Den Europæiske Banktilsynsmyndighed EBA BS 2011 116 endelig

27. september 2011

EBA-retningslinjer vedrørende intern ledelse (GL 44)

London, den 27. september 2011

EBA-retningslinjer vedrørende intern ledelse

Retningslinjernes retlige status

1. Dette dokument indeholder retningslinjer udstedt i henhold til artikel 16 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EBA-forordningen). I overensstemmelse med EBA-forordningens artikel 16, stk. 3, skal de kompetente myndigheder og finansielle markedsdeltagere bestræbe sig på at efterleve disse retningslinjer bedst muligt.
2. Retningslinjerne fastsætter, hvad der i henhold til EBA er hensigtsmæssig tilsynspraksis inden for det europæiske finansielle tilsynssystem, eller hvordan EU-lovgivningen bør anvendes inden for et bestemt område. EBA forventer derfor, at alle kompetente myndigheder og deltagere på de finansielle markeder, som retningslinjerne finder anvendelse på, overholder dem, medmindre andet er anført. Kompetente myndigheder, som er underlagt retningslinjerne, bør overholde disse ved at implementere dem i deres tilsynspraksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsregler og/eller vejlednings- eller tilsynsprocesser), herunder hvor særlige retningslinjer i dokumentet primært er rettet mod institutter.

Indberetningskrav

3. De kompetente myndigheder bør senest den 28. november 2011 meddele EBA, hvorvidt de overholder eller agter at overholde disse retningslinjer, eller angive begrundelser for manglende overholdelse. Meddelelserne indsendes til compliance@eba.europa.eu af personer med behørig beføjelse til at indberette overholdelse på vegne af de kompetente myndigheder.
4. De kompetente myndigheders meddelelse, jf. afsnittet ovenfor, offentliggøres på EBA's websted i henhold til EBA-forordningens artikel 16.

De indrammede tekstbokse i retningslinjerne nedenfor indeholder yderligere forklaringer på specifikke aspekter af retningslinjerne, enten ved eksempler eller gennem information om baggrunden for en bestemmelse.

Indholdsfortegnelse

Afsnit I – Formål, anvendelsesområde og definitioner

1. Formål

Retningslinjerne har til formål at harmonisere forventningerne på tilsynsområdet og at forbedre sund implementering af ordninger for intern ledelse i overensstemmelse med artikel 22 og bilag V i direktiv 2006/48/EF og national selskabslovgivning.

2. Anvendelsesområde og -niveau

1. De kompetente myndigheder bør kræve, at institutterne overholder bestemmelserne i disse retningslinjer for intern ledelse.
2. Anvendelsen af disse retningslinjer bør revideres af de kompetente myndigheder som led i deres tilsyns- og evalueringsproces.

Forklarende note CEBS/EBA har udarbejdet "Guidelines on the Supervisory Review Process", som findes på EBA's websted.

3. Retningslinjerne finder anvendelse på institutter på individuelt selskabsniveau og på moderselskaber og datterselskaber på et konsolideret eller delvist konsolideret basis, medmindre andet er anført.
4. Proportionalitetsprincippet i medfør af direktiv 2006/48 og 2006/49 (som ændret) finder anvendelse på alle bestemmelser i retningslinjerne. Et institut kan påvise, hvordan dets metode, der afspejler arten, omfanget og kompleksiteten af dets aktiviteter, lever op til det resultat, der kræves i retningslinjerne.

3. Definitioner

1. I disse retningslinjer forstås ved *ledelsesorgan*: et styrende organ (eller organer) i et institut, som har tilsyns- og ledelsesfunktioner, har de øverste beslutningsbeføjelser og er bemyndiget til at fastlægge instituttets strategi, målsætninger og generelle ledelsesprincipper. Der bør i ledelsesorganet indgå personer, som varetager den daglige ledelse af et institut.
2. I disse retningslinjer forstås ved *institutter*: kreditinstitutter og investeringsselskaber i medfør af direktiv 2006/48/EF og 2006/49/EF.

Afsnit II - Krav vedrørende institutters interne ledelse

A. Virksomhedsstruktur og -organisation

4. Organisatorisk struktur

1. Ledelsesorganet i et institut bør sikre en passende og gennemsigtig virksomhedsstruktur for dette institut. Strukturen bør fremme og afspejle et instituts effektive og forsigtige forvaltning både på individuelt og på koncernniveau. Rapporteringslinjerne og fordelingen af ansvar og myndighed i et institut bør være klare, veldefinerede, sammenhængende og håndhævede.
2. Ledelsesorganet bør sikre, at et instituts struktur, og i givet fald strukturerne i en koncern, er klare og gennemsigtige, både for instituttets egne medarbejdere og for dets tilsynsførende.
3. Ledelsesorganet bør vurdere, hvordan de forskellige elementer af virksomhedsstrukturen supplerer hinanden og fungerer i samspil med hinanden. Strukturen må ikke hindre ledelsesorganets mulighed for at overvåge og styre de risici effektivt, som instituttet eller koncernen står over for.
4. Ledelsesorganet bør vurdere, hvordan ændringer i koncernstrukturen påvirker dets soliditet. Ledelsesorganet bør gennemføre alle nødvendige justeringer hurtigt.

Forklarende note
Ændringer kan f.eks. være et resultat af oprettelsen af nye datterselskaber, fusioner og overtagelser, frasalg eller opløsning af dele af koncernen, eller eksterne udviklinger.

5. Kontrolforanstaltninger i en koncernstruktur

1. I en koncernstruktur bør ledelsesorganet i et instituts moderselskab have det samlede ansvar for en tilstrækkelig intern styring på tværs af koncernen og for at sikre, at der er en ledelsesramme, der svarer til strukturen, aktiviteterne og risiciene i koncernen og i de enheder, den er sammensat af.
2. Ledelsesorganet i et reguleret datterselskab af en koncern bør med hensyn til den juridiske enhed følge samme værdier og politikker for intern ledelse som dets moderselskab, medmindre juridiske eller tilsynsmæssige krav eller proportionalitetsovervejelser tilsiger noget andet. Tilsvarende bør ledelsesorganet i et reguleret datterselskab inden for dets eget interne ledelsesansvar fastlægge sine politikker, og bør vurdere alle beslutninger eller praksis på koncernniveau for at sikre, at de ikke giver anledning til, at det regulerede datterselskab derved overtræder gældende love eller administrative bestemmelser eller tilsynsregler. Ligeledes bør ledelsesorganet i et reguleret datterselskab sikre, at sådanne beslutninger og praksis ikke er til skade for:

    a. datterselskabets forsvarlige og forsigtige forvaltning

    b. datterselskabets finansielle sundhed

    c. datterselskabets interessenters legitime interesser.

3. Ledelsesorganerne i både moderselskabet og dets datterselskaber bør anvende og tage hensyn til punkterne nedenfor under hensyntagen til virkningerne af koncerndimensionen på deres interne ledelse.
4. Under udøvelsen af sit interne ledelsesansvar bør ledelsesorganet i et instituts moderselskab være bevidst om alle de væsentlige risici og forhold, der vil kunne påvirke koncernen, moderselskabet selv og dets datterselskaber. Det bør derfor udøve tilstrækkeligt tilsyn med sine datterselskaber, samtidig med at det respekterer det uafhængige juridiske og ledelsesmæssige ansvar, der påhviler regulerede datterselskabers ledelsesorganer.
5. For at opfylde sit interne ledelsesansvar bør ledelsesorganet i et instituts moderselskab:

    a. etablere en ledelsesstruktur, der bidrager til et effektivt tilsyn med dets datterselskaber og tager hensyn til arten, omfanget og kompleksiteten af de forskellige risici, som koncernen og dens datterselskaber er eksponeret for

    b. vedtage en intern ledelsespolitik på koncernniveau for dets datterselskaber, som omfatter forpligtelsen til at opfylde alle gældende ledelseskrav

    c. sikre, at der forefindes tilstrækkelige ressourcer for hvert datterselskab til at overholde både koncernstandarder og lokale ledelsesstandarder

    d. have tilstrækkelige midler til at overvåge, at hvert enkelt datterselskab overholder alle gældende krav til intern ledelse

    e. sikre, at rapporteringslinjerne i en koncern er klare og gennemsigtige, især hvor forretningsområderne ikke matcher koncernens juridiske struktur.

6. Et reguleret datterselskab bør overveje, som et element af stærk ledelse, også at have et tilstrækkeligt antal uafhængige medlemmer i ledelsesorganet. Uafhængige medlemmer af ledelsesorganet er menige bestyrelsesmedlemmer, der er uafhængige af datterselskabet og dets koncern, og af den kontrollerende aktionær.

6. Kendskab til strukturen ("Know-your-structure")

1. Ledelsesorganet bør fuldt ud kende og forstå et instituts operationelle struktur ("know-your-structure") og sikre, at denne stemmer overens med instituttets godkendte forretningsstrategi og risikoprofil.

Forklarende note
Det er afgørende, at ledelsesorganet fuldt ud kender og forstår et instituts operationelle struktur. Hvis et institut opretter mange juridiske enheder i sin koncern, kan deres antal, og især de indbyrdes forbindelser og transaktioner mellem dem, give anledning til problemer for udformningen af dets interne

ledelse og for styringen af og tilsynet med koncernens risici som helhed, hvilket i sig selv udgør en risiko.

2. Ledelsesorganet bør lede og forstå instituttets struktur, dets udvikling og begrænsninger og bør sikre, at strukturen er begrundet og ikke medfører unødig eller uhensigtsmæssig kompleksitet. Det er også ansvarligt for vedtagelsen af forsvarlige strategier og politikker for etablering af nye strukturer. Tilsvarende bør ledelsesorganet være bevidst om de risici, som kompleksiteten af den juridiske enheds struktur i sig selv udgør, og bør sikre at instituttet er i stand til at udarbejde rettidig information om type, vedtægter, ejerstruktur og aktivitetsområder for den enkelte juridiske enhed.
3. Ledelsesorganet i et instituts moderselskab bør ikke alene forstå koncernens selskabsform, men også formålet med dens forskellige enheder og sammenhængen og forbindelserne mellem dem. Hertil hører en forståelse af koncernspecifikke operationelle risici, engagementer inden for koncernen, og af, hvordan koncernens finansiering, kapital og risikoprofiler vil kunne påvirkes under normale og under negative omstændigheder.
4. Ledelsesorganet i et instituts moderselskab bør sikre, at de forskellige enheder i koncernen (herunder instituttet selv) modtager tilstrækkelig information, så de hver for sig kan få en klar opfattelse af koncernens generelle mål og risici. Enhver strøm af vigtig information mellem enheder, der er relevant for koncernens operationelle funktion, bør i det nødvendige omfang dokumenteres og straks på forlangende stilles til rådighed for ledelsesorganet, kontrolfunktionerne og tilsynsmyndighederne.
5. Ledelsesorganet i et instituts moderselskab bør sikre, at det holder sig selv informeret om de risici, som koncernens struktur giver anledning til. Hertil hører:

    a. information om væsentlige risikofaktorer, og

    b. regelmæssige rapporter, der vurderer instituttets generelle struktur og vurderer aktiviteterne i de individuelle enheder og deres overholdelse af den godkendte strategi.

7. Ikkestandardiserede eller uigennemsigtige aktiviteter

1. Anvender et institut strukturer til særlige formål eller beslægtede strukturer eller i jurisdiktioner, der hindrer gennemsigtighed, eller som ikke lever op til internationale bankstandarder, bør ledelsesorganet fuldt ud forstå deres formål og struktur samt de særlige risici, der er forbundet med disse. Ledelsesorganet bør kun acceptere disse aktiviteter, når det er betrygget i, at risiciene vil blive håndteret korrekt.

Forklarende note

Ud over disse principper kan de kompetente myndigheder ligeledes anvende Baselkomitéens hovedprincipper om effektivt banktilsyn, "*Core Principles for Effective Banking Supervision"*, når de vurderer forretningsaktiviteter i jurisdiktioner, der ikke er helt gennemsigtige, eller som ikke opfylder internationale bankstandarder.

Instituttet kan have legitime årsager til at operere i visse jurisdiktioner (eller med enheder eller modparter, der opererer inden for disse jurisdiktioner) eller etablere særlige strukturer (f.eks. selskaber oprettet til særlige formål (special purpose vehicles) eller fonde i selskabsform). Der kan imidlertid være specifikke juridiske, omdømmemæssige og finansielle risici forbundet med at operere i jurisdiktioner, der ikke er fuldt gennemsigtige, eller som ikke lever op til internationale bankstandarder (f.eks. med hensyn til tilsyn, skat, bekæmpelse af pengehvidvaskning eller finansiering af terrorisme) eller gennem komplekse eller uigennemskuelige strukturer. De kan også hindre ledelsesorganets mulighed for at gennemføre tilstrækkeligt tilsyn med virksomheden og forhindre et effektivt banktilsyn. De bør derfor kun godkendes og bibeholdes, når deres formål er blevet defineret og forstået, når der er sikret et effektivt tilsyn, og når alle de væsentlige risici, som disse strukturer kunne give anledning til, er blevet håndteret i tilstrækkeligt omfang.

Som konsekvens heraf bør ledelsesorganet være særligt opmærksom på alle disse situationer, idet de giver anledning til betydelige udfordringer for forståelsen af koncernens struktur.

2. Ledelsesorganet bør løbende fastlægge, opretholde og revidere passende strategier, politikker og procedurer for godkendelsen og opretholdelsen af sådanne strukturer og aktiviteter for at sikre, at de fortsat er i overensstemmelse med deres tilsigtede formål.
3. Ledelsesorganet bør sikre, at der træffes passende foranstaltninger for at undgå eller reducere risiciene ved sådanne aktiviteter. Hertil hører, at:

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

    b. information om disse aktiviteter og risiciene i forbindelse hermed er tilgængelig for instituttets hovedkontor og revisorer, og rapporteres til ledelsesorganet og tilsynsmyndighederne

c. instituttet med jævne mellemrum vurderer det fortsatte behov for at gennemføre aktiviteter, der hindrer gennemsigtighed.

4. De samme forholdsregler bør tages, når et institut udfører kundeaktiviteter, der ikke er standard eller ikke er gennemsigtige.

Forklarende note
Kundeaktiviteter, der ikke er standard eller ikke er gennemsigtige (f.eks. hjælp til kunder med at oprette enheder i offshorecentre, udvikling af komplekse strukturer og finansielle transaktioner for dem eller tilbud om formueforvaltning) stiller den interne ledelse over for lignende udfordringer og kan give anledning til betydelige operationelle og omdømmemæssige risici. Derfor bør der træffes de samme foranstaltninger for risikostyring som for institutternes egne forretningsaktiviteter.

5. Alle disse strukturer og aktiviteter bør med jævne mellemrum underkastes interne og eksterne revisionsgennemsyn.

B. Ledelsesorgan

B.1 Ledelsesorganets pligter og opgaver

8. Ledelsesorganets opgaver

1. Ledelsesorganet bør have det samlede ansvar for instituttet og bør fastlægge instituttets strategi. Ledelsesorganets opgaver bør være klart defineret i et skriftligt dokument og være godkendt.

Forklarende note
Korrekt varetagelse af ledelsesorganets opgaver er grundlaget for forsvarlig og forsigtig styring af instituttet. De dokumenterede opgaver bør ligeledes være i overensstemmelse med national selskabsret.

2. Ledelsesorganets hovedopgaver bør omfatte fastlæggelse af og tilsyn med:

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

   b. instituttets generelle risikostrategi og -politik, herunder dets risikotolerance/-villighed og rammerne for dets risikostyring

   c. størrelse, type og fordeling af både intern kapital og basiskapital, der er tilstrækkelig til at afdække instituttets risici

d. en robust og gennemsigtig organisationsstruktur med effektive kommunikations- og rapporteringskanaler

e. en politik for udnævnelse og efterfølgelse af personer med nøglefunktioner i instituttet

f. en aflønningsramme, der afspejler instituttets risikostrategier

g. instituttets principper for god forvaltning og virksomhedsværdier, herunder gennem en adfærdskodeks eller tilsvarende dokument

h. en tilstrækkelig og effektiv intern kontrolramme, der omfatter velfungerende risikokontrol-, compliance- og interne revisioner samt en passende ramme for regnskabsaflæggelse og decharge.

3. Ledelsesorganet bør ligeledes løbende revidere og justere disse politikker og strategier. Ledelsesorganet er ansvarligt for en passende kommunikation med tilsynsmyndigheder og andre interesserede parter.

9. Vurdering af rammen for intern ledelse

1. Ledelsesorganet bør vurdere effektiviteten af instituttets ramme for intern ledelse.

2. Der bør mindst én gang årligt gennemføres en revision af rammen for intern ledelse og gennemførelsen heraf. Den bør fokusere på eventuelle ændringer i de interne og eksterne faktorer, der påvirker instituttet.

10. Ledelsesorganets ledelses- og tilsynsfunktion

1. Et instituts ledelsesorgan varetager ledelses- og tilsynsfunktioner, som bør fungere effektivt i samspil med hinanden.

Forklarende note
Medlemsstaterne anvender normalt én eller to **ledelsesstrukturer** – en enstrenget eller tostrenget ledelsesstruktur. I begge strukturer spiller ledelsesorganet i kraft af hhv. sin ledelsesfunktion og tilsynsfunktion separate roller i instituttets ledelse, direkte eller gennem udvalg.

Ledelsesfunktionen foreslår retningen for instituttet, sikrer en effektiv gennemførelse af strategien og er ansvarlig for instituttets daglige drift.

Tilsynsfunktionen fører tilsyn med ledelsesfunktionen og vejleder denne. Dens tilsynsførende rolle består i at give konstruktivt modspil ved udviklingen af strategien for et institut, overvåge ledelsesfunktionens resultater og udmøntningen af aftalte kort- og langsigtede mål samt sikre de finansielle

oplysningers rigtighed og effektiv risikostyring og interne kontrolforanstaltninger.

For at opnå god ledelse bør et instituts ledelses- og tilsynsfunktioner fungere effektivt i samspil med hinanden for at gennemføre instituttets aftalte strategi, og navnlig for at håndtere de risici, som instituttet står over for. Der kan være betydelige forskelle mellem forskellige landes love og bestemmelser, men disse forskelle bør ikke udelukke et effektivt samspil mellem disse to funktioner, uanset om ledelsesorganet omfatter en eller flere instanser.

2. Ledelsesorganet bør:

   a. i kraft af sin tilsynsfunktion være parat og i stand til at udfordre og på en konstruktiv og kritisk måde gennemgå forslag, redegørelser og oplysninger, som stilles til rådighed af medlemmer af ledelsesorganets ledelsesfunktion

   b. i kraft af sin tilsynsfunktion overvåge, at instituttets strategi, risikotolerance/-villighed og politikker gennemføres konsekvent, og at standarderne for instituttets resultater opretholdes i overensstemmelse med dets langfristede finansielle interesser og solvens

   c. i kraft af sin ledelsesfunktion overvåge, at medlemmerne af ledelsesorganet lever op til disse standarder.

3. Ledelsesorganet bør i kraft af sin ledelsesfunktion koordinere instituttets forretnings- og tilsynsstrategi med ledelsesorganets tilsynsfunktion og bør løbende diskutere gennemførelsen af disse strategier med ledelsesorganets tilsynsfunktion.
4. Hver enkelt funktion bør give den anden funktion tilstrækkelige oplysninger. Ledelsesorganet bør i kraft af sin ledelsesfunktion løbende og uden ugrundet ophold give ledelsesorganets tilsynsfunktion fyldestgørende information om de elementer, der er relevante for vurderingen af en situation, instituttets styring og opretholdelsen af dets finansielle sikkerhed.

B.2 Ledelsesorganets sammensætning og funktion

11. Ledelsesorganets sammensætning, udnævnelse og efterfølgelse af dets medlemmer

1. Ledelsesorganet bør have et tilstrækkeligt antal medlemmer og en passende sammensætning. Ledelsesorganet bør have politikker for udvælgelse, overvågning og overvejelse af mulige emner til at efterfølge medlemmer.
2. Et institut bør fastlægge sit ledelsesorgans størrelse og sammensætning under hensyntagen til instituttets størrelse og kompleksitetsgrad samt arten og omfanget af sine aktiviteter. Udvælgelsen af medlemmer af ledelsesorganet bør sikre tilstrækkelig samlet ekspertise.

3. Ledelsesorganet bør identificere og udvælge kvalificerede og erfarne kandidater og sikre en tilstrækkelig planlægning af efterfølgelse under behørig hensyntagen til eventuelle andre retskrav vedrørende sammensætning, udnævnelse eller efterfølgelse.
4. Ledelsesorganet bør sikre, at et institut har politikker for udvælgelsen af nye medlemmer og genudnævnelse af eksisterende medlemmer. Disse politikker bør omfatte udformningen af en beskrivelse af de nødvendige kompetencer og færdigheder til at sikre tilstrækkelig ekspertise.
5. Medlemmer af ledelsesorganet bør udpeges for et passende tidsrum. Indstillinger med henblik på genansættelse bør være baseret på ovennævnte profil og bør kun finde sted efter nøje overvejelse af det pågældende medlems resultater i forrige mandatperiode.
6. Ledelsesorganet bør i forbindelse med fastlæggelsen af en plan for efterfølgelse af medlemmer tage hensyn til hvert enkelt medlems kontrakt eller mandat for, hvor det er muligt, at forhindre, at for mange medlemmer skal udskiftes samtidigt.

12. Engagement, uafhængighed og styring af interessekonflikter

1. Medlemmer af ledelsesorganet bør engagere sig aktivt i et instituts drift og bør kunne træffe deres egne velovervejede, objektive og uafhængige beslutninger og udøve dømmekraft.
2. Udvælgelsen af medlemmer af ledelsesorganet bør sikre, at der forefindes tilstrækkelig ekspertise og uafhængighed i ledelsesorganet. Et institut bør sikre, at medlemmer af ledelsesorganet er i stand til at afsætte den fornødne tid til deres hverv og yde den fornødne indsats effektivt.
3. Medlemmer af ledelsesorganet bør kun have et begrænset antal mandater eller andre tidskrævende erhvervsmæssige aktiviteter. Desuden bør medlemmerne underrette instituttet om deres sekundære erhvervsmæssige aktiviteter (f.eks. mandater i andre selskaber). Da formanden har flere ansvarsområder og forpligtelser, forventes denne at afsætte mere tid hertil.
4. Det bør i et skriftligt dokument nedfældes, hvor meget tid alle medlemmerne af ledelsesorganet som et minimum bør afsætte. Ved overvejelsen af udnævnelsen af et nyt medlem, eller når et eksisterende medlem giver meddelelse om et fornyet mandat, bør medlemmerne af ledelsesorganet spørge ind til, hvordan den pågældende påtænker at afsætte tilstrækkelig tid til at varetage sine opgaver i instituttet. Medlemmernes deltagelse i ledelsesorganets tilsynsfunktion bør offentliggøres. Et institut bør ligeledes i kraft af sin ledelsesfunktion offentliggøre langtidsfravær af medlemmer af ledelsesorganet.
5. Medlemmerne af ledelsesorganet bør være i stand til at handle objektivt, kritisk og uafhængigt. Forholdsregler, der skal fremme evnen til at udøve objektiv og uafhængig dømmekraft, bør bl.a. omfatte, at medlemmerne rekrutteres fra en

tilstrækkeligt bred kreds af kandidater, og at der et tilstrækkeligt antal menige medlemmer.

Forklarende note
Hvor ledelsesorganet i kraft af sin tilsynsfunktion er formelt adskilt fra ledelsesorganets ledelsesfunktion bør ledelsesorganets objektivitet og uafhængighed i sin tilsynsfunktion fortsat sikres ved en passende udvælgelse af uafhængige medlemmer.

6. Ledelsesorganet bør have en skriftlig politik for håndtering af interessekonflikter for dets medlemmer. Politikken bør angive:

   a. et medlems pligt til at undgå interessekonflikter, som ledelsesorganet ikke har fået underretning om eller har godkendt, men på anden måde sikre, at interessekonflikter behandles hensigtsmæssigt

   b. en revisions- eller godkendelsesproces, som medlemmerne skal følge, før de deltager i visse aktiviteter (som f.eks. medlemskab af et andet ledelsesorgan) for at sikre, at en sådan deltagelse ikke giver anledning til en interessekonflikt

   c. et medlems pligt til at underrette instituttet om et hvilket som helst forhold, der kan give, eller har givet, anledning til en interessekonflikt

   d. et medlems ansvar for at afholde sig fra at deltage i beslutningsprocessen eller en afstemning om noget forhold, hvor medlemmet kan have en interessekonflikt, eller hvor medlemmets objektivitet eller evne til at varetage sine opgaver over for instituttet fuldt ud på anden måde kan blive kompromitteret

   e. passende procedurer for transaktioner med relevante parter, der gennemføres efter armslængdeprincippet

   f. hvordan ledelsesorganet ville forholde sig i tilfælde af manglende overholdelse af politikken.

13. Ledelsesorganets kvalifikationer

1. Medlemmerne af ledelsesorganet bør have de fornødne kvalifikationer, der bør vedligeholdes, bl.a. gennem uddannelse, for at bestride deres poster. De bør have en klar forståelse af instituttets ledelsesprocedurer og af deres rolle heri.
2. Medlemmerne af ledelsesorganet bør, både individuelt og kollektivt, være i besiddelse af den nødvendige ekspertise, erfaring, kompetencer, forståelse og personlige kvaliteter, herunder professionalisme og personlig integritet, til at varetage deres opgaver på forsvarlig måde.
3. Medlemmerne af ledelsesorganet bør have en ajourført forståelse af instituttets forretningsområder på et niveau, der svarer til deres ansvarsområder. Hertil

hører en relevant forståelse af de områder, som de ikke er direkte ansvarlige for, men som de kollektivt kan drages til ansvar for.

4. De bør kollektivt have fuld forståelse af karakteren af aktiviteterne og de dermed forbundne risici og have passende ekspertise og erfaring, der er relevant for hver af de væsentlige aktiviteter, som instituttet planlægger at gennemføre, med henblik på effektiv ledelse og effektivt tilsyn.
5. Et institut bør have en forsvarlig procedure, der sikrer, at medlemmerne af ledelsesorganet, individuelt og kollektivt, er i besiddelse af tilstrækkelige kvalifikationer.
6. Medlemmerne af ledelsesorganet bør erhverve, vedligeholde og udvide deres viden og færdigheder med henblik på at varetage deres funktioner. Institutterne bør sikre, at medlemmerne har adgang til individuelt skræddersyede uddannelsesprogrammer, som bør dække eventuelle huller i den vidensprofil, som instituttet har brug for, i forhold til medlemmernes faktiske viden. De områder, der kunne dækkes, omfatter bl.a. instituttets risikostyringsværktøjer og -modeller, nye udviklingstendenser, ændringer internt i organisationen, komplekse produkter, nye produkter eller markeder samt fusioner. Uddannelsen bør ligeledes omfatte forretningsområder, som de enkelte medlemmer ikke selv er direkte ansvarlige for. Ledelsesorganet bør afsætte tilstrækkelig tid, budget og andre ressourcer til uddannelse.

14. Ledelsesorganets organisatoriske funktion

1. Ledelsesorganet bør definere passende praksis og procedurer for intern ledelse for dets organisation og funktion og have indført de foranstaltninger, der sikrer, at denne praksis følges, og at den med jævne mellemrum revideres med henblik på forbedringer.

Forklarende note Betryggende praksis og procedurer for ledelsesorganets interne ledelse sender vigtige signaler internt og eksternt om instituttets ledelsespolitikker og -målsætninger. Praksis og procedurer omfatter hyppighed, arbejdsprocedurer og mødereferater, formandens rolle og brugen af udvalg.

2. Ledelsesorganet bør jævnligt mødes for at varetage sine opgaver på en korrekt og effektiv måde. Medlemmerne af ledelsesorganet bør afsætte tilstrækkelig tid til forberedelsen af mødet. Denne forberedelse inkluderer fastlæggelsen af en dagsorden. Mødereferatet bør fastlægge punkterne på dagsordenen og klart angive de beslutninger, der er blevet truffet, og de foranstaltninger, der er blevet vedtaget. Denne praksis og disse procedurer bør, sammen med ledelsesorganets rettigheder, opgaver og nøgleaktiviteter, dokumenteres og revideres med jævne mellemrum af ledelsesorganet.

Vurdering af ledelsesorganets funktion

3. Ledelsesorganet bør løbende vurdere den individuelle og kollektive effektivitet og gennemslagskraft af sine aktiviteter, ledelsespraksis og -procedurer, samt udvalgenes funktion. Der kan anvendes eksterne koordinatorer til at gennemføre vurderingen.

Ledelsesorganets formands rolle

4. Formanden bør sikre, at ledelsesorganets beslutninger træffes på et betryggende og velinformeret grundlag. Formanden bør tilskynde til og fremme en åben og kritisk diskussion og sikre, at afvigende synspunkter kan komme til orde og diskuteres i forbindelse med beslutningsprocessen.

Forklarende note
Formanden for ledelsesorganet spiller en afgørende rolle for, at ledelsesorganet kan fungere efter hensigten. Formanden står for ledelsen af ledelsesorganet og er ansvarlig for, at det generelt fungerer effektivt.

5. I en enstrenget ledelsesstruktur må ledelsesorganets formand og den administrative direktør ikke være den samme person. Hvis ledelsesorganets formand også er administrerende direktør for instituttet, bør instituttet have indført foranstaltninger, der minimerer den potentielle påvirkning af dets "checks and balances" (gensidig kontrol og tilsyn).

Forklarende note
"Checks and balances" kan f.eks. omfatte tilfælde, hvor ledelsesorganet i kraft af sin tilsynsfunktion eller en lignende post udpeger et ledende højtstående medlem i organet.

Specialiserede udvalg under ledelsesorganet

6. Ledelsesorganets tilsynsfunktion bør, under hensyntagen til et instituts størrelse og kompleksitet, nedsætte specialiserede udvalg bestående af medlemmer af ledelsesorganet (andre personer kan indbydes til at deltage, hvis deres specifikke ekspertise eller rådgivning er relevant for et givent emne). Specialiserede udvalg kan omfatte et revisionsudvalg, et vederlagsudvalg, et udvælgelses- eller personaleudvalg og/eller et ledelses-, etisk udvalg eller complianceudvalg.

Forklarende note
En uddelegering til sådanne udvalg friholder på ingen måde ledelsesorganets tilsynsfunktion fra kollektivt at leve op til sine pligter og sit ansvar, men kan

være med til på specifikke områder at støtte ledelsesorganet i forbindelse med udviklingen og gennemførelsen af god ledelsespraksis og beslutninger.

7. Et specialiseret udvalg bør have en optimal blanding af ekspertise, kompetencer og erfaring, som tilsammen sætter det i stand til fuldt ud at forstå, objektivt vurdere og tilføre nye idéer til de relevante emner. Det bør have et tilstrækkeligt antal uafhængige medlemmer. Hvert udvalg bør have et dokumenteret mandat (herunder dets ansvarsområde) fra ledelsesorganets tilsynsfunktion og etablerede arbejdsprocedurer. Medlemskab og formandskab af et udvalg kan roteres med jævne mellemrum.

Forklarende note

Rotation af medlemskab og formandskab er med til at undgå unødig koncentration af magt og med til at fremme nye initiativer.

8. De respektive udvalgs formænd bør rapportere regelmæssigt tilbage til ledelsesorganet. De specialiserede udvalg bør fungere i samspil med hinanden i det omfang, det er relevant, for at sikre konsekvens og undgå lakuner. Dette kunne ske gennem krydsdeltagelse: Formanden eller et medlem af et specialiseret udvalg kan ligeledes være medlem af et andet specialiseret udvalg.

Revisionsudvalg

9. Et revisionsudvalg (eller tilsvarende) bør bl.a. overvåge effektiviteten af selskabets interne kontrol, interne revision, og risikostyringssystemer, føre tilsyn med instituttets eksterne revisorer, indstille til ledelsesorganets godkendelse angående udnævnelse, honorering og afskedigelse af de eksterne revisorer, revidere og godkende revisionens omfang og hyppighed, revidere revisionsrapporter samt kontrollere, at ledelsesorganet i kraft af sin ledelsesfunktion træffer de nødvendige afhjælpningsforanstaltninger rettidigt for at imødegå kontrolmæssige svagheder, manglende overholdelse af love, bestemmelser og politikker, samt andre problemer som revisorerne har identificeret. Desuden bør revisionsudvalget føre tilsyn med instituttets fastlæggelse af regnskabspolitikker.

Forklarende note

Se ligeledes artikel 41 i direktiv 2006/43/EF om lovpligtig revision af årsregnskaber og konsoliderede regnskaber.

10. Udvalgets formand bør være uafhængig. Hvis formanden er tidligere medlem af instituttets ledelsesfunktion, bør der være et passende tidsinterval, før den pågældende overtager posten som udvalgsformand.

11. Medlemmerne af revisionsudvalget bør som helhed have nylig og relevant praktisk erfaring på området for finansielle markeder, eller bør, med udgangspunkt i deres tidligere forretningsaktiviteter, have tilstrækkelig erhvervsmæssig erfaring, der er direkte koblet sammen med aktiviteten på de finansielle markeder. Under alle omstændigheder bør revisionsudvalgets formand have specialiseret viden om og erfaring med anvendelsen af regnskabsprincipper og interne kontrolprocesser.

Risikoudvalg

12. Et risikoudvalg (eller tilsvarende) bør være ansvarligt for rådgivning af ledelsesorganet om instituttets generelle nuværende og fremtidige risikotolerance/-villighed og -strategi, og for at føre tilsyn med udmøntningen af denne strategi. For at fremme risikoudvalgets effektivitet bør det løbende kommunikere med instituttets risikostyringsfunktion og den øverste risikoansvarlige og bør, hvor det er relevant, have adgang til ekstern ekspertrådgivning, navnlig i relation til foreslåede strategiske transaktioner, såsom fusioner og virksomhedsovertagelser.

B.3 Ramme for forretningsadfærd

15. Virksomhedsværdier og forretningsadfærd

1. Ledelsesorganet bør udvikle og fremme høje etiske og forretningsmæssige standarder.

Forklarende note
Anfægtes et instituts omdømme, kan den mistede tillid være vanskelig at bygge op igen og kan have konsekvenser på hele markedet. Gennemførelse af relevante standarder (f.eks. en adfærdskodeks) for forretningsmæssig og ansvarlig adfærd i hele instituttet bør være med til at reducere de risici, som det er eksponeret mod. Navnlig vil den operationelle og omdømmemæssige risiko blive reduceret, såfremt disse standarder prioriteres højt og implementeres på forsvarlig måde.

2. Ledelsesorganet bør have klare politikker for, hvordan disse standarder skal efterleves.

3. Der bør gennemføres en fortløbende revision af gennemførelsen og overholdelsen af sådanne standarder. Resultaterne bør indberettes regelmæssigt til ledelsesorganet.

16. Interessekonflikter på institutniveau

1. Ledelsesorganet bør oprette, gennemføre og opretholde effektive politikker til identifikation af faktiske og potentielle interessekonflikter. Interessekonflikter, som ledelsesorganet har fået underretning om og har godkendt, bør håndteres forsvarligt.
2. En skriftlig politik bør identificere de relationer, tjenesteydelser, aktiviteter eller transaktioner i et institut, som kan give anledning til interessekonflikter, og bør beskrive, hvorledes disse konflikter bør håndteres. Denne politik bør dække relationer og transaktioner mellem forskellige kunder i et institut og de forbindelser og transaktioner, der findes mellem et institut og:

    a. dets kunder (som et resultat af forretningsmodellen og/eller de forskellige tjenesteydelser og aktiviteter, som instituttet tilbyder)

    b. dets aktionærer

    c. medlemmerne af dets ledelsesorgan

    d. dets personale

    e. vigtige leverandører eller forretningspartnere, og

    f. andre tilknyttede parter (f.eks. dets moderselskab eller datterselskaber).

3. Et moderselskab bør tage hensyn til og afveje alle dets datterselskabers interesser, og overveje hvordan disse interesser fremadrettet bidrager til selve koncernens fælles målsætning og interesser.
4. Politikken for interessekonflikter bør omfatte foranstaltninger, der skal vedtages for at forebygge eller håndtere interessekonflikter. Sådanne procedurer og foranstaltninger kunne omfatte:

    a. tilstrækkelig funktionsadskillelse, f.eks. ved at overlade modstridende aktiviteter inden for transaktions- eller tjenesteydelseskæden til forskellige personer eller overdrage tilsyns- eller indberetningsansvar for interessekonflikter til forskellige personer

    b. etablering af informationsbarrierer, f.eks. fysisk adskillelse af visse afdelinger

    c. forhindring af, at personer, der også er aktive uden for instituttet, får uhensigtsmæssig indflydelse inden for instituttet vedrørende disse aktiviteter.

17. Interne advarselsprocedurer

1. Ledelsesorganet bør oprette passende interne advarselsprocedurer, som gør det muligt for medarbejdere at gøre opmærksom på problematiske forhold vedrørende den interne ledelse.

2. Et institut bør vedtage passende interne advarselsprocedurer, som personalet kan gøre brug af til at gøre opmærksom på væsentlige og legitime bekymringer vedrørende forhold i forbindelse med den interne ledelse. Disse procedurer bør respektere fortrolighed for medarbejdere, der gør opmærksom på sådanne problemer. For at undgå interessekonflikter bør der være mulighed for at gøre opmærksom på denne type problemer uden for de normale rapporteringslinjer (f.eks. via compliancefunktionen eller den interne revision eller en intern whistleblowerprocedure). Advarselsprocedurerne bør kunne benyttes af alle instituttets medarbejdere. Alle relevante oplysninger, som personalet videregiver via advarselsproceduren, bør videreformidles til ledelsesorganet.

Forklarende note
I nogle medlemsstater kan der ud over eventuelle interne advarselsprocedurer i et institut ligeledes være mulighed for, at medarbejderne kan informere tilsynsmyndigheden om denne type problemer.

B.4 Politikker for outsourcing og aflønning

18. Outsourcing

1. Ledelsesorganet bør godkende og løbende revidere et instituts outsourcingpolitik.

Forklarende note
Denne vejledning er begrænset til outsourcingpolitikken, specifikke outsourcingaspekter behandles i CEBS' "Guidelines on Outsourcing", der findes på EBA's websted. Institutterne forventes at overholde begge sæt retningslinjer. I tilfælde af uoverensstemmelser bør CEBS' retningslinjer for outsourcing have forrang, da de er mere specifikke. Er der tale om et forhold, der ikke er dækket af CEBS' retningslinjer, bør det generelle princip i nærværende retningslinjer finde anvendelse.

2. Outsourcingpolitikken bør beskæftige sig med konsekvenserne af outsourcing for et instituts virksomhed og de risici, det står over for (f.eks. operationel, omdømme- og koncentrationsrisiko). Politikken bør omfatte ordninger for indberetning og overvågning, der bør gennemføres fra en outsourcingaftales start til dens slut (herunder udarbejdelse af en business case for outsourcing, indgåelse af en outsourcingkontrakt, gennemførelsen af kontrakten frem til dens udløb, nødplaner og exitstrategier). Denne politik bør gennemgås og opdateres løbende, og eventuelle ændringer bør gennemføres rettidigt.
3. Et institut vil fortsat være fuldt ansvarligt for alle outsourcede ydelser og aktiviteter samt for ledelsesbeslutninger, der udspringer heraf. I overensstemmelse hermed bør outsourcingpolitikken præcisere, at outsourcing

ikke fritager instituttet fra sine reguleringsforpligtelser og dets ansvar over for sine kunder.

4. Politikken bør præcisere, at outsourcingordninger ikke bør være nogen hindring for en effektiv "on-site" eller "off-site"-overvågning af instituttet og må ikke stride mod eventuelle tilsynsmæssige begrænsninger af tjenesteydelser og aktiviteter. Politikken bør ligeledes omfatte intern outsourcing (f.eks. af en separat juridisk enhed inden for et instituts koncern), og der bør tages hensyn til alle specifikke koncernforhold.

19. Styring af aflønningspolitikken

1. Den endelige overvågning af aflønningspolitikken bør ligge hos et instituts ledelsesorgan.

Forklarende note
Disse retningslinjer opstiller de *generelle* rammer, der gælder for styring af aflønningspolitikken. *Specifikke* aspekter af aflønningsforholdene behandles i CEBS' "Guidelines on Remuneration" fra december 2010. Institutterne forventes at overholde begge sæt retningslinjer.

2. Ledelsesorganet bør i kraft af sin tilsynsfunktion opretholde, godkende og overvåge principperne for instituttets generelle aflønningspolitik. Instituttets procedurer for fastlæggelse af aflønningen bør være klare, veldokumenterede og gennemsigtige internt.
3. Ud over ledelsesorganets generelle ansvar for den samlede aflønningspolitik og kontrollen heraf er det nødvendigt, at kontrolfunktionerne inddrages i det nødvendige omfang. Medlemmerne af ledelsesorganet, medlemmerne af vederlagsudvalget og andre medarbejdere, der er involveret i udformningen og udmøntningen af aflønningspolitikken, bør have relevant ekspertise og bør være i stand til at udforme en uafhængig vurdering af aflønningspolitikkens egnethed, herunder konsekvenserne heraf for risikostyringen.
4. Aflønningspolitikken bør også være rettet mod at forebygge interessekonflikter. Ledelsesorganet må i kraft af sin ledelsesfunktion ikke træffe afgørelse om sin egen aflønning. For at undgå at gøre dette kan det f.eks. overveje at gøre brug af et uafhængigt vederlagsudvalg. Et forretningsområde bør ikke kunne være i stand til at bestemme aflønningen af dets kontrolfunktioner.
5. Ledelsesorganet bør fortsætte overvågningen af anvendelsen af aflønningspolitikken for at sikre, at den fungerer efter hensigten. Udmøntningen af aflønningspolitikken bør ligeledes underlægges central og uafhængig kontrol.

C. Risikostyring

20. Risikokultur

1. Et institut bør udvikle en integreret risikokultur for hele instituttet baseret på fuld forståelse af de risici, det står over for, og af styringen heraf, under hensyntagen til dets risikotolerance/-villighed.

Forklarende note Da et instituts aktiviteter primært består i at tage risici, er det altafgørende, at risiciene håndteres korrekt. En betryggende og konsekvent risikokultur i hele instituttet er et afgørende element i en effektiv risikostyring.

2. Et institut bør udvikle sin risikokultur gennem politikker, eksempler, kommunikation og uddannelse af medarbejderne i deres ansvar i forbindelse med risikostyringen.
3. Hvert medlem af organisationen bør være fuldt ud klar over sit ansvar i forbindelse med risikostyring. Risikostyring bør ikke være begrænset til risikospecialister eller kontrolfunktioner. Forretningsområderne bør, under ledelsesorganets tilsyn, primært være ansvarlige for den daglige styring af risici, under hensyntagen til instituttets risikotolerance/-villighed og i overensstemmelse med dets politikker, procedurer og kontrolforanstaltninger.
4. Et institut bør have en helhedsorienteret ramme for risikostyring, der rækker på tværs af alle dets forretnings-, støtte- og kontrolområder, under fuld anerkendelse af den økonomiske substans af dets risikoengagementer og medtagelse af alle relevante risici (f.eks. finansielle og ikkefinansielle, i eller uden for balancen, uanset om de er uberegnelige eller kontraktmæssige). Omfanget af risikostyringen bør ikke være begrænset til kredit-, markeds-, likviditets- og driftsrisici, men bør også omfatte koncentrations-, omdømme-, compliance- og strategiske risici.
5. Rammen for risikostyring bør sætte instituttet i stand til at træffe kvalificerede beslutninger ud fra oplysninger, der stammer fra identifikation, måling eller vurdering og overvågning af risici. Risici bør evalueres efter "bottom up"- og "top down"-princippet, via ledelseskæden, samt på tværs af forretningsområder, under anvendelse af konsekvent terminologi og kompatible metoder i hele instituttet og dets koncern.
6. Rammen for risikostyring bør være omfattet af en uafhængig intern eller ekstern kontrol og bør revurderes løbende i forhold til instituttets risikotolerance/-villighed, idet oplysninger fra risikostyringsfunktionen og, hvor det er relevant, fra risikoudvalget, tages med i betragtning. Faktorer, der bør tages hensyn til, omfatter interne eller eksterne udviklinger, herunder vækst i balance og indtægter, stigende kompleksitet i instituttets forretning, risikoprofil og driftsstruktur, geografisk ekspansion, fusioner og overtagelser samt indførelse af nye produkter eller forretningsområder.

21. Tilpasning af aflønning til risikoprofil

1. En instituts aflønningspolitik og -praksis bør være i overensstemmelse med dets risikoprofil og bør fremme forsvarlig og effektiv risikostyring.

Forklarende note
Disse retningslinjer opstiller de *generelle* rammer, der gælder for tilpasningen af aflønningspolitikken til et instituts risikoprofil. *Specifikke* aspekter af aflønningspolitikken behandles i CEBS' "Guidelines on Remuneration" fra december 2010. Institutterne forventes at overholde begge sæt retningslinjer.

2. Et instituts generelle aflønningspolitik bør være i overensstemmelse med dets værdier, forretningsstrategi, risikotolerance/-villighed og langsigtede interesser. Det må ikke tilskynde til overdreven risikotagning. En garanteret variabel aflønning eller fratrædelsesgodtgørelser, der ender med at belønne svigt, er ikke i overensstemmelse med forsvarlig risikostyring eller princippet om, at aflønningen bør være afstemt efter resultaterne, og bør som hovedregel forbydes.
3. For medarbejdere, hvis arbejde har væsentlig indflydelse på et instituts risikoprofil (f.eks. medlemmer af ledelsesorganet, ledende medarbejdere, risikotagere i forretningsområder, medarbejdere i interne kontrolfunktioner og enhver medarbejder, hvis samlede løn ligger inden for samme lønramme som ledelsens og risikotagernes), bør aflønningspolitikken fastsætte specifikke ordninger for at tilpasse dem til forsvarlig og effektiv risikostyring.
4. De medarbejdere, der udfører kontrolfunktioner, bør aflønnes i henhold til deres mål og resultater og ikke i forhold til resultaterne på de forretningsområder, de kontrollerer.
5. Er aflønningen resultatafhængig, fastsættes aflønningen på grundlag af en kombination af den enkelte medarbejders og kreditinstituttets samlede resultater. Ved definitionen af den enkelte medarbejders resultater bør der tages hensyn til andre faktorer end finansielle. Måling af resultater med henblik på tildeling af bonus bør omfatte justeringer for alle typer risici, kapitalomkostninger og likviditet.
6. Der bør være en forholdsmæssig fordeling mellem grundløn og bonus. En betydelig bonus bør ikke bare være en kontant forudbetaling, men bør indeholde en fleksibel og udskudt risikojusteret komponent. Timingen af bonusbetalingen bør tage hensyn til de underliggende risikoresultater.

22. Ramme for risikostyring

1. Et instituts ramme for risikostyring bør omfatte politikker, procedurer, grænser og kontrol, der tillader passende, rettidig og vedvarende identifikation, måling eller vurdering, overvågning, afhjælpning og rapportering af de risici, der er forbundet med aktiviteterne i forretningsområderne og på institutniveau.

2. Et instituts risikostyringsramme bør opstille specifikke retningslinjer for implementeringen af dets strategier, som i det relevante omfang bør fastlægge og opretholde interne grænser, der er i overensstemmelse med instituttets risikotolerance/-villighed og står i forhold til dets forsvarlige funktion, finansielle styrke og strategiske mål. Et instituts risikoprofil (dvs. de samlede faktiske og potentielle risikoengagementer) bør holdes inden for disse grænser. Rammen for risikostyring bør sikre, at overtrædelser af grænserne ikke eskalerer, og at der efterfølgende sættes ind over for dette.
3. Identificerer og måler et institut risici, bør det udvikle fremad- og bagudrettede værktøjer, der skal supplere arbejdet med eksisterende engagementer. Disse værktøjer bør gøre det muligt at aggregere risikoengagementer på tværs af forretningsområder og støtte identifikationen af risikokoncentrationer.
4. Fremadrettede værktøjer (som f.eks. scenarieanalyse og stresstest) bør afdække potentielle risikoeksponeringer under en række forskellige negative omstændigheder; bagudrettede værktøjer bør bidrage til at revidere den faktiske risikoprofil i forhold til instituttets risikotolerance/-villighed og dets ramme for risikostyring og give input til eventuelle justeringer.

Forklarende note Retningslinjerne for stresstest findes på EBA's websted.

5. Det endelige ansvar for risikovurdering ligger udelukkende hos et institut, som i overensstemmelse hermed bør evaluere sine risici kritisk, og ikke udelukkende forlade sig på eksterne vurderinger.

Forklarende note F.eks. bør et institut validere en indkøbt risikomodel og tilpasse den til instituttets egne omstændigheder for at sikre en præcis og omfattende måling og analyse af risiko. Eksterne risikovurderinger (herunder eksterne kreditvurderinger eller eksternt indkøbte risikomodeller) kan være med til at give et mere omfattende risikoskøn. Institutterne bør være klar over anvendelsesområdet for sådanne vurderinger.

6. Beslutninger, der bestemmer graden af de risici, der tages, bør ikke alene være baseret på kvantitative oplysninger eller modeloutput, men bør også tage hensyn til de praktiske og begrebsmæssige begrænsninger af metrikker og modeller, ved at gøre brug af en kvalitativ metode (herunder ekspertvurdering og kritisk analyse). Relevante makroøkonomiske tendenser og data bør eksplicit være rettet mod at identificere deres mulige virkning på engagementer og porteføljer. Sådanne vurderinger bør formelt indarbejdes i væsentlige risikobeslutninger.

Forklarende note

Et institut bør have i tankerne, at resultaterne af fremadrettede kvantitative vurderinger og stresstestøvelser er stærkt afhængige af modellernes begrænsninger og antagelser (herunder alvoren og varigheden af chokket og de underliggende risici). Hvis f.eks. modeller viser meget høje afkast af økonomisk kapital, kan det skyldes en svaghed i modellerne (f.eks. at visse relevante risici ikke er medtaget), snarere end det forhold, at instituttet har en overlegen strategi eller gennemførelse.

7. Der bør etableres regelmæssige og gennemsigtige mekanismer, således at ledelsesorganet og alle relevante områder i et institut rettidigt får adgang til rapporter på en forståelig og hensigtsmæssig måde, og at de kan dele relevante oplysninger om identifikation, måling eller vurdering samt overvågning af risici. Rapporteringsrammen bør være veldefineret, dokumenteret og godkendt af ledelsesorganet.
8. Hvis der er nedsat et risikoudvalg, bør dette modtage formelle rapporter og uformel kommunikation i det relevante omfang fra risikostyringsfunktionen og den risikoansvarlige.

Forklarende note

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

23. Nye produkter

1. Et institut bør have indført en veldokumenteret politik for godkendelse af nye produkter, der er godkendt af ledelsesorganet, og som omfatter udviklingen af nye markeder, produkter og tjenesteydelser og væsentlige ændringer af de eksisterende.
2. Et instituts politik for godkendelse af nye produkter bør omfatte enhver overvejelse, der skal gøres, inden der træffes beslutning om at trænge ind på nye markeder, beskæftige sig med nye produkter, lancere en ny tjenesteydelse eller foretage betydelige ændringer i eksisterende produkter eller tjenesteydelser. Politikken for godkendelse af nye produkter bør også omfatte definitionen af "nyt produkt/marked/forretningsområde", der skal anvendes i

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

3. Politikken for godkendelse af nye produkter bør fastlægge de væsentligste spørgsmål, der skal besvares, før der træffes en beslutning. Hertil hører spørgsmålet om overholdelse af lovgivningen, prisfastsættelsesmodeller, konsekvenser for risikoprofilen, kapitaldækning og lønsomhed, adgang til tilstrækkelige frontoffice-, backoffice- og middleoffice-ressourcer og tilstrækkelige interne værktøjer og ekspertise til at forstå og overvåge de dermed forbundne risici. Beslutningen om at påbegynde en ny aktivitet bør klart angive det forretningsområde og de enkeltpersoner, der er ansvarlige for denne aktivitet. En ny aktivitet bør ikke gennemføres, før de fornødne ressourcer til at forstå og håndtere de dermed forbundne risici er til stede.
4. Risikostyringsfunktionen bør involveres i godkendelsen af nye produkter eller væsentlige ændringer af eksisterende produkter. Dens input bør omfatte en fuldstændig og objektiv vurdering af risiciene ved nye aktiviteter under en række forskellige scenarier, af potentielle mangler i instituttets risikostyring og interne kontrolrammer, samt instituttets evne til at håndtere nye risici effektivt. Risikostyringsfunktionen bør ligeledes have et klart overblik over indførelsen af nye produkter (eller væsentlige ændringer af eksisterende produkter) på tværs af forretningsområder og porteføljer og bør have beføjelse til at kræve, at ændringer af eksisterende produkter gennemløber den formelle proces for godkendelse af nye produkter.

D. Intern kontrol

24. Rammer for den interne kontrol

1. Et institut bør udvikle og opretholde en stærk og omfattende ramme for intern kontrol, herunder specifikke uafhængige kontrolfunktioner med tilstrækkelig autoritet til at udføre deres mission.
2. Et instituts interne kontrol bør sikre effektive operationer, tilstrækkelig kontrol af risici, forsigtig forretningsadfærd, pålidelighed af indberettede finansielle og ikkefinansielle oplysninger, både internt og eksternt, samt overholdelse af love, forskrifter, tilsynskrav og instituttets interne regler og beslutninger. Den interne kontrol bør omfatte hele organisationen, herunder aktiviteterne i alle forretnings-, støtte- og kontrolområder. Den interne kontrol bør være passende i forhold til instituttets virksomhed, og bør være i overensstemmelse med principperne om forsvarlig administrativ og regnskabsmæssig praksis.
3. Et institut bør i forbindelse med udviklingen af sin interne kontrolramme sikre, at der er en klar, gennemsigtig og dokumenteret beslutningsproces og en klar fordeling af ansvar og beføjelser til at sikre overholdelse af interne regler og beslutninger. For at indføre et stærkt internt kontrolmiljø på alle instituttets

områder bør forretnings- og støtteområdet være ansvarlige først og fremmest for at etablere og opretholde passende interne kontrolpolitikker og -procedurer.

4. En passende intern kontrol kræver ligeledes, at uafhængige kontrolfunktioner kontrollerer, at disse politikker og procedurer overholdes. Kontrolfunktionerne bør inkludere en risikostyringsfunktion, en compliancefunktion og en intern revisionsfunktion.
5. Kontrolfunktionerne bør etableres på et passende hierarkisk niveau og bør rapportere direkte til ledelsesorganet. De bør være uafhængige af de forretnings- og støtteområder, som de overvåger og kontrollerer samt være organisatorisk uafhængige af hinanden (eftersom de udfører forskellige funktioner). Imidlertid kan risikostyring- og compliancefunktionens opgaver kombineres i mindre komplekse eller mindre institutter. Koncernkontrolfunktionerne bør overvåge datterselskabernes kontrolfunktioner.
6. For at kontrolfunktionen kan betragtes som uafhængig, bør følgende betingelser være opfyldt:

    a. dens medarbejdere udfører ikke opgaver, der falder inden for anvendelsesområdet for de aktiviteter, som kontrolfunktionen forventes at overvåge og kontrollere

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

    c. den ansvarlige for kontrolfunktionen er underordnet en person, der ikke har noget ansvar for at håndtere de aktiviteter, som kontrolfunktionen overvåger og kontrollerer. Den ansvarlige for kontrolfunktionen generelt bør rapportere direkte til ledelsesorganet og alle relevante udvalg og bør regelmæssigt deltage i deres møder, og

    d. aflønningen af kontrolfunktionens medarbejdere bør ikke være knyttet til udøvelsen af de aktiviteter, som kontrolfunktionen overvåger og kontrollerer, og bør ikke på anden måde påvirke deres objektivitet.

7. Kontrolfunktionerne bør have et tilstrækkeligt antal kvalificerede medarbejdere (både i moder- og datterselskaber i koncerner). Medarbejdere bør opkvalificeres løbende og bør modtage passende uddannelse. De bør ligeledes have tilstrækkelige datasystemer og støtte til deres rådighed, med adgang til de interne og eksterne oplysninger, der er nødvendige for at leve op til deres ansvar.
8. Kontrolfunktionerne bør regelmæssigt til ledelsesorganet fremsende formelle rapporter om større identificerede mangler. Disse rapporter omfatter en opfølgning af tidligere konklusioner, og for hver ny identificeret større fejl, de relevante risici, der er involveret, en konsekvensanalyse samt anbefalinger. Ledelsesorganet bør handle rettidigt og effektivt på kontrolfunktionens konklusioner og kræve passende afhjælpningsforanstaltninger.

25. Risikostyringsfunktion

1. Et institut bør oprette en overordnet og uafhængig risikostyringsfunktion.
2. Risikostyringsfunktionen bør sikre, at hver enkelt nøglerisiko for instituttet identificeres og håndteres korrekt af de relevante områder i instituttet, og at ledelsesorganet får tegnet et holistisk billede af alle relevante risici. Risikostyringsfunktionen bør levere relevante uafhængige oplysninger, analyser og ekspertvurdering om risikoengagementer, samt rådgivning om forslag og risikobeslutninger, som ledelsesorganet og forretnings- eller støtteområderne træffer med hensyn til, om de er i overensstemmelse med instituttets risikotoleranc/-villighed. Risikostyringsfunktionen kan foreslå forbedringer af rammen for risikostyring og muligheder for at afhjælpe overtrædelser af risikopolitikker, -procedurer og –grænser.
3. Risikostyringsfunktionen bør være et instituts centrale organisatoriske funktion, der er struktureret, så det kan gennemføre risikopolitikker og kontrollere rammen for risikostyring. Store, komplekse og avancerede institutter kan overveje at oprette specifikke risikostyringsfunktioner for hvert væsentligt forretningsområde. Der bør imidlertid i instituttet være en central risikostyringsfunktion (herunder eventuelt en risikostyringsfunktion i en koncerns moderselskab), der tegner et holistisk billede af hele risikospektret.
4. Risikostyringsfunktionen bør være uafhængig af forretnings- og støtteområderne, hvis risici den kontrollerer, men bør ikke være isoleret fra disse. Den bør være i besiddelse af tilstrækkelig viden om risikostyringsteknikker og -procedurer og om markeder og produkter. Et samspil mellem de operative områder og risikostyringsfunktionen bør lette målsætningen om, at alle instituttets medarbejdere har ansvar for at håndtere risici.

26. Risikostyringsfunktionens rolle

1. Risikostyringsfunktionen bør være aktivt involveret på et tidligt tidspunkt i udformningen af et instituts risikostrategi og i alle væsentlige risikostyringsbeslutninger. Risikostyringsfunktionen bør spille en central rolle i at sikre, at instituttet har indført effektive risikostyringsprocesser.

Risikostyringsfunktionens rolle med hensyn til strategi og beslutninger

2. Risikostyringsfunktionen bør fremsende alle relevante risikorelaterede oplysninger til ledelsesorganet (f.eks. via teknisk analyse af risikoeksponeringer), så det bliver i stand til at fastlægge niveauet for instituttets risikotolerance/-villighed.
3. Risikostyringsfunktionen bør ligeledes vurdere risikostrategien, herunder målsætninger foreslået af forretningsområderne, og rådgive ledelsesorganet,

inden der træffes beslutning. Målsætninger, der involverer kreditvurderinger og satser for egenkapitalforrentning, bør være plausible og konsistente.

4. Risikostyringsfunktionen bør dele ansvaret for gennemførelsen af et instituts risikostrategi og -politik med alle instituttets forretningsområder. Forretningsområderne bør gennemføre de relevante risikogrænser, mens risikostyringsfunktionen bør være ansvarlig for at sikre, at risikogrænserne overholder instituttets generelle risikovillighed/risikotolerance og for løbende at overvåge, at instituttet ikke udviser overdreven risikoadfærd.
5. Risikostyringsfunktionens inddragelse i beslutningsprocesserne bør sikre, at der i tilstrækkeligt omfang kommer til at indgå risikoovervejelser. Imidlertid bør ansvaret for de beslutninger, der træffes, fortsat ligge hos forretnings- og støtteområderne og i sidste instans hos ledelsesorganet.

Risikostyringsfunktionens rolle med hensyn til transaktioner med forbundne parter

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

Risikostyringsfunktionens rolle med hensyn til kompleksiteten af den juridiske struktur

7. Risikostyringsfunktionen bør tilstræbe at identificere væsentlige risici, der opstår som følge af kompleksiteten af et instituts juridiske struktur.

Forklarende note

Risici kan omfatte manglende ledelsesmæssig gennemsigtighed, operationelle risici som følge af indbyrdes forbundne og komplekse finansieringsstrukturer, engagementer inden for koncernen, registreret sikkerhedsstillelse og modpartsrisiko.

Risikostyringsfunktionens rolle med hensyn til væsentlige ændringer

8. Risikostyringsfunktionen bør vurdere, på hvilken måde alle identificerede væsentlige risici kunne påvirke instituttets eller koncernens evne til at håndtere sin risikoprofil og afsætte midler og kapital under normale og negative omstændigheder.
9. Inden der træffes beslutninger om væsentlige ændringer eller ekstraordinære transaktioner, bør risikostyringsfunktionen inddrages i vurderingen af

virkningen af sådanne ændringer og ekstraordinære transaktioner på instituttets og koncernens samlede risiko.

Forklarende note

Væsentlige ændringer eller ekstraordinære transaktioner kan være fusioner og overtagelser, oprettelse eller frasalg af datterselskaber eller virksomheder til specielle formål, nye produkter, ændringer af systemer, risikostyringsramme eller procedurer og ændringer i instituttets organisation.

Se de fælles retningslinjer fra 2008 for de tidligere europæiske tilsynsudvalg (niveau 3-udvalg) i den finansielle sektor (CEBS, CESR, og CEIOPS) om tilsynsmæssig vurdering af erhvervelser og forøgelse af kapitalandele i den finansielle sektor, der er offentliggjort på EBA's websted. Risikostyringsfunktionen bør være aktivt involveret på et tidligt tidspunkt i identifikationen af relevante risici (herunder mulige konsekvenser af gennemførelsen af utilstrækkelig due diligence, der undlader at identificere risici efter en fusion), der vedrører ændringer i koncernens struktur (herunder fusioner og overtagelser) og bør rapportere om sine konklusioner direkte til ledelsesorganet.

Risikostyringsfunktionens rolle med hensyn til måling og vurdering

10. Risikostyringsfunktionen bør sikre, at et instituts interne risikomålinger og -vurderinger omfatter en tilfredsstillende vifte af scenarier og er baseret på tilstrækkeligt konservative skøn vedrørende afhængigheder og korrelationer. Dette bør omfatte kvalitative (herunder med ekspertvurdering) bedømmelser for hele instituttet af forholdet mellem risici og lønsomhed i instituttet og dets eksterne driftsomgivelser.

Risikostyringsfunktionens rolle med hensyn til overvågning

11. Risikostyringsfunktionen bør sikre, at alle identificerede risici kan overvåges effektivt af forretningsområderne. Risikostyringsfunktionen bør regelmæssigt overvåge instituttets faktiske risikoprofil og holde den op mod instituttets strategiske mål og risikotolerance/-villighed, således at ledelsesorganet i kraft af sin ledelsesfunktion kan træffe beslutninger, der kan anfægtes af ledelsesorganet i kraft af sin tilsynsfunktion.
12. Risikostyringsfunktionen bør analysere tendenser og afdække nye risici eller risici i fremvækst som følge af ændrede omstændigheder og forhold. Den bør ligeledes regelmæssigt revidere faktiske risikoresultater i forhold til tidligere skøn (dvs. backtesting) for at vurdere og forbedre nøjagtigheden og effektiviteten af risikostyringsprocessen.

13. Risikostyringsfunktionen for koncernen bør overvåge de risici, som datterselskaberne tager. Uoverensstemmelser i forhold til den godkendte koncernstrategi bør rapporteres til det relevante ledelsesorgan.

Risikostyringsfunktionens rolle med hensyn til ikkegodkendte engagementer

14. Risikostyringsfunktionen bør involveres i tilstrækkeligt omfang i alle ændringer i instituttets strategi, godkendte risikotolerance/-villighed og -grænser.

15. Risikostyringsfunktionen bør uafhængigt vurdere en krænkelse eller overtrædelse (herunder årsagen samt en juridisk og økonomisk analyse af de faktiske omkostninger ved at lukke, reducere eller risikoafdække engagementet i forhold til de faktiske omkostninger ved at beholde det). Risikostyringsfunktionen bør, i det omfang det er relevant, informere de berørte forretningsområder og anbefale eventuelle afhjælpningsforanstaltninger.

Forklarende note

Krænkelser eller overtrædelser af strategier, risikotolerance/-villighed eller -grænser kan forårsages af nye transaktioner, ændringer i markedsvilkårene eller af en udvikling i instituttets strategi, politikker eller procedurer, når risikogrænser eller risikotolerancen/-villigheden ikke ændres tilsvarende.

16. Risikostyringsfunktionen bør spille en central rolle i at sikre, at der træffes beslutning om dens anbefaling på det relevante niveau, at den overholdes af de relevante forretningsområder og i tilstrækkeligt omfang rapporteres til ledelsesorganet, risikoudvalget eller støtteområdet.

17. Et institut bør træffe passende foranstaltninger mod intern eller ekstern svigagtig adfærd og overtrædelser af disciplinen (f.eks. overtrædelse af interne procedurer, overtrædelse af grænser).

Forklarende note

For så vidt angår anvendelsesområdet for disse retningslinjer, dækker "svig" intern og ekstern svig som defineret i direktiv 2006/48/EF, bilag X, del 5. Dette omfatter tab, der skyldes handlinger, der har til formål at begå svig, uberettiget tilegne sig midler eller omgå bestemmelser, lovgivningen eller virksomhedens politik, undtagen begivenheder vedrørende forskellighed/forskelsbehandling, der involverer mindst en intern part (intern svig), og tab, der skyldes handlinger med det formål at begå svig, uberettiget tilegne sig midler eller omgå lovgivningen, begået af tredjemand (ekstern svig).

27. Risikoansvarlig

1. Et institut bør udpege en person, den risikoansvarlige, der har eneansvaret for risikostyringsfunktionen og for overvågning af instituttets risikostyringsramme på tværs af hele organisationen.
2. Den risikoansvarlige (eller en tilsvarende stilling) bør være ansvarlig for at levere omfattende og forståelig information om risici, der sætter ledelsesorganet i stand til at forstå instituttets samlede risikoprofil. Tilsvarende gælder for den risikoansvarlige i et moderinstitut vedrørende hele koncernen.
3. Den risikoansvarlige bør have tilstrækkelig ekspertise, operationel erfaring, uafhængighed og anciennitet til at anfægte beslutninger, der påvirker et instituts risikoeksponering. Et institut bør overveje at tildele den risikoansvarlige vetoret. Den risikoansvarlige og ledelsesorganet eller de relevante udvalg bør være i stand til at kommunikere direkte indbyrdes om centrale risikorelaterede emner, herunder udviklingstendenser, der kan være uforenelige med instituttets risikotolerance/-villighed og -strategi.
4. Såfremt et institut ønsker at tildele den risikoansvarlige ret til at nedlægge veto mod beslutninger, bør dets risikopolitikker fastlægge, under hvilke omstændigheder den risikoansvarlige kan gøre dette og forslagenes art (f.eks. en kredit- eller investeringsbeslutning eller fastlæggelsen af en grænse). Politikkerne bør beskrive procedurerne for at anke eller klage, og hvordan ledelsesorganet informeres.
5. Tilsiger et instituts karakteristika – især dets størrelse, opbygning og karakteren af dets aktiviteter – ikke, at dette ansvar tilføres en særligt udpeget person, vil denne funktion kunne varetages af en anden højtstående person i instituttet, forudsat at der ikke foreligger nogen interessekonflikt.
6. Instituttet bør have indført dokumenterede processer for besættelse af stillingen som risikoansvarlig og for fratagelse af dennes ansvarsområder. Såfremt den risikoansvarlige udskiftes, bør ledelsesorganets tilsynsfunktion godkende dette i forvejen. Generelt bør afskedigelse eller udnævnelse af en risikoansvarlig offentliggøres, og tilsynsmyndigheden informeres om årsagerne hertil.

28. Compliancefunktion

1. Et institut bør oprette en compliancefunktion, der håndterer dets compliancerisiko.
2. Et institut bør godkende og gennemføre en compliancepolitik, der bør kommunikeres til alle medarbejderne.

Forklarende note

Compliancerisiko (der defineres som den øjeblikkelige eller potentielle risiko, der kan påvirke indtjening og kapital som følge af overtrædelser eller

manglende overholdelse af love, regler, forskrifter, aftaler, etableret praksis eller etiske standarder) kan medføre bøder, erstatningskrav og/eller opsigelse af kontrakter og kan forringe et instituts omdømme.

3. Et institut bør oprette en permanent og effektiv compliancefunktion og udpege en person, der er ansvarlig for denne funktion i hele instituttet og koncernen (den complianceansvarlige eller leder af complianceafdelingen). I mindre og mindre komplekse institutter kan denne funktion kombineres med eller støttes af risikostyrings- eller støttefunktionerne (f.eks. personaleafdeling, juridisk afdeling osv.).
4. Compliancefunktionen bør sikre, at compliancepolitikken overholdes, og bør rapportere til ledelsesorganet og i det omfang, det er nødvendigt, til den risikoansvarlige om instituttets håndtering af compliancerisikoen. Compliancefunktionens konklusioner bør indgå i ledelsesorganets og den risikoansvarliges beslutningsproces.
5. Compliancefunktionen bør vejlede ledelsesorganet om de love, regler, forskrifter og standarder, som instituttet skal overholde og vurdere den mulige virkning af eventuelle ændringer i de juridiske eller tilsynsmæssige rammebetingelser i forhold til instituttets aktiviteter.
6. Compliancefunktionen bør ligeledes kontrollere, at nye produkter og nye procedurer overholder de eksisterende juridiske rammer og alle kendte kommende ændringer i lovgivning, forskrifter og tilsynskrav.

Forklarende note

Særlig opmærksomhed er påkrævet, når instituttet udfører visse tjenesteydelser eller opretter strukturer på vegne af kunder (f.eks. når det optræder som agent i forbindelse med oprettelse af selskaber eller partnerskaber, yder forvaltningstjenester, eller udvikler komplekse strukturerede finansieringstransaktioner for kunder), som kan stille den interne ledelse over for særlige udfordringer og tilsynsmæssige overvejelser.

29. Intern revisionsfunktion

1. Den interne revision bør vurdere, om kvaliteten af et instituts interne kontrolmiljø er både virkningsfuld og effektiv.
2. Den interne revision bør have uhindret indsigt i relevante dokumenter og oplysninger i alle operationelle enheder og kontrolenheder.
3. Den interne revision bør evaluere alle et instituts aktiviteter og enheders (herunder risikostyrings- og compliancefunktionen) overholdelse af dets politikker og procedurer. Den interne revision bør derfor ikke kombineres med nogen anden funktion. Den interne revision bør ligeledes vurdere, om eksisterende politikker og procedurer fortsat er tilstrækkelige og overholder juridiske og tilsynsmæssige krav.

4. Den interne revision bør navnlig kontrollere rigtigheden af processerne, og således sikre pålideligheden af instituttets metoder og teknikker, skøn og informationskilder, der anvendes i dets interne modeller (f.eks. risikomodellering og måling af regnskaber). Den bør ligeledes evaluere kvaliteten og brugen af kvalitative værktøjer for identifikation og vurdering af risiko. Den interne revision bør imidlertid, for at styrke sin uafhængighed, ikke blive direkte involveret i udformningen eller udvælgelsen af modeller eller andre risikostyringsværktøjer.
5. Ledelsesorganet bør tilskynde de interne revisorer til at overholde nationale og internationale professionelle standarder. Det interne revisionsarbejde bør udføres i henhold til en revisionsplan og detaljerede revisionsprogrammer, der følger en "risikobaseret" metode. Revisionsplanen bør godkendes af revisionsudvalget og/eller ledelsesorganet.

Forklarende note
Et eksempel på professionelle standarder, der henvises til her, er de standarder, der er udarbejdet af Foreningen af Interne Revisorer.

6. Den interne revision bør rapportere direkte til ledelsesorganet og/eller dettes revisionsudvalg (hvor dette finder anvendelse) om sine konklusioner og forslag til væsentlige forbedringer af den interne kontrol. Alle revisionsanbefalinger bør underkastes en formel procedure for de respektive ledelsesniveauers opfølgning, så det sikres, at der findes en løsning, der skal indberettes.

E. Informationssystemer og beredskabsplaner

30. Informationssystem og kommunikation

1. Et institut bør have effektive og pålidelige informations- og kommunikationssystemer, der dækker alle dets væsentlige aktiviteter.

Forklarende note
Ledelsens beslutninger vil kunne blive påvirket i negativ retning af upålidelig eller vildledende information, som leveres af systemer, der er uhensigtsmæssigt udformet og kontrolleret. En kritisk komponent af et instituts aktiviteter er derfor oprettelsen og vedligeholdelsen af informations- og kommunikationssystemer, der dækker den fulde vifte af dets aktiviteter. Disse oplysninger leveres typisk via både elektroniske og ikkeelektroniske midler. Et institut bør være særlig opmærksomt på de organisatoriske og interne kontrolkrav i forbindelse med behandling af information i elektronisk form og behovet for at have et passende revisionsspor. Det gælder også, såfremt it-systemer udliciteres til en it-serviceleverandør.

2. Informationssystemer, herunder dem, der opbevarer og anvender data i elektronisk form, bør være sikre, uafhængigt overvågede og understøttet af passende nødplaner. Et institut bør overholde generelt accepterede it-standarder, når det implementerer it-systemer.

31. Driftskontinuitet

1. Et institut bør udarbejde forsvarlige beredskabsplaner, som sikrer, at det kan videreføre driften og begrænse sit tab i tilfælde af alvorlige driftsforstyrrelser.

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

2. For at oprette en forsvarlig beredskabsplan bør et institut nøje analysere sin eksponering for alvorlige driftsforstyrrelser og vurdere (kvantitativt og kvalitativt) deres potentielle virkning ved hjælp af interne og/eller eksterne data og scenarioanalyse. Denne analyse bør omfatte alle forretnings- og støtteområder samt risikostyringsfunktionen og tage hensyn til deres indbyrdes afhængighed. Desuden bør en særlig beredskabsfunktion, risikostyringsfunktionen eller den operationelle risikostyringsfunktion inddrages aktivt. Resultaterne af analysen bør bidrage til at definere instituttets prioriteter og målsætninger for genoprettelsen.

Forklarende note
For så vidt angår risikostyringsfunktionen for operationelle risici henvises der ligeledes til direktiv 2006/48/EF, bilag X, del 3, punkt 3, i henhold hvortil institutter med avancerede målingsmetoder skal have en sådan uafhængig funktion. Denne funktions opgaver beskrives i "Guidelines on Validation", punkt 615-620 (offentliggjort i 2006) som findes på EBA's websted.

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

    a. Beredskabs- og kontinuitetsplaner, som sikrer, at et institut reagerer hensigtsmæssigt på nødsituationer og kan opretholde sine vigtigste

driftsfunktioner, hvis der sker en afbrydelse af dets normale driftsprocedurer.

b. Katastrofeplaner for kritiske ressourcer, der skal sætte det i stand til at vende tilbage til almindelige driftsprocedurer inden for en passende tidsfrist. Enhver restrisiko som følge af potentielle driftsforstyrrelser bør være forenelig med instituttets risikotolerance/-villighed.

4. Beredskabs-, kontinuitets- og katastrofeplaner bør dokumenteres og implementeres omhyggeligt. Dokumentationen bør være tilgængelig i forretnings- og støtteområderne og i risikostyringsfunktionen, og lagres på systemer, der er fysisk adskilt og let tilgængelige i tilfælde af en nødsituation. Der bør tilbydes relevant uddannelse. Planerne bør afprøves og opdateres regelmæssigt. Ethvert problem eller enhver fejl, der opstår under afprøvningerne, bør dokumenteres og analyseres, og planerne bør revideres i overensstemmelse hermed.

F. Gennemsigtighed

32. Beføjelser

1. Strategier og politikker bør kommunikeres til alle et instituts medarbejdere.
2. Et instituts medarbejdere bør forstå og overholde politikker og procedurer, der vedrører deres pligter og ansvar.
3. Ledelsesorganet bør i overensstemmelse hermed informere og ajourføre de relevante medarbejdere om instituttets strategier og politikker på en klar og konsistent måde, i det mindste i det omfang dette er nødvendigt for, at disse medarbejdere kan udføre deres specifikke opgaver. Dette kan ske gennem skriftlige retningslinjer, manualer eller lignende midler.

33. Gennemsigtighed i forbindelse med intern ledelse

1. Rammen for et instituts interne ledelse bør være gennemsigtig. Et institut bør på en klar, afbalanceret, præcis og retvisende måde gøre rede for sin nuværende situation og fremtidsudsigter.

Forklarende note Formålet med gennemsigtighed i forbindelse med intern ledelse er at give alle et instituts relevante interessenter (herunder aktionærer, medarbejdere, kunder og offentligheden) de nøgleinformationer, der er nødvendige for at

sætte dem i stand til at vurdere ledelsesorganets effektivitet med hensyn til at lede instituttet.

I henhold til artikel 72 i direktiv 2006/48/EF og artikel 2 i direktiv 2006/49/EF skal moderkreditinstitutter og kreditinstitutter, der er kontrolleret af et finansielt moderholdingselskab i EU, offentliggøre omfattende og nyttige oplysninger, der beskriver deres interne ledelse på konsolideret niveau. Det er god praksis, at det enkelte institut, i det omfang det er relevant, offentliggør oplysninger om dets interne ledelse på individuelt grundlag.

2. Et institut bør offentliggøre mindst følgende:

   a. dets ledelsesstrukturer og -politikker, herunder dets målsætninger, organisatorisk struktur, interne ledelsesordninger, ledelsesorganets struktur og organisation, herunder deltagelse, og instituttets incitaments- og aflønningsstruktur

   b. art, omfang, formål og økonomisk indhold af transaktioner med tilsluttede og forbundne parter, hvis de har en væsentlig indvirkning på instituttet

   c. hvordan dets forretnings- og risikostrategi er udformet (herunder ledelsesorganets involvering) og forventede risikofaktorer

   d. dets nedsatte udvalg samt deres mandater og sammensætning

   e. dets interne kontrolmiljø, og hvordan dets kontrolfunktioner er tilrettelagt, de vigtigste opgaver de udfører, hvordan deres resultater overvåges af ledelsesorganet, og eventuelle planlagte væsentlige ændringer i disse funktioner, og

   f. væsentlige oplysninger om dets finansielle resultater og driftsresultater.

3. Oplysninger om instituttets nuværende situation bør overholde eventuelle juridiske offentliggørelseskrav. Oplysningerne bør være tydelige, nøjagtige, relevante, rettidige og lettilgængelige.
4. I sager, hvor en sikring af en høj grad af nøjagtighed ville forsinke offentliggørelsen af tidsfølsomme oplysninger, bør et institut foretage en vurdering af den passende balance mellem rettidighed og nøjagtighed under hensyntagen til kravet om at give et retvisende billede af dets situation og give en tilfredsstillende forklaring på en eventuel forsinkelse. Denne forklaring bør ikke anvendes til at udskyde kravene til den løbende rapportering.

Afsnit III - Endelige bestemmelser og gennemførelse

34. Ophævelse

Med vedtagelsen og offentliggørelsen af disse retningslinjer for intern ledelse ophæves følgende: afsnit 2.1 i CEBS' "Guidelines on the Application of the Supervisory Review Process" (af 25. januar 2006), med overskriften "Guidelines

on Internal Governance"; "High Level Principles for Remuneration Policies" (af 20. april 2009) og "High Level Principles for Risk Management" (af 16. februar 2010).

35. Ikrafttrædelsesdato

De kompetente myndigheder bør gennemføre retningslinjerne for intern ledelse ved at inkorporere dem i deres tilsynsprocedurer senest den 31. marts 2012. Efter denne dato bør de kompetente myndigheder sikre, at institutterne efterlever retningslinjerne.