EBA/GL/2021/05

2 juli 2021

Utkast till riktlinjer

för intern styrning

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer utfärdade i enlighet med artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 bör de behöriga myndigheterna och finansinstituten med alla tillgängliga medel söka följa riktlinjerna.

2. Av riktlinjerna framgår Europeiska bankmyndighetens (EBA) syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen ska tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till finansinstitut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den (05.12.2021). Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar bör lämnas på det formulär som tillhandahålls på EBA:s webbplats till compliance@eba.europa.eu med hänvisningen ”EBA/GL/2021/05”. Anmälningarna bör lämnas in av personer som har befogenhet att rapportera om hur riktlinjerna följs på de behöriga myndigheternas vägnar. Alla förändringar i graden av efterlevnad måste rapporteras till EBA.

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

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

2. Syfte, tillämpningsområde och definitioner

Syfte

5. Dessa riktlinjer specificerar vidare de interna styrformer, -processer och -mekanismer som institut som omfattas av direktiv 2013/36/EU 2 och värdepappersföretag som omfattas av avdelning VII i direktiv 2013/36/EU vid tillämpning av artikel 1.2 och 1.5 i förordning nr 2019/2033/EU bör genomföra i enlighet med artikel 74.1 i direktiv 2013/36/EU för att säkerställa sin effektiva och ansvarsfulla ledning.

Adressater

Dessa riktlinjer riktar sig till behöriga myndigheter enligt definitionen i artikel 4.2 i i förordning (EU) nr 1093/2010 och till finansinstitut enligt definitionen i artikel 4.1 i förordning (EU) nr 1093/2010 som är antingen institut vid tillämpningen av direktiv 2013/36/EU enligt definitionen i artikel 3.1.3 i direktiv 2013/36/EU och även med beaktande av artikel 3.3 i samma direktiv eller värdepappersföretag som omfattas av avdelning VII i direktiv 2013/36/EU vid tillämpning av artikel 1.2 och 1.5 i förordning 2019/2033/EU (nedan kallade *instituten*).

Tillämpningsområde

6. Dessa riktlinjer tillämpas på institutens styrformer, inbegripet deras organisationsstruktur och motsvarande ansvarsfördelning, deras processer för att identifiera, hantera, övervaka och rapportera de risker[3] som de är eller kan komma att bli exponerade för samt deras ramverk för internkontroll.

7. Riktlinjerna är avsedda att omfatta alla befintliga ledningsstrukturer, och ingen särskild struktur förordas. Riktlinjerna påverkar inte den allmänna fördelningen av befogenheter enligt nationell lagstiftning. De bör följaktligen tillämpas oavsett ledningsstruktur (monistisk och/eller dualistisk ledningsstruktur och/eller annan struktur) i alla medlemsstater. Ledningsorganet enligt definitionen i artikel 3.1.7 och 3.1.8 i direktiv 2013/36/EU bör förstås som ett organ med ledningsfunktioner (verkställande funktioner) och tillsynsfunktioner (icke verkställande funktioner)[4].

8. Termerna ”ledningsorganet i dess/sin ledningsfunktion” och ”ledningsorganet i dess/sin tillsynsfunktion” används genomgående i dessa riktlinjer utan hänvisning till någon specifik

[2] Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG, (EUT L 176, 27.6.2013, s. 338).

[3] Varje hänvisning till risker i dessa riktlinjer bör inkludera risker för penningtvätt och finansiering av terrorism.

[4] Se även skäl 56 i direktiv 2013/36/EU.

styrningsstruktur, och hänvisningar till ledningsfunktioner (verkställande funktioner) och tillsynsfunktioner (icke verkställande funktioner) bör tolkas som gällande för organen eller ledamöterna i det ledningsorgan som är ansvarigt för denna funktion enligt nationell lagstiftning. När behöriga myndigheter genomför dessa riktlinjer bör de ta hänsyn till gällande nationell bolagsrätt och vid behov precisera vilket organ eller vilka ledamöter i ledningsorganet som avses.

9. I medlemsstater där ledningsorganet helt eller delvis delegerar de verkställande funktionerna till en person eller ett internt verkställande organ (t.ex. verkställande direktör (vd), ledningsgrupp eller verkställande kommitté) bör de personer som utövar dessa verkställande funktioner anses utgöra ledningsorganets ledningsfunktion. Vid tillämpningen av dessa riktlinjer bör alla hänvisningar till ledningsorganet i dess ledningsfunktion förstås så att de även innefattar ledamöterna i det verkställande organet eller den verkställande direktören enligt den definition som anges i dessa riktlinjer, även om de inte har föreslagits eller utsetts till formella ledamöter av institutets ledningsorgan enligt nationell lagstiftning.

10. I medlemsstater där vissa ansvarsområden direkt utövas av institutens aktieägare, medlemmar eller ägare i stället för av ledningsorganet bör instituten se till att det ansvar som utövas och de beslut som fattas i samband därmed i så stor utsträckning som möjligt ligger i linje med de riktlinjer som gäller för ledningsorganet.

11. De definitioner av verkställande direktör, finansdirektör och person som innehar nyckelfunktioner som används i dessa riktlinjer är helt och hållet av funktionell karaktär och syftar inte till att föreskriva att sådana direktörer ska tillsättas eller sådana befattningar inrättas, såvida det inte föreskrivs i relevant lagstiftning på EU-nivå eller nationell nivå.

12. Instituten bör följa och de behöriga myndigheterna bör se till att instituten följer dessa riktlinjer på individuell nivå, undergruppsnivå och gruppnivå i enlighet med tillämpningsnivån enligt artikel 109 i direktiv 2013/36/EU.

Definitioner

13. Om inget annat anges har de termer som används och definieras i direktiv 2013/36/EU och i förordning (EU) nr 575/2013 samma innebörd i dessa riktlinjer. Dessutom gäller följande definitioner i dessa riktlinjer:

Riskaptit	den aggregerade risknivå och de risktyper som ett institut är villigt att utsätta sig för inom ramen för sin riskkapacitet, i enlighet med sin affärsmodell, för att uppnå sina strategiska mål.
Riskkapacitet	den maximala risknivå som ett institut kan utsätta sig för med tanke på sin kapitalbas, riskhantering och kontrollkapacitet samt gällande regleringsbegränsningar.

Riskkultur	ett instituts normer, attityder och beteenden som rör riskmedvetenhet, risktagande och riskhantering och de kontroller som ligger till grund för beslut om risker. Riskkulturen inverkar på de beslut som ledningen och medarbetarna fattar i den dagliga verksamheten och påverkar vilka risker de tar.
Personal	alla anställda vid ett institut och de dotterföretag som omfattas av institutets konsolidering, inbegripet dotterföretag som inte omfattas av direktiv 2013/36/EU, och samtliga ledamöter i ledningsorganet i dess ledningsfunktion och dess tillsynsfunktion.
Verkställande direktör (vd)	den person som ansvarar för övergripande ledning och styrning av ett instituts affärsverksamhet.
Finansdirektör	den person som har det övergripande ansvaret för ledningen av samtliga följande aktiviteter: hantering av finansiella resurser, finansiell planering och finansiell rapportering.
Chefer för interna kontrollfunktioner	de personer högst upp i hierarkin som i praktiken ansvarar för ledningen av den dagliga driften av de oberoende funktionerna för riskhantering, efterlevnad och internrevision.
Personer som innehar nyckelfunktioner	Avser personer som har ett betydande inflytande över institutets inriktning, men som varken är ledamöter i ledningsorganet eller vd. Här ingår chefer för interna kontrollfunktioner och finansdirektörer, om dessa inte ingår i ledningsorganet, samt andra personer som innehar nyckelfunktioner när sådana identifieras på riskbasis av instituten. Sådana andra personer som innehar nyckelfunktioner kan vara chefer för viktiga affärsområden, för filialer i EES-/Eftaområdet eller för dotterföretag i tredjeländer, alternativt innehavare av andra interna funktioner.
Konsolidering under tillsyn	tillämpning av de tillsynsregler som fastställs i direktiv 2013/36/EU och förordning (EU) nr 575/2013 på grupp- eller undergruppsnivå i enlighet med del ett, avdelning II, kapitel 2 i förordning (EU) nr 575/2013.[5]
Löneskillnad mellan könen	skillnaden mellan mäns och kvinnors genomsnittliga bruttotimlön uttryckt som en procentandel av mäns genomsnittliga bruttotimlön.
Konsoliderande institut	ett institut som är skyldigt att följa tillsynskraven på grundval av den konsoliderade situationen, i enlighet med del ett, avdelning II, kapitel 2 i förordning (EU) nr 575/2013.

[5] Se även tekniska standarder för konsolidering under tillsyn på https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

Betydande institut	de institut som avses i artikel 131 i direktiv 2013/36/EU (globala systemviktiga institut och andra systemviktiga institut) och i förekommande fall andra institut som fastställs av den behöriga myndigheten eller i nationell lagstiftning baserat på en bedömning av institutens storlek och interna organisation samt deras verksamhets egenskaper, omfattning och komplexitet.
Börsnoterat institut	institut vars finansiella instrument har upptagits till handel på en reglerad marknad eller en multilateral handelsplattform (MTF-plattform), såsom dessa definieras enligt artikel 4.21 och 4.22 i direktiv 2014/65/EU, i en eller flera medlemsstater[6].
Aktieägare	en person som äger aktier i ett institut, eller, beroende på institutets juridiska form, andra ägare av eller medlemmar i institutet.
Uppdrag i ledningsorgan	en position som ledamot i ledningsorganet för ett institut eller en annan juridisk person.

3. Genomförande

Datumet för ikraftträdande

14. Dessa riktlinjer gäller från och med den 31 december 2021.

Upphävande

15. EBA:s riktlinjer för intern styrning (EBA/GL/2017/11) av den 26 september 2017 upphävs med verkan från och med den 31 december 2021.

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

4. Riktlinjer

Avdelning I – Proportionalitet

16. Syftet med den proportionalitetsprincip som anges i artikel 74.2 i direktiv 2013/36/EU är att se till att de interna styrformerna stämmer överens med institutets individuella riskprofil och affärsmodell, så att syftet med de rättsliga och administrativa kraven verkligen uppnås.

17. Ett institut bör ta hänsyn till sin storlek och interna organisation samt till verksamhetens karaktär, omfattning och komplexitet när interna styrformer utvecklas och genomförs. Betydande institut bör ha mer sofistikerade styrformer medan små och mindre komplexa institut kan använda enklare styrformer. Instituten bör emellertid observera att ett instituts storlek eller systemviktighet i sig inte nödvändigtvis visar i vilken omfattning institutet utsätts för risker.

18. För att säkerställa att proportionalitetsprincipen tillämpas och att kraven och dessa riktlinjer genomförs på ett lämpligt sätt bör institut och behöriga myndigheter ta hänsyn till alla följande aspekter:

    a. Storleken vad gäller balansomslutningen för institutet och dess dotterföretag som omfattas av konsolidering under tillsyn.

    b. Institutets geografiska närvaro och storleken på dess verksamhet inom varje jurisdiktion.

    c. Institutets rättsliga form, inbegripet huruvida institutet ingår i en koncern och om så är fallet även proportionalitetsbedömningen för koncernen.

    d. Huruvida institutet är ett börsnoterat institut.

    e. Huruvida institutet har rätt att använda interna modeller för beräkning av kapitalbaskraven (t.ex. internmetoden).

    f. Den typ av auktoriserade verksamheter och tjänster som institutet ägnar sig åt (se också exempelvis bilaga 1 till direktiv 2013/36/EU och bilaga 1 till direktiv 2014/65/EU).

    g. Den underliggande affärsmodellen och affärsstrategin. Affärsverksamhetens karaktär och komplexitet samt institutets organisationsstruktur.

    h. Institutets riskstrategi, riskaptit och faktiska riskprofil, med beaktande även av resultaten av ÖuP-kapitalbedömningen och ÖuP-likviditetsbedömningen.

i. Institutets ägar- och finansieringsstruktur.

j. Typen av kunder (t.ex. detaljhandel, företag, institutioner, mindre företag, offentliga enheter) och produkternas eller avtalens komplexitet.

k. Verksamhet och distributionskanaler som lagts ut på entreprenad.

l. Befintliga it-system, inbegripet reservsystem och utläggning på entreprenad inom detta område.

m. Huruvida institutet omfattas av definitionen för ett litet och icke-komplext institut eller ett stort institut enligt artikel 4.1.145 och 4.1.146 i förordning (EU) nr 575/2013.

Avdelning II – Ledningsorganets och kommittéernas roll och sammansättning

1 Ledningsorganets roll och ansvarsområden

19. I enlighet med artikel 88.1 i direktiv 2013/36/EU måste ledningsorganet ha det yttersta och övergripande ansvaret för institutet. Ledningsorganet definierar, övervakar och är ansvarigt för genomförandet av de styrformer inom institutet som ska säkerställa att det leds på ett effektivt och ansvarsfullt sätt.

20. Ledningsorganets uppgifter bör vara tydligt definierade med en åtskillnad mellan ledningsfunktionens uppgifter (verkställande) och tillsynsfunktionens uppgifter (icke verkställande). Ledningsorganets ansvarsområden och uppgifter bör beskrivas skriftligt i ett dokument och vederbörligen godkännas av ledningsorganet. Alla ledamöter i styrelseorganet bör ha full kännedom om ledningsorganets struktur och ansvarsområden samt om uppgiftsfördelningen mellan ledningsorganets olika funktioner och dess kommittéer.

21. Tillsynsfunktionen och ledningsfunktionen inom ledningsorganet bör samverka på ett effektivt sätt. För båda funktionerna gäller att de bör förse varandra med tillräcklig information för att de båda ska kunna fullgöra sina respektive roller. För att makten över ledningsorganet ska kontrolleras och balanseras på ett lämpligt sätt bör dess beslutsfattande inte domineras av en enskild ledamot eller en liten grupp av ledamöter.

22. Det bör ingå i ledningsorganets ansvarsområden att fastställa, godkänna och övervaka genomförandet av

a. institutets övergripande affärsstrategi och viktigaste policyer inom ramen för tillämpliga lagar och förordningar, med beaktande av institutets långsiktiga ekonomiska intressen och solvens,

b. den övergripande riskstrategin, inbegripet institutets riskaptit och dess ramverk för riskhantering och åtgärder för att säkerställa att ledningsorganet ägnar risk- och riskhanteringsfrågorna tillräckligt med tid,

c. ett tillräckligt och effektivt ramverk för intern styrning och internkontroll enligt definitionen i avdelning V som:

    i. inkluderar en tydligt organisationsstruktur och välfungerande oberoende interna riskhanterings-, efterlevnads- och revisionsfunktioner som har tillräcklig auktoritet och tyngd samt tillräckliga resurser för att fullgöra sina funktioner,

    ii. säkerställer uppfyllande av tillämpliga rättsliga krav avseende förebyggande av penningtvätt och finansiering av terrorism,

d. mängden, typerna och fördelningen av både internt kapital och egna medel som krävs för att täcka institutets risker,

e. mål för institutets likviditetsförvaltning,

f. en ersättningspolicy som ligger i linje med de ersättningsprinciper som fastställs i artiklarna 92–95 i direktiv 2013/36/EU och i EBA:s riktlinjer för en sund ersättningspolicy enligt artiklarna 74.3 och 75.2 i direktiv 2013/36/EU[7],

g. mekanismer för att säkerställa att den individuella och kollektiva lämplighetsbedömningen av ledningsorganet utförs på ett effektivt sätt, att ledningsorganets sammansättning och efterträdarplanering är lämpliga och att ledningsorganet utför sina uppgifter på ett effektivt sätt[8],

h. en process för urval och lämplighetsbedömning av personer med nyckelfunktioner[9],

i. mekanismer för att säkerställa den interna funktionen hos var och en av de kommittéer som inrättas under ledningsorganet, inbegripet redogörelser för

    i. varje kommittés roll, sammansättning och uppgifter,

    ii. ett lämpligt informationsflöde, inbegripet dokumentationen av rekommendationer och slutsatser och rapporteringsvägarna mellan var

[7] EBA:s riktlinjer för en sund ersättningspolicy

[8] Se även Esmas och EBA:s gemensamma riktlinjer för bedömning av lämpligheten hos ledamöter i ledningsorganet och nyckelfunktionsinnehavarna.

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

och en av kommittéerna och ledningsorganet, behöriga myndigheter och andra parter,

j. en riskkultur som ligger i linje med avsnitt 9 i dessa riktlinjer och som omfattar institutets riskmedvetenhet och riskbeteende,

k. en företagskultur och värderingar som ligger i linje med avsnitt 10 och som främjar ett ansvarstagande och etiskt beteende, inklusive en uppförandekod eller ett liknande dokument,

l. en policy om intressekonflikter på institutnivå som ligger i linje med avsnitt 11 och en för personal som ligger i linje med avsnitt 12, och

m. mekanismer för att säkerställa tillförlitligheten hos systemen för redovisning och finansiell rapportering, inbegripet finansiella och operativa kontroller och efterlevnaden av lagstiftning och relevanta standarder.

23. När ledningsorganet fastställer, godkänner och övervakar genomförandet av aspekterna enligt förteckningen i punkt 22 bör ledningsorganet sträva efter att säkerställa en affärsmodell och styrformer, inklusive ett ramverk för riskhantering, som tar hänsyn till alla risker. När instituten beaktar alla risker som de utsätts för bör de ta hänsyn till alla relevanta riskfaktorer, bland annat dem som rör miljö, samhällsansvar och bolagsstyrning. Instituten bör beakta att de sistnämnda kan avgöra deras stabilitetsrisker, inbegripet kreditrisker, t.ex. via riskfaktorer som rör övergången till en hållbar ekonomi eller externa händelser i det fysiska klimatet som kan påverka gäldenärer, marknaden, likviditet, operativa risker och även anseenderisker, t.ex. via riskfaktorer som rör samhällsansvar och bolagsstyrning, t.ex. vad gäller utkontraktering[10]. Sådana risker inkluderar t.ex. juridiska risker inom avtals- eller arbetsrätt, risker förknippade med potentiella överträdelser av mänskliga rättigheter eller andra riskfaktorer som rör miljön, samhällsansvar och bolagsstyrning som kan påverka det land där en tjänsteleverantör är belägen och dennes förmåga att tillhandahålla tjänsten på de överenskomna nivåerna.

24. Ledningsorganet måste övervaka processen för offentliggörande av upplysningar och kommunikation med externa intressenter och behöriga myndigheter.

25. Samtliga ledamöter i ledningsorganet bör vara informerade om institutets verksamhet i allmänhet, dess finansiella situation och dess risksituation, med beaktande av det ekonomiska klimatet, samt om fattade beslut med betydande inverkan på institutets verksamhet.

26. En ledamot i ledningsorganet får ansvara för en sådan intern kontrollfunktion som avses i avdelning V, avsnitt 19.1, förutsatt att ledamoten inte har några andra mandat som skulle

[10] Se EBA:s rapport om hantering och tillsyn av risker som rör miljö, samhällsansvar och bolagsstyrning, publicerad i enlighet med artikel 98.8 i kapitalkravsdirektivet för att beskriva hur EBA betraktar risker som rör miljö, samhällsansvar och bolagsstyrning, överföringskanaler och rekommendationer för system, processer, mekanismer och strategier som instituten bör genomföra för att identifiera, bedöma och hantera risker som rör miljö, samhällsansvar och bolagsstyrning.

kunna inverka menligt på hans eller hennes uppgifter inom internkontroll eller äventyra den interna kontrollfunktionens oberoende.

27. Ledningsorganet bör övervaka, regelbundet se över och åtgärda eventuella brister när det gäller genomförandet av processer, strategier och policyer med koppling till de ansvarsområden som förtecknas i punkterna 22 och 23. Ramverket för intern styrning och dess genomförande bör ses över och uppdateras på regelbunden basis, med beaktande av den proportionalitetsprincip som förklaras närmare i avdelning I. En mer djupgående översyn bör göras vid väsentliga förändringar som påverkar institutet.

2 Ledningsorganets ledningsfunktion

28. Ledningsorganet i sin ledningsfunktion bör vara aktivt engagerat i institutets verksamhet och fatta beslut på sund och välinformerad grund.

29. Ledningsorganet i sin ledningsfunktion bör ansvara för genomförandet av de strategier som ledningsorganet fastställt och regelbundet diskutera strategiernas genomförande och lämplighet med ledningsorganet i dess tillsynsfunktion. Det operativa genomförandet kan utföras av institutets ledning.

30. Ledningsorganet i sin ledningsfunktion bör på ett konstruktivt sätt ifrågasätta och kritiskt granska förslag, förklaringar och information som tas emot när ledningsorganet utövar sitt omdöme och fattar beslut. Ledningsorganet i sin ledningsfunktion bör utförligt rapportera till samt regelbundet och vid behov utan oskäligt dröjsmål informera ledningsorganet i dess tillsynsfunktion om de aspekter som är relevanta för bedömningen av en situation, de risker och skeenden som påverkar eller kan komma att påverka institutet, t.ex. väsentliga beslut om affärsverksamheten och risker som tagits, utvärderingen av det ekonomiska klimat och företagsklimat som institutet verkar i, dess likviditet och sunda kapitalbas samt bedömningen av betydande risker för som institutet exponeras för.

31. Utan att det påverkar det nationella införlivandet av direktiv 2015/849/EU bör ledningsorganet identifiera en av sina ledamöter i enlighet med kraven enligt artikel 46.4 i direktiv 2015/849/EU (penningtvättsdirektivet) som är ansvarig för nödvändigt genomförande av lagar, förordningar och administrativa bestämmelser för att säkerställa efterlevnad av direktivet, bland annat motsvarande policyer och förfaranden för bekämpning av penningtvätt och finansiering av terrorism inom institutet och på ledningsorganets nivå[11].

3 Ledningsorganets tillsynsfunktion

32. I den roll som ledamöterna i ledningsorganet i dess tillsynsfunktion utövar bör det ingå att övervaka och på ett konstruktivt sätt ifrågasätta institutets strategi.

[11] Ledningsorganet i egenskap av ett kollegialt organ är ansvarigt som en helhet.

33. Utan att det påverkar nationell lagstiftning bör ledningsorganet i sin tillsynsfunktion ha oberoende ledamöter såsom fastställs i avsnitt 9.3 i Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorgan och ledande befattningshavare enligt direktiv 2013/36/EU och direktiv 2014/65/EU.

34. Utan att det påverkar tilldelade ansvarsområden enligt gällande nationell bolagsrätt bör ledningsorganet i sin tillsynsfunktion

    a. ha uppsikt över och övervaka ledningens beslut och åtgärder och bedriva en effektiv tillsyn av ledningsorganet i dess ledningsfunktion, inbegripet att övervaka och granska såväl dess prestationer på individuell och kollektiv basis som genomförandet av institutets strategi och mål,

    b. på ett konstruktivt sätt ifrågasätta och kritiskt granska förslag, förklaringar och information från ledamöter i ledningsorganet i dess ledningsfunktion och de beslut som fattas av ledningsorganet i dess ledningsfunktion,

    c. med beaktande av proportionalitetsprincipen enligt avdelning I på ett lämpligt sätt utföra riskkommitténs, ersättningskommitténs och nomineringskommitténs uppgifter och roller i de fall där sådana kommittéer inte har inrättats,

    d. säkerställa och regelbundet utvärdera effektiviteten hos institutets ramverk för intern styrning och vidta lämpliga åtgärder för att avhjälpa eventuella brister,

    e. ha uppsikt över och övervaka att institutets strategiska mål, organisationsstruktur och riskstrategi, inbegripet dess riskaptit och ramverk för riskhantering, såväl som andra policyer (exempelvis ersättningspolicy) och ramverket för offentliggörande av upplysningar genomförs på ett konsekvent sätt,

    f. övervaka att institutets riskkultur genomförs på ett konsekvent sätt,

    g. ha uppsikt över införandet och upprätthållandet av en uppförandekod eller liknande effektiva policyer som syftar till att upptäcka, hantera och minska intressekonflikter,

    h. ha uppsikt över den finansiella informationens och den finansiella rapporteringens tillförlitlighet samt över ramverket för internkontroll, inbegripet ett ramverk för effektiv och sund riskhantering,

    i. säkerställa att cheferna för interna kontrollfunktioner kan agera självständigt och, oaktat ansvaret att rapportera till andra interna organ, affärsområden eller enheter, ge uttryck för oro och varna ledningsorganet i dess tillsynsfunktion direkt när så krävs vid en ogynnsam riskutveckling som påverkar eller kan påverka institutet, samt

    j. övervaka genomförandet av planen för internrevision, efter det att risk- och revisionskommittéerna, i de fall där sådana inrättats, först har involverats.

4 Ordförandens roll i ledningsorganet

35. Ordföranden för ledningsorganet bör leda ledningsorganet, bidra till ett effektivt informationsflöde inom ledningsorganet och mellan ledningsorganet och dess kommittéer i fall där sådana inrättats samt ansvara för att ledningsorganet i stort fungerar effektivt.

36. Ordföranden bör främja en öppen och kritisk diskussion och se till att avvikande åsikter kan uttryckas och diskuteras under beslutsprocessen.

37. Som allmän princip gäller att ordföranden för ledningsorganet bör vara en icke verkställande ledamot. Om ordföranden tillåts ha verkställande uppgifter bör institutet införa åtgärder som minskar den negativa inverkan på kontrollen och balanseringen av makten inom institutet (t.ex. genom att utse en ledande styrelseledamot eller senior oberoende styrelseledamot eller att låta ledningsorganet i sin tillsynsfunktion ha ett större antal icke verkställande ledamöter). I synnerhet gäller i enlighet med artikel 88.1 e i direktiv 2013/36/EU att ordföranden i ledningsorganet i dess tillsynsfunktion avseende ett institut inte samtidigt får vara verkställande direktör i samma institut, om detta inte har motiverats av institutet och godkänts av de behöriga myndigheterna.

38. Ordföranden bör sammanställa mötesdagordningar och se till att strategiska frågor diskuteras med vederbörlig prioritet. Han eller hon bör se till att ledningsorganet fattar sina beslut på sund och välinformerad grund och att dokument och information erhålls i tillräckligt god tid före det aktuella mötet.

39. Ordföranden för ledningsorganet bör bidra till en tydlig uppgiftsfördelning mellan ledningsorganets ledamöter och till ett effektivt informationsflöde dem emellan så att ledamöterna i ledningsorganet i dess tillsynsfunktion kan ge ett konstruktivt bidrag till de diskussioner som förs och avlägga sina röster på sund och välinformerad grund.

5 Kommittéer under ledningsorganet i dess tillsynsfunktion

5.1 Inrättande av kommittéer

40. I enlighet med artikel 109.1 i direktiv 2013/36/EU, jämförd med artiklarna 76.3, 88.2 och 95.1 i direktiv 2013/36/EU, måste alla institut som kan anses betydande när den individuella nivån, undergruppsnivån och gruppnivån beaktas inrätta risk-, nominerings-[12] och ersättningskommittéer[13] som ska bistå ledningsorganet i dess tillsynsfunktion med råd och beredning av de beslut som ledningsorganet ska fatta. Ett institut som inte är betydande är inte skyldigt att inrätta dessa kommittéer, även om institutet omfattas av konsolidering under tillsyn av ett institut som är betydande på undergrupps- eller gruppbasis.

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

[13] Avseende ersättningskommittén se EBA:s riktlinjer för en sund ersättningspolicy.

41. I fall där det inte inrättats någon risk- eller utnämningskommitté bör hänvisningar till sådana kommittéer i dessa riktlinjer i stället förstås som avseende ledningsorganet i dess tillsynsfunktion, med beaktande av proportionalitetsprincipen enligt avdelning I.

42. Ett institut får också, med beaktande av de kriterier som fastställs i avdelning I i dessa riktlinjer, inrätta andra kommittéer (t.ex. kommitté för bekämpning av penningtvätt och finansiering av terrorism, etik-, uppförande- eller efterlevnadskommittéer).

43. Instituten bör säkerställa en tydlig fördelning av ansvarsområden och uppgifter mellan ledningsorganets specialiserade kommittéer.

44. Varje kommitté bör ha ett dokumenterat mandat, där omfattningen av kommitténs ansvar framgår, från ledningsorganet i dess tillsynsfunktion, samt fastställa en lämplig arbetsordning.

45. Kommittéerna bör stödja tillsynsfunktionen inom specifika områden och bidra till att ett hållbart ramverk för intern styrning utvecklas och genomförs. Delegering till kommittéer frigör inte på något sätt ledningsorganet i dess tillsynsfunktion från den kollektiva plikten att fullgöra sina uppgifter och skyldigheter.

5.2 Kommittéernas sammansättning[14]

46. Alla kommittéer bör som ordförande ha en icke verkställande ledamot av ledningsorganet som kan utöva ett objektivt omdöme.

47. Oberoende ledamöter [15] i ledningsorganet i dess tillsynsfunktion bör delta aktivt i kommittéerna.

48. I fall där kommittéer måste inrättas enligt direktiv 2013/36/EU eller nationell lagstiftning bör de bestå av minst tre ledamöter.

49. Instituten bör med beaktande av ledningsorganets storlek och antalet ledamöter i ledningsorganet i dess tillsynsfunktion säkerställa att ingen av kommittéerna består av samma grupp av ledamöter som någon annan kommitté.

50. Instituten bör överväga att då och då byta ordförande och ledamöter i kommittéerna med beaktande av de specifika krav på erfarenhet, kunskap och färdigheter som var och en av kommittéerna antingen individuellt eller kollektivt kräver.

51. Risk- och nomineringskommittéerna bör bestå av icke verkställande ledamöter i det berörda institutets ledningsorgan i dess tillsynsfunktion. Revisionskommitténs sammansättning bör

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

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

följa bestämmelserna i artikel 41 i direktiv 2006/43/EG [16] . Ersättningskommitténs sammansättning bör följa bestämmelserna i avsnitt 2.4.1 i EBA:s riktlinjer för en sund ersättningspolicy[17].

52. När det gäller globala systemviktiga institut och andra systemviktiga institut bör nomineringskommittén bestå av en majoritet oberoende ledamöter och ha en oberoende ledamot som ordförande. När det gäller andra betydande institut, som identifieras av behöriga myndigheter eller i nationell lagstiftning, bör ett tillräckligt antal ledamöter som är oberoende ingå i nomineringskommittén. Sådana institut kan även överväga att som god praxis ha en ordförande för nomineringskommittén som är oberoende.

53. Ledamöterna i nomineringskommittén bör både individuellt och kollektivt besitta de kunskaper, de färdigheter och den sakkunskap som krävs avseende urvalsprocessen och lämplighetskraven i enlighet med direktiv 2013/36/EU.

54. När det gäller globala systemviktiga institut och andra systemviktiga institut bör riskkommittén bestå av en majoritet oberoende ledamöter. I globala systemviktiga institut och andra systemviktiga institut bör riskkommitténs ordförande vara en oberoende ledamot. När det gäller andra betydande institut som identifieras av behöriga myndigheter eller i nationell lagstiftning bör ett tillräckligt antal ledamöter som är oberoende ingå i riskkommittén och denna bör om möjligt ha en oberoende ledamot som ordförande. Oavsett typen av institut får ordföranden för riskkommittén inte vara ordförande för ledningsorganet eller för någon annan kommitté.

55. Ledamöterna i riskkommittén bör både individuellt och kollektivt besitta de kunskaper, de färdigheter och den sakkunskap som krävs avseende riskhantering och kontroller.

5.3 Kommittéernas arbetssätt

56. Kommittéerna bör regelbundet rapportera till ledningsorganet i dess tillsynsfunktion.

57. Kommittéerna bör samverka med varandra på lämpligt sätt. Utan att det påverkar punkt 49 kan denna samverkan bestå i korsvis deltagande i kommittéernas arbete, dvs. att ordföranden eller en ledamot i en kommitté också är ledamot i en annan kommitté.

58. Kommittéernas ledamöter bör föra öppna diskussioner präglade av ett kritiskt förhållningssätt där avvikande åsikter diskuteras på ett konstruktivt sätt.

[16] Europaparlamentets och rådets direktiv 2006/43/EG av den 17 maj 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG (EUT L 157, 9.6.2006, s. 87), senast ändrat genom Europaparlamentets och rådets direktiv 2014/56/EU av den 16 april 2014.

[17] Riktlinjer för en sund ersättningspolicy enligt artiklarna 74.3 och 75.2 i direktiv 2013/36/EU och upplysningar enligt artikel 450 i förordning (EU) nr 575/2013 (EBA/GL/2015/22).

59. Kommittéerna bör dokumentera dagordningarna för sina möten samt de huvudsakliga resultaten och slutsatserna från mötena.

60. Risk- och nomineringskommittéerna bör åtminstone

    a. ha tillgång till all relevant information och uppgifter som behövs för att de ska kunna fullgöra sitt uppdrag, bland annat information och uppgifter från relevanta företags- och kontrollfunktioner (t.ex. juridiska, finansiella och personalfunktioner, it- och internrevisionsfunktioner, risk- och efterlevnadsfunktioner, inklusive information om efterlevnad av kraven på bekämpning av penningtvätt och finansiering av terrorism samt samlad information om rapporter om misstänkta transaktioner och riskfaktorer för penningtvätt och finansiering av terrorism),

    b. erhålla regelbundna rapporter, ad hoc-information, meddelanden och utlåtanden från cheferna för de interna kontrollfunktionerna gällande institutets aktuella riskprofil, dess riskkultur och riskgränser, såväl som alla eventuella väsentliga överträdelser [18] som kan ha inträffat, med detaljerad information och rekommendationer avseende vilka korrigerande åtgärder som vidtagits, ska vidtas eller föreslås för att komma tillrätta med dessa, periodiskt se över och fatta beslut om innehållet, formatet och intervallet för rapportering av riskinformationen till dem och

    c. när så krävs, säkerställa att interna kontrollfunktioner och andra relevanta funktioner (personal-, juridik- och ekonomiavdelningar) involveras på rätt sätt inom sina respektive expertområden och/eller söka extern experthjälp.

5.4 Riskkommitténs roll

61. När en riskkommitté har inrättats bör den åtminstone

    a. bistå ledningsorganet i dess tillsynsfunktion med råd och stöd avseende övervakningen av institutets övergripande faktiska och framtida riskstrategi och riskaptit med beaktande av alla typer av risker för att säkerställa att de ligger linje med institutets affärsstrategi, mål, företagskultur och värderingar,

    b. bistå ledningsorganet i dess tillsynsfunktion när det gäller att övervaka genomförandet av institutets riskstrategi och de motsvarande gränser som fastställts,

    c. ha uppsikt över genomförandet av strategierna för kapital- och likviditetsförvaltning såväl som för andra relevanta risker för institutet, däribland risker kopplade till marknad, kredit, drift (inbegripet rättsliga risker och it-risker) och institutets anseende,

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

i syfte att bedöma hur lämpliga dessa är med tanke på den riskstrategi och riskaptit som godkänts,

d. ge ledningsorganet i dess tillsynsfunktion rekommendationer om nödvändiga justeringar av riskstrategin till följd av exempelvis förändringar i institutets affärsmodell, utvecklingen på marknaden eller rekommendationer från riskhanteringsfunktionen,

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

f. granska ett antal möjliga scenarier, inbegripet stresscenarier, för att bedöma hur institutets riskprofil skulle reagera på externa och interna händelser,

g. ha uppsikt över överensstämmelsen mellan alla väsentliga finansiella produkter och tjänster som erbjuds till kunderna och institutets affärsmodell och riskstrategi[19]. samt bedöma vilka risker dessa finansiella produkter och tjänster medför och beakta överensstämmelsen mellan priset på produkterna och tjänsterna och den vinst de inbringar samt

h. utvärdera rekommendationer från interna eller externa revisorer och följa upp genomförandet av vidtagna åtgärder.

62. Riskkommittén bör samarbeta med andra kommittéer vars aktiviteter kan påverka riskstrategin (t.ex. revisions- och ersättningskommittén) och regelbundet kommunicera med institutets interna kontrollfunktioner, särskilt riskhanteringsfunktionen.

63. Om en riskkommitté har inrättats måste den, utan att det påverkar ersättningskommitténs uppgifter, undersöka huruvida incitamenten i ersättningspolicyn och ersättningspraxis tar hänsyn till institutets risk, kapital och likviditet samt sannolikheten och tidpunkten för resultat.

5.5 Revisionskommitténs roll

64. In enlighet med direktiv 2006/43/EG[20] bör revisionskommittén, om en sådan har inrättats, bland annat

[19] Se även EBA:s riktlinjer om produkttillsyn och styrformer för bankprodukter till privatpersoner och mindre företag, som finns tillgängliga på http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

[20] Europaparlamentets och rådets direktiv 2006/43/EG av den 17 maj 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG (EUT L 157, 9.6.2006, s. 87), senast ändrat genom Europaparlamentets och rådets direktiv 2014/56/EU av den 16 april 2014.

a. övervaka effektiviteten i institutets interna kvalitetskontroll- och riskhanteringssystem och i tillämpliga fall dess internrevision när det gäller det granskade institutets finansiella rapportering, utan att åsidosätta institutets oberoende,

b. ha uppsikt över institutets inrättande av redovisningsprinciper,

c. övervaka den finansiella rapporteringen och lämna rekommendationer eller för att säkerställa dess integritet,

d. granska och övervaka den lagstadgade revisorns eller revisionsföretagets och opartiskhet och självständighet i enlighet med artiklarna 22, 22a, 22b, 24a och 24b i detta direktiv samt artikel 6 i förordning (EU) nr 537/2014[21], särskilt om det är lämpligt att tillhandahålla icke-revisionstjänster till det granskade institutet i enlighet med artikel 5 i den förordningen

e. övervaka den lagstadgade revisionen av årsredovisning eller årsbokslut och koncernredovisning, i synnerhet dess utförande, med beaktande av den behöriga myndighetens resultat och slutsatser i enlighet med artikel 26.6 i förordning (EU) nr 537/2014,

f. ansvara för urvalsförfarandet vid val av en eller flera lagstadgade revisorer eller revisionsföretag och utfärda rekommendationer om vilken eller vilka lagstadgade revisorer eller revisionsföretag som ska utses av institutets behöriga organ (i enlighet med artikel 16 i förordning (EU) nr 537/2014, utom när artikel 16.8 i den förordningen tillämpas) samt om deras ersättning och entledigande,

g. granska inriktningen och omfattningen samt frekvensen av den lagstadgade revisionen av årsredovisning eller koncernredovisning,

h. i enlighet med artikel 39.6 a i direktiv 2006/43/EG informera den granskade enhetens förvaltnings- eller kontrollorgan om resultatet av den lagstadgade revisionen och förklara på vilket sätt den lagstadgade revisionen bidrog till den finansiella rapporteringens tillförlitlighet och vilken roll revisionskommittén spelade i denna process, samt

i. ta emot och beakta revisionsrapporter.

5.6 Kombinerade kommittéer

65. I enlighet med artikel 76.3 i direktiv 2013/36/EU får behöriga myndigheter tillåta att institut som inte betraktas som betydande kombinerar riskkommittén med en sådan revisionskommitté som avses i artikel 39 i direktiv 2006/43/EG, i de fall en sådan har inrättats.

[21] Europaparlamentets och rådets förordning (EU) nr 537/2014 av den 16 april 2014 om särskilda krav avseende lagstadgad revision av företag av allmänt intresse och om upphävande av kommissionens beslut 2005/909/EG (EUT L 158, 27.5.2014, s. 77).

66. Om icke betydande institut inrättar risk- och nomineringskommittéer får dessa kommittéer kombineras. Om kommittéerna kombineras bör instituten dokumentera skälen till att man valt att göra detta samt på vilket sätt målet med kommittéerna uppnås genom den valda strukturen.

67. Instituten bör alltid säkerställa att ledamöterna i en kombinerad kommitté både individuellt och som kollektiv besitter de kunskaper, de färdigheter och den sakkunskap som krävs för att fullt ut förstå de uppgifter som åligger den kombinerade kommittén[22].

Avdelning III – Ramverk för styrning

6 Organisatoriskt ramverk och organisationsstruktur

6.1 Organisatoriskt ramverk

68. Ett instituts ledningsorgan bör säkerställa att institutet har en lämplig och transparent organisatorisk och operativ struktur och att denna finns beskriven i ett skriftligt dokument. Strukturen bör främja och visa på en effektiv och ansvarsfull ledning av institutet på enskild nivå, undergruppsnivå och gruppnivå. Ledningsorganet bör säkerställa att de interna kontrollfunktionerna är oberoende av de affärsområden som de kontrollerar, inbegripet en lämplig åtskillnad mellan arbetsuppgifterna, och att de har tillräckliga ekonomiska resurser och personalresurser samt tillräckliga befogenheter för att effektivt fullgöra sin roll. Rapporteringsvägarna och ansvarsfördelningen inom institutet, särskilt mellan personer som innehar nyckelpositioner, bör vara tydliga, väldefinierade, sammanhängande, verkställbara och vederbörligen dokumenterade. Dokumentationen bör uppdateras på lämpligt sätt.

69. Institutets struktur bör inte inverka menligt på ledningsorganets förmåga att hålla uppsikt över och effektivt hantera de risker som institutet eller koncernen står inför och inte heller på den behöriga myndighetens förmåga att på ett effektivt sätt övervaka institutet.

70. Vid väsentliga förändringar av institutets struktur (t.ex. upprättande av nya dotterföretag, fusioner och förvärv, avyttrande eller avveckling av delar av koncernen eller externa händelser) bör ledningsorganet bedöma huruvida förändringarna påverkar hållbarheten i institutets organisatoriska ramverk, och i så fall hur. Om svagheter identifieras bör ledningsorganet skyndsamt genomföra de justeringar som krävs.

6.2 Kunskap om strukturen

71. Ledningsorganet bör vara ordentligt insatt i och förstå institutets rättsliga, organisatoriska och operativa struktur och se till att den överensstämmer med den fastställda affärsstrategin, riskstrategin och riskaptiten.

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

72. Ledningsorganet bör vara ansvarigt för godkännandet av sunda strategier och policyer för inrättandet av nya strukturer. Om ett institut skapar många juridiska personer inom sin koncern bör deras antal och i synnerhet förbindelserna och transaktionerna mellan dem inte utgöra några problem när det gäller utformningen av den interna styrningen och hanteringen eller övervakningen av riskerna i koncernen som helhet. Ledningsorganet bör säkerställa att ett instituts struktur, och i förekommande fall, strukturerna inom en koncern, med beaktande av de kriterier som anges i avsnitt 7, är tydliga, effektiva och transparenta för institutets personal, aktieägare och andra intressenter samt för den behöriga myndigheten.

73. Ledningsorganet bör styra institutets struktur, dess utveckling och dess begränsningar och se till att strukturen är motiverad, effektiv och inte onödigt eller obefogat komplicerad.

74. Ledningsorganet för ett konsoliderande institut bör inte bara förstå koncernens rättsliga, organisatoriska och operativa struktur, utan även syftet med dess olika enheter, deras aktiviteter och beroenden och förbindelser mellan dem. Detta inbegriper en förståelse för koncernspecifika operativa risker, exponeringar inom koncernen och hur koncernens finansiering, kapital, likviditet och riskprofiler kan påverkas under normala och ogynnsamma omständigheter. Ledningsorganet bör säkerställa att institutet skyndsamt kan ta fram information om koncernen med avseende på alla juridiska personers art, egenskaper, organisationsstruktur, ägandestruktur och verksamheter samt att instituten inom koncernen lever upp till kraven på tillsynsrapportering på individuell nivå, undergruppsnivå och gruppnivå.

75. Ledningsorganet för ett konsoliderande institut bör se till att de olika företagen i koncernen (inbegripet institutet självt) får tillräcklig information för att skapa sig en tydlig bild av koncernens övergripande mål, strategier och riskprofil samt hur det berörda koncernföretaget är införlivat i koncernens struktur och operativa funktionssätt. Sådana uppgifter, liksom alla ändringar av dem, bör dokumenteras och göras tillgängliga för alla relevanta funktioner, inbegripet ledningsorganet, affärsområdena och de interna kontrollfunktionerna. Ledamöterna i ledningsorganet för ett konsoliderande institut bör hålla sig informerade om de risker som koncernens struktur medför, med beaktande av de kriterier som anges i avsnitt 7 i riktlinjerna. I detta ingår att ta emot

    a. information om viktiga riskfaktorer,

    b. regelbundna rapporter om bedömningen av institutets övergripande struktur och utvärderingen av överensstämmelsen mellan enskilda enheters verksamhet och den godkända strategin för koncernen som helhet och

    c. regelbundna rapporter om ämnen där regelverket kräver efterlevnad på individuell nivå, undergruppsnivå och gruppnivå.

6.3 Komplexa strukturer och verksamheter som inte är standardmässiga eller som inte medger insyn

76. Instituten bör undvika att inrätta komplexa strukturer som kan försvåra insynen. Instituten bör i sitt beslutsfattande ta hänsyn till resultaten av en riskanalys som utförts för att undersöka huruvida de aktuella strukturerna skulle kunna utnyttjas i samband med penningtvätt eller annan ekonomisk brottslighet samt till de kontroller som inrättats och den lagstiftning som finns på området[23]. I detta syfte bör instituten åtminstone beakta följande:

    a. I vilken utsträckning den jurisdiktion där strukturen ska inrättas effektivt efterlever EU-standarder och internationella standarder för skattetransparens, bekämpning av penningtvätt och motverkande av finansiering av terrorism[24];

    b. I vilken utsträckning strukturen fyller ett uppenbart ekonomiskt och lagligt syfte.

    c. I vilken utsträckning strukturen skulle kunna användas för att dölja en slutlig faktisk betalningsmottagares identitet.

    d. I vilken utsträckning den kundbegäran som eventuellt ger upphov till att en struktur inrättas ger anledning till oro.

    e. Huruvida strukturen skulle kunna göra det svårare för institutets ledningsorgan att skaffa sig den överblick som krävs eller för institutet att hantera den tillhörande risken.

    f. Huruvida strukturen reser hinder i vägen för en effektiv övervakning från behöriga myndigheters sida.

77. Oavsett ovanstående får instituten inte inrätta några otydliga eller onödigt komplicerade strukturer om dessa saknar tydlig ekonomisk motivering eller lagligt syfte eller om instituten hyser farhågor om att strukturerna skulle kunna användas i syften kopplade till ekonomisk brottslighet.

78. Om sådana strukturer inrättas bör ledningsorganet förstå strukturerna och deras syfte och de särskilda risker som de medför samt säkerställa att de interna kontrollfunktionerna deltar på lämpligt sätt. Sådana strukturer får endast godkännas och upprätthållas om de har ett tydligt definierat syfte som de berörda förstår och om ledningsorganet är övertygat om att alla betydande risker, inbegripet anseenderisker, har identifierats, att alla risker kan hanteras effektivt och rapporteras på lämpligt sätt samt att en effektiv övervakning har säkerställts. Ju

[23] Instituten kan även se mer detaljerad information om bedömning av risken i det aktuella landet och den risk som förknippas med enskilda produkter och kunder i de gemensamma riktlinjerna för riskfaktorer för penningtvätt och finansiering av terrorism (EBA GL JC/2017/37) som för närvarande håller på att granskas.

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

mer komplex och otydlig den organisatoriska och operativa strukturen är och ju större riskerna är desto noggrannare bör strukturen övervakas.

79. Instituten bör dokumentera sina beslut och kunna motivera dem inför behöriga myndigheter.

80. Ledningsorganen bör se till att lämpliga åtgärder vidtas för att undanröja eller minska riskerna av den verksamhet som bedrivs inom sådana strukturer. I detta ingår att säkerställa att

    a. institutet har lämpliga policyer och förfaranden och dokumenterade processer (till exempel tillämpliga riskgränser, informationskrav) för bedömning, efterlevnad, godkännande och riskhantering av sådan verksamhet med beaktande av följderna för koncernens organisatoriska och operativa struktur, dess riskprofil och anseenderisk,

    b. information om verksamheten och dess risker är tillgänglig för det konsoliderande institutet och för interna och externa revisorer och att den rapporteras till ledningsorganet i dess tillsynsfunktion och till den behöriga myndighet som beviljat tillstånd samt

    c. att institutet regelbundet utvärderar behovet av att ha kvar strukturerna.

81. Dessa strukturer och verksamheter, inbegripet deras förenlighet med gällande lagstiftning och branschstandarder, bör regelbundet ses över av internrevisionsfunktionen i enlighet med en riskbaserad metod.

82. Ett institut bör vidta samma riskhanteringsåtgärder som för sin egen affärsverksamhet när det på uppdrag av kunder bedriver verksamhet som inte är standardmässig eller som inte medger insyn (t.ex. om institutet hjälper kunder att starta mellanhandsföretag i offshore-jurisdiktioner, utvecklar komplexa strukturer, finansierar transaktioner för kunderna eller tillhandahåller förvaltningstjänster) och som innebär liknande utmaningar när det gäller den interna styrningen och medför avsevärda operativa risker och anseenderisker. I synnerhet bör instituten analysera anledningen till att en kund vill inrätta en viss struktur.

7 Organisatoriskt ramverk i koncernkontext

83. I enlighet med artikel 109.2 i direktiv 2013/36/EU bör moder- och dotterföretag som omfattas av detta direktiv säkerställa att deras styrformer, processer och rutiner är enhetliga och väl integrerade på gruppnivå och undergruppsnivå. I detta syfte bör moder- och dotterföretag som omfattas av konsolidering under tillsyn genomföra sådana styrformer, processer och rutiner i sina dotterföretag som inte omfattas av direktiv 2013/36/EU, inbegripet sådana som har etablerats i tredjeländer, inbegripet sådana som är belägna i offshore-finanscentrum, för att säkerställa robusta styrformer på gruppnivå och undergruppsnivå. I frågor om ersättningskrav gäller vissa undantag i enlighet med artikel 109.4 och 109.5[25]. Behöriga funktioner inom det konsoliderande institutet och dess dotterföretag bör samverka och utbyta uppgifter och

[25] Se även EBA:s riktlinjer för en sund ersättningspolicy

information på lämpligt sätt. Styrformerna, processerna och rutinerna bör säkerställa att det konsoliderande institutet har tillräcklig tillgång till uppgifter och information och kan bedöma hela koncernens riskprofil, i enlighet med vad som anges i avsnitt 6.2.

84. Ledningsorganet för ett dotterföretag som omfattas av direktiv 2013/36/EU bör på individuell nivå anta och genomföra de koncerngemensamma policyer för styrning som fastställts på grupp- eller undergruppsnivå, på ett sätt som uppfyller alla specifika krav i EU:s lagstiftning och den nationella lagstiftningen.

85. På grupp- och undergruppsnivå bör det konsoliderande institutet se till att de koncerngemensamma policyerna för styrning och ramverket för internkontroll följs av alla institut och andra enheter som omfattas av konsolidering under tillsyn, inbegripet dotterföretag till dessa som inte själva omfattas av direktiv 2013/36/EU. Vid genomförande av policyer för styrning bör det konsoliderande institutet se till att det finns robusta styrformer på plats för varje dotterföretag samt överväga specifika former, processer och rutiner där affärsverksamheten inte delas in i separata juridiska personer utan organiseras i en matris över olika affärsområden som vart och ett innefattar flera juridiska personer.

86. Ett konsoliderande institut bör ta hänsyn till alla sina dotterföretags intressen och bedöma hur strategier och policyer bidrar till varje dotterföretags intressen och hela koncernens intressen på lång sikt.

87. Moderföretag och deras dotterföretag bör se till att instituten och företagen i koncernen uppfyller alla specifika krav i alla relevanta jurisdiktioner.

88. Det konsoliderande institutet bör se till att dotterföretag som inrättats i tredjeländer och som omfattas av konsolidering under tillsyn har styrformer, processer och rutiner som överensstämmer med koncerngemensamma policyer för styrning och lever upp till kraven i artiklarna 74–96 i direktiv 2013/36/EU och i dessa riktlinjer, så länge det inte bryter mot lagstiftningen i det aktuella tredjelandet.

89. De krav angående styrning som anges i direktiv 2013/36/EU och dessa riktlinjer gäller för institut även om de är dotterföretag till ett moderföretag i ett tredjeland. Om ett EU-dotterföretag till ett moderföretag i ett tredjeland är ett konsoliderande institut omfattar konsolideringen under tillsyn inte nivån för det moderföretag som ligger i ett tredjeland eller andra direkta dotterföretag till det moderföretaget. Det konsoliderande institutet bör se till att den koncerngemensamma policyn för styrning för moderföretaget i ett tredjeland beaktas i det konsoliderande institutets egen styrpolicy, så länge detta inte strider mot de krav som anges i gällande EU-lagstiftning, inbegripet direktiv 2013/36/EU och vidare i dessa riktlinjer.

90. När policyer fastställs och styrformer dokumenteras bör instituten ta hänsyn till de aspekter som förtecknas i bilaga 1 till dessa riktlinjer. Det är tillåtet att ha separata dokument för policyer och dokumentation, men instituten bör överväga att kombinera dem eller hänvisa till dem i ett samlat dokument om styrformerna.

8 Policy om utkontraktering[26]

91. Ett instituts ledningsorgan bör godkänna och regelbundet se över och uppdatera sin policy om utkontraktering samt se till att lämpliga ändringar införs utan dröjsmål.

92. Policyn om utkontraktering bör ta hänsyn till utkontrakteringens inverkan på institutets verksamhet och de risker det exponeras för (såsom operativa risker, inklusive rättsliga risker och it-risker, anseenderisker och koncentrationsrisker). Policyn bör omfatta de rapporterings- och övervakningsförfaranden som bör tillämpas i alla steg vid utkontraktering (såsom att sammanställa projektbeskrivningar som motiverar utkontraktering, ingå ett avtal om utkontraktering, fullfölja avtalet under hela avtalstiden och upprätta beredskapsplaner och utträdesstrategier). Institutet har det fulla ansvaret för alla tjänster och all verksamhet som utkontrakteras samt de ledningsbeslut de ger upphov till. Följaktligen bör det i policyn om utkontraktering klargöras att utkontraktering inte innebär att institutet befrias från sina skyldigheter enligt lag eller sitt ansvar gentemot kunderna.

93. Det bör framå av policyn att utkontraktering inte får hindra en ändamålsenlig tillsyn på plats eller utanför institutet och inte heller strida mot några begränsningar av tjänster eller verksamhet som följer av tillsynsreglerna. Policyn bör även omfatta utkontraktering inom en och samma koncern (dvs. tjänster som tillhandahålls av en separat juridisk person inom den koncern som institutet tillhör) och ta hänsyn till alla eventuella omständigheter som är specifika för den aktuella koncernen.

Avdelning IV – Riskkultur och uppförande

9 Riskkultur

94. Som en avgörande del i en effektiv riskhantering bör instituten ha en sund och konsekvent riskkultur som hjälper dem att fatta sunda och välgrundade beslut.

95. Varje institut bör utforma en integrerad riskkultur som omfattar hela institutet och som bygger på full kunskap om och en helhetssyn på de risker det exponeras för och hur de hanteras, med hänsyn tagen till riskaptiten.

96. Instituten bör utveckla en riskkultur med hjälp av policyer, kommunikation och personalutbildning om institutets verksamhet, strategi och riskprofil, där kommunikation och personalutbildning bör anpassas till personalens ansvar när det gäller risktagande och riskhantering.

97. Personalen bör vara fullt medveten om sitt ansvar avseende riskhanteringen. Riskhanteringen bör inte överlåtas enbart till riskspecialister eller intern kontrollfunktion. Affärsenheterna bör, under insyn av ledningsorganet, ta huvudansvaret för att på daglig basis hantera risker i linje

[26] Se även: EBA:s riktlinjer för utkontraktering, som finns tillgängliga på https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

med institutets policyer, förfaranden och kontroller, med beaktande av institutets riskaptit och riskkapacitet.

98. En stark riskkultur bör omfatta, men behöver inte vara begränsad till, följande:

a. Ledningens exempel: Ledningsorganet bör ansvara för att fastställa och förmedla institutets kärnvärden och förväntningar. Ledamöterna bör uppföra sig på ett sätt som speglar de värderingar som institutet står för. Institutets ledning, inbegripet personer som innehar nyckelpositioner, bör bidra till att kärnvärden och förväntningar förmedlas internt. Personalen bör agera i enlighet med alla gällande lagar och regler och skyndsamt anmäla överträdelser som observeras inom eller utanför institutet (exempelvis till den behöriga myndigheten via ett förfarande för visselblåsning). Ledningsorganet bör kontinuerligt främja, övervaka och utvärdera institutets riskkultur, bedöma riskkulturens påverkan på institutets finansiella stabilitet, riskprofil och robusta styrning samt införa ändringar vid behov.

b. Ansvarsskyldighet: Berörd personal på alla nivåer bör känna till och förstå institutets kärnvärden och, i den mån deras roll kräver det, institutets riskaptit och riskkapacitet. De bör ha förmåga att utöva sina roller och vara medvetna om att de kommer att hållas ansvariga för sina handlingar när det gäller institutets risktagande.

c. Effektiv kommunikation och ifrågasättande: En sund riskkultur bör främja en miljö med öppen kommunikation och ett effektivt ifrågasättande där beslutsprocesserna gynnar ett brett spektrum av åsikter, ger möjlighet att pröva gällande praxis, stimulerar till en konstruktivt kritisk inställning hos personalen och främjar en miljö präglad av öppet och konstruktivt engagemang i hela organisationen.

d. Incitament: Lämpliga incitament bör spela en nyckelroll när det gäller att få riskbeteendet att ligga i linje med institutets riskprofil och dess långsiktiga intressen[27].

10 Företagens värderingar och uppförandekod

99. Ledningsorganet bör utveckla, anta, följa och främja höga etiska och yrkesmässiga normer, med beaktande av institutets specifika behov och egenskaper, och säkerställa att sådana normer genomförs (med hjälp av en uppförandekod eller ett liknande instrument). Ledningsorganet bör även hålla uppsikt över personalens efterlevnad av normerna. I förekommande fall får ledningsorganet anta och genomföra institutets koncerngemensamma normer eller allmänna normer utfärdade av sammanslutningar eller andra relevanta organisationer.

100. Instituten bör säkerställa att personal inte diskrimineras på grund av kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller

[27] Se även EBA:s riktlinjer för en sund ersättningspolicy enligt artiklarna 74.3 och 75.2 i direktiv 2013/36/EU och upplysningar enligt artikel 450 i förordning (EU) nr 575/2013 (EBA/GL/2015/22), som finns tillgängliga på https://www.eba.europa.eu/regulation-and-policy/remuneration.

annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionsnedsättning, ålder eller sexuell läggning.

101. Institutens policyer bör vara könsneutrala. Detta inkluderar men är inte begränsat till ersättning, rekryteringspolicyer, karriärutveckling och efterträdarplanering, tillgång till utbildning och möjligheter att söka interna lediga jobb. Instituten bör säkerställa lika möjligheter[28] för all personal oavsett kön, bland annat när det gäller karriärmöjligheter, och sträva efter att förbättra representationen av det underrepresenterade könet på befattningar inom ledningsorganet och gruppen av anställda med ledningsansvar enligt definitionen i kommissionens delegerade förordning (tekniska standarder om identifierad personal). [29] Instituten bör övervaka utvecklingen av löneskillnaderna mellan könen separat hos identifierad personal (utom ledningsorganets ledamöter), ledamöterna i ledningsorganets i dess ledningsfunktion, ledamöterna i ledningsorganet i dess tillsynsfunktion och övrig personal. Instituten bör ha policyer som underlättar återintegrering av anställda efter föräldraledighet.

102. De genomförda normerna bör syfta till att minska de risker som institutet exponeras för, i synnerhet operativa risker och anseenderisker, som kan få avsevärda negativa konsekvenser för ett instituts lönsamhet och hållbarhet till följd av böter, rättegångskostnader, begränsningar som införs av behöriga myndigheter, andra ekonomiska och straffrättsliga påföljder och förluster när det gäller varumärkets värde och konsumenternas förtroende.

103. Ledningsorganet bör ha en tydlig, dokumenterad policy för hur dessa normer ska upprätthållas. Denna policy bör

a. påminna läsarna om att alla delar av institutets verksamhet bör bedrivas i enlighet med tillämplig lagstiftning och med institutets värderingar som företag,

b. främja riskmedvetenhet genom en stark riskkultur som ligger i linje med avsnitt 9 i riktlinjerna, och som signalerar att ledningsorganet förväntar sig att ingen del av verksamheten överskrider den fastställda riskaptiten och de gränser som anges av institutet eller indikeras i personalens respektive ansvarsområden,

c. ange principer för och ge exempel på acceptabelt och oacceptabelt beteende, i synnerhet när det gäller felaktig finansiell rapportering och misskötsamhet samt ekonomisk och finansiell brottslighet, som inbegriper men inte är begränsad till bedrägeri, penningtvätt och finansiering av terrorism, åtgärder mot konkurrensbegränsande samverkan, finansiella sanktioner, mutbrott och korruption, otillbörlig marknadspåverkan, vilseledande försäljning och andra överträdelser av konsumentskyddslagstiftningen, skattebrott, oavsett om dessa är direkta eller indirekta, inbegripet olagliga eller förbjudna system för utdelningsarbitrage,

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

[29] Se även EBA:s riktlinjer för en könsneutral ersättningspolicy

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

e. säkerställa att personalen känner till de interna och externa disciplinåtgärder, rättsliga åtgärder och påföljder som kan bli följden av misskötsamhet eller icke godtagbara beteenden.

104. Instituten bör övervaka efterlevnaden av normerna och se till att personalens medvetenhet om dem är god, till exempel genom att erbjuda utbildning. Instituten bör ange vilken funktion som är ansvarig för att övervaka efterlevnaden och bedöma överträdelser av uppförandekoden eller motsvarande instrument samt inrätta ett förfarande för hantering av överträdelser. Resultaten bör rapporteras regelbundet till ledningsorganet.

11 Policy om intressekonflikter på institutnivå

105. Ledningsorganet bör vara ansvarigt för att fastställa, godkänna och övervaka genomförandet och upprätthållandet av effektiva policyer för att identifiera, bedöma, hantera och minska eller förebygga faktiska eller potentiella intressekonflikter på institutnivå., t.ex. på grund av att institutet bedriver flera olika verksamheter och har flera olika roller, att flera institut omfattas av konsolidering under tillsyn, att institutet innefattar flera olika affärsområden eller enheter eller med hänsyn till externa intressenter.

106. Instituten bör inom ramen för sina organisatoriska och administrativa system vidta tillräckliga åtgärder för att förhindra att intressekonflikter skadar kundernas intressen.

107. Institutens åtgärder för att hantera eller i förekommande fall minska intressekonflikterna bör dokumenteras och bland annat innefatta följande:

a. Lämplig åtskillnad mellan ansvarsområdena, till exempel genom att anförtro verksamheter inom transaktionskedjan eller i fråga om tjänster som kan innebära en intressekonflikt till olika personer eller genom att anförtro övervakningen och rapporteringen av sådana verksamheter till olika personer.

b. Upprättande av informationsbarriärer, t.ex. genom en fysisk åtskillnad mellan vissa affärsområden eller enheter.

12 Policy om intressekonflikter för personal[30]

108. Ledningsorganet bör vara ansvarigt för att fastställa, godkänna och övervaka genomförandet och upprätthållandet av effektiva policyer för att identifiera, bedöma, hantera och minska eller förebygga faktiska eller potentiella konflikter mellan institutets intressen och privata intressen hos personalen, inbegripet ledningsorganets ledamöter, som kan inverka

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

menligt på deras fullgörande av sina uppgifter och ansvarsområden. Ett konsoliderande institut bör beakta olika intressen i en koncerngemensam policy om intressekonflikter på grupp- eller undergruppsnivå.

109. Policyn bör syfta till att identifiera intressekonflikter hos personalen, inbegripet deras nära familjemedlemmars intressen. Instituten bör ta hänsyn till att intressekonflikter inte enbart kan uppstå till följd av aktuella relationer utan även till följd av tidigare personliga eller yrkesmässiga relationer. När intressekonflikter uppstår bör instituten bedöma hur betydande de är samt besluta om och genomföra lämpliga åtgärder för att minska konflikterna.

110. När det gäller intressekonflikter som kan uppstå till följd av tidigare relationer bör instituten fastställa hur långt tillbaka personalens rapportering av sådana intressekonflikter bör sträcka sig mot bakgrund av att konflikterna fortfarande kan påverka personalens beteende och deras deltagande i beslutsfattandet.

111. Policyn bör omfatta åtminstone följande situationer eller relationer där intressekonflikter kan uppstå:

a. Ekonomiska intressen (t.ex. aktieinnehav, andra äganderätter och medlemskap, finansiella innehav och andra ekonomiska intressen i företagskunder, immateriella rättigheter, lån som institutet beviljat ett företag som ägs av personalen, medlemskap i ett organ eller en enhet med intressen som står i strid med institutets).

b. Personliga eller yrkesmässiga relationer till ägare till kvalificerade innehav i institutet.

c. Personliga eller yrkesmässiga relationer till personal som arbetar för institutet eller företagen som omfattas av konsolidering under tillsyn (exempelvis familjerelationer).

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

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

f. Politiskt inflytande eller politiska relationer.

112. Utan hinder av ovanstående bör instituten ta hänsyn till att det faktum att personal äger aktier i ett institut eller har privata konton eller lån eller på annat sätt använder ett instituts tjänster inte bör leda till att personalen anses befinna sig i intressekonflikt så länge involveringen inte överskrider en rimlig minimitröskel.

113. Policyn bör innehålla förfaranden för rapportering och informationsöverföring till den funktion som är ansvarig enligt policyn. Personalen bör omfattas av en plikt att skyndsamt internt redovisa alla eventuella situationer som kan ge upphov till, eller som redan har gett upphov till, en intressekonflikt.

114. Policyn bör skilja mellan intressekonflikter som kvarstår över längre tid och behöver hanteras permanent och intressekonflikter som inträder oväntat till följd av en enskild händelse (t.ex. en transaktion, valet av en viss tjänsteleverantör osv.) och oftast kan hanteras genom en engångsåtgärd. Under alla omständigheter bör institutets intressen vara centrala för de beslut som fattas.

115. Policyn bör innehålla bestämmelser om förfaranden, åtgärder, dokumentationskrav och ansvarsområden för identifiering och förebyggande av intressekonflikter, bedömning av hur betydande konflikterna är samt vidtagande av åtgärder för att minska konflikterna. Dessa förfaranden, krav, ansvarsområden och åtgärder bör inkludera följande:

a. Att anförtro verksamheter eller transaktioner där motstridiga intressen står mot varandra till olika personer.

b. Att hindra personal som även bedriver verksamhet utanför institutet från att utöva ett otillbörligt inflytande på dessa områden inom institutet.

c. Att fastslå att ledningsorganets ledamöter är ansvariga för att avstå från att rösta i ärenden där en ledamot befinner sig eller skulle kunna befinna sig i en intressekonflikt eller där ledamotens objektivitet eller förmåga att fullt ut fullgöra sina plikter gentemot institutet på annat sätt riskerar att äventyras.

d. Att se till att ledningsorganets ledamöter inte har uppdrag i ledningsorganen för konkurrerande institut, såvida det inte rör sig om institut som tillhör samma institutionella skyddssystem i enlighet med artikel 113.7 i förordning (EU) nr 575/2013, kreditinstitut som är permanent underställda ett centralt organ i enlighet med artikel 10 i förordning (EU) nr 575/2013 eller institut som omfattas av konsolidering under tillsyn.

116. Policyn bör i synnerhet omfatta riskerna för intressekonflikter på ledningsorganets nivå och ge tillräcklig vägledning för identifiering och hantering av intressekonflikter som kan äventyra ledningsorganets ledamöters förmåga att fatta objektiva och opartiska beslut som syftar till att tillvarata institutets intressen. Instituten bör ta i beaktande att intressekonflikter kan påverka oberoendet hos ledningsorganets ledamöter[31].

117. När instituten mildrar identifierade intressekonflikter hos ledningsorganets ledamöter bör de även dokumentera de vidtagna åtgärderna, bland annat resonemanget om hur dessa effektivt säkerställer objektivt beslutsfattande.

118. Faktiska eller potentiella intressekonflikter som redovisats för den ansvariga funktionen inom institutet bör bedömas och hanteras på lämpligt sätt. Om en intressekonflikt hos personalen identifieras bör institutet dokumentera det beslut som fattas, särskilt om

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

intressekonflikten och de risker den medför accepteras, och, om konflikten har accepterats, hur den på tillfredsställande sätt har mildrats eller lösts.

119. Alla faktiska och potentiella intressekonflikter på ledningsorgansnivå, oavsett om de är individuella eller kollektiva, bör dokumenteras på lämpligt sätt och kommuniceras till ledningsorganet som bör besluta om konflikterna och hantera dem korrekt.

12.1 Policyn om intressekonflikter med avseende på lån och andra transaktioner med ledningsorganets ledamöter och deras närstående parter

120. Som en del av sina policyer om intressekonflikter för personalen (avsnitt 12) och hantering av intressekonflikter hos ledningsorganets ledamöter i enlighet med punkt 117 bör ledningsorganet fastställa ett ramverk för att identifiera och hantera intressekonflikter med avseende på beviljande av lån och genomförande av andra transaktioner (t.ex. factoring, leasing, fastighetstransaktioner osv.) med ledningsorganets ledamöter och deras närstående parter.

121. Utan att det påverkar det nationella införlivandet av direktiv 2013/36/EU[32]kan instituten överväga ytterligare kategorier av närstående parter som de antingen helt eller delvis omfattar i sitt ramverk för intressekonflikter med avseende på lån och andra transaktioner.

122. Ramverket för intressekonflikter bör säkerställa att beslut om beviljande av lån till och genomförande av andra transaktioner med ledningsorganets ledamöter och deras närstående parter fattas på ett objektivt sätt, utan någon otillbörlig inverkan av intressekonflikter, och genomförs i princip på normala marknadsvillkor.

123. Ledningsorganet bör fastställa de tillämpliga processerna för beslutsfattande om beviljande av lån till och genomförande av andra transaktioner med ledningsorganets ledamöter och deras närstående parter. Detta ramverk kan säkerställa åtskillnad mellan vanliga affärstransaktioner [33] som sker inom ramen för normal affärsverksamhet på normala marknadsvillkor och lån till och transaktioner med personal som genomförs på villkor som finns tillgängliga för hela personalen. Ramverket för intressekonflikter och processen för beslutsfattande kan vidare göra åtskillnad mellan väsentliga och icke väsentliga lån och andra transaktioner, olika typer av lån och andra transaktioner samt nivån av de faktiska eller potentiella intressekonflikter som de kan ge upphov till.

124. Som en del av ramverket för intressekonflikter bör ledningsorganet fastställa lämpliga trösklar (t.ex. efter produkttyp eller beroende på villkoren) som lånet eller annan transaktion med ledningsorganets ledamot eller hans eller hennes närstående parter kräver alltid ledningsorganets godkännande. Beslut om väsentliga lån eller andra väsentliga transaktioner

[32] Se även Baselkommitténs huvudprincip 20

[33] Affärstransaktioner inkluderar lån och andra transaktioner (t.ex. leasing, factoring, tjänster som rör börsintroduktioner, fusioner och förvärv samt försäljning och köp av fast egendom).

med ledningsorganets ledamöter som inte genomförs enligt normala marknadsvillkor, utan enligt villkor som finns tillgängliga för hela personalen, bör alltid fattas av ledningsorganet.

125. En ledamot i ledningsorganet som skulle dra nytta av ett sådant väsentligt lån eller annan transaktion eller en ledamot som är närstående till motparten får inte delta i beslutsfattandet.

126. Vid beslutsfattande om ett lån eller annan transaktion med en ledamot i ledningsorganet eller hans eller hennes närstående parter bör instituten före beslutsfattandet bedöma den risk som transaktionen kan medföra för institutet.

127. Vid lån i form av kreditfacilitet (t.ex. checkräkningskrediter) bör det ursprungliga beslutet och ändringar i detta dokumenteras. Eventuellt utnyttjande av sådana överenskomna kreditfaciliteter inom de överenskomna gränserna får inte betraktas som ett nytt beslut om ett lån till en ledamot i ledningsorganet eller hans eller hennes närstående part. Om en ändring i en kreditfacilitet betraktas som väsentlig i enlighet med institutets policy bör en ny bedömning göras och ett nytt beslut fattas.

128. För att säkra efterlevnad av sina policyer om intressekonflikter bör instituten säkerställa att alla relevanta interna kontrollförfaranden tillämpas fullt ut på lån och andra transaktioner med ledningsorganets ledamöter eller deras närstående parter och att det finns ett lämpligt ramverk för uppsikt över ledningsorganets nivå i dess tillsynsfunktion.

12.2 Dokumentering av lån till ledningsorganets ledamöter och deras närstående parter samt ytterligare information

129. Vid tillämpning av artikel 88.1 i direktiv 2013/36/EU bör instituten korrekt dokumentera uppgifter om lån[34] till ledningsorganets ledamöter och deras närstående parter, inklusive åtminstone följande:

a. Namnet på gäldenären och gäldenärens status (dvs. ledamot i ledningsorganet eller närstående part) och vid lån till en närstående part den ledamot i ledningsorganet som parten är närstående till och uppgifter om partens relation till ledamoten.

b. Lånets typ/karaktär och lånebeloppet.

c. Villkor som tillämpas på lånet.

d. Datumet för godkännande av lånet.

e. Namnet på den person eller det organ (inklusive sammansättning av organet) som har fattat beslutet om godkännande av lånet och de tillämpliga villkoren.

f. Huruvida lånet har beviljats i enlighet med marknadsvillkoren (ja/nej).

[34] Se även EBA:s riktlinjer om låneutgivning, som finns tillgängliga på https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

g. Huruvida lånet har beviljats i enlighet med villkor som finns tillgängliga för hela personalen (ja/nej).

130. Instituten bör säkerställa att dokumentationen om alla lån till ledningsorganets ledamöter och deras närstående parter är fullständig och uppdaterad och att institutet vid begäran utan dröjsmål kan tillhandahålla hela dokumentationen till behöriga myndigheter i ett lämpligt format.

131. Vid ett lån till en ledamot i ledningsorganet eller en ledamots närstående part som överstiger 200 000 euro bör instituten på begäran kunna tillhandahålla följande ytterligare information till den behöriga myndigheten:

a. Procentandelen för lånet och procentandelen för summan av alla utestående lånebelopp till samma gäldenär jämfört med

i. summan av dess primärkapital och sekundärkapital samt

ii. institutets kärnprimärkapital,

b. huruvida lånet utgör en del av en större exponering[35] samt

c. den relativa vikten av den sammanlagda summan av alla utestående lånebelopp till samma gäldenär, beräknad som en procentandel genom att det sammanlagda utestående beloppet delas med det sammanlagda beloppet på alla utestående lån till ledningsorganets ledamöter och deras närstående parter.

13 Interna förfaranden för uppgiftslämning

132. Instituten bör inrätta och upprätthålla lämpliga policyer för uppgiftslämning och förfaranden för att personalen, via en särskild, oberoende och självständig kanal, ska kunna rapportera överträdelser av lagar och regler eller av interna krav, inbegripet men inte begränsat till kraven i förordning (EU) nr 575/2013 och nationella bestämmelser om införlivande av direktiv 2013/36/EU samt krav som ställs enligt interna styrformer. Personalen ska inte behöva ha bevis för en överträdelse för att kunna rapportera den, men den som rapporterar bör vara tillräckligt säker på uppgiften för att det ska finnas tillräckliga skäl att inleda en utredning. Instituten bör även genomföra lämpliga processer och förfaranden som säkerställer att de fullgör sina skyldigheter i enlighet med det nationella införlivandet av Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten.

133. För att undvika intressekonflikter bör personalen ha möjlighet att rapportera överträdelser utanför de vanliga rapporteringsvägarna (till exempel genom efterlevnadsfunktionen, internrevisionsfunktionen eller ett oberoende internt förfarande för visselblåsning). Förfarandena för uppgiftslämning bör säkerställa att personuppgifterna skyddas, både för den person som rapporterar överträdelsen och den fysiska person som påstås vara ansvarig för

[35] Se även del IV av förordning (EU) nr 575/2013, särskilt artikel 392.

överträdelsen, i enlighet med förordning nr 2016/679/EG [36] (den allmänna dataskyddsförordningen).

134. Förfarandena för uppgiftslämning bör kunna användas av all personal vid institutet.

135. Uppgifter som personalen lämnat enligt förfarandena för uppgiftslämning bör, om det är lämpligt, göras tillgängliga för ledningsorganet och andra ansvariga funktioner som definierats i den interna policyn om uppgiftslämning. När den person i personalen som rapporterar en överträdelse så önskar bör uppgifterna anonymiseras innan de vidarebefordras till ledningsorganet och andra ansvariga funktioner. Instituten kan även välja att inrätta ett förfarande för visselblåsning som medger att uppgifterna lämnas in i anonymiserad form.

136. Instituten bör säkerställa att den som rapporterar överträdelsen skyddas från alla eventuella negativa följder såsom repressalier, diskriminering och andra former av orättvis behandling. Institutet bör säkerställa att ingen person som står under institutets kontroll utsätter en person som rapporterat en överträdelse för bestraffning eller diskriminering och bör om så sker vidta lämpliga åtgärder mot de ansvariga.

137. Instituten bör även skydda personer som är föremål för rapportering från negativa följder om inga bevis som motiverar åtgärder mot personen framkommer under utredningen. Om åtgärder vidtas bör det göras på ett sätt som syftar till att skydda den berörda personen från oavsiktliga negativa effekter som går utöver avsikten med åtgärderna.

138. I synnerhet bör interna förfaranden för uppgiftslämning

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

b. omfatta tydliga regler som säkerställer att uppgifter om den som rapporterar en överträdelse, den som är föremål för rapportering och överträdelsen i sig behandlas konfidentiellt i enlighet med direktiv 95/2016/EG, såvida inte offentliggörande i enlighet med nationell lagstiftning krävs i samband med ytterligare utredningar eller efterföljande rättsliga förfaranden,

c. skydda personal som tar upp problem mot att drabbas av bestraffning eller diskriminering till följd av att de röjt överträdelser som kan rapporteras,

d. säkerställa att de potentiella eller faktiska överträdelser som tas upp bedöms och rapporteras, när det är lämpligt även till relevant behörig myndighet eller brottsbekämpande organ,

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

e. säkerställa, där så är möjligt, att personal som rapporterat en potentiell eller faktisk överträdelse får en bekräftelse på att uppgifterna tagits emot,

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

g. säkerställa lämplig registerhållning.

14 Rapportering av överträdelser till behöriga myndigheter

139. Behöriga myndigheter bör inrätta effektiva och tillförlitliga mekanismer för att underlätta för institutens personal att rapportera till behöriga myndigheter om potentiella eller faktiska överträdelser av rättsliga och administrativa krav, inklusive men inte begränsat till kraven i förordning (EU) nr 575/2013 och nationella bestämmelser om införlivande av direktiv 2013/36/EU. Dessa mekanismer bör åtminstone omfatta

a. särskilda förfaranden för mottagande av rapporter om överträdelser och uppföljning av dem, exempelvis en särskild avdelning, enhet eller funktion för visselblåsning,

b. lämpligt skydd såsom beskrivs i avsnitt 13,

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

d. tydliga förfaranden i enlighet med avsnitt 13.

140. Utan att det påverkar möjligheten att rapportera överträdelser via behöriga myndigheters mekanismer kan dessa myndigheter uppmuntra personalen att först försöka använda de interna förfarandena för uppgiftslämning vid det institut där de arbetar.

Avdelning V – Ramverk och mekanismer för internkontroll

15 Ramverket för internkontroll

141. Instituten bör utveckla och upprätthålla en kultur som främjar en positiv inställning till riskkontroll och efterlevnad inom institutet samt ett robust och heltäckande ramverk för internkontroll. Inom detta ramverk bör institutets olika affärsområden vara ansvariga för hanteringen av de risker som deras respektive verksamhet medför och tillämpa kontroller i syfte att säkerställa efterlevnaden av interna och externa krav. Som en del av detta ramverk bör instituten ha interna kontrollfunktioner med lämplig och tillräcklig auktoritet, tyngd och tillgång till ledningsorganet för att kunna fullgöra sitt uppdrag samt ett ramverk för riskhantering.

142. Det berörda institutets ramverk för internkontroll bör vara anpassat på individuell nivå till dess verksamhets specifika karaktär, dess komplexitet och de medföljande riskerna, med beaktande av koncernkontexten. Berörda institut bör organisera det nödvändiga informationsutbytet på ett sätt som säkerställer att varje ledningsorgan, affärsområde och intern enhet, inklusive varje intern kontrollfunktion, kan utföra sina uppgifter. Detta innebär exempelvis ett nödvändigt och tillräckligt informationsutbyte mellan affärsområdena och efterlevnadsfunktionen och efterlevnadsfunktionen i frågor om bekämpning av penningtvätt och finansiering av terrorism (om den utgör en separat kontrollfunktion) på koncernnivå samt mellan cheferna för interna kontrollfunktioner på koncernnivå och institutets ledningsorgan.

143. Instituten bör genomföra lämpliga processer och förfaranden som säkerställer att de fullgör sina skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism. Instituten bör bedöma sin exponering för risken för att de kan utnyttjas för penningtvätt eller finansiering av terrorism och vid behov vidta mildrande åtgärder för att minska dessa risker samt sina tillhörande operativa och anseendemässiga risker. Instituten bör vidta åtgärder för att säkerställa att personalen är medveten om sådana risker för penningtvätt och finansiering av terrorism samt om hur penningtvätt och finansiering av terrorism påverkar institutet och det finansiella systemets integritet.

144. Ramverket för internkontroll bör omfatta hela organisationen, inklusive ledningsorganets ansvarsområden och uppgifter, och samtliga affärsområdens och interna enheters verksamheter, inbegripet interna kontrollfunktioner samt utkontrakteradverksamhet och distributionskanaler.

145. Institutets ramverk för internkontroll bör säkerställa

a. ändamålsenlig och effektiv drift,

b. verksamhet som bedrivs på ett ansvarsfullt sätt,

c. tillräcklig identifiering, mätning och minskning av riskerna,

d. tillförlitlig rapportering av både finansiell och icke-finansiell information, såväl internt som externt,

e. sunda administrations- och redovisningsförfaranden samt

f. efterlevnad av lagar, förordningar, tillsynskrav och institutets interna policyer, processer, regler och beslut.

16 Genomförande av ett ramverk för internkontroll

146. Ledningsorganet bör vara ansvarigt för att inrätta ett ramverk, processer och mekanismer för internkontroll, övervaka att dessa fungerar tillfredsställande och effektivt samt ha uppsikt

över alla affärsområden och interna enheter, inbegripet interna kontrollfunktioner (såsom riskhanterings- och efterlevnadsfunktionen, efterlevnadsfunktionen i frågor om bekämpning av penningtvätt och finansiering av terrorism, om den är åtskild från efterlevnadsfunktionen, samt internrevisionsfunktionen). Instituten bör inrätta, upprätthålla och regelbundet uppdatera lämpliga skriftliga policyer, mekanismer och förfaranden för internkontroll som bör godkännas av ledningsorganet.

147. Ett institut bör inom ramverket för internkontroll ha en tydlig, transparent och dokumenterad process för beslutsfattande och en tydlig fördelning av ansvar och befogenheter som omfattar dess affärsområden, interna enheter och interna kontrollfunktioner.

148. Instituten bör informera all personal om dessa policyer, mekanismer och förfaranden, samt informera varje gång väsentliga förändringar av dessa har gjorts.

149. Vid genomförandet av ramverket för internkontroll bör instituten säkerställa en tillräcklig åtskillnad mellan arbetsuppgifterna – till exempel genom att anförtro verksamheter inom transaktionskedjan eller i fråga om tjänster som kan innebära en intressekonflikt till olika personer eller genom att anförtro övervakningen och rapporteringen av sådana verksamheter till olika personer – och upprätta informationsbarriärer, t.ex. genom en fysisk åtskillnad mellan vissa avdelningar.

150. De interna kontrollfunktionerna bör kontrollera att de policyer, mekanismer och förfaranden som fastställs i ramverket för internkontroll genomförs på ett korrekt sätt inom deras respektive kompetensområden.

151. De interna kontrollfunktionerna bör regelbundet överlämna skriftliga rapporter till ledningsorganet om de väsentliga brister som har upptäckts. Rapporterna bör, för varje ny identifierad större brist, innehålla beskrivningar av relevanta risker, en konsekvensanalys, rekommendationer samt korrigerande åtgärder som ska vidtas. Ledningsorganet bör följa upp de interna kontrollfunktionernas slutsatser i god tid och på ett effektivt sätt och ska utfärda krav om lämpliga korrigerande åtgärder. Ett formellt uppföljningsförfarande för slutsatser och korrigerande åtgärder som har vidtagits bör etableras.

17 Ramverk för riskhantering

152. Som en del av det övergripande ramverket för internkontroll bör instituten ha ett heltäckande ramverk för riskhantering som innefattar hela institutet och som sträcker sig över samtliga affärsområden och interna enheter, inbegripet de interna kontrollfunktionerna, där den ekonomiska innebörden av samtliga riskexponeringar beaktas fullt ut. Ramverket för riskhantering bör göra det möjligt för institutet att fatta väl underbyggda beslut om risktagande. Ramverket för riskhantering bör innefatta risker inom och utanför balansräkningen såväl som faktiska risker och framtida risker som institutet kan komma att utsättas för. Riskbedömningar bör göras nedifrån och upp och uppifrån och ned, inom och mellan affärsområden, med en konsekvent terminologi och kompatibla metoder inom hela

institutet och på grupp- och undergruppsnivå. Alla relevanta risker bör omfattas av ramverket för riskhantering med lämplig hänsyn till både ekonomiska och icke-ekonomiska risker, inbegripet kredit-, marknads-, likviditets- och koncentrationsrisker, operativa risker, it- och anseenderisker, juridiska risker, uppföranderisker, efterlevnadsrisker i fråga om penningtvätt, finansiering av terrorism och övrig ekonomisk brottslighet, risker som rör miljö, samhällsansvar och bolagsstyrning samt strategiska risker.

153. Institutets ramverk för riskhantering bör innefatta policyer, förfaranden, riskgränser och riskkontroller som säkerställer en tillfredsställande, skyndsam och kontinuerlig identifiering, mätning eller bedömning, övervakning, hantering, reducering och rapportering av riskerna på affärsområdes-, institut- och grupp- eller undergruppsnivå.

154. Institutets ramverk för riskhantering bör ge särskild vägledning för genomförandet av dess strategier. Inom ramen för denna vägledning bör institutet, när så är lämpligt, fastställa och upprätthålla interna riskgränser som motsvarar institutets riskaptit och är förenliga med dess förvaltning, finansiella styrka, kapitalbas och strategiska mål. Institutets riskprofil bör hållas inom dessa fastställda gränser. Ramverket för riskhantering bör säkerställa att det, för den händelse riskgränserna överskrids, finns en fastställd process för hur incidenten ska rapporteras och hanteras, med ett lämpligt uppföljningsförfarande.

155. Ramverket för riskhantering bör vara föremål för oberoende intern granskning, exempelvis utförd av internrevisionsfunktionen, och regelbundet ses över i förhållande till institutets riskaptit, med hänsyn tagen till information från riskhanteringsfunktionen och riskkommittén, i de fall en sådan har inrättats. Exempel på faktorer som bör beaktas är den interna och externa utvecklingen, däribland förändringar i balansräkningen och intäkterna, eventuell ökad komplexitetsgrad för institutets verksamhet, riskprofil eller verksamhetsstruktur, geografisk expansion, fusioner och förvärv samt införande av nya produkter eller affärsområden.

156. I samband med identifiering och mätning eller bedömning av risker bör institutet utveckla lämpliga metoder som omfattar både framåt- och bakåtblickande verktyg. Dessa metoder bör göra det möjligt att aggregera riskexponeringen för olika affärsområden och stödja identifieringen av riskkoncentrationer. Verktygen bör innefatta såväl bedömning av den faktiska riskprofilen i förhållande till institutets riskaptit som identifiering och bedömning av potentiella riskexponeringar och riskexponeringar vid stress i en rad olika scenarier med ogynnsamma omständigheter i förhållande till institutets riskkapacitet. Verktygen bör ge information om alla eventuella justeringar av riskprofilen som krävs. När instituten målar upp stresscenarier bör de vara rimligt konservativa i sina antaganden.

157. Instituten bör tänka på att resultaten av kvantitativa bedömningsmetoder, inklusive stresstest, till stor del beror på modellernas begränsningar och de antaganden som görs (till exempel om den extrema situationens allvar och varaktighet och de underliggande riskerna). Om en modell till exempel visar mycket hög avkastning på ekonomiskt kapital kan det bero på en svaghet hos modellen (t.ex. att vissa relevanta risker inte tas med i beräkningen), inte på att institutet har en överlägsen strategi eller genomför den på ett utmärkt sätt. Risknivån bör

därför inte bedömas enbart på grundval av kvantitativ information eller modellresultat, utan bedömningen bör även omfatta ett kvalitativt tillvägagångssätt (med expertutlåtanden och kritisk analys). Relevanta makroekonomiska trender och uppgifter bör särskilt uppmärksammas så att deras potentiella inverkan på exponeringar och portföljer kan fastställas.

158. Det är institutet som har det yttersta ansvaret för riskbedömningen och institutet bör således göra en kritisk granskning av sina risker i stället för att enbart förlita sig på externa bedömningar. Institutet bör till exempel utvärdera en färdigköpt riskmodell och anpassa den till sina egna omständigheter för att se till att riskerna fångas upp och analyseras på ett korrekt och heltäckande sätt i modellen.

159. Instituten bör vara fullt medvetna om modellernas och mätmetodernas begränsningar och inte uteslutande använda kvantitativa riskbedömningsverktyg, utan även kvalitativa verktyg (däribland expertutlåtanden och kritisk analys).

160. Utöver sina egna bedömningar kan ett institut även använda externa riskbedömningar (såsom externa kreditvärderingar eller externt inköpta riskmodeller). Instituten bör känna till exakt vad som ingår i bedömningarna och vilka deras begränsningar är.

161. Mekanismer för regelbunden och öppen rapportering bör fastställas så att ledningsorganet, dess riskkommitté (om en sådan har inrättats) och alla relevanta enheter inom ett institut får korrekta, koncisa, begripliga och meningsfulla rapporter i tid och kan utbyta relevant information om identifieringen, mätningen eller bedömningen, övervakningen och hanteringen av riskerna. Ramverket för rapportering bör vara väl definierat och dokumenterat.

162. En effektiv spridning av riskinformation och en stark riskmedvetenhet är avgörande för hela riskhanteringen, inbegripet granskningen och beslutsfattandet, och bidrar till att förhindra beslut som omedvetet kan öka riskerna. En effektiv riskrapportering inbegriper en sund intern behandling och kommunikation av riskstrategin och relevanta riskuppgifter (till exempel exponeringar och viktiga riskindikatorer) både horisontellt inom institutet och uppåt och nedåt i ledningskedjan.

18 Nya produkter och väsentliga förändringar[37]

163. Institutet bör ha en väldokumenterad policy för godkännande av nya produkter som är godkänd av ledningsorganet och som behandlar utvecklingen av nya marknader, produkter och tjänster, väsentliga förändringar av befintliga marknader, produkter och tjänster samt exceptionella transaktioner. Denna policy bör även omfatta väsentliga förändringar av tillhörande processer (t.ex. nya utkontrakteringsavtal) och system (t.ex. it-förändringsprocesser). Policyn för godkännande av nya produkter bör säkerställa att de

[37] Se även EBA:s riktlinjer om produkttillsyn och styrkrav för producenter och distributörer av bankprodukter till privatpersoner och mindre företag, som finns tillgängliga på https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

produkter och förändringar som godkänns är förenliga med institutets riskstrategi och riskaptit och med de motsvarande riskgränserna, eller att nödvändiga ändringar görs.

164. Väsentliga förändringar eller exceptionella transaktioner kan innefatta fusioner och förvärv, bland annat de möjliga konsekvenserna av en otillräcklig granskning (due diligence) där risker och kostnader i samband med fusionen inte har identifierats korrekt, upprättande av strukturer (t.ex. nya dotterföretag eller bolag som bildats för ett specifikt ändamål), nya produkter, förändringar i systemen eller ramverket eller förfarandena för riskhantering eller förändringar i institutets organisation.

165. Institutet bör ha specifika förfaranden för att bedöma efterlevnaden av dessa policyer där synpunkter från riskhanteringsfunktionen vägs in. Dessa förfaranden bör innefatta en systematisk förhandsbedömning och dokumenterade utlåtanden från efterlevnadsfunktionen om nya produkter eller betydande ändringar av befintliga produkter.

166. Institutets policy för godkännande av nya produkter bör omfatta allt som ska tas med i beräkningen innan ett beslut fattas om att gå in på nya marknader, erbjuda nya produkter, lansera nya tjänster eller göra väsentliga förändringar av befintliga produkter eller tjänster. Policyn för godkännande av nya produkter bör även omfatta de definitioner av ”ny produkt/marknad/verksamhet” och ”väsentliga förändringar” som ska användas i organisationen och vilka interna funktioner som ska vara delaktiga i beslutsprocessen.

167. Policyn för godkännande av nya produkter bör ange de viktigaste frågorna som bör beaktas innan ett beslut fattas. Exempel på sådana frågor är regelefterlevnad, redovisning, prissättningsmodeller, påverkan på riskprofil, kapitalkrav och lönsamhet, tillgång till tillräckliga front-, back- och middle office-resurser samt till interna verktyg och sakkunskaper som gör att man kan förstå och övervaka de medföljande riskerna. För att fullgöra sina skyldigheter enligt direktiv (EU) 2015/849 bör instituten vidare identifiera och bedöma den risk för penningtvätt och finansiering av terrorism som förknippas med den nya produkten eller affärsmetoden samt fastställa de åtgärder som bör vidtas för att minska dessa risker. Vilken affärsenhet och vilka personer som ansvarar för att lansera en ny verksamhet bör framgå tydligt av lanseringsbeslutet. Ingen ny verksamhet bör inledas förrän det finns tillräckliga resurser för att förstå och hantera de risker den medför.

168. Riskhanterings- och efterlevnadsfunktionerna bör delta i godkännandet av nya produkter eller väsentliga förändringar av befintliga produkter, processer och system. De bör bland annat göra en fullständig och objektiv bedömning av riskerna med ny verksamhet i en mängd olika scenarier, av potentiella brister i institutets ramverk för riskhantering och internkontroll samt av institutets förmåga att hantera nya risker på ett effektivt sätt. Riskhanteringsfunktionen bör även ha en god bild av införandet av nya produkter (eller väsentliga förändringar av befintliga produkter, processer och system) inom olika affärsområden och i olika portföljer samt befogenhet att kräva att ändringar i befintliga produkter genomförs enligt den formella policyn för godkännande av nya produkter.

19 Interna kontrollfunktioner

169. De interna kontrollfunktionerna bör omfatta en riskhanteringsfunktion (se avsnitt 20), en efterlevnadsfunktion (se avsnitt 21) och en internrevisionsfunktion (se avsnitt 22). Riskhanterings- och efterlevnadsfunktionerna bör granskas av internrevisionsfunktionen. Kontrollfunktionernas ansvar inkluderar även säkerställande av efterlevnad av kraven på bekämpning av penningtvätt och finansiering av terrorism.

170. Om de proportionalitetskriterier som anges i avdelning I beaktas får de interna kontrollfunktionernas operativa uppgifter, inom ramen för utkontraktering, anförtros det konsoliderande institutet eller en annan enhet inom eller utanför koncernen, förutsatt att ledningsorganen för de berörda instituten godkänner detta. Även om de operativa uppgifterna för internkontroll helt eller delvis utkontrakteras är det chefen för den berörda interna kontrollfunktionen och ledningsorganet som har ansvaret för uppgifterna och för att upprätthålla en funktion för internkontroll inom institutet.

171. Utan att det påverkar den nationella lagstiftningen för införlivande av direktiv 2015/849/EU bör instituten tilldela ansvaret för säkerställande av institutets efterlevnad av kraven enligt detta direktiv och institutets policyer och förfaranden till en anställd (t.ex. chefen för efterlevnadsfunktionen). Instituten kan inrätta en separat efterlevnadsfunktion för bekämpning av penningtvätt och finansiering av terrorism som en självständig kontrollfunktion.[38] Den ansvariga personen för bekämpning av penningtvätt och finansiering av terrorism bör vid behov kunna rapportera direkt till ledningsorganet i sin lednings- och tillsynsfunktion.

19.1 Chefer för interna kontrollfunktioner

172. Befattningen som chef för en intern kontrollfunktion bör inrättas på en lämplig nivå i hierarkin som ger cheferna tillräcklig auktoritet och tyngd för att kunna utöva sitt ansvar. Oaktat ledningsorganets övergripande ansvar bör cheferna för de interna kontrollfunktionerna vara oberoende i förhållande till de affärsområden eller enheter som de kontrollerar. Därför bör cheferna för riskhanterings-, efterlevnads- och internrevisionsfunktionerna rapportera till och vara direkt ansvariga inför ledningsorganet, och deras arbete bör granskas av ledningsorganet.

173. Cheferna för interna kontrollfunktioner bör i tillämpliga fall ha tillgång och rapportera direkt till ledningsorganet inom funktionens tillsynsenhet, i syfte att kunna lyfta frågor och problem samt varna tillsynsenheten när specifika skeenden påverkar eller kan komma att påverka institutet. Detta bör inte hindra cheferna för de interna kontrollfunktionerna från att också rapportera enligt ordinarie rapporteringsvägar.

[38] Se även EBA:s riktlinjer om efterlevnadsfunktionen för bekämpning av penningtvätt och finansiering av terrorism (under utarbetande)

174. Institutet bör ha dokumenterade processer för hur en chef för en intern kontrollfunktion tillsätts och hur han eller hon befrias från sina ansvarsområden. Under alla omständigheter bör cheferna för interna kontrollfunktioner inte kunna avsättas utan att ledningsorganet i sin tillsynsfunktion först godkänt detta. När det gäller chefen för riskhanteringsfunktionen är det enligt artikel 76.5 i direktiv 2013/36/EU obligatoriskt att inhämta ett sådant godkännande. När det gäller betydande institut bör behöriga myndigheter skyndsamt informeras om godkännandet och de huvudsakliga skälen till att chefen för en intern kontrollfunktion avsatts.

19.2 De interna kontrollfunktionernas oberoende

175. För att de interna kontrollfunktionerna ska betraktas som oberoende bör följande villkor vara uppfyllda:

a. Deras personal utför inga operativa uppgifter som rör den verksamhet som den aktuella interna kontrollfunktionen ska övervaka och kontrollera.

b. De är organisatoriskt åtskilda från de verksamheter som de ska övervaka och kontrollera.

c. Oaktat det övergripande ansvar som vilar på ledamöterna i institutets ledningsorgan bör chefen för en intern kontrollfunktion inte vara underordnad någon person som har ett ledningsansvar för den verksamhet som den interna kontrollfunktionen övervakar och kontrollerar.

d. Ersättningen till de interna kontrollfunktionernas personal bör inte vara kopplad till den verksamhet som respektive kontrollfunktion ska övervaka och kontrollera och inte heller på annat sätt kunna äventyra deras objektivitet[39].

19.3 Kombinering av interna kontrollfunktioner

176. Med beaktande av de proportionalitetskriterier som anges i avdelning I får riskhanterings- och efterlevnadsfunktionerna kombineras. Internrevisionsfunktionen får inte kombineras med någon annan intern kontrollfunktion.

19.4 De interna kontrollfunktionernas resurser

177. De interna kontrollfunktionerna bör ha tillräckliga resurser. De bör ha en kvalificerad och tillräckligt stor personalstyrka (både på moderföretags- och dotterföretagsnivå). Personalens kvalifikationer bör upprätthållas och de bör få lämplig utbildning efter behov.

178. De interna kontrollfunktionerna bör ha tillgång till lämpliga it-system och stödtjänster samt den interna och externa information som krävs för att utföra arbetsuppgifterna. De bör ha

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

tillgång till all nödvändig information om alla affärsområden och relevanta riskbärande dotterföretag, särskilt sådana som skulle kunna generera betydande risker för instituten.

20 Riskhanteringsfunktion

179. Varje institut bör inrätta en riskhanteringsfunktion som omfattar hela institutet. Riskhanteringsfunktionen bör ha tillräcklig auktoritet och tyngd och tillräckliga resurser, med beaktande av de proportionalitetskriterier som anges avdelning I, för att genomföra institutets riskpolicyer och ramverket för riskhantering i enlighet med avsnitt 17.

180. Vid behov bör riskhanteringsfunktionen ha direkt tillgång till ledningsorganet i dess tillsynsfunktion och i förekommande fall dess kommittéer, särskilt riskkommittén.

181. Riskhanteringsfunktionen bör ha tillgång till alla affärsområden och andra interna enheter vars verksamheter kan medföra risker, såväl som till relevanta dotterföretag och närstående företag.

182. Riskhanteringsfunktionens personal bör i tillräcklig utsträckning besitta kunskaper, färdigheter och sakkunskap om metoder och förfaranden för riskhantering och om marknader och produkter, och de bör ha tillgång till regelbunden utbildning.

183. Riskhanteringsfunktionen bör vara oberoende av de affärs- och stödenheter vars risker den kontrollerar, men inte förhindras från att samverka med dem. De operativa funktionerna och riskhanteringsfunktionen bör samverka med målet att hela institutets personal ska ta ansvar för riskhanteringen.

184. Riskhanteringsfunktionen bör vara ett centralt inslag i institutets organisation och ha en struktur som möjliggör för funktionen att genomföra riskpolicyer och kontrollera ramverket för riskhantering. Riskhanteringsfunktionen bör spela en viktig roll när det gäller att se till att institutet har effektiva riskhanteringsprocesser. Riskhanteringsfunktionen bör vara aktivt delaktig i alla betydande riskhanteringsbeslut.

185. Betydande institut kan överväga att inrätta särskilda riskhanteringsfunktioner för alla större affärsområden. Det bör dock finnas en central riskhanteringsfunktion, inbegripet en koncerngemensam funktion i det konsoliderande institutet, som kan ge en heltäckande, koncernövergripande bild av alla risker och se till att riskstrategin följs.

186. Riskhanteringsfunktionen bör tillhandahålla relevant och oberoende information, analyser och expertutlåtanden om riskexponeringar, ge råd i fråga om förslag och riskbeslut från affärsområden eller interna enheter samt informera ledningsorganet om huruvida dessa är förenliga med institutets riskstrategi och riskaptit. Riskhanteringsfunktionen kan rekommendera förbättringar av ramverket för riskhantering och olika sätt att komma till rätta med överträdelser av policyer, förfaranden och gränser för risktagandet.

20.1 Riskhanteringsfunktionens roll i fråga om strategi och beslutsfattande

187. Riskhanteringsfunktionen bör, aktivt och i ett tidigt skede, delta i utformandet av institutets riskstrategi och i inrättandet av effektiva processer för institutets riskhantering. Riskhanteringsfunktionen bör förse ledningsorganet med all relevant riskinformation som krävs för att ledningsorganet ska kunna fastställa institutets riskaptitnivå. Riskhanteringsfunktionen bör bedöma hur robusta och hållbara riskstrategin och riskaptiten är. Funktionen bör också se till att riskaptiten på lämpligt sätt omvandlas till specifika riskgränser. Riskhanteringsfunktionen bör även bedöma affärsenheternas riskstrategier, inbegripet de målsättningar som enheterna föreslår, och vara delaktig innan ledningsorganet fattar beslut gällande riskstrategierna och riskaptiten. Målsättningarna bör vara rimliga och förenliga med institutets riskstrategi.

188. Riskhanteringsfunktionen bör vara delaktig i beslutsprocessen för att säkerställa att riskerna beaktas i tillräcklig omfattning. Ansvaret för de fattade besluten bör dock ligga hos affärsenheterna och de interna enheterna, och ytterst hos ledningsorganet.

20.2 Riskhanteringsfunktionens roll i fråga om väsentliga förändringar

189. I linje med avsnitt 18 bör riskhanteringsfunktionen, innan beslut om väsentliga förändringar eller exceptionella transaktioner fattas, delta i bedömningen av ändringarnas och transaktionernas inverkan på institutets och koncernens övergripande riskexponering och rapportera sina resultat direkt till ledningsorganet innan ett beslut fattas.

190. Riskhanteringsfunktionen bör bedöma hur identifierade risker kan påverka institutets eller koncernens förmåga att hantera sin riskprofil och sin likviditet och att upprätthålla en sund kapitalbas under normala och ogynnsamma omständigheter.

20.3 Riskhanteringsfunktionens roll i att identifiera, mäta, bedöma, hantera, reducera, övervaka och rapportera om risker

191. Riskhanteringsfunktionen bör se till att alla risker identifieras, bedöms, mäts, övervakas och hanteras samt att relevanta enheter inom institutet rapporterar om riskerna.

192. Riskhanteringsfunktionen bör se till att identifiering och bedömning inte enbart utgår från kvantitativ information eller modellresultat, utan även tar kvalitativa metoder i beaktande. Riskhanteringsfunktionen bör informera ledningsorganet om de antaganden som används i riskmodellerna och analyserna samt om potentiella brister i dessa modeller och analyser.

193. Riskhanteringsfunktionen bör se till att transaktioner med närstående parter granskas och att de risker de medför för institutet identifieras och bedöms i tillräcklig omfattning.

194. Riskhanteringsfunktionen bör se till att alla identifierade risker övervakas effektivt av affärsenheterna.

195. Riskhanteringsfunktionen bör regelbundet övervaka institutets faktiska riskprofil och granska den i förhållande till dess strategiska mål och riskaptit så att ledningsorganet kan fatta beslut i sin ledningsfunktion respektive göra kritiska granskningar i sin tillsynsfunktion.

196. Riskhanteringsfunktionen bör analysera trender och urskilja nya, framväxande eller ökande risker som följer av förändrade omständigheter och villkor. Den bör även regelbundet granska de faktiska riskerna i förhållande till tidigare uppskattningar (dvs. göra utfallstest) för att bedöma och förbättra riskhanteringens tillförlitlighet och ändamålsenlighet.

197. Riskhanteringsfunktionen bör utvärdera olika sätt att reducera riskerna. Dess rapporter till ledningsorganet bör innefatta förslag till lämpliga riskreducerande åtgärder.

20.4 Riskhanteringsfunktionens roll i fråga om icke godkända exponeringar

198. Riskhanteringsfunktionen bör göra självständiga bedömningar av överskridanden av riskaptit eller riskgränser (inbegripet fastställande av orsaken och genomförande av en rättslig och ekonomisk analys av de faktiska kostnaderna för att eliminera, reducera eller säkra exponeringen i förhållande till de potentiella kostnaderna för att behålla den). Riskhanteringsfunktionen bör informera berörda affärsenheter och ledningsorganet samt rekommendera möjliga lösningar. Riskhanteringsfunktionen bör rapportera direkt till ledningsorganet i dess tillsynsfunktion när överskridandet är betydande, utan att detta påverkar riskhanteringsfunktionens rapportering till andra interna funktioner och kommittéer.

199. Riskhanteringsfunktionen bör spela en viktig roll när det gäller att se till att beslut om dess rekommendationer fattas på lämplig nivå, följs av berörda affärsenheter samt rapporteras till ledningsorganet och i förekommande fall till riskkommittén.

20.5 Chefen för riskhanteringsfunktionen

200. Chefen för riskhanteringsfunktionen bör vara ansvarig för att tillhandahålla heltäckande och begriplig information om risker och ge ledningsorganet råd, så att ledningsorganet förstår institutets övergripande riskprofil. Chefen för riskhanteringsfunktionen i ett moderföretag har samma ansvar avseende den konsoliderade situationen.

201. Chefen för riskhanteringsfunktionen bör ha den sakkunskap, självständighet och ställning som krävs för att ifrågasätta beslut som påverkar institutets exponering för risker. Om chefen för riskhanteringsfunktionen inte är ledamot i ledningsorganet bör betydande institut utse en oberoende chef för riskhanteringsfunktionen som inte har några uppgifter inom andra funktioner och som rapporterar direkt till ledningsorganet. Om det med beaktande av den proportionalitetsprincip som fastställs i avdelning I inte är proportionerligt att utse en person

som endast har rollen som chef för riskhanteringsfunktionen kan denna roll kombineras med rollen som efterlevnadschef eller utövas av någon annan högre befattningshavare, förutsatt att det inte föreligger några intressekonflikter mellan de roller som kombineras. Under alla omständigheter bör personen i fråga ha tillräcklig auktoritet, tyngd och självständighet (såsom exempelvis chefen för juridikavdelningen).

202. Chefen för riskhanteringsfunktionen bör kunna ifrågasätta de beslut som fattas av institutets ledning och dess ledningsorgan, och skälen till invändningarna bör dokumenteras formellt. Om ett institut vill ge chefen för riskhanteringsfunktionen rätt att lägga in sitt veto mot beslut (t.ex. ett kredit- eller investeringsbeslut eller fastställandet av en riskgräns) som fattas på lägre nivåer än ledningsorganet, bör institutet ange omfattningen av vetorätten, förfarandena för rapportering eller överklagande samt hur ledningsorganet ska involveras.

203. Institutet bör inrätta stärkta processer för godkännande av de beslut som chefen för riskhanteringsfunktionen uttalat sig negativt om. Ledningsorganet i sin tillsynsfunktion bör kunna kommunicera direkt med chefen för riskhanteringsfunktionen om viktiga riskrelaterade problem, inbegripet områden där utvecklingen eventuellt inte är förenlig med institutets riskaptit och strategi.

21 Funktion för regelefterlevnad

204. Instituten bör inrätta en permanent och effektiv efterlevnadsfunktion för hantering av efterlevnadsrisker och utse en person som är ansvarig för denna funktion i hela institutet (efterlevnadsansvarig eller efterlevnadschef).

205. Om det med beaktande av den proportionalitetsprincip som fastställs i avdelning I inte är proportionerligt att utse en person som endast har rollen som efterlevnadschef kan denna roll kombineras med rollen som chef för riskhanteringsfunktionen eller utövas av någon annan högre befattningshavare (t.ex. chefen för juridikavdelningen), förutsatt att det inte föreligger några intressekonflikter mellan de roller som kombineras.

206. Efterlevnadsfunktionen, inbegripet efterlevnadschefen, bör vara oberoende av de affärsområden och interna enheter som den kontrollerar och ha tillräcklig auktoritet och tyngd samt tillräckliga resurser. Med beaktande av de proportionalitetskriterier som anges i avdelning I kan denna funktion stödjas av riskhanteringsfunktionen alternativt kombineras med denna eller med andra lämpliga funktioner såsom juridik- eller personalavdelningen.

207. Efterlevnadsfunktionens personal bör besitta tillräckliga kunskaper och färdigheter samt tillräcklig erfarenhet gällande efterlevnad och relevanta förfaranden, och de bör ha tillgång till regelbunden utbildning.

208. Ledningsorganet i sin tillsynsfunktion bör övervaka genomförandet av en väldokumenterad efterlevnadspolicy som bör kommuniceras till hela personalen. Instituten bör inrätta en process för regelbunden bedömning av förändringar av lagar och förordningar av betydelse för deras verksamhet.

209. Efterlevnadsfunktionen bör ge ledningsorganet råd om åtgärder som kan vidtas för att säkerställa efterlevnaden av tillämpliga lagar, regler, förordningar och standarder. Efterlevnadsfunktionen bör också bedöma hur ändringar i lagstiftningen eller regelverket kan komma att påverka institutets verksamhet och ramverk för efterlevnad.

210. Efterlevnadsfunktionen bör se till att efterlevnaden övervakas med hjälp av ett strukturerat och väldefinierat program för efterlevnadsövervakning och att efterlevnadspolicyn följs. Efterlevnadsfunktionen bör rapportera till ledningsorganet och på lämpligt sätt kommunicera med riskhanteringsfunktionen om institutets efterlevnadsrisker och hur de hanteras. Efterlevnadsfunktionen och riskhanteringsfunktionen bör samarbeta och utbyta information på ett sätt som är lämpligt för utförandet av deras respektive uppgifter. Efterlevnadsfunktionens slutsatser bör beaktas av ledningsorganet och riskhanteringsfunktionen i beslutsprocesserna.

211. I linje med avsnitt 18 i dessa riktlinjer bör efterlevnadsfunktionen även i nära samarbete med riskhanteringsfunktionen och juridikavdelningen kontrollera att nya produkter och nya förfaranden följer gällande lagstiftning och i tillämpliga fall alla kända kommande ändringar av lagar, förordningar och tillsynskrav.

212. Instituten bör vidta lämpliga åtgärder mot sådana interna eller externa beteenden som kan underlätta eller möjliggöra bedrägeri, penningtvätt och finansiering av terrorism eller annan ekonomisk brottslighet samt disciplinbrott (t.ex. överträdelser av interna förfaranden, överträdelser av gränser).

213. Instituten bör se till att deras dotterföretag och filialer vidtar åtgärder för att säkerställa att deras verksamhet följer lokala lagar och förordningar. Om lokala lagar och förordningar lägger hinder i vägen för tillämpningen av striktare förfaranden och efterlevnadssystem som koncernen har genomfört, och särskilt om de förhindrar att nödvändig information röjs eller utbyts mellan koncernens företag, bör dotterföretag och filialer informera det konsoliderande institutets efterlevnadsansvariga eller efterlevnadschef.

22 Internrevisionsfunktion

214. Varje institut bör inrätta en oberoende och effektiv internrevisionsfunktion med beaktande av de proportionalitetskriterier som anges i avdelning I och utse en person som ansvarar för denna funktion i hela institutet. Internrevisionsfunktionen bör vara oberoende och ha tillräcklig auktoritet och tyngd samt tillräckliga resurser. I synnerhet bör institutet se till att internrevisionsfunktionens personal är tillräckligt kvalificerad och att funktionen har tillräckliga resurser, särskilt när det gäller revisionsverktyg och metoder för riskanalys, för institutets storlek och de platser där det verkar samt för karaktären, omfattningen och komplexiteten hos de risker som institutets affärsmodell, verksamhet, riskkultur och riskaptit medför.

215. Internrevisionsfunktionen bör vara oberoende av de granskade verksamheterna. Därför får internrevisionsfunktionen inte kombineras med någon annan funktion.

216. Internrevisionsfunktionen bör, på grundval av en riskbaserad metod, utföra en oberoende granskning och ge en objektiv försäkran om att samtliga institutets verksamheter och enheter, inklusive den verksamhet som omfattas av utkontraktering, följer såväl institutets policyer och förfaranden som alla externa krav. Alla enheter inom koncernen bör omfattas av internrevisionsfunktionens arbete.

217. Internrevisionsfunktionen bör inte delta i utformningen, valet, inrättandet eller genomförandet av specifika policyer, mekanismer och förfaranden för internkontroll eller av riskgränser. Detta bör emellertid inte hindra ledningsorganet i sin ledningsfunktion från att begära utlåtanden från internrevisionen om ärenden som berör risk, internkontroll och efterlevnad av gällande regler.

218. Internrevisionsfunktionen bör bedöma huruvida institutets ramverk för internkontroll enligt avsnitt 15 är ändamålsenligt och effektivt. I synnerhet bör internrevisionsfunktionen bedöma

a. lämpligheten i institutets ramverk för styrning,

b. huruvida befintliga policyer och förfaranden är fortsatt lämpliga, följer lagar och förordningar och är förenliga med institutets riskstrategi och riskaptit,

c. efterlevnaden av förfarandena inom ramen för gällande lagar och förordningar samt ledningsorganets beslut,

d. huruvida förfarandena genomförs korrekt och effektivt (t.ex. efterlevnad i samband med transaktioner, faktisk risknivå osv.) samt

e. tillräckligheten, kvaliteten och ändamålsenligheten hos de kontroller och den rapportering som utförs av affärsenheterna med försvarsinriktning och av riskhanterings- och efterlevnadsfunktionerna.

219. Internrevisionsfunktionen bör särskilt granska de processer som säkerställer att institutets metoder och tekniker, dess antaganden och de informationskällor som används i dess interna modeller (t.ex. riskmodeller och redovisningsberäkningar) är tillförlitliga. Den bör även utvärdera kvaliteten och användningen av verktyg för identifiering och bedömning av kvalitativa risker samt de åtgärder som vidtagits för att reducera riskerna.

220. Internrevisionsfunktionen bör ha obegränsad tillgång till institutets register, dokument, information och byggnader. Detta bör innefatta tillgång till ledningsinformationssystem och protokoll från samtliga kommittéer och beslutsfattande organ.

221. Internrevisionsfunktionen bör följa nationella och internationella branschstandarder. Exempel på sådana branschstandarder är de standarder som utarbetats av institutet för internrevisorer (Institute of Internal Auditors).

222. Internrevisionen bör genomföras i enlighet med en revisionsplan och ett detaljerat revisionsprogram på grundval av en riskbaserad strategi.

223. En internrevisionsplan bör upprättas minst en gång om året med utgångspunkt i internrevisionens årliga kontrollmål. Internrevisionsplanen bör godkännas av ledningsorganet.

224. Alla rekommendationer från revisorerna bör bli föremål för formella uppföljningar på respektive ledningsnivå, för att säkerställa att de skyndsamt och effektivt beaktas och att resultaten rapporteras.

Avdelning VI – Kontinuitetshantering[40]

225. Varje institut bör inrätta en plan för god kontinuitetshantering och återhämtning för att säkerställa institutets förmåga att upprätthålla verksamheten och begränsa förlusterna vid en allvarlig störning i verksamheten.

226. Instituten kan inrätta en särskild, oberoende kontinuitetsfunktion, t.ex. som en del av riskhanteringsfunktionen[41].

227. Institutets verksamhet är beroende av många olika viktiga resurser (t.ex. it-system inklusive molntjänster, kommunikationssystem, nyckelpersonal och byggnader). Syftet med kontinuitetshanteringen är att mildra de operativa, finansiella, rättsliga, anseendemässiga och andra väsentliga konsekvenserna av ett haveri eller långvarigt avbrott i tillgången till dessa resurser som stör institutets normala verksamhet. Andra riskhanteringsåtgärder kan syfta till att minska sannolikheten för sådana händelser eller överföra de ekonomiska konsekvenserna till tredje parter (till exempel genom försäkringar).

228. För att ha en god kontinuitetshanteringsplan bör institutet noggrant analysera riskfaktorer och sin exponering för allvarliga verksamhetsstörningar och göra (kvantitativa och kvalitativa) bedömningar av deras potentiella inverkan med hjälp av interna och/eller externa uppgifter och scenarioanalyser. Denna analys bör omfatta alla affärsområden och interna enheter, inbegripet riskhanteringsfunktionen, och ta hänsyn till deras beroende av varandra. Resultaten av analysen bör ligga till grund för fastställandet av institutets prioriteringar och mål under återhämtningsskedet.

229. På grundval av ovannämnda analys bör institutet utarbeta

a. beredskaps- och kontinuitetsplaner som säkerställer att institutet reagerar på nödsituationer på lämpligt sätt och kan upprätthålla sin viktigaste verksamhet om de vanliga rutinerna störs, och

[40] Instituten bör även beakta EBA:s riktlinjer om IKT-risker, som finns tillgängliga på https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[41] Se även artikel 312 i förordning (EU) nr 575/2013.

b. återhämtningsplaner för viktiga resurser, så att institutet kan återgå till sina vanliga rutiner inom rimlig tid. Eventuella återstående risker till följd av verksamhetsstörningar bör vara förenliga med institutets riskaptit.

230. Beredskaps-, kontinuitets- och återhämtningsplaner bör vara dokumenterade och genomföras omsorgsfullt. Dokumentationen bör finnas tillgänglig hos affärsområdena, de interna enheterna och riskhanteringsfunktionen och lagras i system som är fysiskt åtskilda och lätt tillgängliga i en nödsituation. Lämplig utbildning bör tillhandahållas. Planerna bör provas och uppdateras regelbundet. Eventuella problem eller misslyckanden under testerna bör dokumenteras och analyseras och ligga till grund för en översyn av planerna.

Avdelning VII – Insyn

231. Strategier, policyer och förfaranden bör kommuniceras till all berörd personal vid institutet. Institutets personal bör förstå och följa policyer och förfaranden som har med deras uppgifter och ansvarsområden att göra.

232. Följaktligen bör ledningsorganet informera den berörda personalen och hålla den uppdaterad om institutets strategier och policyer på ett tydligt och konsekvent sätt, åtminstone i den utsträckning som krävs för att den ska kunna utföra sina uppgifter. Detta kan göras med hjälp av skriftliga riktlinjer, manualer eller andra metoder.

233. I fall där behöriga myndigheter, i enlighet med artikel 106.2 i direktiv 2013/36/EU, kräver att moderföretag årligen offentliggör en beskrivning av sin rättsliga struktur samt lednings- och organisationsstrukturen för gruppen av institut, ska informationen omfatta alla enheter i koncernstrukturen, såsom anges i direktiv 2013/34/EU[42], uppdelad efter land.

234. I denna beskrivning bör åtminstone följande ingå:

a. En översikt över institutens interna organisation och koncernstrukturen enligt direktiv 2013/34/EU och ändringar av dessa, inbegripet huvudsakliga rapporteringsvägar och ansvarsområden.

b. Alla väsentliga förändringar som gjorts sedan offentliggörandet av föregående beskrivning samt datum för dessa.

c. Nya rättsliga strukturer, styrningsstrukturer eller organisationsstrukturer.

d. Uppgifter om ledningsorganets struktur, organisation och ledamöter, inbegripet antalet ledamöter och antalet av dessa som är oberoende samt uppgifter om kön och mandatperiodens längd för varje ledamot i ledningsorganet.

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

e. Ledningsorganets viktigaste ansvarsområden.

f. En förteckning över kommittéerna i ledningsorganet i dess tillsynsfunktion och deras sammansättning.

g. En översikt över den policy om intressekonflikter som gäller för instituten och för ledningsorganet.

h. En översikt över ramverket för internkontroll.

i. En översikt över ramverket för kontinuitetshantering.

Bilaga I – Aspekter som måste beaktas när en policy för intern styrning formuleras

I enlighet med avdelning III bör instituten beakta följande aspekter när policyer och metoder för intern styrning dokumenteras:

1. Aktieägarstruktur
2. Koncernstruktur, i tillämpliga fall (rättslig och funktionell struktur)
3. Ledningsorganets sammansättning och arbetssätt
   a) Valkriterier, bland annat hur mångfald beaktas
   b) Antal, mandatperiod, omsättning, ålder
   c) Oberoende ledamöter i ledningsorganet
   d) Verkställande ledamöter i ledningsorganet
   e) Icke verkställande ledamöter i ledningsorganet
   f) Intern uppdelning av arbetsuppgifter, i tillämpliga fall
4. Styrstruktur och organisationsschema (samt påverkan på gruppen i tillämpliga fall)
   a) Specialiserade kommittéer
      i. Sammansättning
      ii. Arbetssätt
   b) Verkställande kommitté, i förekommande fall
      i. Sammansättning
      ii. Arbetssätt
5. Personer som innehar nyckelfunktioner
   a) Chef för riskhanteringsfunktionen
   b) Chef för efterlevnadsfunktionen
   c) Chef för internrevisionsfunktionen
   d) Finansdirektör
   e) Andra personer som innehar nyckelfunktioner
6. Ramverket för internkontroll
   a) Beskrivning av varje funktion, inbegripet organisation, resurser, tyngd och auktoritet
7. Beskrivning av riskstrategin och ramverket för riskhantering
8. Organisationsstruktur (samt påverkan på koncernen i tillämpliga fall)

a) Operativ struktur, affärsområden och fördelning av behörigheter och ansvarsområden

b) Utkontraktering

c) Utbud av produkter och tjänster

d) Verksamhetens geografiska omfattning

e) Tillhandahållande av tjänster i enlighet med systemet för friheten att tillhandahålla tjänster

f) Filialer

g) Dotterföretag, samriskföretag osv.

h) Användning av offshore-centrum

9. Uppförandekod (samt påverkan på koncernen i tillämpliga fall)

a) Strategiska mål och företagets värderingar

b) Interna koder och regler, policy för förebyggande åtgärder

c) Policy om intressekonflikter

d) Visselblåsning

10. Status för policyn för intern styrning, med datum

a) Utarbetande

b) Senaste ändring

c) Senaste utvärdering

d) Godkännande från ledningsorganet.