. Risikostyringsfunktionen bør analysere tendenser og afdække nye risici eller risici i fremvækst og øgede risici som følge af ændrede omstændigheder og forhold. Den bør ligeledes regelmæssigt revidere faktiske risikoresultater i forhold til tidligere skøn (dvs. backtesting) for at vurdere og forbedre nøjagtigheden og effektiviteten af risikostyringsprocessen.

198. Risikostyringsfunktionen bør vurdere, hvordan det er muligt at afhjælpe risici. Rapporteringen til ledelsesorganet bør omfatte forslag til hensigtsmæssige risikoafhjælpende foranstaltninger.

20.4 Risikostyringsfunktionens rolle med hensyn til ikke-godkendte eksponeringer

199. Risikostyringsfunktionen bør uafhængigt vurdere overtrædelser af risikoappetit eller grænser (herunder fastslå årsagen og foretage en juridisk og økonomisk analyse af de faktiske omkostninger ved at lukke, reducere eller risikoafdække eksponeringen i forhold til de faktiske omkostninger ved at beholde den). Risikostyringsfunktionen bør informere de berørte forretningsenheder og ledelsesorganet og anbefale eventuelle afhjælpningsforanstaltninger. Risikostyringsfunktionen bør rapportere direkte til ledelsesorganet i dets tilsynsfunktion, når overtrædelsen er væsentlig, uden at dette berører risikostyringsfunktionens mulighed for at rapportere til andre interne funktioner og udvalg.

200. Risikostyringsfunktionen bør spille en central rolle med hensyn til at sikre, at der træffes beslutning om dens anbefaling på det relevante niveau, at den overholdes af de relevante forretningsenheder og i tilstrækkeligt omfang rapporteres til ledelsesorganet og risikoudvalget, hvis et sådant er nedsat.

20.5 Leder af risikostyringsfunktionen

201. Lederen af risikostyringsfunktionen bør være ansvarlig for at levere omfattende og forståelig information om risici og rådgive ledelsesorganet og derved sætte dette organ i stand til at forstå instituttets samlede risikoprofil. Tilsvarende gælder for lederen af risikostyringsfunktionen i et moderinstitut vedrørende den konsoliderede situation.

202. Lederen af risikostyringsfunktionen bør have tilstrækkelig ekspertise, uafhængighed og anciennitet til at anfægte beslutninger, der påvirker et instituts risikoeksponering. Er lederen af risikostyringsfunktionen ikke medlem af ledelsesorganet, bør væsentlige institutter udpege en uafhængig leder af risikostyringsfunktionen, som ikke har ansvar for andre funktioner og rapporterer direkte til ledelsesorganet. Er det ikke forholdsmæssigt at udpege en person, som alene skal varetage rollen som leder af risikostyringsfunktionen, kan, under hensyntagen til det i del I anførte proportionalitetsprincip, denne funktion kombineres med rollen som leder af compliancefunktionen eller kan varetages af en anden højtstående person, forudsat at der ikke foreligger nogen interessekonflikt mellem de kombinerede funktioner. Under alle omstændigheder bør denne person i tilstrækkeligt omfang have autoritet, vægt og uafhængighed (f.eks. lederen af juridisk afdeling).

203. Lederen af risikostyringsfunktionen bør være i stand til at anfægte beslutninger truffet af instituttets ledelse og dets ledelsesorgan, og begrundelsen for indsigelser bør dokumenteres formelt. Såfremt et institut ønsker at tildele lederen af risikostyringsfunktionen ret til at nedlægge veto mod beslutninger (f.eks. en kredit- eller investeringsbeslutning eller

fastlæggelsen af en grænse) truffet på niveauer under ledelsesorganet, bør det præcisere anvendelsesområdet for en sådan vetoret, procedurerne for anke eller klage, og hvordan ledelsesorganet vil blive involveret.

204. Institutterne bør fastsætte skærpede processer for godkendelsen af beslutninger, hvor lederen af risikostyringsfunktionen har givet udtryk for en negativ opfattelse. Ledelsesorganet i dets tilsynsfunktion bør være i stand til at kommunikere direkte med lederen af risikostyringsfunktionen om centrale risikorelaterede emner, herunder udviklingstendenser, der kan være uforenelige med instituttets risikostrategi og risikoappetit.

21 Compliancefunktion

205. Institutterne bør oprette en permanent og effektiv compliancefunktion til at håndtere compliancerisikoen, og udpege en person, der er ansvarlig for denne funktion i hele instituttet (den complianceansvarlige eller leder af complianceafdelingen).

206. Er det ikke forholdsmæssigt at udpege en person, som alene skal varetage rollen som leder af complianceafdelingen, kan denne funktion, under hensyntagen til det i del I anførte proportionalitetsprincip, kombineres med rollen som leder af risikostyringsfunktionen eller kan varetages af en anden højtstående person (f.eks. lederen af afdelingen for juridiske anliggender), forudsat at der ikke foreligger nogen interessekonflikt mellem de kombinerede funktioner.

207. Compliancefunktionen, herunder lederen af complianceafdelingen, bør være uafhængig af de forretningsområder og interne enheder, den kontrollerer, og i tilstrækkeligt omfang have autoritet, vægt og ressourcer. Under hensyntagen til de i del I anførte proportionalitetskriterier kan denne funktion bistås af risikostyringsfunktionen eller kombineres med risikostyringsfunktionen eller andre hensigtsmæssige funktioner, f.eks. retlige anliggender eller menneskelige ressourcer.

208. Medarbejdere inden for compliancefunktionen bør være i besiddelse af tilstrækkelig viden, kompetence og ekspertise med hensyn til compliance og relevante procedurer og have adgang til løbende uddannelse.

209. Ledelsesorganet i dets tilsynsfunktion bør føre tilsyn med gennemførelsen af en veldokumenteret compliancepolitik, der bør kommunikeres til alle medarbejdere. Institutterne bør oprette en proces til løbende at vurdere ændringer i de love og bestemmelser, der gælder for deres aktiviteter.

210. Compliancefunktionen bør vejlede ledelsesorganet om foranstaltninger, der skal træffes for at sikre overholdelse af gældende love, regler, forskrifter og standarder, og bør vurdere den mulige virkning af eventuelle ændringer i de juridiske eller tilsynsmæssige rammebetingelser i forhold til instituttets aktiviteter og compliancerramme.

211. Compliancefunktionen bør sikre, at complianceovervågningen foretages på grundlag af et struktureret og veldefineret program for complianceovervågning, og at compliancepolitikken overholdes. Compliancefunktionen bør rapportere til ledelsesorganet og i det omfang, det er nødvendigt, kommunikere med risikostyringsfunktionen om instituttets compliancerisiko og håndteringen heraf. Compliancefunktionen og risikostyringsfunktionen bør samarbejde og udveksle oplysninger efter behov med henblik på at udføre deres respektive opgaver. Compliancefunktionens konklusioner bør indgå i ledelsesorganets og risikostyringsfunktionens beslutningsprocesser.

212. I overensstemmelse med afsnit 18 i disse retningslinjer bør compliancefunktionen i tæt samarbejde med risikostyringsfunktionen og den juridiske enhed ligeledes kontrollere, at nye produkter og nye procedurer overholder de eksisterende retlige rammer og i givet fald alle kendte kommende ændringer i lovgivning, forskrifter og tilsynskrav.

213. Institutterne bør træffe passende foranstaltninger mod intern eller ekstern adfærd, der kan lette eller muliggøre svig, ML/TF eller anden økonomisk kriminalitet og brud på tjenestepligterne (f.eks. overtrædelser af interne procedurer, overskridelser af grænser).

214. Institutterne bør sikre, at deres datterselskaber og filialer tager skridt til at sikre, at deres aktiviteter overholder lokale love og bestemmelser. Hvis lokale love og bestemmelser er til hinder for at anvende strengere procedurer og compliancesystemer, der er gennemført af koncernen, navnlig hvis de forhindrer videregivelse og udveksling af nødvendige oplysninger mellem enheder inden for koncernen, bør datterselskaber og filialer informere det konsoliderende instituts complianceansvarlige eller leder af complianceafdelingen.

22 Intern revisionsfunktion

215. Institutterne bør oprette en uafhængig og effektiv intern revisionsfunktion, under hensyntagen til de i del I anførte proportionalitetskriterier, og udpege en person, der er ansvarlig for denne funktion i hele instituttet. Den interne revisionsfunktion bør være uafhængig og i tilstrækkeligt omfang have autoritet, vægt og ressourcer. Navnlig bør instituttet sikre, at den interne revisionsfunktions medarbejdere er tilstrækkeligt kvalificerede, og at dens ressourcer, navnlig dens revisionsværktøjer og metoder til risikoanalyse, er tilstrækkelige i forhold til instituttets størrelse og placeringer samt arten, omfanget og kompleksiteten af de risici, der er forbundet med instituttets forretningsmodel, aktiviteter, risikokultur og risikoappetit.

216. Den interne revisionsfunktion bør være uafhængig af de reviderede aktiviteter. Den interne revisionsfunktion bør derfor ikke kombineres med andre funktioner.

217. Den interne revisionsfunktion bør på grundlag af en risikobaseret tilgang uafhængigt revidere og foretage objektiv kontrol af, at alle et instituts aktiviteter og enheder, herunder outsourcede aktiviteter, overholder instituttets politikker og procedurer samt eksterne krav. Hver enhed inden for koncernen bør være omfattet af den interne revisionsfunktion.

218. Den interne revisionsfunktion bør ikke være involveret i at udforme, udvælge, fastsætte og gennemføre specifikke interne kontrolpolitikker, -mekanismer og -procedurer samt risikogrænser. Dette bør imidlertid ikke hindre ledelsesorganet i dets ledelsesfunktion i at anmode om input fra den interne revision om spørgsmål vedrørende risiko, intern kontrol og overholdelse af gældende regler.

219. Den interne revisionsfunktion bør vurdere, om instituttets ramme for intern kontrol, jf. afsnit 15, er både virkningsfuld og effektiv. Navnlig bør den interne revisionsfunktion vurdere:

a. hensigtsmæssigheden af instituttets ledelsesramme

b. om eksisterende politikker og procedurer fortsat er tilstrækkelige og overholder juridiske og tilsynsmæssige krav samt instituttets risikostrategi og risikoappetit

c. procedurernes overholdelse af de gældende love og bestemmelser og af ledelsesorganets beslutninger

d. om procedurerne gennemføres korrekt og effektivt (f.eks. transaktioners overensstemmelse, det faktiske risikoniveau osv.) og

e. tilstrækkeligheden, kvaliteten og effektiviteten af den kontrol og rapportering, der er foretaget af forretningsenhederne og risikostyrings- og compliancefunktionen.

220. Den interne revisionsfunktion bør navnlig kontrollere rigtigheden af processerne og således sikre pålideligheden af instituttets metoder og teknikker samt de antagelser og informationskilder, der anvendes i dets interne modeller (f.eks. risikomodellering og regnskabsmæssige målinger). Den bør ligeledes evaluere kvaliteten og brugen af kvalitative værktøjer til identifikation og vurdering af risiko og de risikoafhjælpende foranstaltninger, der er truffet.

221. Den interne revisionsfunktion bør i hele instituttet have uhindret adgang til alle instituttets registre, dokumenter, oplysninger og bygninger. Dette bør omfatte adgang til ledelsesinformationssystemer og referater fra alle udvalg og beslutningstagende organer.

222. Den interne revisionsfunktion bør overholde nationale og internationale faglige standarder. Et eksempel på de faglige standarder, der henvises til her, er de standarder, der er udarbejdet af Foreningen af Interne Revisorer.

223. Det interne revisionsarbejde bør udføres i henhold til en revisionsplan og et detaljeret revisionsprogram, der følger en risikobaseret metode.

224. En intern revisionsplan bør udarbejdes mindst én gang om året på grundlag af de årlige mål for den interne revisionskontrol. Den interne revisionsplan bør godkendes af ledelsesorganet.

225. Der bør være en formel opfølgning på alle revisionsanbefalinger på det relevante ledelsesniveau, så det sikres, at der findes en effektiv og rettidig løsning, der rapporteres om.

Del VI — Driftskontinuitet[40]

226. Institutterne bør udarbejde en forsvarlig kontinuitets- og katastrofeplan, som sikrer, at de kan videreføre driften og begrænse deres tab i tilfælde af alvorlige driftsforstyrrelser.

227. Institutterne kan oprette en særlig uafhængig beredskabsfunktion, f.eks. som en del af risikostyringsfunktionen[41].

228. Et instituts drift hviler på flere kritiske ressourcer (f.eks. IT-systemer, herunder cloudtjenester, kommunikationssystemer, nøglemedarbejdere og bygninger). Formålet med håndtering af driftskontinuitet er at begrænse de operationelle, finansielle, juridiske, omdømmemæssige og andre væsentlige konsekvenser af en ulykke eller en længerevarende afbrydelse af disse ressourcer og deraf følgende afbrydelse af instituttets almindelige driftsprocedurer. Andre risikostyringsforanstaltninger kunne have til formål at reducere sandsynligheden for sådanne hændelser eller at overføre de finansielle konsekvenser heraf til tredjeparter (f.eks. via forsikring).

229. For at oprette en forsvarlig beredskabsplan bør et institut nøje analysere risikofaktorer for og sin eksponering for alvorlige driftsforstyrrelser og vurdere (kvantitativt og kvalitativt) deres potentielle virkning ved hjælp af interne og/eller eksterne data og scenarieanalyse. Denne analyse bør omfatte alle forretningsområder og interne enheder, herunder risikostyringsfunktionen, og tage hensyn til deres indbyrdes afhængighed. Resultaterne af analysen bør bidrage til at definere instituttets prioriteter og målsætninger for genoprettelsen.

230. Instituttet bør på grundlag af ovennævnte analyse udarbejde følgende:

a. beredskabs- og kontinuitetsplaner, som sikrer, at instituttet reagerer hensigtsmæssigt på nødsituationer og kan opretholde sine vigtigste driftsfunktioner, hvis der sker en afbrydelse af dets normale driftsprocedurer, og

b. katastrofeplaner for kritiske ressourcer, der skal sætte instituttet i stand til at vende tilbage til almindelige driftsprocedurer inden for en passende tidsfrist. Enhver restrisiko som følge af potentielle driftsforstyrrelser bør være forenelig med instituttets risikoappetit.

231. Beredskabs-, kontinuitets- og katastrofeplaner bør dokumenteres og implementeres omhyggeligt. Dokumentationen bør være tilgængelig i forretningsområderne, de interne enheder og risikostyringsfunktionen og bør lagres på systemer, der er fysisk adskilt og let

[40] Institutterne bør også henvise til EBA's retningslinjer vedrørende IKT-risiko, findes på: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
[41] Jf. også artikel 312 i forordning (EU) nr. 575/2013.

tilgængelige i tilfælde af en nødsituation. Der bør tilbydes relevant uddannelse. Planerne bør afprøves og opdateres regelmæssigt. Ethvert problem eller enhver fejl, der opstår under afprøvningerne, bør dokumenteres og analyseres, og planerne bør revideres i overensstemmelse hermed.

Del VII — Gennemsigtighed

232. Strategier, politikker og procedurer bør kommunikeres til alle relevante medarbejdere i et institut. Et instituts medarbejdere bør forstå og overholde politikker og procedurer, der vedrører deres pligter og ansvar.

233. Ledelsesorganet bør i overensstemmelse hermed informere og ajourføre de relevante medarbejdere om instituttets strategier og politikker på en klar og konsistent måde, i det mindste i det omfang dette er nødvendigt for, at disse medarbejdere kan udføre deres specifikke opgaver. Dette kan ske gennem skriftlige retningslinjer, manualer eller lignende midler.

234. I tilfælde hvor kompetente myndigheder i henhold artikel 106, stk. 2, i direktiv 2013/36/EU stiller krav om, at moderselskaber en gang om året offentliggør en beskrivelse af deres juridiske struktur og koncernens ledelsesstruktur og organisatoriske struktur, bør oplysningerne omfatte alle enheder inden for koncernstrukturen, som defineret i direktiv 2013/34/EU[42], efter land.

235. Offentliggørelsen bør som minimum omfatte:

a. en oversigt over institutternes interne organisation og koncernstrukturen som defineret i direktiv 2013/34/EU og ændringer heraf, herunder de vigtigste rapporteringslinjer og ansvarsområder

b. eventuelle væsentlige ændringer siden sidste offentliggørelse og datoen for den væsentlige ændring

c. nye juridiske, ledelsesmæssige eller organisatoriske strukturer

d. oplysninger om ledelsesorganets struktur, organisation og medlemmer, herunder antallet af medlemmer og antallet af medlemmer, der betragtes som uafhængige, og med angivelse af hvert enkelt medlem af ledelsesorganets køn og varigheden af den pågældendes mandat

e. ledelsesorganets vigtigste ansvarsområder

[42] Europa-Parlamentets og Rådets direktiv 2013/34/EU af 26. juni 2013 om årsregnskaber, konsoliderede regnskaber og tilhørende beretninger for visse virksomhedsformer, om ændring af Europa-Parlamentets og Rådets direktiv 2006/43/EF og om ophævelse af Rådets direktiv 78/660/EØF og 83/349/EØF (EUT L 182 af 29.6.2013, s. 19).

f. en liste over udvalgene under ledelsesorganet i dets tilsynsfunktion og deres sammensætning

g. en oversigt over den politik for interessekonflikter, der gælder for institutterne og ledelsesorganet

h. en oversigt over rammen for intern kontrol og

i. en oversigt over kontinuitetsplanen.

Bilag I — Aspekter, der kan tages i betragtning ved udviklingen af en intern ledelsespolitik

I overensstemmelse med del III bør institutterne tage følgende aspekter i betragtning, når de dokumenterer interne ledelsespolitikker og -ordninger:

1. Ejerstruktur
2. Koncernstruktur, hvis relevant (retlig og funktionel struktur)
3. Ledelsesorganets sammensætning og funktion
   a) udvælgelseskriterier, herunder hvordan der tages hensyn til diversitet
   b) antal, varighed af mandat, rotation, alder
   c) uafhængige medlemmer af ledelsesorganet
   d) ledende medlemmer af ledelsesorganet
   e) ikke-ledende medlemmer af ledelsesorganet
   f) intern opgavefordeling, hvis relevant
4. Ledelsesstruktur og organisationsplan (med indvirkning på koncernen, hvis relevant)
   a) specialiserede udvalg
      i. sammensætning
      ii. funktion
   b) forretningsudvalg, hvis et sådant findes
      i. sammensætning
      ii. funktion
5. Personer med nøglefunktioner
   a) leder af risikostyringsfunktionen
   b) leder af compliancefunktionen
   c) leder af den interne revisionsfunktion
   d) økonomidirektør
   e) andre personer med nøglefunktioner
6. Ramme for intern kontrol
   a) beskrivelse af hver funktion, herunder dens organisation, ressourcer, vægt og autoritet
7. beskrivelse af risikostrategien og risikostyringsrammen

8. organisatorisk struktur (med indvirkning på koncernen, hvis relevant)
    a) operationel struktur, forretningsområder og kompetence- og ansvarsfordeling
    b) outsourcing
    c) udvalg af produkter og tjenesteydelser
    d) aktiviteternes geografiske udstrækning
    e) udveksling af tjenesteydelser i henhold til ordningen om fri udveksling af tjenesteydelser
    f) filialer
    g) datterselskaber, joint ventures osv.
    h) anvendelse af offshorecentre
9. Adfærdskodeks (med indvirkning på koncernen, hvis relevant)
    a) strategiske mål og virksomhedsværdier
    b) interne kodekser og bestemmelser, forebyggelsespolitik
    c) politik for interessekonflikter
    d) whistleblowing
10. Status for den interne ledelsespolitik, med dato
    a) udvikling
    b) seneste ændring
    c) seneste vurdering
    d) ledelsesorganets godkendelse.