EBA/GL/2017/11

21/03/2018

Retningslinjer

vedrørende intern ledelse

1. Compliance- og indberetningsforpligtelser

Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der 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 institutioner 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. De kompetente myndigheder, 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 institutioner.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den 21/05/2018 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 de kompetente myndigheder for ikke at efterleve retningslinjerne. Underretninger fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, til compliance@eba.europa.eu med referencen "EBA/GL/2017/11". Underretninger fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndigheder. 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.

[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, -procedurer og -mekanismer, som kreditinstitutter og investeringsselskaber skal gennemføre i henhold til artikel 74, stk. 1, i direktiv 2013/36/EU[2] for at sikre en effektiv og forsigtig ledelse af instituttet.

Adressater

6. Målgruppen for disse retningslinjer er kompetente myndigheder som defineret i artikel 4, stk. 1, nr. 40), i forordning (EU) nr. 575/2013[3], herunder Den Europæiske Centralbank med hensyn til forhold, der vedrører de opgaver, den er pålagt ved forordning (EU) nr. 1024/2013, og institutter som defineret i artikel 4, stk. 1, nr. 3), i forordning (EU) nr. 575/2013.

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 de risici, 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 berører ikke 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, som udøver en ledelsesfunktion (ledende funktion) og en tilsynsfunktion (ikke-ledende funktion)[4].

9. Udtrykkene "ledelsesorganet i dets ledelsesfunktion" og "ledelsesorganet i dets tilsynsfunktion" anvendes i disse retningslinjer uden at henvise til en specifik ledelsesstruktur, og henvisninger til ledelsesfunktionen (ledende funktion) eller tilsynsfunktionen (ikke-ledende funktion) bør forstås således, at de gælder for organerne eller medlemmerne af

[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] Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1-337).

[4] Jf. også betragtning 56 til direktiv 2013/36/EU.

ledelsesorganet, der har ansvar for den pågældende funktion i overensstemmelse med national ret. Når de kompetente myndigheder gennemfører 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 de ledende funktioner til en person eller et internt ledende organ (f.eks. en administrerende direktør, et ledelsesteam eller et forretningsudvalg), bør de personer, der varetager disse ledende funktioner på grundlag af denne delegering, forstås således, at de udgør 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. De definitioner af administrerende direktør, økonomidirektør og nøglepersoner, 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 angivet, har de udtryk, der er anvendt og defineret i direktiv 2013/36/EU, den samme betydning i retningslinjerne. I disse retningslinjer gælder derudover følgende definitioner:

Risikovillighed	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.
Risikokapacitet	Den maksimale risiko, som et institut kan påtage sig i betragtning af dets kapitalgrundlag, dets risikostyrings- og kontrolkapacitet og dets regulatoriske restriktioner.
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.
Institutter	Kreditinstitutter og investeringsselskaber som defineret i henholdsvis artikel 4, stk. 1, nr. 1), og artikel 4, stk. 1, nr. 2), i forordning (EU) nr. 575/2013.
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.
Administrerende direktør	Den person, som har ansvar for at forvalte og styre et instituts samlede forretningsmæssige aktiviteter.
Økonomidirektør	Den person, som har overordnet ansvar for at forvalte alle følgende aktiviteter: forvaltning af finansielle ressourcer, finansiel planlægning og finansiel rapportering.
Ledere af interne kontrolfunktioner	Personerne med øverste ansvar for den faktiske daglige ledelse af den uafhængige risikostyringsfunktion, compliancefunktion og intern revisionsfunktion.
Nøglepersoner	Personer, som har betydelig indflydelse på instituttets ledelsesprincipper, men som ikke er medlem af ledelsesorganet og ikke er administrerende direktør. De omfatter lederne af interne kontrolfunktioner og økonomidirektøren, når de ikke er medlem af ledelsesorganet, og andre nøglepersoner, 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.
Konsolideringsreglerne	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. Den tilsynsmæssige konsolidering omfatter alle datterselskaber, som er institutter eller finansieringsinstitutter som defineret i henholdsvis artikel 4, stk. 1, nr. 3), og artikel 4, stk. 1, nr. 26), i forordning (EU) nr. 575/2013, og kan også omfatte accessoriske servicevirksomheder som defineret i forordningens artikel 4, stk. 1, nr. 18), i og uden for EU.

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.
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.
Noteret institut, der er omfattet af kapitalkravsdirektivet	Institutter, hvis finansielle instrumenter er optaget til handel på et reguleret marked eller i en multilateral handelsfacilitet, jf. artikel 4, stk. 1, nr. 21) og 22), i direktiv 2014/65/EU, i en eller flere medlemsstater[5].
Aktionær	En person, der ejer aktier i et institut, eller, afhængigt af instituttets retlige form, andre ejere eller medlemmer af instituttet.
Direktør- og bestyrelsespost	En stilling som medlem af et instituts eller en anden juridisk enheds ledelsesorgan.

3. Gennemførelse

Anvendelsesdato

15. Disse retningslinjer finder anvendelse fra den 30. juni 2018.

Ophævelse

16. EBA-retningslinjerne vedrørende intern ledelse (GL 44) af 27. september 2011 ophæves med virkning fra den 30. juni 2018.

[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).

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 regulatoriske krav faktisk opfyldes.

18. Institutterne bør tage hensyn til deres størrelse og interne organisation samt arten, omfanget og kompleksiteten af deres aktiviteter, når de udvikler og implementerer interne ledelsesordninger. Væsentlige institutter bør have mere avancerede ledelsesordninger, mens små og mindre komplekse institutter kan implementere simplere ledelsesordninger.

19. Med henblik på anvendelse af proportionalitetsprincippet og for at sikre en passende implementering af kravene bør institutterne og de kompetente myndigheder tage hensyn til følgende kriterier:

    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 noteret eller ej

    e. om instituttet har tilladelse til at anvende interne modeller til beregning af kapitalkrav (f.eks. den interne ratings-baserede metode)

    f. typen af godkendte aktiviteter og tjenester, der udføres af instituttet (se f.eks. 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, risikovillighed 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 myndigheder) og produkternes eller kontrakternes kompleksitet

k. de outsourcede aktiviteter og distributionskanaler og

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

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 øverste og overordnede ansvar for instituttet og fastlægger, fører tilsyn med og er ansvarligt for implementeringen 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 (ledende funktion) og tilsynsfunktionen (ikke-ledende funktion). Ledelsesorganets ansvar og opgaver bør beskrives i et skriftligt dokument og godkendes behørigt af ledelsesorganet.

22. Alle medlemmer af ledelsesorganet bør have fuldt kendskab til ledelsesorganets struktur og ansvar og til opgavefordelingen mellem forskellige funktioner i ledelsesorganet og dets udvalg. Med henblik på at indføre hensigtsmæssige kontrolforanstaltninger bør dets beslutningstagning ikke være domineret af et enkelt medlem eller en lille delmængde af dets medlemmer. 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.

23. Ledelsesorganets ansvar bør omfatte fastsættelse af, godkendelse af og tilsyn med implementeringen 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, herunder instituttets risikovillighed og rammerne for dets risikostyring og foranstaltninger til at sikre, at ledelsesorganet afsætter tilstrækkelig tid til risikospørgsmål

c. en tilstrækkelig og effektiv ramme for intern ledelse og intern kontrol, der omfatter en klar organisatorisk struktur og velfungerende uafhængige interne risikostyrings-,

compliance- og revisionsfunktioner, som i tilstrækkeligt omfang har autoritet, betydning og ressourcer til at varetage deres funktioner

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 om forsvarlige aflønningspolitikker i henhold til artikel 74, stk. 3, og artikel 75, stk. 2, i direktiv 2013/36/EU[6]

g. ordninger, der har til formål at sikre, at de individuelle og kollektive egnethedsvurderinger af ledelsesorganet implementeres effektivt, at ledelsesorganets sammensætning og successionsplanlægning er hensigtsmæssig, og at ledelsesorganet varetager sine funktioner effektivt[7]

h. en udvælgelses- og egnethedsvurderingsproces for nøglepersoner[8]

i. ordninger, der har til formål at sikre den interne drift 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

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

[6] EBA's retningslinjer om 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).

[7] Jf. også ESMA's og EBA's fælles retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

[8] Jf. også ESMA's og EBA's fælles retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

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

25. 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.

26. Et medlem af ledelsesorganet kan kun 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.

27. Ledelsesorganet bør overvåge, regelmæssigt gennemgå og afhjælpe eventuelle svagheder, der er identificeret vedrørende implementering af processer, strategier og politikker i forbindelse med de ansvarsområder, der er omhandlet i punkt 23 og 24. Rammen for intern ledelse og implementeringen 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

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

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

30. Ledelsesorganet i dets ledelsesfunktion bør konstruktivt udfordre og kritisk gennemgå oplæg, redegørelser og oplysninger, der modtages, når det foretager sin vurdering 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.

3 Ledelsesorganets tilsynsfunktion

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

32. 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 for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

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

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

    b. konstruktivt udfordre og kritisk gennemgå oplæg 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, herunder dets risikovillighed og rammer for risikostyring, samt andre politikker (f.eks. aflønningspolitik) og offentliggørelsesramme gennemføres konsekvent

    f. overvåge, at instituttets risikokultur er implementeret konsekvent

    g. føre tilsyn med implementeringen og opretholdelsen af en adfærdskodeks eller lignende og effektive politikker til identifikation, håndtering og begrænsning 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 betryggende 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 implementeringen af den interne revisionsplan, efter forudgående inddragelse af risikoudvalget og revisionsudvalget, hvis sådanne udvalg er nedsat.

4 Ledelsesorganets formands rolle

34. 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.

35. 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.

36. 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 begrænse 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.

37. Formanden bør fastlægge mødedagsordener og sikre, at drøftelsen af strategiske spørgsmål prioriteres. Formanden bør sikre, at ledelsesorganets beslutninger træffes på et betryggende og velinformeret grundlag, og at dokumenter modtages i tilstrækkelig god tid inden mødet.

38. 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

39. 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-[9] og aflønningsudvalg[10] 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 konsolideringsreglerne, der er væsentligt i en delkonsolideret eller konsolideret situation, er ikke forpligtet til at nedsætte disse udvalg.

40. 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.

41. Institutterne kan under hensyntagen til kriterierne i del I i disse retningslinjer nedsætte andre udvalg (f.eks. etisk udvalg, adfærds- og complianceudvalg).

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

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

44. Udvalgene bør understøtte tilsynsfunktionen på specifikke områder og fremme udviklingen og implementeringen 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[11]

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

46. Uafhængige medlemmer[12] af ledelsesorganet i dets tilsynsfunktion bør deltage aktivt i udvalg.

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

48. 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.

[9] Jf. også ESMA's og EBA's fælles retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

[10] Med hensyn til aflønningsudvalget henvises til EBA's retningslinjer om forsvarlig aflønningspraksis.

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

[12] Som defineret i afsnit 9.3 i ESMA's og EBA's fælles retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

49. 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.

50. 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[13]. Aflønningsudvalget bør være sammensat i overensstemmelse med afsnit 2.4.1 i EBA's retningslinjer om forsvarlige aflønningspolitikker[14].

51. 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.

52. Medlemmerne af nomineringsudvalget bør individuelt eller kollektivt have tilstrækkelig viden, kompetence og ekspertise vedrørende udvælgelsesprocessen og egnethedskravene.

53. 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.

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

5.3 Udvalgsprocesser

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

56. Udvalgene bør fungere i samspil med hinanden i det omfang, det er relevant. Med forbehold af punkt 48 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.

[13] 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.

[14] EMA's retningslinjer om 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).

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

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

59. 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 juridisk enhed, økonomi, personaleafdelingen, IT, risiko, compliance, revision osv.)

    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, der måtte have fundet sted, med detaljerede oplysninger om og anbefalinger til korrigerende foranstaltninger, der er truffet, skal træffes eller er forslået med henblik på at afhjælpe dem

    c. regelmæssigt gennemgå og fastsætte indholdet, formatet og hyppigheden af de risikooplysninger, der skal rapporteres til dem, og

    d. når det er nødvendigt, sikre passende inddragelse af de interne kontrolfunktioner og andre relevante funktioner (personaleafdelingen, juridisk enhed, økonomi) inden for deres respektive ekspertiseområder og/eller søge ekstern ekspertrådgivning.

5.4 Risikoudvalgets rolle

60. 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 risikovillighed og -strategi, 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 implementeringen af instituttets risikostrategi og de tilsvarende grænser, der er fastsat

    c. føre tilsyn med implementeringen af strategierne for kapital- og likviditetsstyring samt for alle andre relevante risici for et institut, såsom markeds- og kreditrisiko, operationelle risici (herunder retlige risici og IT-risici) og omdømmerisiko, for at vurdere deres tilstrækkelighed i forhold til den godkendte risikovillighed og -strategi

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 valg af eksterne konsulenter, som tilsynsfunktionen måtte beslutte at engagere med henblik på rådgivning eller støtte

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 de væsentlige finansielle produkter og tjenesteydelser, der tilbydes kunderne, og instituttets forretningsmodel og risikostrategi[15]; 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.

61. 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.

62. 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

63. I henhold til direktiv 2006/43/EF[16] 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 finansiel rapportering i det reviderede institut, uden at krænke dets uafhængighed

b. føre tilsyn med instituttets fastlæggelse af regnskabspolitikker

[15] Jf. også EBA's retningslinjer for 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.

[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.

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 6 i forordning (EU) nr. 537/2014[17], 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 fjernelse

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 den finansielle rapporterings integritet, og hvad revisionsudvalgets rolle var i den proces, og

i. modtage og tage hensyn til revisionsrapporter.

5.6 Kombinerede udvalg

64. 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.

65. 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 lever op til udvalgenes formål.

[17] 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).

66. 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[18].

Del III – Ledelsesramme

6 Organisatorisk ramme og struktur

6.1 Organisatorisk ramme

67. 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 nøglepersoner, i et institut bør være klare, veldefinerede og sammenhængende, kunne håndhæves og være behørigt dokumenteret. Dokumentationen bør opdateres efter behov.

68. 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.

69. 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")

70. 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 risikovillighed.

71. 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

[18] Jf. også ESMA's og EBA's fælles retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

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.

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

73. 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. Dette inkluderer en forståelse af koncernspecifikke operationelle risici og eksponeringer 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.

74. 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

75. 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 hvidvask af penge eller anden økonomisk kriminalitet, og de respektive kontrolforanstaltninger og retlige rammer, der er indført [19]. 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 hvidvask af penge og finansiering af terrorisme

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.

76. Under alle omstændigheder bør institutterne ikke etablere uigennemsigtige og unødvendigt komplekse strukturer, som ikke har nogen klar økonomisk begrundelse eller et retligt formål, eller hvis institutterne er bekymrede over, at disse strukturer kunne anvendes til et formål i tilknytning til økonomisk kriminalitet.

77. 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.

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

79. Ledelsesorganet bør sikre, at der træffes passende foranstaltninger for at undgå eller begrænse risiciene ved aktiviteter inden for sådanne strukturer. Hertil hører sikring af, at:

[19] For yderligere oplysninger om vurderingen af landerisiko og den risiko, der er forbundet med individuelle produkter og kunder, bør institutterne også henholde sig til to de endelige fælles retningslinjer om risikofaktorer (når de er udstedt): https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

a. instituttet har indført passende politikker og procedurer samt dokumenterede processer (f.eks. gældende grænser, informationskrav), 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.

80. 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.

81. 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

82. 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 konsolideret og delkonsolideret grundlag. Med henblik herpå bør moderselskaber og datterselskaber inden for konsolideringsreglernes anvendelsesområde implementere sådanne ordninger, processer og mekanismer i deres datterselskaber, som ikke er omfattet af direktiv 2013/36/EU, for at sikre robuste ledelsesordninger på konsolideret og delkonsolideret grundlag. 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.

83. Ledelsesorganet i et datterselskab, som er omfattet af direktiv 2013/36/EU, bør på individuelt niveau vedtage og implementere 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.

84. På konsolideret og delkonsolideret niveau bør det konsoliderende institut sikre, at alle institutter og andre enheder inden for konsolideringsreglernes anvendelsesområde, herunder deres datterselskaber, som ikke selv er omfattet af direktiv 2013/36/EU, overholder koncernledelsespolitikkerne. Ved implementeringen 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.

85. 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.

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

87. 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.

88. Ledelseskravene i direktiv 2013/36/EU og 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 disse retningslinjer.

89. 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[20]

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

[20] Disse retningslinjer er begrænset til den generelle outsourcingpolitik; specifikke outsourcingaspekter behandles i CEBS' retningslinjer for outsourcing, som skal revideres. Disse retningslinjer findes på https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

91. 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 implementeres fra en outsourcingaftales start til dens slut (herunder udarbejdelse af en business case for outsourcing, indgåelse 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.

92. 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.

93. Politikken bør kræve, at når instituttet vælger væsentlige eksterne tjenesteudbydere, eller når det outsourcer aktiviteter, skal det tage hensyn til, om tjenesteudbyderen har indført passende etiske standarder eller en adfærdskodeks.

Del IV – Risikokultur og forretningsadfærd

9 Risikokultur

94. En betryggende 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.

95. 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 risikovillighed.

96. 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.

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

98. 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 nøglepersoner, 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, 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 risikovillighed 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[21].

10 Virksomhedsværdier og adfærdskodeks

99. Ledelsesorganet bør udvikle, indføre, overholde og fremme høje etiske og faglige standarder, under hensyntagen til instituttets specifikke behov og karakteristika, og bør sikre implementeringen 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 implementere instituttets koncernstandarder eller fælles standarder udgivet af sammenslutninger eller andre relevante organisationer.

100. De gennemførte standarder bør tilsigte at 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.

[21] Jf. også EMA's retningslinjer om 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. Ledelsesorganet bør have klare og dokumenterede politikker for, hvordan disse standarder skal efterleves. Disse politikker bør:

    a. minde læserne om, at alle instituttets aktiviteter bør udføres 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 risikovillighed 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 svig, hvidvask af penge og kartelpraksis, finansielle sanktioner, bestikkelse og korruption, kursmanipulation, uhensigtsmæssigt salg og andre overtrædelser af lovgivningen om forbrugerbeskyttelse)

    d. præcisere, at foruden at overholde lov- og reguleringskrav 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.

102. 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

103. Ledelsesorganet bør være ansvarligt for at fastsætte, godkende og føre tilsyn med implementeringen og opretholdelsen af effektive politikker til at identificere, vurdere, håndtere og begrænse 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.

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

105. Institutternes foranstaltninger til at håndtere eller i givet fald begrænse 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, og

    c. etablering af passende procedurer for transaktioner med forbundne parter, f.eks. krav om, at transaktioner skal udføres på armslængdevilkår.

12 Politik for interessekonflikter i forbindelse med medarbejdere[22]

106. Ledelsesorganet bør være ansvarligt for at fastsætte, godkende og føre tilsyn med implementeringen og opretholdelsen af effektive politikker til at identificere, vurdere, håndtere og begrænse 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.

107. 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 begrænsende foranstaltninger.

108. 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.

109. 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, immaterielle rettigheder, lån ydet af instituttet til en virksomhed ejet af en medarbejder,

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

medlemskab af et organ eller ejerskab af et organ eller en enhed med modstridende interesser)

b. personlige eller faglige relationer til ejerne af kvalificerede kapitalandele 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

f. politisk indflydelse eller politiske relationer.

110. 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.

111. 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.

112. 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.

113. 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 begrænsende foranstaltninger. Sådanne procedurer, krav, 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. etablering af passende procedurer for transaktioner med forbundne parter (institutterne kan bl.a. overveje at stille krav om, at transaktioner skal gennemføres på armslængdevilkår, at alle relevante interne kontrolprocedurer fuldt ud finder anvendelse på sådanne transaktioner, og stille krav om bindende vejledning fra uafhængige medlemmer af ledelsesorganet, og om, at aktionærer skal godkende de mest relevante transaktioner og begrænse eksponeringen til sådanne transaktioner) og

e. 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.

114. 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[23].

115. 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.

116. 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.

13 Interne advarselsprocedurer

117. 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 indberetning, at have bevis for en

[23] Jf. også ESMA's og EBA's fælles retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og nøglepersoner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU.

overtrædelse; de bør imidlertid have tilstrækkelig sikkerhed, som giver tilstrækkelig grund til at iværksætte en undersøgelse.

118. 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 direktiv 95/46/EF.

119. Advarselsprocedurerne bør kunne benyttes af alle instituttets medarbejdere.

120. 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.

121. 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 person under instituttets kontrol udøver repressalier mod en person, der har indberettet en overtrædelse, og bør træffe passende foranstaltninger mod de ansvarlige for sådanne repressalier.

122. 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 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.

123. 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 direktiv 95/46/EF, 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

124. 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 implementering 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 95/46/EF og

d. klare procedurer, jf. punkt 123.

125. 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 – Ramme for og mekanismer for intern kontrol

15 Ramme for intern kontrol

126. Institutterne bør udvikle og opretholde en kultur, der tilskynder til en positiv holdning til risikostyring og overholdelse 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 bør 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, betydning og adgang til ledelsesorganet til at udføre deres mission, og en ramme for risikostyring.

127. Det pågældende instituts interne kontrol bør på individuelt grundlag tilpasses den særlige karakter af dets virksomhed, dets kompleksitet og de dermed forbundne risici, under hensyntagen til koncernsammenhængen. De pågældende institutter skal tilrettelægge udvekslingen af de nødvendige oplysninger på en måde, der sikrer, at hvert ledelsesorgan og 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 på koncernniveau og mellem lederne af de interne kontrolfunktioner på koncernniveau og instituttets ledelsesorgan.

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

129. Et instituts ramme for intern kontrol bør sikre:

a. effektive operationer

b. forsigtig forretningsadfærd

c. tilstrækkelig identifikation, måling og begrænsning 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 Implementering af en ramme for intern kontrol

130. 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 risikostyringsfunktion, compliancefunktion og intern revisionsfunktion). Institutterne bør fastlægge, opretholde og regelmæssigt ajourføre hensigtsmæssige skriftlige politikker, mekanismer og procedurer for den interne kontrol, som bør godkendes af ledelsesorganet.

131. 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.

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

133. Ved implementeringen 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.

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

135. De interne kontrolfunktioner bør regelmæssigt fremsende skriftlige rapporter om større identificerede mangler til ledelsesorganet. Disse rapporter bør for hver ny identificeret større mangel omfatte de relevante risici, der er involveret, en konsekvensanalyse, anbefalinger og korrigerende foranstaltninger, der skal træffes. Ledelsesorganet bør rettidigt og effektivt følge op på de interne kontrolfunktioners konklusioner og kræve passende afhjælpningsforanstaltninger. Der bør indføres en formel opfølgningsprocedure vedrørende konklusioner og korrigerende foranstaltninger, der er truffet.

17 Ramme for risikostyring

136. Som en del af den overordnede ramme for intern kontrol bør institutterne have en helhedsorienteret 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 kvalificerede 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-, koncentrations-, drifts-, IT-, omdømme-, retlige, adfærds-, compliance- og strategiske risici.

137. Et instituts ramme for risikostyring bør omfatte politikker, procedurer, risikogrænser og risikokontrolforanstaltninger, der sikrer passende, rettidig og vedvarende identifikation,

måling eller vurdering, overvågning, styring, begrænsning og rapportering af risiciene i forretningsområderne, på institutniveau og konsolideret eller delkonsolideret niveau.

138. 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 risikovillighed 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.

139. 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 risikovillighed, 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.

140. 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 risikovillighed 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.

141. 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.

142. 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.

143. 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).

144. 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.

145. 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.

146. 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[24]

147. 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 risikovillighed og de tilsvarende grænser, eller at de nødvendige revisioner foretages.

148. Væsentlige ændringer eller ekstraordinære transaktioner kan være fusioner og overtagelser, herunder de mulige konsekvenser af at udføre 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.

[24] Jf. også EBA's retningslinjer for 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.

149. 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.

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

151. 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. 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.

152. 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

153. 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.

154. 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.

19.1 Ledere af de interne kontrolfunktioner

155. Ledere af interne kontrolfunktion bør etableres på et passende hierarkisk niveau, som giver lederen af kontrolfunktionen den nødvendige autoritet og betydning til, at den pågældende kan opfylde sit ansvar. 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.

156. Lederne af interne kontrolfunktioner bør om nødvendigt have adgang og kunne rapportere direkte til ledelsesorganet i dets tilsynsfunktion for at give udtryk for betænkeligheder og advare tilsynsfunktionen, når det er hensigtsmæssigt, i tilfælde hvor specifikke udviklinger påvirker eller kan påvirke instituttet. Dette bør ikke hindre lederne af interne kontrolfunktioner i ligeledes at rapportere inden for de normale rapporteringslinjer.

157. 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

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

d. aflønningen af de intern 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[25].

19.3 Kombination af interne kontrolfunktioner

159. 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

160. 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.

161. 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

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

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

164. 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.

165. 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.

166. 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

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

operationelle funktioner og risikostyringsfunktionen bør bidrage til at nå målsætningen om, at alle instituttets medarbejdere har ansvar for at håndtere risici.

167. Risikostyringsfunktionen bør være en central organisatorisk funktion, der er struktureret, så den kan implementere 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.

168. 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.

169. 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 risikovillighed og -strategi. 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

170. Risikostyringsfunktionen bør være aktivt involveret på et tidligt tidspunkt i udformningen af et instituts 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 risikovillighed. Risikostyringsfunktionen bør vurdere soliditeten og bæredygtigheden af risikostrategien og -villigheden. Den bør sikre, at risikovilligheden på passende vis omsættes til specifikke risikogrænser. Risikostyringsfunktionen bør ligeledes vurdere risikostrategierne i forretningsenheder, herunder målsætninger foreslået af forretningsenhederne, og bør involveres, inden ledelsesorganet træffer beslutning vedrørende risikostrategierne. Målsætningerne bør være opnåelige og i overensstemmelse med instituttets risikostrategi.

171. Risikostyringsfunktionens inddragelse i beslutningsprocesser bør sikre, at der i tilstrækkeligt omfang kommer til at indgå risikooovervejelser. 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

172. 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.

173. 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, begrænsning, overvågning og rapportering af risici

174. Risikostyringsfunktionen bør sikre, at alle risici identificeres, vurderes, måles, overvåges, håndteres og rapporteres korrekt af de relevante enheder i instituttet.

175. Risikostyringsfunktionen bør sikre, at identifikationen og vurderingen ikke alene 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.

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

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

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

179. 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.

180. Risikostyringsfunktionen bør vurdere, hvordan det er muligt at begrænse risici. Rapporteringen til ledelsesorganet bør omfatte forslag til hensigtsmæssige risikobegrænsende foranstaltninger.

20.4 Risikostyringsfunktionens rolle med hensyn til ikke-godkendte eksponeringer

181. Risikostyringsfunktionen bør uafhængigt vurdere overtrædelser af risikovillighed 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.

182. 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

183. 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.

184. 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, betydning og uafhængighed (f.eks. lederen af juridisk afdeling).

185. 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.

186. 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 risikovillighed og -strategi.

21 Compliancefunktion

187. 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).

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

189. Compliancefunktionen, herunder lederen af complianceafdelingen, bør være uafhængig af de forretningsområder og interne enheder, den kontrollerer, og i tilstrækkeligt omfang have autoritet, betydning 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. juridisk afdeling eller personaleafdelingen.

190. 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 regelmæssig uddannelse.

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

192. 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 complianceramme.

193. 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.

194. 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.

195. Institutterne bør træffe passende foranstaltninger mod intern eller ekstern svigagtig adfærd og disciplinære overtrædelser (f.eks. overtrædelser af interne procedurer, overtrædelser af grænser).

196. 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

197. 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, betydning 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 risikovillighed.

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

199. 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.

200. Den interne revisionsfunktion bør ikke være involveret i at udforme, udvælge, fastsætte og implementere 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.

201. 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 risikovillighed og -strategi

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

    d. om procedurerne implementeres 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.

202. 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 risikobegrænsende foranstaltninger, der er truffet.

203. 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.

204. 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.

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

206. 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.

207. Alle revisionsanbefalinger bør underkastes en formel procedure for de relevante ledelsesniveauers opfølgning, så det sikres, at der findes en effektiv og rettidig løsning, der skal indberettes.

Del VI – Driftskontinuitet

208. Institutterne bør udarbejde en forsvarlig beredskabsplan, som sikrer, at de kan videreføre driften og begrænse deres tab i tilfælde af alvorlige driftsforstyrrelser.

209. Institutterne kan oprette en særlig beredskabsfunktion, f.eks. som en del af risikostyringsfunktionen[26].

210. Et instituts drift hviler på flere kritiske ressourcer (f.eks. IT-systemer, herunder cloudtjenester, kommunikationssystemer 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).

211. For at oprette en forsvarlig beredskabsplan bør et institut nøje analysere 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.

212. 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 risikovillighed.

213. 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 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.

[26] Jf. også artikel 312 i forordning (EU) nr. 575/2013.

Del VII – Gennemsigtighed

214. 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.

215. 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.

216. 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[27], efter land.

217. 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

    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

[27] 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).

h. en oversigt over rammen for intern kontrol og

i. en oversigt over beredskabsplanen.

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. Aktionærstruktur
2. Koncernstruktur, hvis relevant (retlig og funktionel struktur)
3. Ledelsesorganets sammensætning og funktion
   a) udvælgelseskriterier
   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. Nøglepersoner
   a) leder af risikostyringsfunktionen
   b) leder af compliancefunktionen
   c) leder af den interne revisionsfunktion
   d) økonomidirektør
   e) andre nøglepersoner

6. Ramme for intern kontrol
    a) beskrivelse af hver funktion, herunder dens organisation, ressourcer, betydning og autoritet
    b) beskrivelse af rammen for risikostyring, herunder risikostrategien
7. 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) aktiviteterne geografiske udstrækning
    e) fri udveksling af tjenesteydelser
    f) filialer
    g) datterselskaber, joint ventures osv.
    h) anvendelse af offshorecentre
8. Adfærdskodeks (med indvirkning på koncernen, hvis relevant)
    a) strategiske mål og virksomhedsværdier
    b) interne kodekser og bestemmelser, forebyggelsespolitik
    c) politik for interessekonflikter
    d) whistleblowing
9. Status for den interne ledelsespolitik, med dato
    a) udvikling
    b) seneste ændring
    c) seneste vurdering
    d) ledelsesorganets godkendelse.