Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.[1]

I medfør af § 65, stk. 2, § 70, stk. 6, § 71, stk. 3, § 152, stk. 2, § 343 r, stk. 2 og 5, og § 373, stk. 4, i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 1447 af 11. september 2020, [som ændret ved § 1 i lov nr. xx af xx december 2020], § 67, stk. 6, § 68, stk. 2, § 94, stk. 2, og § 258, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og –aktiviteter og § 21 og § 39, stk. 3, i lov om realkreditlån og realkreditobligationer m.v., jf. lovbekendtgørelse nr. 1188 af 19. september 2018, fastsættes:

Kapitel 1

Anvendelsesområde

§ 1. Bekendtgørelsen finder anvendelse på følgende virksomheder, jf. dog stk. 4-9:

1) Pengeinstitutter.
2) Realkreditinstitutter.
3) Danmarks Skibskredit A/S.
4) Fondsmæglerselskaber, jf. dog stk. 7.
5) Investeringsforvaltningsselskaber, dog ikke investeringsforvaltningsselskabers administration af danske UCITS.
6) Finansielle holdingvirksomheder med de tilpasninger, som koncernforholdet nødvendiggør.
7) Filialer her i landet af kreditinstitutter, investeringsselskaber og administrationsselskaber, der er meddelt tilladelse i et land udenfor den Europæiske Union, som Unionen ikke har indgået aftale med på det finansielle område, med de afvigelser, som filialforholdet nødvendiggør, eller som er fastsat i eller i henhold til international aftale.

Stk. 2. Virksomheder omfattet af stk. 1, der kun har tilladelse til at udføre visse nærmere afgrænsede tjenesteydelser, skal følge bekendtgørelsens regler på de områder, som virksomheden har tilladelse til.

Stk. 3. § 2, stk. 1, § 3, stk. 1, nr. 5-7, 10, 11 og 13, og stk. 2, § 4, stk. 2, nr. 6 og 8, § 16, bilag 5 og bilag 7, nr. 1-9, 11, 12, 14, 16-19, 22 og 24, finder anvendelse på fælles datacentraler.

Stk. 4. § 4, stk. 2, nr. 7, § 5, stk. 3, nr. 4, og bilag 8 finder ikke anvendelse for virksomheder omfattet af stk. 1, nr. 5-7.

Stk. 5. Bilag 5, nr. 70, finder anvendelse på filialer af penge- og realkreditinstitutter, der er udpeget som operatører af væsentlige tjenester i medfør af § 307 a, stk. 1, 2. pkt., i lov om finansiel virksomhed.

Stk. 6. § 16 finder ikke anvendelse på finansielle holdingvirksomheder.

Stk. 7. §§ 16 og 17 finder ikke anvendelse på virksomheder, der alene har tilladelse som fondsmæglerselskab.

Stk. 8. § 25 finder alene anvendelse på virksomheder omfattet af stk. 1, nr. 1, 2, 4, 6 og 7, og securitiseringsenheder med særligt formål, jf. artikel 2, stk. 1, nr. 2, i Europa-Parlamentets og Rådets forordning 2017/2402/EU af 12. december 2017.

Stk. 9. § 5, stk. 3, nr. 5, finder ikke anvendelse for virksomheder omfattet af § 1, stk. 1, nr. 5 og 6.

Kapitel 2

[1] Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF, EU-Tidende 2013, nr. L 176, side 338, dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019 om ændring af direktiv 2013/36/EU, for så vidt angår fritagne enheder, finansielle holdingselskaber, blandede finansielle holdingselskaber, aflønning, tilsynsforanstaltninger og -beføjelser og kapitalbevaringsforanstaltninger, EU-Tidende 2019, nr. L 150, side 253, dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, side 1, og dele af Europa-Parlamentets og Rådets direktiv 2019/2034/EU af 27. november 2019 om tilsyn med investeringsselskaber og om ændring af direktiv 2002/87/EF, 2009/65/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU og 2014/65/EU, EU-Tidende 2019, nr. L 314, side 64. I bekendtgørelsen er medtaget visse bestemmelser fra Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og om ændring af forordning (EU) nr. 648/2012, EU-Tidende 2013, nr. L 176, side 1, Europa-Parlamentet og Rådets forordning (EU) 2019/630 af 17. april 2019 om ændring af forordning (EU) nr. 575/2013, for så vidt angår krav til minimumsdækning af tab for misligholdte eksponeringer, EU-Tidende 2019, nr. L 111, side 4, samt visse bestemmelser fra Europa-Parlamentets og Rådets forordning (EU) 2019/876 af 20. maj 2019 om ændring af forordning (EU) nr. 575/2013 for så vidt angår gearingsgrad, net stable funding ratio, krav til kapitalgrundlag og nedskrivningsrelevante passiver, modpartskreditrisiko, markedsrisiko, eksponeringer mod centrale modparter, eksponeringer mod kollektive investeringsordninger, store eksponeringer og indberetnings- og oplysningskrav, og forordning (EU) nr. 648/2012, EU-Tidende 2019, nr. L 150, side 1. Ifølge artikel 288 i EUF-traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i bekendtgørelsen er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

Betryggende foranstaltninger

§ 2. Bestyrelsen henholdsvis direktionen i de virksomheder, der er omfattet af § 1, stk. 1 og 3, skal træffe foranstaltninger, der er tilstrækkelige til, at virksomheden drives betryggende. Bestyrelsen henholdsvis direktionen skal herunder tage stilling til, hvilke foranstaltninger der er tilstrækkelige til, at bekendtgørelsen overholdes. Hvilke foranstaltninger, der er tilstrækkelige, vil afhænge af virksomhedens forretningsmodel samt

1) virksomhedens størrelse,
2) virksomhedens struktur samt strukturen af den koncern, hvori virksomheden måtte indgå,
3) de forretningsmæssige og geografiske områder, som virksomheden opererer på,
4) de finansielle tjenesteydelser, som virksomheden tilbyder, og
5) de finansielle produkter, som virksomheden handler med.

Stk. 2. Bestyrelsen henholdsvis direktionen i de virksomheder, der er omfattet af § 1, stk. 1, nr. 1-6, og som har datterselskaber, skal træffe foranstaltninger, der er tilstrækkelige til, at koncernen drives på betryggende vis.

Stk. 3. Bestyrelsen henholdsvis direktionen i de virksomheder, der er omfattet af § 1, stk. 1, nr. 1 og 2, og som i medfør af §§ 308 eller 310 i lov om finansiel virksomhed er udpeget som systemisk vigtige finansielle institutter (SIFI) eller globalt systemisk vigtige finansielle institutter (G-SIFI), skal ved vurderingen efter stk. 1 inddrage hensynet til opretholdelsen af en stabil finansiel sektor ved vurdering af risikostyringsområdet og hensynet til opretholdelsen af en stabil finansiel infrastruktur ved vurdering af it-sikkerhedsområdet.

Kapitel 3

Bestyrelsens opgaver og ansvar

§ 3. Bestyrelsen skal som led i varetagelsen af den overordnede og strategiske ledelse af virksomheden

1) træffe beslutning om virksomhedens forretningsmodel, herunder målsætninger for de forhold, der er nævnt under § 2, stk. 1, nr. 1-5,
2) på grundlag af forretningsmodellen træffe beslutning om virksomhedens politikker, jf. § 4,
3) løbende, dog mindst én gang om året, foretage en vurdering af virksomhedens enkelte og samlede risici, jf. § 5, herunder tage stilling til, om risiciene er acceptable,
4) vurdere og træffe beslutning om virksomhedens budgetter, kapital, likviditet, væsentlige dispositioner, særlige risici og overordnede forsikringsforhold,
5) vurdere om direktionen varetager sine opgaver på en betryggende måde og i overensstemmelse med den fastlagte risikoprofil, de fastlagte politikker samt retningslinjerne til direktionen,
6) vurdere om virksomheden har en klar organisatorisk struktur med en veldefineret ansvarsfordeling under hensyntagen til virksomhedens forretningsmodel og risikoprofil,
7) træffe beslutning om frekvensen for og omfanget af direktionens rapportering og information til bestyrelsen således, at bestyrelsen har et indgående overblik over virksomheden og dens risici, og at rapporteringen i øvrigt er fyldestgørende for bestyrelsens arbejde,
8) løbende og mindst én gang om året træffe beslutning om virksomhedens individuelle solvensbehov, jf. § 124, stk. 2, og § 126 a, stk. 1, i lov om finansiel virksomhed og § 118, stk. 2, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter,
9) tilrettelægge sit arbejde således, at ledelsen af virksomheden er betryggende, jf. bilag 6,
10) vurdere, om virksomhedens politikker, kommunikation, trænings- og udviklingsaktiviteter m.v. fremmer udvikling af en adfærd i organisationen, som understøtter virksomhedens mål og værdier,
11) vurdere, om virksomheden har en betryggende offentliggørelses- og kommunikationsproces,
12) godkende den rapport, som direktionen har pligt til at udarbejde med en opgørelse og vurdering af virksomhedens likviditetsposition og likviditetsrisici, jf. § 8, stk. 9, og
13) vurdere og godkende virksomhedens it-strategi, jf. bilag 5.

Stk. 2. Bestyrelsen skal sikre, at den har det fornødne informationsgrundlag til at træffe beslutninger som nævnt i stk. 1.

§ 4. Virksomhedens politikker, jf. § 3, stk. 1, nr. 2, skal indeholde virksomhedens overordnede strategiske mål for de pågældende risikoområder, herunder identifikation og afgrænsning af de risici, som virksomheden ønsker at påtage sig på de pågældende områder, og anvisninger på, hvordan de strategiske mål opnås.

Stk. 2. Politikkerne skal, hvor det er relevant, omfatte følgende:

1) Kreditpolitik, jf. bilag 1.
2) Markedsrisikopolitik, jf. bilag 2.
3) Politik for operationelle risici, jf. bilag 3.

4) Politik for forsikringsmæssig afdækning af risici.
5) Likviditetspolitik, herunder en beredskabsplan i tilfælde af utilstrækkelig eller manglende likviditet, jf. bilag 4.
6) It-strategi, it-risikostyringspolitik og it-sikkerhedspolitik, jf. bilag 5.
7) Politik for risikoen for overdreven gearing, jf. bilag 8.
8) Øvrige risikoområder, som bestyrelsen vurderer, er af betydning for virksomheden.

Stk. 3. Virksomhedens politikker, jf. stk. 2, nr. 1-3, samt i relevant omfang nr. 4-8, skal udover virksomhedens overordnede strategiske mål for de pågældende risikoområder indeholde retningslinjer for de risici, der udspringer af miljømæssige, sociale og ledelsesmæssige forhold, som virksomheden ønsker at påtage sig.
Stk. 4. Virksomhedens politikker skal være forsvarlige i forhold til virksomhedens indtjening og kapitalgrundlag.

§ 5. Ved opfyldelse af § 3, stk. 1, nr. 3, skal bestyrelsen løbende vurdere, om virksomhedens politikker, jf. § 4, samt retningslinjerne til direktionen, jf. §§ 6 og 7, er betryggende i forhold til virksomhedens forretningsmæssige aktiviteter, organisation og ressourcer samt de markedsforhold, som virksomhedens aktiviteter drives under.
Stk. 2. Vurderingen efter stk. 1 skal foretages i forhold til
1) hvilke risici virksomheden er udsat for, herunder forretningsmodellens indflydelse på risici og risikoniveauer,
2) hvilke aktiviteter de pågældende risici er tilknyttet,
3) omfanget af de enkelte risici, og
4) hvordan risikotyperne påvirker hinanden, hvis dette er relevant.

Stk. 3. Vurderingen efter stk. 1 skal i fornødent omfang desuden indeholde en stillingtagen til
1) om virksomheden har et betryggende antal medarbejdere og kompetencer på risikobehæftede aktiviteter,
2) om virksomheden har betryggende it-systemer,
3) om virksomheden har betryggende procedurer for hurtig og effektiv kommunikation på tværs af virksomheden og koncernen,
4) om virksomheden har betryggende processer til identifikation, styring og overvågning af overdreven gearingsrisiko, jf. bilag 8, og
5) om virksomheden har et betryggende antal medarbejdere, kompetencer, politikker, retningslinjer og processer for styring af nødlidende eksponeringer (non-performing exposures) og eksponeringer med kreditlempelser (forborne exposures), jf. artikel 47a og artikel 47b, i Europa-Parlamentets og Rådets forordning (EU) nr. 2019/630 af 17. april 2019 for så vidt angår krav til minimumsdækning af tab for misligholdte eksponeringer, herunder om virksomheden har et passende beredskab til at håndtere en eventuel væsentlig forringelse af kvaliteten i kreditporteføljen.

Stk. 4. Den risikoansvarliges rapport, jf. bilag 7, skal indgå i bestyrelsens samlede vurderingsgrundlag, jf. stk. 1.

§ 6. På grundlag af risikovurderingen, jf. § 5, og i henhold til de politikker, der er vedtaget i medfør af § 4, skal bestyrelsen udstede skriftlige retningslinjer til direktionen.
Stk. 2. Retningslinjerne efter stk. 1 skal angive, hvilke dispositioner direktionen kan foretage som led i dens stilling, og hvilke beslutninger direktionen eventuelt kan træffe med efterfølgende orientering af bestyrelsen.
Stk. 3. Bestyrelsen kan ikke henlægge beføjelser til direktionen, der hører til bestyrelsens overordnede ledelsesopgaver, jf. §§ 3-5, eller i øvrigt er af usædvanlig art eller af stor betydning for virksomheden, herunder følgende beføjelser:
1) Beslutning om rammer og betingelser for outsourcing af kritiske og vigtige processer, tjenesteydelser eller aktiviteter.
2) Bevilling af usædvanlige eller betydende eksponeringer, jf. dog § 117, stk. 1, 3. og 4. pkt., i selskabsloven, og eksponeringer omfattet af § 78 i lov om finansiel virksomhed og § 88 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.
3) Den årlige gennemgang af større aktiver og passiver, jf. principperne i § 115, nr. 1, i selskabsloven.
4) Ansættelse af direktion og revisionschef.
5) Beslutning om principper for opgørelse af risici, jf. § 7, stk. 1, nr. 2, herunder anvendelse af interne modeller, der ikke er omfattet af nr. 6.
6) Beslutning om ansøgning om godkendelse af IRB-, VaR-, AMA- og EPE-modeller og andre interne modeller til opgørelse af virksomhedens solvens, jf. Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og Europa-Parlamentets og Rådets forordning (EU) 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber.
7) Beslutning om virksomhedens individuelle solvensbehov, jf. § 124, stk. 2, og § 126 a, stk. 1, i lov om finansiel virksomhed og § 118, stk. 2, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.

§ 7. Retningslinjerne efter § 6 skal
1) indeholde kontrollerbare grænser for størrelsen af de risici, som direktionen er bemyndiget til at tage på virksomhedens vegne, og

2) fastlægge principperne for, hvordan udnyttelse af grænserne for hver type af risiko opgøres, herunder for hvordan risiko fra finansielle instrumenter og midler, der på virksomhedens vegne forvaltes af eksterne porteføljeforvaltere, indgår i den samlede risikoopgørelse.

Stk. 2. Retningslinjernes grænser på kreditrisiko-, markedsrisiko- og likviditetsrisikoområdet, jf. bilag 1, 2 og 4, skal utvetydigt angive størrelsen af den enkelte fastsatte grænse for risiko for eksempel som absolutte tal, eller ved at risikoen sættes i forhold til virksomhedens kapitalgrundlag.

Stk. 3. Retningslinjerne kan kun undtagelsesvis give mulighed for, at direktionen kan disponere risici i en størrelsesorden, der ligger udenfor den fastlagte risikoprofil og retningslinjernes grænser og da kun, hvis forudsætningerne herfor fremgår af retningslinjerne. Kan disse forudsætninger ikke fastlægges, kan forudgående beføjelser til overskridelser af retningslinjernes grænser ikke gives til direktionen.

Stk. 4. Bestyrelsen skal ved udformningen af retningslinjerne til direktionen være betrygget i, at direktøren eller direktionens medlemmer tilsammen besidder den fornødne viden og erfaring til at anvende de beføjelser, som retningslinjerne indeholder, på en for virksomheden betryggende måde.

Stk. 5. Det skal fremgå af retningslinjerne, hvordan og hvor hyppigt rapportering til bestyrelsen skal ske. Herunder skal det fremgå, hvordan og hvor hyppigt direktionen skal rapportere på de områder, hvor bestyrelsen har fastsat grænser for direktionen, eller hvor der er fastsat grænser i lovgivningen.

Kapitel 4

Direktionens opgaver og ansvar

§ 8. Direktionen skal forestå den daglige ledelse af virksomheden i overensstemmelse med lovgivningens bestemmelser, herunder selskabsloven og lov om finansiel virksomhed eller lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, og de politikker og retningslinjer, som er vedtaget og givet af bestyrelsen, jf. §§ 4, 6 og 7, samt eventuelle andre mundtlige eller skriftlige beslutninger og anvisninger fra bestyrelsen.

Stk. 2. Direktionen skal sikre, at de politikker og retningslinjer, som er vedtaget af bestyrelsen, implementeres i virksomhedens daglige drift.

Stk. 3. Direktionen er forpligtet til at videregive information til bestyrelsen, som bestyrelsen har anmodet om samt information, som direktionen vurderer, kan være af betydning for bestyrelsens arbejde.

Stk. 4. Direktionen er forpligtet til at videregive information til den risikoansvarlige og den complianceansvarlige, som direktionen vurderer kan være af betydning for den risikoansvarlige og den complianceansvarliges arbejde.

Stk. 5. Direktionen har det daglige ledelsesmæssige ansvar for, at virksomheden kun træffer dispositioner, som direktionen og medarbejdere i fornødent omfang kan vurdere risiciene ved og konsekvenserne af.

Stk. 6. Direktionen skal sikre, at der er forretningsgange for dokumentation af alle væsentlige beslutninger i organisationen, herunder oplysninger om, hvem der har truffet en given beslutning, hvornår den er truffet, og under hvilken beføjelse og på hvilket grundlag den er truffet.

Stk. 7. Direktionen skal godkende virksomhedens forretningsgange, jf. § 13, stk. 1, eller udpege en eller flere personer eller organisatoriske enheder med den nødvendige faglige viden til at gøre dette.

Stk. 8. Direktionen skal sikre, at der er anvisninger for, hvilke tiltag der skal iværksættes i forbindelse med alvorlige driftsforstyrrelser, it-nedbrud, øvrige driftsforstyrrelser samt for nøglemedarbejderes fratrædelse.

Stk. 9. Direktionen skal godkende virksomhedens retningslinjer for udvikling og godkendelse af nye tjenesteydelser og produkter, der kan medføre væsentlige risici for virksomheden, modparter eller kunder, herunder ændringer i eksisterende produkter, hvorved produktets risikoprofil ændres væsentligt.

Stk. 10. Direktionen i virksomheder omfattet af § 1, stk. 1, nr. 1-3, skal mindst én gang om året udarbejde en rapport med en opgørelse og vurdering af virksomhedens likviditetsposition og likviditetsrisici.

Stk. 11. Direktionen skal mindst én gang om året vurdere kvaliteten af data, som virksomheden anvender som grundlag for at vurdere risici og træffe forretningsmæssige beslutninger, samt iværksætte nødvendige tiltag, hvis direktionen finder kvaliteten utilstrækkelig.

Stk. 12. Direktionen skal løbende overvåge, udfordre og føre tilsyn med ledende medarbejderes arbejde i organisationen, herunder sikre at der sker betryggende rapportering, jf. §§ 20 og 21.

Stk. 13. Direktionen skal foretage en tilstrækkelig undersøgelse af forholdene, hvis den får mistanke om medarbejderes samarbejde med kunder, leverandører eller andre eksterne parter om deltagelse i kriminalitet eller får mistanke om medarbejderes kendskab til kunders, leverandørers eller andre eksterne parters kriminalitet. Direktionen skal i denne situation vurdere tildelingen af opgaver til pågældende medarbejdere.

Kapitel 5

Organisation og ansvarsfordeling

Opgaver og ressourcer

§ 9. Virksomheden skal være indrettet i organisatoriske enheder med klart definerede arbejdsopgaver, herunder skal alle medarbejdere have klare beføjelser, ansvarsområder og referencelinjer. Det skal herunder være klart for de enkelte enheder og medarbejdere, hvilke opgaver der skal udføres, og hvordan opgaverne skal udføres.
Stk. 2. De organisatoriske enheder skal være bemandet ressource- og kompetencemæssigt således, at enhederne på betryggende vis kan løse de opgaver, det påhviler enhederne at udføre.
Stk. 3. Virksomheden skal have foranstaltninger, som sikrer, at overholdelse af politikker og forretningsgange indgår i ledelsens vurdering af de organisatoriske enheders og medarbejdernes løsning af deres respektive opgaver.

Information af bestyrelsen og øvrige ledelsesniveauer m.v.

§ 10. Virksomheden skal være indrettet, så den information, der skal tilgå bestyrelse, direktion og ledelse på øvrige organisatoriske niveauer samt den risikoansvarlige og den complianceansvarlige, kan tilgå disse i retvisende og dækkende form for disses arbejde, herunder indenfor tidsmæssige rammer og i en form, der sikrer, at eventuelle foranstaltninger kan sættes i værk uden unødigt ophold.

Interessekonflikter og funktionsadskillelse

§ 11. Virksomheden skal sikre, at
1) der foreligger procedurer med henblik på forebyggelse, identifikation og håndtering af interessekonflikter,
2) virksomheden er indrettet, så der er betryggende funktionsadskillelse, herunder at disponerende medarbejdere, medarbejdere, der udfører afvikling, og medarbejdere, der udfører resultat- og risikoopgørelser samt kontrol og rapportering, refererer til hver sin leder, og
3) virksomheden er indrettet, så der er klart definerede rapporteringslinjer.

Stk. 2. Virksomhedens afvikling, udarbejdelse af resultat- og risikoopgørelser, kontrol og rapportering kan udføres i samme enhed, hvis dette kan anses for betryggende, jf. § 2, og under hensyntagen til arten af enhedens øvrige opgaver.
Stk. 3. I virksomheder, hvor der ikke opretholdes funktionsadskillelse i overensstemmelse med stk. 1, nr. 2, skal der, jf. § 2, indføres betryggende kompenserende foranstaltninger, der skal sikre, at der ikke påføres virksomheden unødige risici eller tab.

Kapitel 6
Administrativ og regnskabsmæssig praksis

Administrativ praksis

§ 12. Virksomheden skal være indrettet, så de enkelte enheder og medarbejderne har de forretningsgange, manualer, beredskabsplaner, systemer og øvrige redskaber til rådighed, der er nødvendige for udførelsen af deres opgaver.

§ 13. Virksomheden skal have forretningsgange på alle væsentlige aktivitetsområder. Aktiviteter, der vedrører virksomheden i dens egenskab af finansiel virksomhed, anses som udgangspunkt for væsentlige.
Stk. 2. Forretningsgangene skal som minimum
1) være lettilgængelige og overskuelige,
2) på fyldestgørende måde beskrive de aktiviteter, der skal udføres, herunder sikre at lovgivningen og anden relevant regulering samt de politikker og retningslinjer, som virksomhedens ledelse har vedtaget, efterleves og overholdes,
3) angive, hvilken organisatorisk enhed, personer eller grupper af personer der skal udføre de enkelte opgaver eller delopgaver, og
4) opdateres løbende ved ændring i interne forhold eller i relevant regulering.

Stk. 3. Forretningsgangene kan foreligge elektronisk. Direktionen skal dog sikre, at de er tilgængelige i tilfælde af systemnedbrud i virksomheden.

§ 14. Direktionen skal sikre, at der er fornøden dokumentation for virksomhedens aktiviteter, herunder at der er forretningsgange for,
1) i hvilket omfang beslutninger, beføjelser, udførte opgaver og forretninger samt opståede hændelser skal dokumenteres,
2) i hvilken form dokumentationen skal ske,
3) hvordan der sikres tilgængelighed til dokumentationen,
4) hvor længe dokumentationen skal opbevares, og

5) hvis relevant, til hvem dokumentationen kan og skal videregives.

Stk. 2. Dokumentationen, jf. stk. 1, skal foreligge enten skriftligt eller elektronisk.

Regnskabsmæssig praksis

§ 15. Virksomheden skal have en god regnskabsmæssig praksis. Det indebærer blandt andet, at

1) virksomheden, jf. § 14, kan dokumentere, at offentliggjorte års- og delårsrapporter, herunder alle enkeltposter og noter, er udarbejdet i overensstemmelse med det regelsæt, der gælder for den pågældende rapport, og
2) virksomheden indhenter nødvendig information til brug for udarbejdelse af års- og delårsrapporter, herunder al relevant information til brug for fastlæggelse af regnskabsposter, der baseres på regnskabsmæssige skøn.

Kapitel 7

Risikostyring og compliance

Risikoansvarlig og risikostyringsfunktion

§ 16. Direktionen skal sikre, at virksomheden har en risikostyringsfunktion og en risikoansvarlig, jf. bilag 7. Direktionen skal sikre, at risikostyringsfunktionen i nødvendigt omfang kan rette henvendelse og rapportere direkte til bestyrelsen uafhængigt af direktionen, og at risikostyringsfunktionen kan give udtryk for betænkeligheder og advare bestyrelsen i de tilfælde, hvor specifikke risikoudviklinger påvirker eller kan påvirke virksomheden, uden at dette berører det ansvar, som bestyrelsen har.

Stk. 2. Afskedigelse af den risikoansvarlige kræver bestyrelsens forudgående godkendelse.

Stk. 3. Direktionen skal følge op på den risikoansvarliges konklusioner og anbefalinger samt i relevant omfang gennemføre korrigerende foranstaltninger. Virksomheden skal have retningslinjer for opfølgning på den risikoansvarliges konklusioner.

Stk. 4. Advarsler og betænkeligheder afgivet af risikostyringsfunktionen skal dokumenteres, og virksomheden skal have procedurer til at sikre dette.

Compliance

§ 17. Virksomheden skal have metoder og procedurer, der er egnede til at opdage og mindske risikoen for virksomhedens manglende overholdelse af den lovgivning, der gælder for virksomheden, markedsstandarder og interne regelsæt (compliancerisici).

Stk. 2. Virksomheden skal have en compliancefunktion, der fungerer uafhængigt, og som skal kontrollere og vurdere, om metoderne og procedurerne efter stk. 1 og de foranstaltninger, der træffes for at afhjælpe eventuelle mangler, er effektive.

Stk. 3. I virksomheder, der er værdipapirhandlere, skal compliancefunktionen for den del af virksomheden, der vedrører handel med finansielle instrumenter, udføre compliance og yde rådgivning af og bistand til de personer, der har ansvaret for at yde investeringsservice og udføre investeringsaktiviteter i overensstemmelse med artikel 22, stk. 1-3, i Kommissionens delegerede forordning (EU) nr. 2017/565 af 25. april 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/65/EU for så vidt angår de organisatoriske krav til og vilkårene for drift af investeringsselskaber samt definitioner af begreber med henblik på nævnte direktiv.

Stk. 4. For at sikre at compliancefunktionen kan varetage sine ansvarsområder korrekt og uafhængigt, skal direktionen sikre, at følgende betingelser opfyldes:

1) Compliancefunktionen skal have de nødvendige ressourcer, den nødvendige kompetence og sagkundskab samt adgang til regelmæssig uddannelse og alle relevante oplysninger.
2) En medarbejder, der er udpeget af direktionen, skal være ansvarlig for compliancefunktionen og for rapportering til bestyrelsen og direktionen. Rapporteringen skal ske mindst én gang om året. Den complianceansvarlige skal i øvrigt have mulighed for at udtale sig direkte til bestyrelsen, hvis den complianceansvarlige skønner det nødvendigt.
3) Medarbejdere, der er involveret i compliancefunktionen, må ikke deltage i leveringen af de tjenesteydelser eller udførelsen af de aktiviteter, de kontrollerer.
4) Metoden til at fastsætte vederlag til medarbejdere i compliancefunktionen må ikke bringe deres uafhængighed i fare.

Stk. 5. Stk. 4, nr. 3 og 4, finder ikke anvendelse, hvis det kan godtgøres, at disse krav ikke står i rimeligt forhold til arten, omfanget og sammensætningen af virksomhedens aktiviteter.

Stk. 6. Vurderer direktionen, at virksomhedens størrelse eller sammensætningen af virksomhedens aktiviteter berettiger hertil, kan den samme person udpeges til at være complianceansvarlig og risikoansvarlig. Det skal dog altid sikres, at medarbejdere ikke er involveret i udførelsen af opgaver, som de kontrollerer som led i deres complianceopgaver.

Stk. 7. Direktionen skal følge op på den complianceansvarliges konklusioner og anbefalinger samt i relevant omfang gennemføre korrigerende foranstaltninger. Virksomheden skal have retningslinjer for opfølgning på den complianceansvarliges konklusioner.

Stk. 8. Advarsler og betænkeligheder afgivet af compliancefunktionen skal dokumenteres og virksomheden skal have procedurer til at sikre dette.

Videregivelse af beføjelser

§ 18. Videregivelse af beføjelser fra bestyrelse, direktion og øvrige ledelsesniveauer skal dokumenteres, jf. § 14, og proceduren herfor skal fremgå af forretningsgangene, jf. § 13.
Stk. 2. Videregivelse af beføjelser kan kun ske til medarbejdere, der har den fornødne viden, indsigt og erfaring til betryggende at kunne anvende beføjelserne.
Stk. 3. Videregivne beføjelser skal som minimum angive

1) arten og størrelsen af den eller de videregivne beføjelser,
2) principperne for opgørelse af udnyttelse af beføjelserne,
3) hvilke produkter eller handlinger beføjelsen omfatter,
4) eventuelle supplerende grænser for risiko samt principperne for opgørelse af sådanne beføjelser, der opfylder kravene i § 7, stk. 1, og
5) hvordan, hvor ofte og af hvilken person eller organisatorisk enhed rapportering skal foretages til afgiver af beføjelsen og eventuelle andre.

Stk. 4. Ingen kan videregive beføjelser, der går udover de beføjelser, den pågældende selv har modtaget. Summen af videregivne beføjelser, herunder beføjelser givet til grupper af medarbejdere, må ikke overstige de beføjelser, som fremgår af bestyrelsens retningslinjer til direktionen.
Stk. 5. Er der fastsat supplerende risikomål i forbindelse med videregivne beføjelser, skal den, der afgiver beføjelserne, sikre sig, at anvendelse af de supplerende risikomål finder sted på en måde, der sikrer, at der ikke sker overskridelse af øvrige tildelte beføjelser.

Kontroller

§ 19. Direktionen skal sikre, at der foretages kontrol af alle væsentlige risikobehæftede opgaver, herunder af

1) overholdelse af samtlige grænser fastsat af bestyrelsen i henhold til § 7, stk. 1, nr. 1, i de retningslinjer, som bestyrelsen har givet til direktionen, og grænser i lovgivningen,
2) overholdelse af videregivne beføjelser,
3) dispositioner, hvor virksomheden handler i henhold til fuldmagt fra kunder eller modparter, og hvor virksomheden har forpligtet sig til at overholde grænser for risici, herunder placeringsgrænser,
4) dispositioner, hvor virksomheden har forpligtet sig til at overholde grænser for risici aftalt med modparter, for eksempel i rammeaftaler om handel med finansielle instrumenter,
5) indsamling og behandling af data, som virksomheden anvender som grundlag for at vurdere risici og træffe forretningsmæssige beslutninger, og
6) andre opgaver, som af anden årsag kan medføre væsentlige økonomiske eller andre væsentlige risici for virksomheden, herunder disponering af virksomhedens konti og opgaver i forbindelse med fremskaffelse eller udarbejdelse af grundlag for regnskab og fastsættelse af virksomhedens individuelle solvensbehov.

Stk. 2. Kontrol skal udføres af en anden enhed end den, der har udført opgaven, jf. § 11, stk. 1, medmindre kontrollen har karakter af afstemning, overvågning af om forretningsgange overholdes, fejlfinding eller lignende, og kontrollen i det konkrete tilfælde er betryggende.
Stk. 3. Kontroller omfattet af stk. 1 skal foretages med passende intervaller, afhængigt af virksomhedens størrelse, den enkelte risikos væsentlighed og størrelse set i forhold til virksomhedens forretningsmodel, aktivitetsområde, kompleksiteten af de pågældende risici og virksomhedens kapitalforhold. Kontrollerne skal, hvor der løbende sker dispositioner hen over dagen, omfatte overholdelse af grænser intra-dag. Intra-dag kontroller kan, hvor dette er betryggende, foretages på stikprøvebasis.
Stk. 4. Virksomheden skal have passende overvågning af, at administrative opgaver udføres på en betryggende og ensartet måde, og at forretningsgange m.v. bliver overholdt.

Intern rapportering

§ 20. Direktionen skal sikre, at der løbende sker skriftlig og betryggende rapportering på alle relevante ledelsesmæssige niveauer om overholdelsen og udnyttelsen af væsentlige grænser for risikotagning, der fremgår af bestyrelsens vedtagne retningslinjer efter § 6 eller i den videregivne beføjelse. Direktionen skal også sikre, at der sker rapportering om overholdelse af de grænser, der er fastsat i lovgivningen for risiko, på de områder, hvor dette er relevant for den pågældende virksomhed. Rapporteringen skal omfatte risici, der styres på virksomhedens vegne af porteføljeforvaltere.

Stk. 2. Rapporteringen skal ske i overskuelig form og give bestyrelse, direktion og øvrige ledelsesniveauer, der har videregivet beføjelser, jf. § 18, oplysning om den aktuelle udnyttelse af de væsentlige grænser og om udnyttelsen over tid. Uanset 1. pkt. og stk. 1 skal der ske rapportering om overskridelse af samtlige grænser.
Stk. 3. Anvender virksomheden interne modeller til opgørelse af risici, skal rapporteringen desuden omfatte relevante back-tests til dokumentation af modellens pålidelighed.
Stk. 4. Rapportering om videregivne beføjelser, herunder overskridelse af disse, skal ske til den, der har afgivet beføjelserne med intervaller, der afspejler afgiverens involvering i den daglige disponering, og som fremgår af beføjelserne. Overskridelsen skal sædvanligvis rapporteres senest dagen efter, at overskridelsen er konstateret.

§ 21. Direktionen skal sikre, at der sker rapportering om andre væsentlige forhold, der ikke er omfattet af beføjelser fastsat i retningslinjerne eller i videregivne beføjelser, jf. stk. 2. Det kan for eksempel dreje sig om rapportering vedrørende afstemningsfejl, tab som følge af operationelle forhold, fejl i regnskab eller budgetter, nøglepersoners fratræden, mulige lovovertrædelser, mangelfulde kontroller, uhensigtsmæssig adfærd eller andre uregelmæssigheder.
Stk. 2. Direktionen skal sikre, at virksomhedens forretningsgange i videst muligt omfang indeholder anvisninger om, hvilke forhold der skal eller bør rapporteres om, og til hvem rapporteringen skal foretages, herunder skal det fremgå, om rapportering i særlige tilfælde kan eller skal ske til andre end den pågældendes daglige leder eller dennes leder.

Nye tjenesteydelser og produkter

§ 22. Direktionen skal sikre, at der udarbejdes retningslinjer for udvikling og godkendelse af nye tjenesteydelser og produkter, herunder ændringer i eksisterende tjenesteydelser og produkter, hvorved tjenesteydelsernes og produkternes risikoprofil ændres væsentligt, jf. § 8, stk. 9. Retningslinjerne skal som minimum

1) afgrænse, hvornår der er tale om et nyt produkt eller tjenesteydelse, i det omfang det er muligt,
2) angive, hvilken eller hvilke organisatoriske enheder, udvalg eller ad hoc-udvalg der skal forestå udviklingsprocessen, eventuelt opdelt pr. risikoområde,
3) indeholde retningslinjer for, hvem der som minimum skal inddrages i udviklingsprocessen, så det sikres, at alle relevante forhold belyses,
4) indeholde retningslinjer for, hvilke overordnede forhold der skal analyseres og dokumenteres, herunder arten, størrelsen og opgørelsen af risici for virksomheden, påvirkning af virksomhedens omkostninger og indtjening, virksomhedens muligheder for at agere på nye markeder, påvirkning af virksomhedens solvens, regnskabsmæssig behandling og påvirkning af virksomhedens kunders risici og omkostninger,
5) indeholde krav om, at analysen skal godtgøre, at virksomheden har tilstrækkelig ekspertise, systemer, kapital og ressourcer til at håndtere det nye produkt eller tjenesteydelsen på betryggende vis, og
6) indeholde bestemmelse om retningslinjer for, at nye produkter og tjenesteydelser, der kan medføre væsentlige nye risici for virksomheden eller virksomhedens kunder, skal forelægges bestyrelsen med henblik på dennes stillingtagen til, om anvendelsen af det nye produkt giver anledning til ændring af politikker eller retningslinjer, der er vedtaget i medfør af §§ 4, 6 og 7, herunder til fastsættelse af særlige principper for opgørelse af de risici, der knytter sig til produktet.

§ 23. Den risikoansvarlige og den complianceansvarlige skal deltage eller som minimum høres i forbindelse med udvikling og godkendelse af nye tjenesteydelser og produkter. Den risikoansvarlige og den complianceansvarlige skal løbende være informeret om forløbet af godkendelsesprocessen.
Stk. 2. Den risikoansvarlige og den complianceansvarlige skal høres i forbindelse med stillingtagen til, om ændring af eksisterende produkter har et omfang, der medfører, at ændringen skal være omfattet af kravene til udvikling og godkendelse af nye produkter. Den risikoansvarlige og den complianceansvarlige skal altid kunne kræve, at en ændring af et eksisterende produkt skal behandles som et nyt produkt.

Gearingsrisiko

§ 24. Ved gearing forstås i denne bekendtgørelse gearing som defineret i artikel 4, stk. 1, nr. 93, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter.
Stk. 2. Ved overdreven gearingsrisiko forstås overdreven gearingsrisiko som defineret i artikel 4, stk. 1, nr. 94, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter.

Risici forbundet med securitisering

§ 25. Deltagelse i securitiseringsaktiviteter som defineret i artikel 4, stk. 1, nr. 61, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter kan ske ved, at

1) virksomheden eksponeres mod securitiseringspositioner, herunder eksponeringer fra investering i securitiseringspositioner eller udbud af kreditrisikoafdækning, eller
2) virksomheden selv eller i samarbejde med andre etablerer eller arrangerer securitiseringstransaktioner, programmer for kortfristede gældsbreve eller ABCP-programmer, jf. artikel 242, nr. 9, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter.

Stk. 2. Virksomheder, der deltager i securitiseringsaktiviteter, skal have betryggende politikker og forretningsgange på området, som skal sikre, at virksomheden vurderer og håndterer risici forbundet med securitisering, herunder omdømmemæssige risici, der kan opstå i forbindelse med deltagelse i komplekse strukturer, og at securitiseringsaktiviteternes økonomiske indhold afspejles i risikovurderingen og ledelsesbeslutningerne.

Kapitel 8
Straf

§ 26. Overtrædelse af §§ 3-7, § 8, stk. 2-4 og 6-13, § 9, § 11, stk. 1 og 3, § 12, § 13, stk. 1, 1. pkt., stk. 2 og stk. 3, 2. pkt., §§ 14 og 15, § 16, stk. 1, 3 og 4, § 17, stk. 1-4, stk. 6, 2. pkt., og stk. 7 og 8, § 18, § 19, stk. 1 og 2, stk. 3, 1. og 2. pkt., og stk. 4, § 20, § 21, stk. 1, 1. pkt., og stk. 2, §§ 22 og 23, § 25, stk. 2, og bilag 1-8 straffes med bøde. Med bøde straffes desuden den, der ikke efterkommer et påbud om at foretage eller undlade at foretage bestemte handlinger med henblik på at overholde bekendtgørelsens bestemmelser eller bilag.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 9
Ikrafttræden og overgangsbestemmelser

§ 27. Bekendtgørelsen træder i kraft den 26. juni 2021.

Stk. 2. Bekendtgørelse nr. 1706 af 27. november 2020 om ledelse og styring af pengeinstitutter m.fl. ophæves.

Finanstilsynet, den dd.mm.yyyy

- 1. underskriver

/2. underskriver

Bilag 1. Kreditområdet

Bestyrelsens opgaver og ansvar på kreditområdet

Kreditpolitikken

1) Bestyrelsen skal efter et princip om forsigtighed vedtage en kreditpolitik, jf. § 4, stk. 2, nr. 1, som dækker alle typer af kreditrisiko i alle virksomhedens enheder og forretningsaktiviteter. Kreditpolitikken skal, afhængigt af den finansielle virksomheds type og størrelse, bestyrelsens, direktionens og medarbejdernes kompetencer, de anvendte it-systemer m.v. samt kompleksiteten af virksomhedens kreditrisikobehæftede aktiviteter, indeholde stillingtagen til, hvilken kreditrisikoprofil bestyrelsen ønsker, at virksomheden skal have. Bestyrelsen skal sikre, at den ønskede kreditrisikoprofil er i overensstemmelse med målene for virksomhedens generelle risikoprofil og med dens kapitalplanlægning og likviditetsplanlægning. Kreditpolitikken skal udformes på en måde, så den fremmer en forståelse og en adfærd i organisationen, som sikrer, at kreditgivning foretages i overensstemmelse med kundens interesser og evner til at overholde påtagne forpligtelser, imod passende sikkerhedsstillelse og under hensyntagen til miljømæssige, sociale og ledelsesmæssige forhold.
2) Kreditpolitikken skal indeholde principper for typen og omfanget af kreditrisici, herunder principper for:
    a) Ønskede kundetyper (for eksempel erhvervskunder, privatkunder, formuende kunder, helkunder m.fl.).
    b) Kundernes ønskede risikoprofil, for eksempel
        i. hvad der karakteriserer en person eller virksomhed m.v., man ønsker eller ikke ønsker som ny kunde, og
        ii. hvad der karakteriserer eksisterende privat- og erhvervskunder m.v., hvor man ønsker at forøge, opretholde, reducere eller afvikle eksponeringen.
    c) De typer af produkter, der ønskes udbudt af virksomheden, herunder ønsker til rente- og afviklingsprofil og lån i fremmed valuta.
    d) I hvilket omfang og under hvilke forudsætninger virksomheden ønsker store eksponeringer, der for eksempel overstiger 2 eller 5 pct. af virksomhedens kapitalgrundlag.
    e) Omfanget af øvrige koncentrationsrisici, herunder maksimale samlede eksponeringer indenfor forskellige brancher og indenfor andre ensartede typer af risici, hvor virksomhedens risikokoncentration er væsentlig.
    f) Geografisk eksponering, herunder virksomhedens maksimale eksponering indenfor udvalgte geografiske områder, herunder udenlandske aktiviteter.
    g) I hvilket omfang og under hvilke forudsætninger virksomheden ønsker eksponeringer mod kapitalfonde og lignende kunder, som sædvanligvis er karakteriseret ved høj gæld i forhold til kundernes indtjening i de aktiviteter, som skal skabe likviditet til eksponeringens tilbagebetaling.
    h) Hvilken renteføl somhed virksomheden ønsker at acceptere for kunder med boligfinansiering, øvrige privatkunder, landbrugskunder og forskellige typer af andre erhvervskunder samt for den samlede portefølje på erhvervsområdet.
    i) Hvordan det sikres, at kreditbeslutninger i tilstrækkeligt omfang baseres på robustheden af kundens fremtidige indtjening og likviditet og ikke i for høj grad baseres på stillede sikkerheder, som kan falde i værdi.
    j) Hvordan det sikres, at kreditbeslutninger i tilstrækkeligt omfang tager højde for de miljømæssige, sociale og ledelsesmæssige risici, som kunden er udsat for.
    k) De typer af sikkerheder, som virksomheden vil lade indgå i sine kreditbeslutninger, herunder virksomhedens maksimale samlede eksponeringer hvor udvalgte typer af sikkerheder indgår i kreditbeslutningen.
    l) Den finansielle virksomheds ønskede indtjening i forhold til den valgte risikoprofil, herunder prisfastsættelse af produkter m.v.
3) Kreditpolitikken skal desuden indeholde principper for følgende områder:
    a) Klassifikation af kunder ud fra den skønnede kreditrisiko.
    b) Konsolidering af eksponeringer med indbyrdes forbundne kunder i overensstemmelse med principperne for opgørelse af store eksponeringer i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter og i Europa-Parlamentets og Rådets forordning (EU) 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber.
    c) Værdiansættelse af sikkerheder.
    d) Håndtering af nødlidende eksponeringer og eksponeringer med kreditlempelse samt øvrige eksponeringer med højere risiko end ønsket, herunder fastlæggelse af handlingsplaner for det videre forløb. Principperne skal blandt andet angive, hvilke typer af kreditlempelser virksomheden ønsker at anvende, samt i hvilket omfang og under hvilke omstændigheder virksomheden ønsker at anvende sådanne.
    e) Medarbejderes habilitet så eventuelle interessekonflikter håndteres betryggende.
    f) Det interne kontrolsystem på kreditområdet.

g) Hvilken rapportering bestyrelsen skal modtage på kreditområdet, jf. nr. 38-43.
h) Afvigelser og undtagelser fra hovedregler og grænser fastsat i kreditpolitikken, herunder
    i. betingelser for accept af afvigelser og undtagelser samt krav om kompenserende forhold,
    ii. særlige krav til godkendelsesproces og kriterier for krav om godkendelse af en beslutningstager på et højere niveau,
    iii. kriterier for hvordan og hvornår bestyrelsen skal involveres eller underrettes og
    iv. særlige krav til kontrol og overvågning.
i) Identifikation, vurdering og håndtering af risikoen for, at virksomhedens kreditgivning udnyttes i forbindelse med hvidvask og finansiering af terror. Ved fastlæggelse af principperne skal virksomheden blandt andet overveje risikoen, der er forbundet med særlige kundetyper, geografiske områder, produkttyper og distributionskanaler.
j) Løbende overvågning af kreditrisikoen, herunder udvælgelse af relevante kvalitative og kvantitative indikatorer på forhøjet kreditrisiko.

4) Bestyrelsen skal vurdere behovet for at fastsætte specifikke principper i kreditpolitikken, der gælder for forretningsenheder eller risikokoncentrationer, hvor kompleksiteten, omfanget eller andre særlige karakteristika taler for det. Bestyrelsen skal blandt andet vurdere behovet for specifikke principper for kreditgivning til projektfinansiering, ejendomsudlejning, shipping, landbrug og kapitalfonde m.v.
5) Hvis de faktiske forhold på de områder, der dækkes af virksomhedens kreditpolitik, afviger markant fra kreditpolitikken, skal bestyrelsen godkende en plan for nødvendige ændringer for at gennemføre den vedtagne kreditpolitik.

Bestyrelsens retningslinjer til direktionen på kreditområdet

6) Retningslinjerne til direktionen på kreditområdet skal udover opfyldelsen af de generelle krav i § 6 udmønte kreditpolitikken i konkrete retningslinjer til direktionen. Eksponeringer omfattet af § 6, stk. 3, nr. 2, kan ikke bevilges af andre end bestyrelsen. Tilsvarende gælder som udgangspunkt eksponeringer, som udgør over 2 pct. af virksomhedens kapitalgrundlag, medmindre bestyrelsen har fastsat en lavere grænse.
   Den del af eksponeringen, som bevilges med pant i ubetinget gode sikkerheder, indgår ikke i opgørelsen af 2 pct.-grænsen. Ubetinget gode sikkerheder består af indlån, garantier og kautioner stillet af stater, regioner eller kommuner, anfordringsgarantier fra pengeinstitutter, statsobligationer og real- og skibskreditobligationer samt pant i ejerboliger til helårsbrug indenfor maksimalt 50 pct. af dagsværdien.
   Forhøjelser af eksponeringer, hvor bestyrelsen indenfor de sidste 18 måneder har bevilget en eksponering, og hvor forhøjelsen maksimalt udgør 25 pct. af beløbet bevilget af bestyrelsen, er undtaget fra 2 pct.-grænsen.
   Hvis en grænse på 2 pct. medfører, at bestyrelsen ikke får et betryggende indblik i eksponeringernes samlede kreditkvalitet, skal bestyrelsen fastsætte en lavere grænse.
   Grænsen kan i større virksomheder, der har tilladelse til at anvende IRB-metoden til kapitaldækningsformål, sættes højere, hvis bestyrelsen får en rapportering om udviklingen i virksomhedens kreditrisici, som overstiger minimumskravene i nr. 38-43. For øvrige virksomheder kan grænsen ligeledes sættes højere, i det omfang eksponeringer over 2 pct. af virksomhedens kapitalgrundlag er ukomplicerede, som for eksempel privatkundeeksponeringer, eller hvor en grænse på 2 pct. vil medføre, at bestyrelsen skal bevilge uforholdsmæssigt mange eksponeringer. De virksomheder, der har en grænse over 2 pct., skal være særligt opmærksomme på, at rapporteringen på områderne nævnt i nr. 38-43 sammen med de eksponeringer, som bestyrelsen skal bevilge, rapporteringen fra den risikoansvarlige til bestyrelsen samt øvrige oplysninger om kreditrisici til bestyrelsen skal sikre, at bestyrelsen har et betryggende grundlag for at træffe de beslutninger, som fremgår af nr. 43. Dette omfatter beslutninger om forretningsmodellen, kreditpolitikken og retningslinjerne til direktionen samt direktionens opgavevaretagelse på kreditområdet.
7) Retningslinjerne til direktionen skal indeholde bestemmelser om:
    a) Størrelsen af de eksponeringer, som direktionen kan bevilge uden bestyrelsens deltagelse.
    b) Hvordan eksponeringen opgøres i henhold til retningslinjernes grænser.
    c) Direktionens beføjelser til at bevilge eksponeringer i presserende tilfælde (hastesager som efterfølgende forelægges bestyrelsen til efterretning).
    d) Beføjelser til at bevilge kreditlempelser, herunder akkord/moratorium, nedsat rente og omlægning af betalinger, samt til at frigive sikkerheder, fastsætte nedskrivninger på udlån, hensættelser på finansielle garantier, lånetilsagn og tabsafskrivninger (regnskabsmæssigt ophør med indregning).
    e) Grænsen for eksponeringer, som direktionen kan bevilge, men som efterfølgende forelægges bestyrelsen til orientering.

Årlig gennemgang af de væsentligste eksponeringer

8) Bestyrelsen skal i forbindelse med den årlige gennemgang af større aktiver og passiver, jf. § 6, stk. 3, nr. 3, gennemgå virksomhedens væsentligste eksponeringer. Bestyrelsen skal ved gennemgangen blandt andet vurdere risikoen og den

lagte strategi for den enkelte eksponering, herunder tage stilling til behovet for opfølgning. Ved gennemgangen skal bestyrelsen tillige vurdere, om foretagne nedskrivninger m.v. er tilstrækkelige.

Direktionens ansvar ved ændringer i kreditpolitikken

9) Direktionen skal sikre, at der ved bestyrelsens beslutning om ændringer i kreditpolitikken, jf. nr. 1-5, sker en betryggende indførelse heraf i virksomhedens organisation, herunder i virksomhedens forretningsgange, risikostyring, interne kontroller og rapportering.

Funktionsadskillelse på kreditområdet

10) På kreditområdet skal der, jf. § 11, som hovedregel være etableret funktionsadskillelse mellem på den ene side en person, grupper af personer og organisatoriske enheder med ansvar for bevilling og etablering af kreditfaciliteter og på den anden side en person, grupper af personer og organisatoriske enheder med ansvar for kontrol og rapportering. Hvis virksomheden er et SIFI eller G-SIFI, skal opgørelse af og beslutning om nedskrivninger og hensættelser også som udgangspunkt foretages af en person, grupper af personer eller organisatoriske enheder, der ikke har medvirket ved bevilling af kreditfaciliteten. Der er ikke krav om funktionsadskillelse på direktionsniveau.
11) Det primære ansvar for kreditrisikoen på en eksponering skal være placeret hos en person eller en organisatorisk enhed igennem hele eksponeringens løbetid.
12) Hvis der, jf. § 11, stk. 3, ikke opretholdes funktionsadskillelse på kreditområdet, skal virksomhedens kompenserende foranstaltninger omfatte uafhængige kontroller udført af en person, gruppe af personer eller organisatorisk enhed udenfor kreditområdet.
13) Virksomheden skal sikre, at kvaliteten af uafhængige kontroller som kompenserende foranstaltning er betryggende. Det indebærer for eksempel, at de uafhængige kontroller skal udføres af personer med indgående erfaring på kreditområdet.
14) Uafhængige kontroller af kreditområdet kan være stikprøvebaseret, hvis virksomheden kan godtgøre, at stikprøverne er repræsentative og tilvejebringer en høj grad af sikkerhed for, at opgavevaretagelsen er betryggende givet den valgte organisering af området.
15) En virksomhed, hvor det henset til virksomhedens begrænsede størrelse ikke er muligt at etablere fyldestgørende uafhængige kontroller i virksomhedens organisation, kan etablere andre kompenserende foranstaltninger, hvis den kan godtgøre, at opgavevaretagelsen er betryggende. Det kan for eksempel omfatte en øget involvering af virksomhedens bestyrelse.

Forretningsgange på kreditområdet

Forretningsgange for bevilling af eksponeringer

16) Et pengeinstitut skal have forretningsgange, som fastlægger principper for bevilling af eksponeringer i overensstemmelse med dets kreditpolitik, dets ønskede risikoprofil og relevant regulering. Forretningsgangene skal sikre, at pengeinstituttet har en passende viden om risiciene, herunder kundernes økonomiske forhold og de stillede sikkerheder. Forretningsgangene skal desuden sikre, at kreditbeslutninger i tilstrækkeligt omfang baseres på robustheden af kundens fremtidige indtjening og likviditet og ikke i for høj grad baseres på stillede sikkerheder, medmindre tilbagebetalingen af lånet ifølge låneaftalen er baseret på salg af sikkerheder. Forretningsgangene skal dog samtidig sikre, at risikoen i relevant omfang nedbringes ved, at pengeinstituttet tager sikkerheder, bl.a. i form af pant samt kautioner fra hovedaktionærer.
    a) Et betryggende beslutningsgrundlag ved bevillinger vil almindeligvis som minimum indeholde følgende elementer:
        i. Vurdering af robustheden af kundens fremtidige indtjening og likviditet samt kundens evne og vilje til at overholde indgåede forpligtelser, herunder ved en eventuel forværring af kundens økonomiske forhold.
        ii. For privatkunder oplysninger om bl.a. kundens reelle formue, gældsfaktor og rådighedsbeløb under forudsætning af traditionel fast forrentet finansiering med afvikling.
        iii. For privatkunder, der køber fast ejendom, oplysninger om kundens økonomi efter købet.
        iv. For erhvervskunder oplysninger om bl.a. kundens forretningsmodel, strategi, kompetencer inden for forretningsområdet, risikovillighed, afhængighed af nøglepersoner, kunder, leverandører m.v., nuværende og skønnede fremtidige indtjenings- og likviditetsforhold samt de reelle kapitalforhold og relevante koncernsammenhænge.
        v. Beskrivelse og vurdering af stillede sikkerheder.
        vi. Oplysninger om, hvordan eksponeringen skal tilbagebetales og forrentes.

vii. Analyse af kundens muligheder for at overholde en hurtigere tilbagebetaling.
viii. Analyse af kundens følsomhed over for rentestigninger, hvis kunden i væsentligt omfang har eller ønsker variabel rente.
ix. Analyse af kundens følsomhed over for ændrede valutakurser, hvis kunden i væsentligt omfang har eller ønsker lån optaget i fremmed valuta.
x. Analyse af kundens eventuelle risici, der udspringer af miljømæssige, sociale og ledelsesmæssige forhold.
xi. Andre oplysninger, der er relevante for pengeinstituttets vurdering af eksponeringens risiko og afvikling.
xii. Pengeinstituttets samlede vurdering samt stillingtagen til, om den forventede indtjening står i et forsvarligt forhold til den risiko, pengeinstituttet påtager sig ved bevillingen.

b) I de situationer, hvor det er relevant, vil et beslutningsgrundlag almindeligvis også som minimum indeholde:
i. En samlet risikovurdering af ejendomsprojekter og øvrige projekter, for eksempel risikoen ved ledelse, styring, adgang til kompetente rådgivere og entreprenører, indhentelse af relevante tilladelser, finansiering, udførelse, færdiggørelse, udlejning og salg.
ii. For ejendomsprojekter og øvrige projekter kravene til udlejning eller salg, inden lånet udbetales.
iii. For ejendomsprojekter og øvrige projekter en vurdering af, om kunden stiller med tilstrækkelig egenfinansiering, inden lånet udbetales.
iv. Oplysninger om relevante kautionisters nuværende og skønnede fremtidige indtjenings- og likviditetsforhold samt de reelle kapitalforhold.
v. Krav om yderligere risikoreducerende foranstaltninger, herunder garantier, pantsætningserklæringer, transporter og andre vilkår og betingelser under hensyntagen til den samlede risikovurdering.

c) Der skal foreligge dokumentation af enhver bevilling af kreditfaciliteter i form af et beslutningsgrundlag, jf. litra a og b.

17) Pengeinstitutters forretningsgange for bevilling af eksponeringer vil desuden almindeligvis indeholde principper for:
a) I hvilke tilfælde pengeinstituttet stiller krav om sikkerhedsstillelse, herunder de typer af sikkerhedsstillelser, som pengeinstituttet kræver, for eksempel krav om pantsikkerhed ved finansiering af aktiver og kaution af hovedaktionærer.
b) Hvordan sikkerheder skal værdiansættes forsigtigt i lyset af de gældende markedsforhold, herunder principper for:
i. Valg af værdiansættelsesmetode i form af interne eller eksterne vurderingseksperter eller af statistiske modeller, indeksregulering eller anden standardiseret metode. Ved valg af metode skal pengeinstituttet tage hensyn til særlige egenskaber og kompleksitet ved forskellige typer af sikkerheder.
ii. Udpegning af interne og eksterne vurderingseksperter. Principperne skal sikre tilstrækkelig ekspertise og imødegå mulige interessekonflikter i forhold til udfaldet af værdiansættelsen eller af kreditbevillingen.
iii. Inddragelse af miljømæssige, sociale og ledelsesmæssige forhold, som må antages at påvirke værdien af sikkerheden.
c) I hvilket omfang anvendelsen af rating eller kreditscoring kan reducere kravene til det øvrige beslutningsgrundlag i de tilfælde, hvor pengeinstituttet anvender ratings eller kreditscoremodeller i forbindelse med kreditvurderingen af kunden.
d) Hvordan eksponeringerne opgøres, herunder konsolidering af eksponeringer med indbyrdes forbundne kunder, jf. nr. 3, litra b, samt opgørelse af eksponeringer i form af markeds- og modpartsrisici.
e) I hvilket omfang der fra kunden eller fra andre tilgængelige kilder skal indhentes bekræftelse af oplysninger, som indgår i bevillingsgrundlaget.
f) Hvordan dokumentation af kreditbeslutningen og udformning af aftalegrundlaget sikres, så de i videst muligt omfang imødegår potentielle misforståelser og fejlfortolkninger internt i pengeinstituttet og i forhold til kunden eller andre relevante parter.
g) Håndtering af afvigelser og undtagelser fra kreditpolitikkens hovedregler og grænser i overensstemmelse med nr. 3, litra h.

18) Et realkreditinstitut skal have forretningsgange, som fastlægger principper for bevilling af eksponeringer i overensstemmelse med dets kreditpolitik, dets ønskede risikoprofil samt relevant regulering. Forretningsgangene skal sikre, at virksomheden har en passende viden om risiciene ved eksponeringerne, herunder kundernes økonomiske forhold og de stillede sikkerheder. Forretningsgangene skal desuden sikre, at kreditbeslutninger i tilstrækkeligt omfang baseres på robustheden af kundens fremtidige indtjening og likviditet og ikke i for høj grad baseres på stillede sikkerheder, medmindre tilbagebetalingen af lånet ifølge låneaftalen er baseret på salg af sikkerheder.
a) Et betryggende beslutningsgrundlag ved bevillinger vil almindeligvis som minimum indeholde følgende:

i. Vurdering af robustheden af kundens fremtidige indtjening og likviditet samt kundens evne og vilje til at overholde indgåede forpligtelser, herunder ved en forværring af kundens økonomiske forhold.
ii. For privatkunder oplysninger om bl.a. kundens reelle formue, gældsfaktor samt rådighedsbeløb under forudsætning af traditionel fast forrentet finansiering med afvikling.
iii. For privatkunder, der køber fast ejendom, oplysninger om kundens økonomi efter købet.
iv. For erhvervskunder oplysninger om bl.a. kundens forretningsmodel, strategi, kompetencer inden for forretningsområdet, risikovillighed, afhængighed af nøglepersoner, kunder, leverandører m.v., nuværende og skønnede fremtidige indtjenings- og likviditetsforhold samt de reelle kapitalforhold og relevante koncernsammenhænge.
v. Beskrivelse og vurdering af stillede sikkerheder.
vi. Analyse af kundens eventuelle risici, der udspringer af miljømæssige, sociale og ledelsesmæssige forhold.
vii. Værdiansættelse af den faste ejendom i overensstemmelse med lovregler herom.
viii. Analyse af kundens følsomhed over for rentestigninger, hvis kunden i væsentligt omfang har eller ønsker variabel rente.
ix. Analyse af kundens følsomhed over for ændrede valutakurser, hvis kunden i væsentligt omfang har eller ønsker lån optaget i fremmed valuta.
x. Beskrivelse af anvendelse af rating og kreditscoring, hvor dette er relevant.
xi. Hvordan eksponeringerne opgøres, herunder konsolidering af eksponeringer med indbyrdes forbundne kunder, jf. nr. 3, litra b.
xii. I hvilke tilfælde virksomheden stiller krav om yderligere sikkerhedsstillelse, herunder kaution af hovedaktionær.
xiii. I hvilket omfang der fra kunden eller fra andre tilgængelige kilder skal indhentes bekræftelse af oplysninger, som indgår i bevillingsgrundlaget.
xiv. Hvordan dokumentation af kreditbeslutningen og udformning af aftalegrundlaget sikres, så de i videst muligt omfang imødegår potentielle misforståelser og fejlfortolkninger internt i virksomheden og i forhold til kunden eller andre relevante parter.
xv. Håndtering af afvigelser og undtagelser fra kreditpolitikkens hovedregler og grænser i overensstemmelse med nr. 3, litra h.

b) Der skal foreligge dokumentation ved enhver bevilling af kreditfaciliteter i form af et beslutningsgrundlag, jf. litra a.

19) I det omfang det er relevant for virksomheden, vil forretningsgangene for bevilling af eksponeringer også almindeligvis indeholde principper for:
a) Byggelånsfinansiering, herunder krav til et kvalificeret byggetilsyn, og hvordan betalinger af byggerater skal ske i takt med byggeriets færdiggørelse.
b) Finansiering af kapitalfonde m.v., herunder afgrænsning af hvilke typer af transaktioner virksomheden ønsker at deltage i, krav til kundens kreditværdighed, krav til sikkerhedsstillelse og andre vilkår.
c) Hvordan stop-loss klausuler fastsættes ved bevilling af eksponeringer, der indeholder sikkerhedsstillelse i værdipapirer eller positioner i afledte finansielle instrumenter.
d) Hvordan der tages højde for kreditrisikoen ved lån i fremmed valuta.
e) Miljømæssig bæredygtig finansiering, herunder kriterier for klassificering som bæredygtig, og hvordan det sikres, at låneformålet opfylder kriterierne, og at kunden har evnen og viljen til løbende at overholde dem.

20) En virksomhed kan som udgangspunkt kun finansiere ejendomme, hvor kundens hensigt med ejendommen hovedsageligt er udlejning til koncerneksterne parter, hvis ejendommen genererer positiv likviditet. Der skal her forudsættes traditionel fast forrentning og afvikling.
a) Virksomheden kan dog i særlige tilfælde finansiere ejendomme uden positiv likviditet, hvis virksomheden kan godtgøre, at det er kreditmæssigt forsvarligt. I disse tilfælde, herunder ved finansiering af udvikling og opførelse af denne type ejendomme, skal forretningsgangene indeholde principper for, hvilke kompenserende krav eller foranstaltninger der skal foreligge for at sikre, at finansieringen er kreditmæssig forsvarlig. De kompenserende krav eller foranstaltninger vil almindeligvis som minimum indeholde krav om, at
i. kunden er velindtjenende med en god likviditet og soliditet,
ii. virksomheden vurderer, at kunden har erfaring og kompetencer indenfor det pågældende område,
iii. kunden stiller med en passende egenfinansiering, og
iv. der foreligger sandsynliggørelse af, at likviditeten i ejendommen indenfor maksimalt 3 år bliver positiv, eller at ejendommen bliver solgt med fuld indfrielse af virksomhedens finansiering.

Punkt iv vil dog i en række tilfælde ikke gælde for finansiering af grundstykker. Virksomhedens samlede risiko ved finansiering af grundstykker skal være betryggende.

b) Virksomhedens vurdering af ejendommens evne til at generere likviditet vil typisk omfatte en vurdering af robustheden af ejendommens pengestrømme med følgende elementer under hensyntagen til ejendommens type, størrelse og beliggenhed samt lånets løbetid:
    i. Sammensætningen af lejerne og lejevilkår samt lejernes betalingsadfærd.
    ii. Mulighederne for genudlejning og effekten på pengestrømmene ved eventuel genudlejning på ændrede vilkår.
    iii. Behovet for vedligeholdelse og renovering af ejendommen.

Forretningsgange for løbende overvågning af eksponeringer og kreditrisici i øvrigt

21) Et pengeinstitut skal have forretningsgange, som fastlægger principper for den løbende overvågning af eksponeringer og kreditrisici i øvrigt. Forretningsgangene skal sikre, at pengeinstituttet på kunde- og porteføljeniveau har et opdateret overblik over udviklingen i pengeinstituttets påtagne kreditrisici. Pengeinstituttet vil dermed have et betryggende grundlag for at træffe beslutninger, som skal reducere kreditrisikoen.
    a) En betryggende overvågning af pengeinstituttets kreditrisici vil almindeligvis som minimum omfatte følgende elementer:
        i. Korrekt løbende klassifikation ud fra den skønnede kreditrisiko, jf. nr. 25, herunder en test én gang om året af, om pengeinstituttet er i stand til at risikoklassificere kunderne korrekt.
        ii. Identifikation, overvågning og håndtering af nødlidende eksponeringer og eksponeringer med kreditlempelse samt øvrige eksponeringer med højere risiko end ønsket, og at der fastlægges handlingsplaner for det videre forløb for disse eksponeringer.
        iii. Opfølgning på pengeinstituttet koncentrationer af risici, herunder koncentrationer indenfor specifikke brancher, koncentrationer indenfor specifikke typer af sikkerheder og koncentrationer i form af store eksponeringer, der for eksempel overstiger 2 eller 5 pct. af pengeinstituttets kapitalgrundlag.
        iv. Løbende overvågning af grænserne for renterisici fastsat af pengeinstituttet, jf. nr. 2, litra h.
        v. Løbende overvågning af at indtjeningen på portefølje-, delportefølje- og enkelteksponeringsniveau står i forsvarligt forhold til den risiko, som pengeinstituttet er udsat for.
        vi. Løbende overvågning af relevante kvantitative og kvalitative indikatorer på forhøjet kreditrisiko på portefølje-, delportefølje- og enkelteksponeringsniveau.
    b) En betryggende overvågning af pengeinstituttets enkelte eksponeringer vil almindeligvis som minimum omfatte følgende elementer:
        i. En forsvarlig overtræksadministration, der sikrer, at pengeinstituttet hurtigst muligt får identificeret og håndteret de kunder, hvor overtrækket eller restancen skyldes en forværring af kundens økonomi.
        ii. Både retningslinjer for en daglig behandling af overtræk og restancer og retningslinjer for en periodevis behandling af større eller gentagne overtræk og restancer, hvor gentagne overtræk og restancer som udgangspunkt er en indikation for kreditforringelse, jf. nr. 37 i bilag 10 til bekendtgørelse om finansielle rapporter for kreditinstitutter og fondsmæglerselskaber m.fl.
        iii. Gennemgang af regnskabsmateriale, årsopgørelser og budgetter m.v. fra kunder og kautionister m.fl., herunder en vurdering af om interne eller eksterne forhold væsentligt har ændret evnen til at servicere gælden igennem hele restløbetiden.
        iv. Løbende fyldestgørende, opdateret og forsigtig værdiansættelse af sikkerheder.
        v. Løbende opfølgning på at vilkår og betingelser for kreditgivningen er overholdt, og at kreditrisikoen er i overensstemmelse med pengeinstituttets kreditpolitik.
        vi. Identifikation af andre forhold, som kan have væsentlig betydning for kundens evne til at servicere gælden, herunder ledelsesmæssige, markedsmæssige, konkurrencemæssige og teknologiske forhold.
        vii. Løbende overvågning af likviditeten i udlejningsejendomme, jf. nr. 20, og risikoen for forværret likviditet, særligt hvor en væsentlig del af finansieringen er med variabel rente eller afdragsfrihed.
    c) Overvågning af eksponeringer med højere risiko end ønsket kræver pengeinstituttets særlige bevågenhed og vil almindeligvis som minimum omfatte følgende elementer:
        i. En handlingsplan, der konkretiserer pengeinstituttets fremadrettede tiltag over for kunden, med henblik på tabsminimering eller reduktion af pengeinstituttets risiko på kunden. En handlingsplan tager udgangspunkt i, om pengeinstituttet ønsker at fastholde eller afvikle eksponeringen med kunden. Typisk vil handlingsplanen indeholde en stillingtagen til anvendelse af kreditlempelser, realisering af sikkerheder, etablering af nye sikkerheder, udvidelse eller opsigelse af kundens eksponering, løbende opfølgning af kundens drift, mødefrekvens m.v.

ii. Retningslinjer for, hvornår pengeinstituttet skal indhente opdateret og revideret materiale om kundens økonomiske forhold samt hyppigheden af denne rapportering.
iii. En stillingtagen til kundens reelle kapitalforhold. Vurderingen omfatter både de aktiver, som pengeinstituttet har pant i, og andre aktiver, hvis disse har væsentlig betydning for kundens kapitalforhold.
iv. Retningslinjer for anvendelse og registrering af og opfølgning på kreditlempelser samt retningslinjer for vurdering af, hvorvidt anvendelsen af kreditlempelser vil føre til, at eksponeringen skal klassificeres som nødlidende. Anvendelsen af kreditlempelser skal så vidt muligt tilstræbe en varig løsning af kundens økonomiske vanskeligheder ved at kombinere kortvarige og længerevarende kreditlempelser. Ved en kundes åbenlyst forbigående økonomiske vanskeligheder, eller hvor det midlertidigt ikke er muligt at etablere en varig løsning, bør virksomheden overveje at anvende kreditlempelser med en tidshorisont på højst to år, forudsat at kunden forud for hændelsen har demonstreret evne og vilje til at overholde sine forpligtelser og til at samarbejde med pengeinstituttet.
v. Retningslinjer for ophør af eksponeringers klassifikation som nødlidende og for ophør af kreditlempelser.
vi. Overvågning af, at anvendte kreditlempelser medfører de ønskede forbedringer, og at der ikke anvendes gentagne kreditlempelser på den samme eksponering.

d) Det skal fremgå, hvordan den årlige gennemgang af eksponeringer, som ikke er omfattet af bestyrelsens gennemgang, jf. § 6, stk. 3, nr. 3, skal foregå, herunder hvilke eksponeringer der skal gennemgås, på hvilke niveauer i organisationen gennemgangen skal foregå, og hvordan rapportering af resultatet heraf skal ske.
e) I de situationer, hvor det er relevant, vil overvågningen af pengeinstituttets eksponeringer almindeligvis videre omfatte:
i. Overvågning af byggelånsfinansiering, herunder ved et kvalificeret byggetilsyn og ved betalinger af byggerater i takt med byggeriets færdiggørelse.
ii. Overvågning af enhver form for projekter, herunder af risikoen ved ledelse, styring, adgang til kompetente rådgivere og entreprenører, indhentelse af relevante tilladelser, finansiering, udførelse, færdiggørelse, udlejning og salg.
iii. Den løbende værdiansættelse af belånte pantebreve, herunder reguleringer for misligholdte pantebreve, overvågning af den fastsatte belåningsprocent, som er gældende for eksponeringen, samt pantebrevenes spredning, prioritetsstilling, udformning, øvrige indhold, omsættelighed og om den løbende administration af de belånte pantebreve.
iv. Overvågning af kunders positioner i værdipapirer, afledte finansielle instrumenter og lån i fremmed valuta, herunder overholdelse af stop-loss klausuler.

f) Forretningsgangene skal indeholde krav til hyppigheden for udførelsen af pengeinstituttets overvågning.

22) Et pengeinstitut, der har tilladelse til at udstede særligt dækkede obligationer, skal tillige have forretningsgange om løbende overvågning af LTV og om beregning og stillelse af supplerende sikkerhed i overensstemmelse med lovgivningen.
23) Et realkreditinstitut skal have forretningsgange, der fastlægger principper for den løbende overvågning. En betryggende overvågning af realkreditinstituttets eksponeringer vil almindeligvis indeholde følgende elementer:
a) Behandling af restancer.
b) Hvordan der skal ske opfølgning på enkelteksponeringer, herunder gennemgang af regnskabsmateriale, årsopgørelser og budgetter m.v. fra kunder og kautionister m.fl.
c) Løbende overvågning af LTV.
d) Løbende overvågning af værdien af pantsatte ejendomme i overensstemmelse med artikel 208, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber, herunder principper for:
i. Hyppigheden af overvågning af værdierne under hensyntagen til typen af ejendomme, ejendommens stand, dens værdi, kreditkvaliteten af lånet, belåningsgraden og udviklingen i markedsforholdene. Sikkerheder i boligejendomme skal overvåges mindst hvert tredje år, og sikkerheder i erhvervsejendomme skal overvåges mindst én gang om året.
ii. Metoder til overvågning. Valg af metode skal være afpasset typen af ejendom og ejendommens værdi. Metoderne skal omfatte en passende validering af estimerede værdier.
iii. Forhold der skal udløse en revurdering af sikkerheder på grundlag af overvågningen eller andre omstændigheder.

e) Realkreditinstituttets anvendelse af statistiske modeller, indeksregulering eller anden standardiseret metode til værdiansættelse og overvågning af værdien af sikkerheder. Principperne skal omfatte tilstrækkelig overvågning og styring af modelrisiko og modelusikkerhed.
f) Løbende overvågning af grænserne for renterisici fastsat af realkreditinstituttet, jf. nr. 2, litra h.

g) Beregning og stillelse af supplerende sikkerhed i overensstemmelse med lovgivningen.
h) Korrekt løbende klassifikation ud fra den skønnede kreditrisiko, jf. nr. 25, herunder en test én gang om året af, om realkreditinstituttet er i stand til at risikoklassificere kunderne korrekt.
i) Identifikation, overvågning og håndtering af nødlidende eksponeringer, eksponeringer med kreditlempelser samt øvrige eksponeringer med højere risiko end ønsket, og at der fastlægges handlingsplaner for det videre forløb for disse eksponeringer. Uanset realkreditinstituttets generelle valg af metode skal værdiansættelse af sikkerheder for nødlidende eksponeringer over 2 mio. kr. foretages af en intern eller ekstern vurderingsekspert mindst hvert tredje år for boligejendomme og mindst én gang om året for erhvervsejendomme.
j) Retningslinjer for anvendelse og registrering af og opfølgning på kreditlempelser samt retningslinjer for vurdering af, hvorvidt anvendelsen af kreditlempelser vil føre til, at eksponeringen skal klassificeres som nødlidende. Anvendelsen af kreditlempelser skal så vidt muligt tilstræbe en varig løsning af kundens økonomiske vanskeligheder ved at kombinere kortvarige og længerevarende kreditlempelser. Ved en kundes åbenlyst forbigående økonomiske vanskeligheder, eller hvor det midlertidigt ikke er muligt at etablere en varig løsning, bør realkreditinstituttet overveje at anvende kreditlempelser med en tidshorisont på højst to år, forudsat at kunden forud for hændelsen har demonstreret evne og vilje til at overholde sine forpligtelser og til at samarbejde med realkreditinstituttet.
k) Retningslinjer for ophør af eksponeringers klassifikation som nødlidende og for ophør af kreditlempelser.
l) Overvågning af, at anvendte kreditlempelser medfører de ønskede forbedringer, og at der ikke anvendes gentagne kreditlempelser på den samme eksponering.
m) Opfølgning på realkreditinstituttets koncentrationer af risici, herunder koncentrationer indenfor specifikke brancher, koncentrationer indenfor specifikke typer af finansierede ejendomme og koncentrationer i form af store eksponeringer, der for eksempel overstiger 2 eller 5 pct. af realkreditinstituttets kapitalgrundlag.
n) Løbende opfølgning på at vilkår og betingelser for kreditgivningen er overholdt, og at kreditrisikoen er i overensstemmelse med realkreditinstituttets kreditpolitik.
o) Løbende overvågning af likviditeten i udlejningsejendomme, jf. nr. 20, og risikoen for forværret likviditet, særligt hvor en væsentlig del af finansieringen er med variabel rente eller afdragsfrihed.

24) Virksomhedens forretningsgange for overvågning af kreditrisiko på porteføljе-, delporteføljе- og enkelteksponeringsniveau skal sikre, at en negativ udvikling eller en negativ afvigelse i forhold til virksomhedens ønskede risikoprofil uden unødig forsinkelse bliver rapporteret som minimum til det niveau i organisationen, som har ansvaret for at vurdere udviklingen og træffe beslutning om passende foranstaltninger.

Forretningsgange for risikoklassifikation af kunderne

25) En virksomhed skal have forretningsgange, som fastlægger principper for risikoklassifikation af virksomhedens kunder ved anvendelse af modeller eller på anden måde for porteføljer. Forretningsgangene skal sikre, at virksomheden risikoklassificerer sine kunder korrekt, hvilket medvirker til, at virksomheden har et overblik over de kreditrisici, der er forbundet med dens kunder.
For porteføljer, der ikke er omfattet af en IRB-tilladelse fra Finanstilsynet, vil forretningsgange for risikoklassifikation af virksomhedens kunder almindeligvis som minimum indeholde følgende elementer:
a) For de virksomheder, der ikke anvender modeller til klassifikation af kunderne: Angivelse af de karakteristika, der kendetegner kunder med forskellig type bonitet. Dette omfatter som minimum en klassifikation svarende til Finanstilsynets karaktersystem.
b) For de virksomheder, der anvender modeller til klassifikation af kunderne: Præcise beskrivelser af såvel model som vedtagne regelsæt, herunder hvilken skala der beskriver kundernes klassifikation.
c) Retningslinjer, der sikrer, at virksomhedens klassifikation af kunderne ikke giver et for positivt billede af risikoen.
d) Retningslinjer, der sikrer, at virksomhedens løbende kontrol og regelmæssige tests af klassifikationen er grundige og veldokumenterede.

Særligt om forretningsgange i forbindelse med belåning af fast ejendom

26) Et pengeinstitut, som belåner fast ejendom, herunder ejendomsprojekter og pantebreve, skal have forretningsgange herfor. Forretningsgangene skal tage højde for de reduktioner i værdierne, som kan forekomme. Dette kan ske ved fradrag (haircuts), som afspejler mulige fremtidige fald i værdierne. Herunder skal der tages højde for erfaringerne med forskelle i prisfald på forskellige typer ejendomme, bl.a. som følge af forskelle i robustheden af den likviditet, som ejendommene skaber. Forretningsgangene skal fastlægge principper for:
a) Forsigtig værdiansættelse af pant i fast ejendom.
b) Hvordan den forsigtige værdiansættelse af pant i fast ejendom opgøres, og hvilke aktuelle oplysninger der som minimum skal være til stede i virksomheden og indgå i vurderingen, herunder angående:

i. Ejendommens adresse, postnummer samt ejendomskategori, herunder en kort beskrivelse af ejendommen (evt. BBR meddelelse).
ii. Bygningsarealer (fordeling på bolig, kontor, lager, butik m.v.).
iii. Ejendommens stand og beliggenhed. Ved bevilling af nye lån skal værdiansættelsen være baseret på en indvendig og udvendig besigtigelse af ejendommen. Forretningsgangene kan dog tillade, at boligejendomme i områder, hvor ejendomsmarkedet er veldefineret og gennemskueligt, ved bevilling af nye lån kan værdiansættes af en vurderingsekspert med udgangspunkt i en statistisk model, indeksregulering eller anden standardiseret metode og uden besigtigelse af ejendommen. Ved bevillinger af mindre, nye lån, hvor pantets værdi ikke er afgørende for bevillingen, kan forretningsgangene også tillade, at indvendig og udvendig besigtigelse undlades. Værdiansættelsen skal indeholde passende fradrag for usikkerheden som følge af den manglende besigtigelse.
iv. Den løbende drift på udlejningsejendomme, herunder bruttoleje, nettoleje, afkastkrav, risikoen for lejenedsættelser, risikoen for yderligere tomgang samt aktuelle og forventede fremtidige driftsomkostninger.
v. Omkostninger til nødvendige investeringer.
vi. Seneste købsdato og handelspris.
vii. Realiserede salgspriser for sammenlignelige ejendomme.
viii. Aktuel og reel handelspris svarende til den pris, som ejendommen skønnes at kunne sælges til ved en aftale mellem en salgsinteresseret ejer og en uafhængig, villig køber på normale handelsvilkår.
ix. Skønnede salgsomkostninger.
x. Foranstående prioriteter i form af aktuel restgæld og lånevilkår.

c) Pengeinstituttets vurdering af risikoen for mulige fremtidige fald i ejendommens værdi, bl.a. i lyset af robustheden af den likviditet, som ejendommen skaber.
d) Hvilke typer af omkostninger der skal fradrages ved realisation af sikkerheder i fast ejendom.
e) Løbende overvågning af værdien af pantsatte ejendomme i overensstemmelse med artikel 208, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber, herunder principper for:
i. Hyppigheden af overvågning af værdierne under hensyntagen til typen af ejendomme, ejendommens stand, dens værdi, kreditkvaliteten af lånet, belåningsgraden og udviklingen i markedsforholdene. Værdien af sikkerheder i boligejendomme skal overvåges mindst hvert tredje år, og værdien af sikkerheder i erhvervsejendomme skal overvåges mindst én gang om året.
ii. Metoder til overvågning. Valg af metode skal være afpasset typen af ejendom og ejendommens værdi. Metoderne skal omfatte en passende validering af estimerede værdier.
iii. Hvad der skal udløse en revurdering af sikkerheder på grundlag af overvågningen eller andre omstændigheder.
f) Pengeinstituttets anvendelse af statistiske modeller, indeksregulering eller anden standardiseret metode til værdiansættelse og overvågning af værdien af sikkerheder. Principperne skal omfatte tilstrækkelig overvågning og styring af modelrisiko og modelusikkerhed. I tillæg til kravene i artikel 208, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber skal værdiansættelsen for nødlidende eksponeringer over 2 mio. kr. foretages af en intern eller ekstern vurderingsekspert mindst hvert tredje år for boligejendomme og mindst én gang om året for erhvervsejendomme.
g) Løbende overvågning af belåningsprocenten ved belåning af pantebreve i fast ejendom, krav til pantebrevenes spredning, prioritetsstilling, udformning, øvrige indhold og omsættelighed samt bestemmelser om en betryggende løbende administration af de belånte pantebreve.

Krav til håndtering af et særligt stort omfang af nødlidende eksponeringer

27) Senest når en virksomheds andel af nødlidende udlån udgør 5 pct. af de samlede udlån (opgjort som regnskabsmæssige bruttoværdier), skal den vedtage og gennemføre en strategi med en tidsplan for nedbringelse af nødlidende eksponeringer. Kravet gælder ved opgørelse af andelen på individuelt, delkonsolideret eller konsolideret niveau og anvendes på de enheder, hvor andelen af nødlidende udlån udgør 5 pct. eller mere, eller hvis virksomheden bliver pålagt krav herom fra Finanstilsynet. Gennemførelsen af strategien skal tage hensyn til relevante regler for forbrugerbeskyttelse. Ved fastlæggelse af strategien skal virksomheden forholde sig til følgende elementer:
a) Årsager til omfanget af nødlidende eksponeringer.
b) Inddeling af nødlidende eksponeringer i homogene grupper, som kan fremme målrettede indsatser.
c) Erfaringer med hidtil anvendte foranstaltninger, herunder kreditlempelser, og effektiviteten af dem.

d) De ressourcer, kompetencer, systemer, procedurer, m.v., som er nødvendige for at gennemføre strategien, herunder til
    i. tidlig identifikation af nødlidende eksponeringer,
    ii. anvendelse af og opfølgning på kreditlempelser,
    iii. værdiansættelse af sikkerheder,
    iv. inddrivelse, retslige procedurer og tvangsrealisationer,
    v. håndtering af aktiver, som virksomheden har overtaget som led i inddrivelsen,
    vi. opgørelse af nedskrivninger og tabsafskrivninger og
    vii. overvågning og rapportering.
e) De økonomiske, markedsmæssige, retslige og andre vilkår, som er af væsentlig betydning for at fastlægge mål for strategien og for at gennemføre den.
f) Behovet for opdeling af strategiens mål og indsatser på kort sigt (1 år), mellemlang sigt (1-3 år) og i relevant omfang også på lang sigt (over 3 år).
g) De regnskabsmæssige, kapitalmæssige og likviditetsmæssige konsekvenser af strategiens gennemførelse.

28) Strategien, inklusive dens mål og plan for gennemførelse, skal godkendes af bestyrelsen. Bestyrelsen skal revurdere strategien mindst én gang om året på grundlag af en rapport om fremdriften i nedbringelse af omfanget af nødlidende eksponeringer i forhold til de fastsatte mål.
29) Hvis virksomheden konstaterer, at gennemførelse af strategien ikke vil medføre den ønskede nedbringelse af nødlidende eksponeringer indenfor den planlagte tidshorisont, skal dette i fornødent omfang afspejles i den anvendte praksis for opgørelse af nedskrivninger og tabsafskrivninger.
30) Strategien og dens gennemførelse skal i relevant omfang indarbejdes i virksomhedens generelle ledelse, styring, kontroller, overvågning og rapportering, så strategiens konsekvenser inddrages i relevante sammenhænge, og der sikres fornøden fokus på dens gennemførelse.
31) Under hensyntagen til nr. 30 samt til virksomhedens størrelse og kompleksitet skal virksomheden overveje etablering af særlige enheder eller andre organisatoriske tiltag, som kan fremme strategiens gennemførelse. Virksomhedens eventuelle tiltag skal ske under hensyntagen til bestemmelser om kontroller, imødegåelse af potentielle interessekonflikter og sikring af funktionsadskillelse.

Risikostyring på kreditområdet

Risikoansvarlig og risikostyringsfunktion

32) Den risikoansvarlige skal udover de generelle krav i bilag 7 overvåge, at der i virksomheden sker en forsvarlig styring af kreditrisiciene, herunder overvåge, at:
    a) Bevilling af eksponeringer foregår på betryggende vis i overensstemmelse med kreditpolitikken.
    b) Der løbende sker en vurdering af, om der i virksomheden er tilstrækkelige ressourcer, viden og it-systemer m.v. til en betryggende opfølgning på og håndtering af virksomhedens kreditrisici.
    c) Der sker en rettidig identifikation af nødlidende eksponeringer og eksponeringer med kreditlempelser samt øvrige eksponeringer med en højere risiko end ønsket, og at der fastlægges handlingsplaner for det videre forløb for disse eksponeringer.
    d) Der sker en konstatering af indikation for kreditforringelse, en opgørelse af nedskrivningsbehovet samt tabsafskrivning, i overensstemmelse med regnskabsreglerne.
    e) Der sker en rettidig og korrekt klassifikation af virksomhedens eksponeringer, herunder en test minimum én gang om året af, om virksomheden er i stand til at risikoklassificere kunderne korrekt.
    f) Der løbende foretages en forsvarlig opfølgning på enkelteksponeringer, herunder særligt (hvor relevant), at der:
        i. Sker en rettidig behandling af overtræk og restancer.
        ii. Løbende foretages en opfølgning på værdiansættelsen af de stillede sikkerheder.
        iii. Sker en rettidig opfølgning på virksomhedens investeringseksponeringer.
        iv. Sker en vurdering af, hvorvidt anvendelsen af kreditlempelser vil føre til, at eksponeringen skal klassificeres som nødlidende.
        v. Løbende foretages en overvågning af byggelånsfinansiering og ejendomsudviklingsprojekter.
        vi. Løbende foretages en overvågning af udviklingen i belånte pantebreve.
    g) Der løbende foretages en vurdering af og stillingtagen til virksomhedens koncentrationer af risici.
    h) Der løbende sker overvågning af relevante kvalitative og kvantitative indikatorer på forhøjet kreditrisiko.
    i) Kravene til håndtering af et særligt stort omfang af nødlidende eksponeringer, jf. nr. 27-31 er overholdt.
    j) Der løbende foretages en vurdering af, om prisfastsættelsen af kreditrisici er forsvarlig i forhold til de påtagne kreditrisici.

33) Den risikoansvarlige skal udover de generelle krav i bilag 7 desuden overvåge:
    a) At virksomhedens interne kontrolsystem på kreditområdet er betryggende, herunder at virksomheden har forretningsgange, der beskriver virksomhedens interne kontrolsystem på kreditområdet.
    b) At der i virksomheden er iværksat de fornødne kontrolprocedurer på kreditområdet, jf. § 19 samt nr. 35-37 i dette bilag.
    c) At rapportering, der udarbejdes til bestyrelsen og på andre niveauer, giver et retvisende billede af virksomhedens kreditrisici og aktiviteter på kreditområdet.
    d) At der i virksomheden sker en årlig gennemgang af eksponeringer, som ikke er omfattet af bestyrelsens gennemgang i henhold til § 6, stk. 3, nr. 3.
    e) At der sker betryggende styring af modelrisiko, jf. bilag 3, nr. 13 og 14.
    f) At der løbende foreligger dokumentation af den risikoansvarliges arbejde på kreditområdet, herunder dokumentation om:
        i. Hvilke opgaver der løses af den risikoansvarlige eller risikostyringsfunktionen, og hvilke opgaver der løses af andre med rapportering til den risikoansvarlige.
        ii. Alle den risikoansvarliges væsentlige konklusioner og hvem de er rapporteret til.

Videregivelse af bevillingsbeføjelser

34) Videregivne kreditbeføjelser skal udover de generelle krav i § 18 som minimum indeholde:
    a) Konkrete grænser for, hvor store eksponeringer og hvilke produkttyper modtageren af beføjelsen må bevilge.
    b) Hvilke kundekategorier der er omfattet af bevillingsbeføjelsen.
    c) Hvordan eksponeringen opgøres i henhold til beføjelsens grænser.
    d) Beskrivelse af beføjelser til at bevilge eksponeringer i presserende tilfælde (hastesager som efterfølgende forelægges bestyrelsen til efterretning), herunder at antallet af disse bevillinger skal begrænses mest muligt.
    e) Konkrete grænser for beføjelser til bevilling af kreditlempelser, herunder akkord/moratorium, nedsat rente og omlægning af betalinger, samt bevilling af tabsafskrivninger, frigivelse af sikkerheder, fastsættelse af nedskrivninger på udlån og hensættelser på finansielle garantier og lånetilsagn.
    f) Regler for bevilling af eksponeringer med højere risiko end ønsket, jf. nr. 2, litra b, herunder udlån med nedskrivning og garantier med hensættelse.
    g) Konkrete grænser for, hvilke af de bevilgede eksponeringer m.v. der skal rapporteres til den, der afgiver beføjelsen.

Kontroller på kreditområdet

35) Virksomheden skal, jf. § 19, etablere uafhængige interne kontroller af alle væsentlige aktiviteter på kreditområdet og have forretningsgange herfor. Der skal som minimum foretages regelmæssig intern kontrol af, at:
    a) Kreditpolitikken efterleves af virksomhedens medarbejdere.
    b) Bevillingsbeføjelserne overholdes.
    c) Der er funktionsadskillelse eller betryggende kompenserende foranstaltninger.
    d) Bevillingsgrundlaget, jf. nr. 16-20, er til stede ved bevilling af kreditrisici.
    e) Eksponeringerne etableres korrekt og i overensstemmelse med kreditbevillingen, herunder med korrekte dokumenter, iagttagelse af sikringsakter m.v.
    f) Der sker betryggende værdiansættelse af sikkerheder.
    g) Der sker betryggende opfølgning på overtræk og restancer.
    h) Der sker betryggende identifikation og opfølgning på nødlidende eksponeringer, eksponeringer med kreditlempelser samt øvrige eksponeringer med en højere risiko end ønsket, herunder at der fastlægges handlingsplaner for det videre forløb af disse eksponeringer.
    i) Der sker regelmæssig vurdering af effekten af virksomhedens praksis for anvendelse af kreditlempelser og anvendelsen af de enkelte typer af kreditlempelser på aggregeret niveau og i enkeltsager.
    j) Der sker betryggende vurdering af, hvorvidt anvendelsen af kreditlempelser vil føre til, at eksponeringen skal klassificeres som nødlidende, og hvorvidt omfanget af nødlidende eksponeringer er vurderet forsigtigt.
    k) Risikoklassifikationen af kunderne er opdateret og klassificerer kunderne korrekt.
    l) Der sker betryggende opfølgning på virksomhedens koncentrationer af risici, herunder indenfor specifikke brancher, koncentrationer indenfor specifikke typer af sikkerheder og koncentrationer i form af store eksponeringer, der for eksempel overstiger 2 eller 5 pct. af virksomhedens kapitalgrundlag.
    m) Der foretages de nødvendige nedskrivninger og tabsafskrivninger på udlån samt hensættelser på garantier i overensstemmelse med regnskabsreglerne.
    n) Indsamlingen og behandlingen af data, som virksomheden anvender som grundlag for at vurdere risici og træffe kreditmæssige beslutninger og vurderinger, er betryggende.

36) Virksomhedens interne kontroller på kreditområdet kan ske ved stikprøvevise gennemgange, hvis disse giver tilstrækkelig sikkerhed for, at aktiviteterne på de kontrollerede områder sker på betryggende vis.
37) Virksomheden skal dokumentere de foretagne interne kontroller.

Rapportering til bestyrelsen på kreditområdet

38) Bestyrelsen skal mindst hvert kvartal modtage rapportering på kreditområdet. Mindst to af rapporteringerne i løbet af et år skal i fuldt omfang opfylde kravene i nr. 39-43, mens de øvrige rapporteringer kan være mindre omfattende.
39) Rapporteringen til bestyrelsen skal belyse, hvordan virksomheden efterlever de enkelte elementer i kreditpolitikken, jf. nr. 2-5, samt bestyrelsens retningslinjer til direktionen på kreditområdet, jf. nr. 7.
40) Rapporteringen skal give bestyrelsen et dækkende overblik over virksomhedens samlede kreditrisici og relevante opdelinger heraf samt overblik over udviklingen i kreditrisici over tid. Herunder skal rapporteringen beskrive de forhold, som fremadrettet kan have væsentlig betydning for udviklingen i virksomhedens kreditrisiko, herunder makroøkonomiske og demografiske forhold.
41) Så vidt det er muligt, skal der i rapporteringen til bestyrelsen mindst én gang om året være benchmarking til sammenlignelige pengeinstitutter eller realkreditinstitutter. I forbindelse hermed skal der, bl.a. baseret på Finanstilsynets offentliggjorte redegørelser, tages stilling til, i hvilket omfang disse institutter forekommer veldrevne.
42) I det omfang det er relevant for bestyrelsens forståelse af rapporteringen, gælder for alle dele heraf, at rapporteringen af talmateriale skal suppleres med understøttende beskrivelser, analyser og vurderinger. Dette gælder særligt ved indikationer af væsentligt forhøjede kreditrisici.
43) Formålet med rapporteringen er at bidrage til bestyrelsens grundlag for at træffe beslutninger om virksomhedens kreditrisici, herunder ændringer i forretningsmodellen, kreditpolitikken og retningslinjerne til direktionen. Tilsvarende skal rapporteringen bidrage til bestyrelsens grundlag for at vurdere, om direktionen løser opgaverne på kreditområdet tilfredsstillende.

Regnskabsmæssig praksis

44) Virksomheden skal have betryggende dokumentation for, hvordan nedskrivningerne indregnet under regnskabsposten "nedskrivninger på udlån og tilgodehavender m.v." er fremkommet. Udover kravene til dokumentation i bilag 10 til bekendtgørelse om finansielle rapporter for kreditinstitutter og fondsmæglerselskabet m.fl. skal betryggende dokumentation som minimum omfatte følgende:
    a) For alle udlån skal der foreligge en nedskrivningsberegning. Beregningen skal lede frem til den nedskrivning, der er indregnet i regnskabet, hvilket kan være en nedskrivning på nul.
    b) For de udlån, hvor der anvendes beregningsmodeller eller porteføljebaserede metoder til opgørelse af nedskrivninger, skal der foreligge beskrivelser af, hvordan de nedskrivninger, der er indregnet i regnskabet, er opgjort.
    c) For alle svage udlån, hvor virksomheden vurderer, at der ikke er indtrådt indikation for kreditforringelse, skal det fremgå, hvorfor der ikke er indtrådt en indikation. Svage udlån omfatter i denne forbindelse som minimum udlån svarende til Finanstilsynets bonitetskategori 2c.
    d) For alle udlån, hvor der er indtrådt indikation for kreditforringelse, og hvor virksomheden vurderer, at udlånet ikke er kreditforringet, skal det fremgå, hvorfor der ikke er indtrådt kreditforringelse.
    e) For hvert udlån, som virksomheden i forhold til sidste regnskabsaflæggelse vurderer ikke længere er kreditforringet, skal der foreligge dokumentation for, at den pågældende kreditforringelse ikke længere er til stede.
45) Der skal foreligge dokumentation for, at bestyrelsen og direktionen har forholdt sig til de resultater, der er fremkommet ved de anvendte beregningsmodeller. Herunder dokumentation for at bestyrelsen og direktionen har korrigeret i forhold til de beregnede nedskrivninger, hvis det vurderes, at modellerne ikke eller ikke fuldt ud tager højde for alle relevante forhold i overensstemmelse med regnskabsreglerne.

Bilag 2. Markedsrisiko

Anvendelsesområder og definitioner

1) Ved markedsrisici forstås rente-, valuta-, aktie-, og råvarerisici, herunder relaterede risici, der er forbundet med afledte finansielle instrumenter, for eksempel optionsrisici. Renterisici omfatter blandt andet renterisici på alle balance- og ikke-balanceførte poster, herunder også på fastforrentede ind- og udlån og fastforrentet finansiering. Renterisici omfatter også rentestrukturrisici.
2) Virksomheden skal have procedurer til at identificere, vurdere og styre risikoen som følge af ændringer i rentesatser, kurser, priser og øvrige mål og værdier på markedsrisikoområdet.
3) Virksomheden skal have procedurer til at identificere, vurdere, styre og afbøde de risici, som opstår som følge af potentielle ændringer af rentesatserne, der påvirker både den økonomiske værdi af en virksomheds kapitalgrundlag og nettorenteindtægterne fra virksomhedens ikke-handelsmæssige aktiviteter.
4) Virksomheden skal have procedurer til at vurdere og overvåge de risici, der opstår som følge af potentielle ændringer af kreditspænd, som påvirker både den økonomiske værdi af en virksomheds kapitalgrundlag og nettorenteindtægterne fra virksomhedens ikke-handelsmæssige aktiviteter.

Bestyrelsens opgaver og ansvar

Markedsrisikopolitikken

5) Politikken på markedsrisikoområdet skal udover de generelle krav i § 4, stk. 1, som minimum indeholde relevante overordnede anvisninger om,
    a) hvilke typer af risici virksomheden henregner til markedsrisikoområdet,
    b) det ønskede eller acceptable risikoniveau samlet og for de enkelte typer af markedsrisiko, eksempelvis ved angivelse af, om risikoen kan være lav, mellem eller høj,
    c) med hvilke formål de enkelte typer af markedsrisici må påtages, eksempelvis. risikoafdækning, aktiv risikotagning i forbindelse med investering af virksomhedens midler, herunder virksomhedens likviditetsplaceringer, eller handel for kunder, og
    d) principper for den organisatoriske ansvarsfordeling på markedsrisikoområdet, herunder for risikotagning, risikostyring, kontrol og rapportering.
6) Politikken skal tage højde for de markedsrisici, der følger af virksomhedens ind- og udlånsvirksomhed.
7) Politikken skal afspejle kompleksiteten af virksomhedens forretninger på markedsrisikoområdet, og skal samtidig afspejle markedsrisikoområdets betydning for virksomhedens samlede indtjening og risiko. Politikken skal særligt tage højde for de enkeltrisici, der kan have betydning for virksomhedens indtjening og solvens. Risici, der er ubetydelige i forhold til virksomhedens solvens og indtjening, kan afgrænses mere summarisk:
    a) Eksempelvis skal en stor virksomhed med omfattende og/eller komplekse forretninger på markedsrisikoområdet have en tilsvarende omfattende politik. For de typer af markedsrisici, som bestyrelsen har besluttet, at virksomheden kan tage, men som er ubetydelige for virksomheden, kan bestyrelsen nøjes med at fastsætte, at disse skal holdes på et minimum.
    b) En mindre virksomhed, der eksempelvis placerer likviditet i danske statsobligationer og lignende instrumenter og ikke har andre aktiviteter på markedsrisikoområdet, kan omvendt have en relativt simpel politik, der kun omfatter renterisikoen. Har virksomheden renterisiko udenfor handelsbeholdningen, for eksempel fastforrentede ind- og udlån, skal dette dog afspejles i politikken.

Bestyrelsens retningslinjer til direktionen på markedsrisikoområdet

8) På markedsrisikoområdet skal retningslinjerne opfylde generelle krav i § 7, og i det omfang det er relevant for den finansielle virksomhed, indeholde
    a) grænser for den finansielle virksomheds samlede rente-, valuta-, aktie- og råvarerisici,
    b) hvordan de enkelte risici opgøres, og hvordan de enkelte instrumenter medregnes ved opgørelsen,
    c) grænser for særlige risici, der knytter sig til komplekse eller usædvanlige produkter, herunder risici ved strukturerede produkter, eller til virksomhedens aktiviteter på markedsrisikoområdet i øvrigt som for eksempel optionsrisici, rentekurverisici, spændrisici m.v., medmindre omfanget af disse risici er af uvæsentlig størrelse,
    d) angivelse af, med hvilket formål værdipapirer, valutaer og afledte finansielle instrumenter må handles, for eksempel risikoafdækning, aktiv risikotagning i forbindelse med investering af virksomhedens midler, herunder virksomhedens likviditetsplaceringer, eller handel for kunder,
    e) hvilke valutaer eller grupper af valutaer der må handles eller tages positioner i, og til hvilke formål der må handles henholdsvis tages positioner,

f) hvilke typer af finansielle instrumenter der må handles eller tages positioner i, og
g) bestemmelser om, på hvilke markeder eller handelspladser samt i hvilke lande eller grupper af lande der må handles.

9) For realkreditinstitutter og pengeinstitutter med tilladelse til at udstede SDO'er skal politikken og retningslinjerne på markedsrisikoområdet udformes under iagttagelse af de relevante bestemmelser i bekendtgørelse om obligationsudstedelse, balanceprincip og risikostyring.

Interessekonflikter og funktionsadskillelse på markedsrisikoområdet

10) På markedsrisikoområdet skal der for at imødegå interessekonflikter som hovedregel være etableret funktionsadskillelse i overensstemmelse med § 11, stk. 1, nr. 2.
11) Afvikling, udarbejdelse af resultat- og risikoopgørelser, kontrol og rapportering kan udføres i samme enhed, jf. § 11, stk. 2, hvis virksomheden kan dokumentere, at dette kan anses for betryggende, jf. § 2.
12) For SIFI'er og G-SIFI'er samt for virksomheder med omfattende og/eller komplekse forretninger på markedsrisikoområdet skal der være etableret funktionsadskillelse på markedsrisikoområdet, jf. nr. 8. Er funktionsadskillelsen ikke etableret på direktionsniveau, skal virksomheden kunne dokumentere, at den etablerede funktionsadskillelse er betryggende, jf. § 2.
13) I mindre virksomheder, der kun har beskedne aktiviteter på markedsrisikoområdet, og hvor virksomhedens egen risikotagning er begrænset til placering af egne midler, herunder virksomhedens likviditetsplaceringer, i ikke-komplekse finansielle instrumenter, kan der være grundlag for ikke at etablere funktionsadskillelse på markedsrisikoområdet, jf. nr. 8. I sådanne tilfælde skal der indføres betryggende kompenserende foranstaltninger, jf. § 11, stk. 3, eksempelvis i form af uafhængige kontroller udført udenfor markedsrisikoområdet. Virksomheden skal kunne dokumentere, at kvaliteten af de kompenserende foranstaltninger er betryggende.
14) Funktionsadskillelse på markedsrisikoområdet indebærer også, at interne modeller til opgørelse af solvens til dækning af markedsrisiko, VaR-modeller, jf. Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og Europa-Parlamentets og Rådets forordning (EU) 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber, skal underlægges uafhængig validering og/eller kompenserende foranstaltninger. Det samme gælder interne modeller til opgørelse af markedsrisici eller til værdiansættelse af finansielle instrumenter.

Risikoopgørelser og opgørelser af gevinst/tab m.v.

15) Beregner virksomheden selv risici og gevinst eller tab samt værdier af finansielle instrumenter og andre poster med markedsrisici, skal direktionen sikre, at virksomheden har betryggende metoder hertil, herunder at det kan kontrolleres, at det sker korrekt.
16) Indhenter virksomheden risikoopgørelser og opgørelser af gevinst eller tab samt værdier af finansielle instrumenter og andre poster med markedsrisici fra eksterne parter, skal direktionen sikre sig, at de pågældende udfører opgaven på en betryggende måde. Direktionen skal desuden sikre sig, at virksomheden løbende evaluerer, om de anvendte kurser, parametre m.v., som er modtaget fra eksterne parter, er korrekte og dermed sikrer et retvisende billede af virksomhedens risici samt korrekt opgjorte regnskabsposter.

Konstatering af om risici ligger indenfor beføjelser

17) Det skal være muligt for disponerende medarbejdere at konstatere, om de handler, de har til hensigt at indgå, ligger indenfor deres beføjelser. Tilsvarende gælder ved kollektive beføjelser, hvor flere medarbejdere kan disponere indenfor en fælles beføjelse.
18) Nr. 15 gælder også, hvor medarbejdere disponerer i henhold til beføjelser modtaget fra kunder under en aftale om diskretionær porteføljepleje.

Kontroller på markedsrisikoområdet

19) Kontrollerne af virksomhedens markedsrisikobehæftede aktiviteter vil afhænge af omfanget og kompleksiteten på området. Kontrollerne skal omfatte
a) kontrol af om beføjelser overholdes. Samtlige grænser og samtlige personer, der har beføjelser, skal være omfattet af kontrollen. For virksomheder med en vis aktivitet på området skal der desuden foretages kontrol af, om beføjelser overholdes indenfor dagen, som minimum på stikprøvebasis, hvor stikprøvens størrelse og hyppighed skal afspejle aktivitetsomfanget,
b) om opgørelse af og rapportering om positioner og risici sker korrekt,

c) om investeringsgrænser i porteføljeplejeaftaler med kunder overholdes,
d) om handler indgås til korrekte kurser og priser,
e) om gevinst eller tab på markedsrisikobehæftede dispositioner for egen og for kunders regning opgøres korrekt,
f) afstemning af beholdninger af værdipapirer, finansielle instrumenter og konti, og
g) om de anvendte kurser, parametre m.v., som er modtaget fra eksterne parter, er korrekte og dermed sikrer et retvisende billede af virksomhedens risici.

20) For realkreditinstitutter og pengeinstitutter med tilladelse til at udstede SDO'er skal kontrollerne på markedsrisikoområdet udformes, så de sikrer en iagttagelse af de relevante bestemmelser i bekendtgørelse om obligationsudstedelse, balanceprincip og risikostyring.

Rapportering på markedsrisikoområdet

Rapportering om overholdelse af grænser

21) For realkreditinstitutter og pengeinstitutter med tilladelse til at udstede SDO'er skal rapporteringen på markedsrisikoområdet udformes med henblik på at sikre, at den også omfatter de grænser, der fremgår af bekendtgørelse om obligationsudstedelse, balanceprincip og risikostyring.

Rapportering til bestyrelsen

22) Rapporteringen på markedsrisikoområdet skal give bestyrelsen et dækkende overblik over virksomhedens væsentlige markedsrisici og understøtte bestyrelsens beslutninger på markedsrisikoområdet, herunder ændringer i forretningsmodellen, markedsrisikopolitikken og retningslinjerne til direktionen. Rapporteringen skal derudover bidrage til bestyrelsens grundlag for at vurdere, om direktionen løser opgaverne på markedsrisikoområdet tilfredsstillende.
23) Bestyrelsen skal mindst hvert kvartal modtage rapportering på markedsrisikoområdet. Dog kan rapporteringen i mindre virksomheder, der eksempelvis placerer likviditet i danske statsobligationer og lignende instrumenter og ikke har andre aktiviteter på markedsrisikoområdet, tilgå bestyrelsen med en lavere hyppighed. Rapporteringen om overholdelse af grænser for risikotagning fastsat i bestyrelsens retningslinjer skal foretages med den hyppighed, som bestyrelsen beslutter, men kan være en integreret del af rapporteringen efter 1. og 2. punktum.
24) Rapporteringen skal udformes på en sådan måde, at alle væsentlige markedsrisici og udviklingen indenfor disse fremhæves. I det omfang det er relevant for bestyrelsens forståelse af rapporteringen, gælder for alle dele heraf, at rapporteringen af talmateriale skal suppleres med understøttende beskrivelser, analyser og vurderinger. Dette gælder særligt i tilfælde af et ændret risikobillede på markedsrisikoområdet.
25) For SIFI'er, G-SIFI'er og virksomheder med omfattende og/eller komplekse forretninger på markedsrisikoområdet skal rapporteringen gøre det muligt for bestyrelsen at foretage en vurdering af, om indtjeningen på markedsrisikoområdet står mål med de markedsrisici, der er taget.
26) For virksomheder, der anvender interne modeller til opgørelse af solvens til dækning af markedsrisiko, VaR-modeller, jf. Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og Europa-Parlamentets og Rådets forordning (EU) 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber og/eller interne metoder til opgørelse af markedsrisici, skal rapporteringen omfatte et grundlag for bestyrelsens vurdering af de anvendte metoders pålidelighed.
27) For virksomheder, der anvender eksterne porteføljeforvaltere, skal den løbende rapportering til bestyrelsen, omfatte rapportering om midler og risici fra de midler, der forvaltes af den eksterne porteføljeforvalter.

Bilag 3. Operationelle risici

Anvendelsesområder og definitioner

1) Ved operationel risiko forstås risiko for tab som følge af uhensigtsmæssige eller mangelfulde interne procedurer, menneskelige fejl og systemmæssige fejl eller som følge af eksterne begivenheder, herunder juridiske risici og risici som følge af outsourcing. Omdømmerisiko og strategiske risici anses ikke for operationelle risici i denne bekendtgørelse, men skal i det omfang, det er relevant, behandles efter de samme principper som operationel risiko.
2) Ved modelrisiko forstås risiko for tab som følge af beslutninger, der hovedsagelig baseres på resultater fra interne modeller, på grund af fejl i udviklingen, gennemførelsen eller anvendelsen af sådanne modeller.
3) Ved risici som følge af outsourcing forstås risiko for tab som direkte eller indirekte kan henføres til virksomhedens eller leverandørens operationelle håndtering i forbindelse med outsourcing af processer, tjenesteydelser eller aktiviteter til en leverandør, herunder også ved koncernintern outsourcing.
4) Med tabshændelser forstås begivenheder, der kan medføre tab, har medført tab eller som kunne have medført tab, jf. nr. 1, for virksomheden.

Bestyrelsens opgaver og ansvar

Politik for operationel risiko

5) Med udgangspunkt i virksomhedens forretningsmodel, aktiviteter og organisering skal bestyrelsen udarbejde en politik for operationel risiko, som afspejler virksomhedens størrelse og kompleksitet og som, udover de generelle krav i § 4 skal indeholde:
    a) Identifikation af, hvilke operationelle risici virksomheden kan være udsat for, herunder risici, der forventes at indtræde med lav sandsynlighed, men med store potentielle tab til følge.
    b) Stillingtagen til, hvordan virksomhedens operationelle risici nedbringes til et acceptabelt niveau.
    c) Overordnede principper, som virksomheden skal indrettes efter med henblik på at holde operationelle risici på et for bestyrelsen acceptabelt niveau.
    d) Stillingtagen til
        i. operationelle risici som følge af outsourcing, herunder afhængighed af underleverandører,
        ii. operationelle risici knyttet til virksomhedens produkter og/eller kundegrupper,
        iii. omfanget af manuelle rutiner, for eksempel i forbindelse med kontrol og afvikling af handler,
        iv. integrationen og egnetheden af virksomhedens it-systemer,
        v. afhængighed af eksterne forhold,
        vi. operationelle risici knyttet til virksomhedens organisering, herunder manglende funktionsadskillelse, jf. § 11,
        vii. fysisk sikkerhed, og
        viii. modelrisiko.
    e) Overordnede principper for, hvordan virksomheden skal registrere og kategorisere tabshændelser.
    f) Overordnede principper for rapportering om tabshændelser til bestyrelsen, der skal sikre, at bestyrelsen til enhver tid har et tilstrækkeligt indblik i virksomhedens operationelle risici og udviklingen heri.
6) Bestyrelsen skal ved udarbejdelse af politikken, i det omfang det er relevant, forholde sig til
    a) om tidligere indtrufne hændelser kan gentage sig i fremtiden, og
    b) om medarbejdernes generelle kompetenceniveau er tilstrækkeligt.

Bestyrelsens retningslinjer til direktionen på området for operationel risiko

7) Bestyrelsens retningslinjer til direktionen, jf. §§ 6 og 7, skal indeholde følgende:
    a) Retningslinjer, for, hvordan operationelle tabshændelser identificeres.
    b) Konkrete metoder, der sikrer, at direktionen løbende vurderer de tabshændelser, der er indtruffet, eller som forventes at indtræffe med lav sandsynlighed, men med store tab til følge (halebegivenheder). Disse metoder kan for eksempel omfatte scenarioanalyser, der udarbejdes i samarbejde med de relevante ledere, eller for eksempel analyser af tabsregistreringer og risikoindikatorer.
    c) Retningslinjer for, hvordan direktionen skal registrere tabshændelser, herunder hvilke oplysninger vedrørende tabshændelserne der skal registreres, i hvilket omfang registrering skal foretages, samt eventuelle beløbsmæssige grænser for registreringen af hændelser, der har medført tab, såvel som hændelser, der kunne have medført tab.
    d) Retningslinjer for, hvordan virksomheden skal kategorisere tabshændelser.

e) Retningslinjer for rapportering af tabshændelser. Disse retningslinjer skal som minimum indeholde nærmere angivelse af
    i. eventuelle beløbsmæssige tærskelværdier for rapportering af tabshændelser, til bestyrelse, direktion og andre relevante medarbejdere, samt
    ii. rapporteringens indhold, omfang og frekvens.

Direktionens opgaver og ansvar

8) Direktionen skal indrette den finansielle virksomhed således, at operationelle risici begrænses, særligt at de styres indenfor de principper, der er fastsat af bestyrelsen, samt sikre, at alle relevante medarbejdere har kendskab til virksomhedens politik for operationelle risici.
9) Det påhviler direktionen at sikre, at
    a) oplysninger om tabshændelser i alle virksomhedens forretningsområder registreres i overensstemmelse med bestyrelsens politik for operationelle risici og retningslinjerne til direktionen,
    b) alle relevante medarbejdere har kendskab til virksomhedens politik for operationel risiko,
    c) alle medarbejdere har tilstrækkelig viden om operationelle risici til at løse deres opgaver på området,
    d) der er etableret effektive systemer og metoder til at identificere, registrere, kategorisere, rapportere og opbevare oplysninger om tabshændelser i virksomhedens væsentlige forretningsområder,
    e) der er forretningsgange for identificering, registrering og kategorisering af tabshændelser, og
    f) der er forretningsgange for opgørelse og rapportering til bestyrelsen om operationelle tabshændelser.
10) Direktionen skal på forhånd vurdere om og i hvilket omfang, beslutninger kan medføre operationelle risici, der er i strid med politikken og strategien på området fastsat af bestyrelsen. Dette gælder såvel for principielle beslutninger på de forretningsmæssige områder, herunder udførelsen af nye tjenesteydelser eller handel med nye finansielle instrumenter, som væsentlige beslutninger om virksomhedens drift og indretning. Dette kan kræve, at direktionen inddrager den risikoansvarlige, jf. § 16 samt bilag 7.
11) Direktionen skal løbende vurdere, om der er områder, hvor de operationelle risici skal søges minimeret, og i givet fald foretage de fornødne foranstaltninger.

Orientering af Finanstilsynet

12) Direktionen skal sikre, at virksomheden orienterer Finanstilsynet ved væsentlige tabshændelser.

Modelrisiko

13) En virksomhed, som anvender modeller til risikostyring, herunder opgørelse af risiko, prisfastsættelse af aktiver, klassifikation af kunder, vurdering af sikkerheder, automatisering af beslutninger m.v., skal have passende foranstaltninger til styring af de risici, som anvendelsen af disse modeller foranlediger. Foranstaltningerne skal som minimum omfatte:
    a) Virksomhedens definition af modeller.
    b) Et register over de modeller, som virksomheden anvender.
    c) Placering af det organisatoriske ansvar for udvikling, godkendelse, anvendelse, overvågning, validering og vedligeholdelse af modeller herunder ansvar for at vurdere resultater af overvågning og validering og træffe beslutninger om nødvendige foranstaltninger.
    d) Forretningsgange for udvikling, godkendelse, anvendelse, overvågning og validering af modeller.

14) Virksomheden skal inddrage følgende hensyn i tilrettelæggelsen af foranstaltninger, jf. nr. 13, under hensyntagen til omfanget og kompleksiteten af virksomhedens anvendelse af modeller:
    a) Passende ressourcer, viden og it-ressourcer til en betryggende udvikling, implementering, validering, vedligeholdelse og anvendelse af modellerne.
    b) Identifikation, håndtering og overvågning af risici forbundet med udvikling, implementering, vedligeholdelse og anvendelse af modellerne. Herunder skal virksomheden have foranstaltninger til at identificere og håndtere utilsigtede tendenser i modellernes output, som kan give anledning til uprækcis opgørelse af risikoen eller til uønsket risikotagning.
    c) Regelmæssig validering og backtest af modellernes output.
    d) Indsigt i antagelser, konsekvenser og begrænsninger ved anvendelsen af modellerne hos bestyrelsen, direktionen og andre relevante ledelsesniveauer under hensyntagen til deres opgaver og ansvar.
    e) Gennemsigtighed og sporbarhed igennem hele processen fra opsamling af data til input i modeller til anvendelse af modellernes output.
    f) Robusthed af kvaliteten i modellernes output ved ændrede niveauer af risiko.
    g) Robusthed af driften af modellerne over for driftsforstyrrelser, herunder passende nødplaner.

h) Et passende og veldefineret kontrolmiljø.
i) Kvaliteten af data, som modellerne anvender, herunder en klar placering af ansvaret for definitioner, dataopsamling, monitorering, kontroller og dokumentation.
j) Dokumentation af modellernes indbyggede metodik, antagelser og dataanvendelse samt af kontrol- og overvågningsforanstaltninger herunder versionsstyring, ændringslog og testmiljø.
k) Overholdelse af relevante regler om forbruger- og databeskyttelse.

Bilag 4. Likviditetsrisici

Anvendelsesområder og definitioner

1) Med likviditetsrisici forstås risikoen for, at
    a) virksomhedens omkostninger til likviditetsfremskaffelse stiger uforholdsmæssigt meget,
    b) manglende finansiering forhindrer virksomheden i at opretholde sin nuværende forretningsmodel, og
    c) virksomheden ultimativt ikke kan opfylde sine betalingsforpligtelser på grund af manglende finansiering.
2) Bestyrelsen og direktionen skal ved fastlæggelse af, hvilke foranstaltninger der er tilstrækkelige i henhold til § 2 tage hensyn til virksomhedens likviditetsmæssige kompleksitet, risikoprofil og forretningsmodel. Desuden skal virksomheden tage højde for virksomhedens betydning i både Danmark og de andre lande, hvor den udøver aktiviteter, herunder om virksomheden er udpeget som et systemisk vigtigt finansielt institut (SIFI) eller som en væsentlig filial.
3) For realkreditinstitutter, hvor der er en meget snæver betalingsmæssig sammenhæng mellem udlån og de bagvedliggende obligationer, der finansierer udlånet, vil de primære likviditetsrisici stamme fra refinansiering af finansieringen og eventuelle krav om supplerende sikkerhed som følge af efterfølgende lånegrænseoverskridelser. Dele af bekendtgørelsens specifikke krav vil derfor kunne opfyldes med forklarende henvisning til bekendtgørelsen om obligationsudstedelse, balanceprincip og risikostyring.
4) For pengeinstitutter med tilladelse til at udstede særligt dækkede obligationer skal likviditetspolitikken, retningslinjerne til direktionen, forretningsgangene, kontrollerne og rapporteringen på likviditetsområdet udformes under iagttagelse af bekendtgørelse om obligationsudstedelse, balanceprincip og risikostyring.

Bestyrelsens opgaver og ansvar på likviditetsområdet

Likviditetspolitikken

5) Bestyrelsen skal vedtage en skriftlig likviditetspolitik, jf. § 4, stk. 2, nr. 5. Likviditetspolitikken skal angive, hvilken likviditetsrisikoprofil bestyrelsen ønsker, at virksomheden skal have.
6) Bestyrelsen skal sikre, at likviditetspolitikken er tilpas forsigtig og til enhver tid sikrer en forsvarlig likviditet, herunder en forsvarlig likviditetsbuffer og en forsvarlig finansieringsstruktur. Hvis virksomheden vurderer, at de mulige beredskabstiltag, jf. nr. 16-20, har begrænset effekt, skal dette være afspejlet i virksomhedens risikoprofil.
7) Likviditetspolitikken skal indeholde:
    a) Principper for, hvordan virksomheden identificerer og opgør sine likviditetsrisici.
    b) Grænser for virksomhedens likviditetsrisici, herunder grænser for overdækning til liquidity coverage ratio (LCR), net stable funding ratio (NSFR) og eventuelle søjle II-likviditetskrav. Grænserne skal afspejle volatilitet og måleusikkerheder. Grænserne skal også tage højde for virksomhedens likviditetsstresstests.
8) Likviditetspolitikken skal indeholde principper for virksomhedens likviditetsbuffer, der omfatter følgende:
    a) Størrelsen af virksomhedens likviditetsbuffer.
    b) Sammensætningen af virksomhedens likviditetsbuffer, herunder hvilke aktiver der kan indgå i likviditetsbufferen.
    c) Principper der sikrer, at likviditetsbufferen er tilstrækkelig diversificeret og tager højde for koncentrationsrisici og valutarisici.
9) Likviditetspolitikken skal indeholde principper for virksomhedens finansieringsstruktur, der omfatter følgende:
    a) Grænser for anvendelse og koncentration af de forskellige finansieringstyper.
    b) Principper der sikrer en forsvarlig løbetid på finansiering.
    c) I relevant omfang grænser for finansiering i forskellige valutaer.
    d) Metoder til vurdering af indlånets stabilitet.
    e) I relevant omfang metoder til vurdering af indlånets geografiske koncentration.
10) Likviditetspolitikken skal indeholde principper for virksomhedens aktivbehæftelse, der omfatter følgende:
    a) Principper for anvendelsen af aktivbehæftelse.
    b) Principper for overvågning og styring af virksomhedens behæftelsesniveau og de medfølgende risici.
    c) Metoder til overvågning af andelen af ubehæftede aktiver, der kan anvendes som sikkerhed, hvis der opstår et uventet finansieringsbehov.
    d) Metoder til at skelne mellem
        i. aktiver, der er benyttet som sikkerhedsstillelse i forbindelse med afvikling og clearing af betalinger,
        ii. aktiver, der er behæftet i centralbanker, og

iii. andre behæftede aktiver.

11) Det skal fremgå af likviditetspolitikken, hvis der er juridiske eller andre begrænsninger på overførsel af aktiver inden for virksomheden, herunder om de forskellige former for aktiver anerkendes inden for likviditetsreglerne i de lande, som virksomheden opererer i.
12) Likviditetspolitikken skal indeholde principper for den organisatoriske ansvarsfordeling på likviditetsrisikoområdet, herunder for risikotagning, risikostyring, kontrol og rapportering, herunder så der sikres funktionsadskillelse i overensstemmelse med nr. 38-39.
13) Likviditetspolitikken skal indeholde procedurer for opfølgning på likviditetspolitikken, jf. § 5, stk. 1.
14) Likviditetspolitikken skal indeholde principper for den løbende rapportering til bestyrelsen på likviditetsområdet, jf. nr. 47-51.
15) Likviditetspolitikken skal revideres efter behov og mindst én gang om året.

Beredskabsplan

16) Bestyrelsen skal vedtage en beredskabsplan for fremskaffelse af likviditet og finansiering, der kan sættes i værk, hvis virksomheden får likviditetsmæssige udfordringer.
17) Bestyrelsen skal i beredskabsplanen som minimum
    a) tage stilling til, vurdere og vedtage tiltag for fremskaffelse af likviditet og finansiering, herunder foretage en prioritering af tiltagene og lave en vurdering af sandsynligheden for, at de enkelte tiltag kan gennemføres inden for den forventede tidshorisont, samt vurdere virksomhedens markedsadgang under stress og evne til at fremskaffe markedsfinansiering,
    b) definere, hvilke hændelser som medfører, at planen iværksættes, herunder definition af tidlige indikatorer for potentiel krisesituation, og
    c) definere, hvilke enheder der har ansvar for at iværksætte beredskabsplanen.
18) Tiltagene i beredskabsplanen skal afprøves mindst én gang om året, i det omfang det er muligt, og afprøvningen skal dokumenteres.
19) Bestyrelsen skal sikre, at virksomheden etablerer lokale beredskabsplaner, hvis virksomheden har juridiske enheder, hvor likviditeten ikke flyder frit mellem enhederne.
20) Beredskabsplanen skal revideres efter behov og mindst én gang om året.

Stresstest

21) Bestyrelsen skal vedtage metoder og antagelser til vurdering af institutspecifikke og markedsomfattende stress i form af likviditetsstresstests. De vedtagne metoder og antagelser skal dokumenteres.
22) Likviditetsstresstests skal i tilstrækkelig grad tage højde for
    a) institutspecifik stress, markedsomfattende stress og kombinerede alternative scenarier,
    b) forskellige perioder og grader af stress,
    c) at stressscenarier skal være usandsynlige, men ikke utænkelige scenarier,
    d) at stresstests er baseret på pengestrømme, der fremskrives,
    e) at antagelserne, der ligger til grund for stresstests, tages op til revision mindst én gang om året,
    f) aktivbehæftelse, ikke-balanceførte poster og andre eventualforpligtelser i relevant omfang, som potentielt kan føre til likviditetstræk.
23) Er virksomheden en modervirksomhed, skal virksomheden stressteste både på koncernniveau og soloniveau. De øvrige virksomheder i koncernen skal hver især stressteste i tilstrækkeligt omfang.
24) Likviditetsstresstests skal udføres regelmæssigt og minimum én gang månedligt og skal dokumenteres.
25) Bestyrelsen skal sikre, at udviklingen i likviditetsbufferen i stresstests overvåges, herunder, at det overvåges, hvor lang tid der går, før virksomheden ikke længere kan overholde lovgivningsmæssige likviditetskrav i sine stresstests.

Intern fordeling af likviditetsomkostninger

26) Bestyrelsen skal sikre, at virksomheden har principper for opgørelse og fordeling af likviditetsomkostninger i relevant omfang. Principperne skal dokumenteres. Er virksomheden udpeget som et systemisk vigtigt finansielt institut (SIFI), skal bestyrelsen sikre, at likviditetsrisici og andre risici indgår i den interne prisfastsættelse af finansielle produkter på forsvarlig vis.

Bestyrelsens retningslinjer til direktionen på likviditetsområdet

27) Bestyrelsens retningslinjer til direktionen skal udmønte likviditetspolitikken i konkrete retningslinjer, der skal indeholde bestemmelser om følgende:

a) Opgørelse af likviditet i henhold til gældende lovgivningsmæssige likviditetskrav og eventuelle søjle II-likviditetskrav.
b) Metoder til opgørelse af likviditetsrisici og tidshorisonter for opgørelserne. Opgørelserne af likviditetsrisici skal omfatte både balanceførte og ikke-balanceførte poster.
c) Under hvilke omstændigheder direktionen skal sikre bestyrelsens stillingtagen til, om den finansielle virksomhed skal fastholde de valgte risikoniveauer samt proceduren herfor.
d) Eventuelle yderligere grænser udover de i likviditetspolitikken fastsætte grænser.

Direktionens opgaver og ansvar på likviditetsområdet

28) Direktionen skal sikre, at der ved introduktion af nye produkter med likviditetsrisici og ved væsentlige ændringer i bestående produkter, der øger instituttets likviditetsrisici, jf. §§ 22 og 23, sker en betryggende indførelse heraf i virksomhedens organisation, herunder i virksomhedens forretningsgange, risikostyring, rapportering og interne kontroller.
29) Direktionens skal sikre, at LCR og volatiliteten i LCR overvåges og styres. Herunder skal direktionen sikre, at overvågningen giveret overblik over de poster, der giver anledning til væsentlige bevægelser i nettopengestrømmene.
30) Direktionen skal sikre, at udviklingen i likviditeten følges på daglig basis. Direktionen skal dokumentere, hvordan virksomheden opgør sit daglige behov for likviditet, og hvordan det følger likviditeten på daglig basis, så virksomheden overholder de fastsatte grænser for likviditetsrisici.
31) Direktionen skal sikre, at den daglige likviditetsstyring i tilstrækkelig grad tager højde for
    a) det aktuelle og det forventede likviditetsbehov inden for de kommende dage, herunder afviklingen af virksomhedens betalinger m.v. via andre kreditinstitutter,
    b) volatiliteten i likviditetsbehovet over tid,
    c) håndtering af pludseligt opståede likviditetsbehov som følge af forsinkede betalinger, it-fejl, menneskelige fejl m.v.,
    d) likviditetstræk fra eksterne kilder, såsom f.eks. kreditinstitutter og centralbanker,
    e) likviditetsbehovet i valutaer,
    f) eventuelle juridiske eller lovgivningsmæssige begrænsninger for overførsel af likviditet, og
    g) intradagslikviditetsrisiko og den løbende overvågning og kontrol af intradagslikviditeten.
32) Direktionen skal sikre, at virksomheden mindst én gang om året revurderer sit forventede finansieringsbehov.
33) Direktionen i virksomheder, som foranstalter revolverende securitiseringstransaktioner, der er underlagt en bestemmelse om indfrielse før tid, skal sikre, at de relevante organisatoriske enheder udarbejder likviditetsplaner med henblik på at tage højde for konsekvenserne af både indfrielse ved udløb og indfrielse før tid.

Forretningsgange og dokumentation på likviditetsområdet

Forretningsgange for den løbende opgørelse af likviditet og finansiering

34) En virksomhed skal have forretningsgange for den løbende identifikation, måling, styring, overvågning og rapportering af virksomhedens likviditetsrisici. I den udstrækning funktioner helt eller delvist er outsourcet, skal virksomheden have forretningsgange for håndtering af risici forbundet hermed.
35) Forretningsgangene skal udover de generelle krav i § 13 indeholde bestemmelser, som sikrer, at virksomheden, i det omfang det er relevant, tager hensyn til lovgivningsmæssige, administrative og operationelle begrænsninger, som påvirker mulighederne for at overføre likviditet og ubehæftede aktiver mellem enheder i forskellige lande.
36) Udover de nævnte krav i § 14 til dokumentation skal virksomheden have dokumentation for antagelser, metodevalg og processer i forbindelse med opgørelse af lovgivningsmæssige mål, herunder LCR og NSFR, såvel som bestyrelsesfastsatte og andre relevante likviditetsrisikomål, herunder dokumentation for,
    a) hvilke metoder virksomheden har valgt til opgørelse af virksomhedens likviditetsstrømme,
    b) fastlæggelse af et forventet tidspunkt for mulig realisering af aktiver i likviditetsbufferen, og hvordan aktiverne kan realiseres i overensstemmelse med virksomhedens forventninger,
    c) antagelser om tidspunktet for udløb for aktiver og passiver, som kan være både kontraktuelt bestemt og adfærdsbestemt, og
    d) løbende revurdering af opgørelserne for virksomhedens likviditetsstrømme, herunder validering af antagelserne om likviditetsstrømme.

Forretningsgange for opgørelse af modtagne og stillede sikkerheder

37) En virksomhed skal, i det omfang det er relevant, have forretningsgange for opgørelse af modtagne og stillede sikkerheder, der udover de generelle krav i § 13 som minimum skal indeholde følgende:
    a) Bestemmelser, der sikrer, at virksomheden identificerer og estimerer aktuelle og potentielle behov for at stille

sikkerheder og modtage sikkerheder over forskellige tidshorisonter.

b) Bestemmelser, der fastlægger, hvordan virksomheden skal beregne likviditetsværdien af virksomhedens nuværende og potentielle sikkerheder. Likviditetsværdien er den værdi, som virksomheden kan forvente at opnå, hvis en sikkerhed skal sælges eller belånes i en krisesituation, hvilket normalt ikke svarer til den regnskabsmæssige værdi.
c) Bestemmelser, der sikrer, at likviditetsværdien til enhver tid opgøres forsigtigt, og at virksomheden tager højde for, at det kan være meget vanskeligt at sælge eller belåne visse aktiver inden for en rimelig tidshorisont. Virksomheden skal ved beregning af likviditetsværdi anvende et relevant fradrag, hvor udsving i aktivets markedsværdi er et væsentligt element.
d) Bestemmelser, der sikrer, at virksomheden tager højde for eventuelle juridiske og operationelle begrænsninger i forbindelse med belåning eller salg af sikkerheder.

Funktionsadskillelse på likviditetsområdet

38) På likviditetsområdet skal der for at imødegå interessekonflikter som hovedregel være etableret funktionsadskillelse i overensstemmelse med § 11, stk. 1, nr. 2.
39) Virksomheder, der har et begrænset antal likviditetsdisponeringer på daglig basis og desuden har fyldestgørende instrukser og forretningsgange på likviditetsområdet, kan have en mindre omfattende organisering og kontrol af likviditetsområdet, idet virksomheden dog skal indføre betryggende kompenserende foranstaltninger, der skal sikre, at der ikke påføres virksomheden unødige risici eller tab, jf. § 11, stk. 3. Dette gælder dog ikke for SIFI'er og G-SIFI'er samt for virksomheder med omfattende og/eller komplekse forretninger på likviditetsområdet.

Risikostyring på likviditetsområdet

Risikoansvarlig og risikostyringsfunktion

40) Den risikoansvarlige skal, udover de generelle krav i § 16 og bilag 7, sikre, at der i virksomheden sker en forsvarlig styring af likviditetsrisiciene, og herunder sikre
    a) at virksomhedens likviditet, herunder intradagslikviditeten, løbende overvåges og kontrolleres,
    b) at beredskabsplanen afprøves mindst én gang om året i videst muligt omfang, jf. nr. 13,
    c) at de fastlagte grænser løbende revurderes,
    d) at niveau og udvikling i omfanget af aktivbehæftelse, samt typer af aktivbehæftelse og relaterede kilder til behæftelse, som for eksempel sikret finansiering, løbende overvåges,
    e) at mængden og kreditkvaliteten af ubehæftede, men behæftbare aktiver, overvåges, og
    f) at mængden og typen af eventuel yderligere behæftelse af aktiver i stressscenarier, overvåges.
41) Risikostyringsfunktionen skal validere virksomhedens likviditetsopgørelser og -antagelser, og valideringen skal dokumenteres.

Kontroller på likviditetsområdet

42) Virksomheden skal, jf. § 19, etablere uafhængige interne kontroller af alle væsentlige aktiviteter på likviditetsområdet. Der skal som minimum foretages regelmæssig intern kontrol af, at
    a) likviditetspolitikken efterleves af virksomhedens medarbejdere,
    b) bevillingsbeføjelserne overholdes, og
    c) rapporteringen i virksomheden er korrekt.
43) Virksomheden skal dokumentere de foretagne interne kontroller.

Rapportering på likviditetsområdet

Rapportering om overholdelse af grænser

44) Virksomheden skal foretage rapportering for alle fastsatte grænser på likviditetsområdet til dem, der har fastsat grænserne.
45) Frekvensen for rapportering om overholdelse af grænser afhænger af risikomålet og den likviditetsmæssige kompleksitet, risikoprofil og arbejdsområde.
46) En overskridelse af en grænse skal som udgangspunkt rapporteres senest dagen efter, at overskridelsen er konstateret.

Rapportering til bestyrelsen

47) Rapporteringen til bestyrelsen skal give bestyrelsen et fuldt overblik over virksomhedens likviditetsrisici og være fyldestgørende og præcis, jf. § 3, stk. 1, nr. 7.
48) Rapporteringen skal understøtte bestyrelsens grundlag for at træffe beslutninger om virksomhedens likviditetsrisici,

herunder ændringer i forretningsmodellen, likviditetspolitikken og retningslinjerne til direktionen. Tilsvarende skal rapporteringen bidrage til bestyrelsens grundlag for at vurdere, om direktionen løser opgaverne på likviditetsområdet tilfredsstillende.

49) Bestyrelsen skal orienteres om status på de i likviditetspolitikken fastsatte grænser på de ordinære bestyrelsesmøder, eller med en højere frekvens såfremt udviklingen i likviditetsrisici tilsiger det.
50) Bestyrelsen skal hurtigst muligt og uden ophør gøres bekendt med væsentlige fejl i likviditetsopgørelser.
51) Rapporteringen til bestyrelsen skal opfylde følgende:
    a) Udformes på en sådan måde at alle væsentlige likviditetsrisici og udviklingen inden for disse fremhæves.
    b) Opdateres løbende.
    c) Omhandle den faktiske og den forventede fremtidige udvikling i likviditeten. Virksomhedens forventninger til udviklingen i likviditeten skal enten opgøres kvantitativt ved hjælp af stresstests eller ved hjælp af kvalitative vurderinger.
    d) Dokumentere virksomhedens ledelsestiltag og beslutninger om ændringer i likviditetsforholdene.

Bilag 5. It-strategi, it-risikostyringspolitik og it-sikkerhedspolitik

Anvendelsesområde

1) Dette bilag indeholder bestemmelser om de forhold i bekendtgørelsen, der relaterer sig til informationsteknologi (it), herunder kommunikationsteknologi, informationssikkerhed samt risikostyring og kontrolforanstaltninger i forbindelse hermed.

2) Virksomheder omfattet af bilaget skal overholde bestemmelserne på en måde, der står i et rimeligt forhold til og tager hensyn til virksomhedens størrelse, dens interne organisation og anvendelse af en fælles datacentral. Desuden skal det stå i et rimelig forhold til arten, omfanget og kompleksiteten af, samt risikoen ved, de tjenesteydelser og produkter, som virksomheden leverer eller har til hensigt at levere.

Bestyrelsens opgaver og ansvar

It-strategi

3) Bestyrelsen har ansvaret for at sikre, at virksomheden har en egnet organisering og tilstrækkelig intern styring og kontrol af alle risici i forbindelse med dens it-anvendelse.

4) Den besluttede it-strategi skal være i overensstemmelse med virksomhedens overordnede strategi og fastlægge:

   a) Hvordan virksomhedens it skal udvikles, herunder organisering af it-arbejdet, ændringer i it-systemer og væsentlig afhængighed af tredjeparter.

   b) Klare it-sikkerhedsmålsætninger med fokus på it-systemer, it-tjenester, personale og processer.

5) Bestyrelsen skal løbende, og mindst én gang om året, revurdere og godkende it-strategien.

It-risikostyringspolitik

6) Bestyrelsen skal sikre, at virksomheden har en politik for it-risikostyring, jf. § 4, stk. 2, nr. 6. Politikken kan være en særskilt politik eller indgå som en del af øvrige relevante politikker. Politikken skal som minimum indeholde:

   a) It-risikotolerancen i overensstemmelse med virksomhedens overordnede risikotolerance.

   b) Metodekrav til identifikation af, hvilke it-risici virksomheden er og kan være udsat for, herunder risici knyttet til virksomhedens

      i. processer, aktiviteter, tjenester, systemer og data,

      ii. afhængighed af eksterne forhold, herunder leverandører,

      iii. organisering, herunder manglende funktionsadskillelse.

   c) Krav til at it-sikkerhedshændelser inddrages i risikostyringen.

   d) Krav til omfang og frekvens af risikovurderinger.

7) Bestyrelsen skal løbende, og mindst én gang om året, revurdere og godkende politikken for it-risikostyring.

It-sikkerhedspolitik

8) Bestyrelsen skal på baggrund af en samlet risikovurdering af virksomhedens anvendelse af it, herunder it-outsourcing, beslutte en it-sikkerhedspolitik.

9) It-sikkerhedspolitikken skal ud fra den ønskede risikoprofil på it-området indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden, herunder principper og regler for at beskytte fortroligheden, integriteten og tilgængeligheden af virksomhedens og kundernes data, og virksomhedens væsentlige forretningsfunktioner. Hvad der er væsentligt, afhænger bl.a. af virksomhedens størrelse, forretningsmodel, omfanget og kompleksiteten af virksomhedens it-anvendelse samt virksomhedens potentielle påvirkning af det finansielle system. It-sikkerhedspolitikken skal være i overensstemmelse med virksomhedens it-sikkerhedsmålsætninger, jf. nr. 4, litra b, og være baseret på de relevante resultater af risikovurderingen.

   Følgende forhold skal der som minimum tages stilling til:
   a) Organisering af it-arbejdet, herunder funktionsadskillelse mellem
      i. systemudvikling/-vedligeholdelse,
      ii. it-drift og
      iii. virksomhedens forretningsførelse.
   b) Regelmæssige risikovurderinger.
   c) Beskyttelse af systemer, data, maskinel og kommunikationsveje.
   d) Systemudvikling og vedligeholdelse af systemer.
   e) Projektstyring.
   f) It-driftsafvikling.
   g) It-hændelses- og problemstyring.
   h) Logning og overvågning.
   i) Funktionsadskillelse.
   j) Backup.
   k) Målsætning for forretningskontinuitet herunder beredskab og genopretning.
   l) Kvalitetssikring.
   m) Test og gennemgang af it-sikkerhed.
   n) Adgangsstyring.
   o) Principper for implementering af politikken i uddybende forretningsgange, m.v.
   p) Forholdsregler i tilfælde af brud på it-sikkerhedspolitik og sikkerhedsregler.
   q) Overholdelse af relevant lovgivning.
   r) Rapportering, kontrol og opfølgning.
   s) Eventuelle dispensationer fra it-sikkerhedspolitikken.
   t) Uddannelse i it-sikkerhed.
   u) Virksomhedens evt. status som operatør af en væsentlig tjeneste jf. nr. 70.

10) Politikken skal fastsætte krav til personale og konsulenter, processer og teknologi. Ligeledes skal politikken sikre fortrolighed, integritet og tilgængelighed af kritiske logiske og fysiske aktiver, ressourcer og følsomme data, ved opbevaring, overførsel og anvendelse.

11) Politikken skal formidles til alle relevante medarbejdere og konsulenter.

12) It-sikkerhedspolitikken skal indeholde en stillingtagen til behovet for etablering af flercenterdrift på alle forretningskritiske it-systemer.

13) Bestyrelsen skal regelmæssigt og mindst én gang om året revurdere og godkende it-sikkerhedspolitikken på baggrund af en opdateret samlet risikovurdering, der bygger på virksomhedens løbende vedligeholdte it-risikoregister, jf. nr. 107,

litra a. Bestyrelsen skal i den forbindelse vurdere, om it-sikkerhedspolitikken er tilstrækkelig til at sikre, at risici, som it-anvendelsen medfører og forventes at medføre, er på et acceptabelt niveau for virksomheden.

14) It-sikkerhedspolitikken skal i videst muligt omfang være uafhængig af anvendt teknologi.

Direktionens opgaver og ansvar
It-strategi

15) Direktionen skal sikre, at der opstilles handlingsplaner, der sikrer implementeringen af it-strategiens mål. Alle relevante medarbejdere, konsulenter og leverandører skal orienteres om disse handlingsplaner. Handlingsplanerne skal revideres minimum én gang om året for at sikre, at de er relevante og hensigtsmæssige.

16) Direktionen skal sikre, at der bliver identificeret og tildelt centrale roller og ansvarsområder for alle funktioner vedrørende it.

17) Direktionen skal sikre, at der føres kontrol med implementeringen af it-strategien.

Implementering af it-risikostyringspolitikken

Organisation og mål

18) Direktionen skal sikre, i henhold til nr. 7, at virksomhedens it-risikostyringspolitik efterleves, samt har passende rammer og forretningsgange for it-risikostyring og kontrol.

19) Direktionen skal sikre, at der er tilstrækkeligt og kvalificeret personale til løbende at understøtte virksomhedens operationelle it-behov og it-risikostyringsprocesser. Direktionen skal sikre, at det tildelte budget er tilstrækkeligt. Desuden skal direktionen sikre, at relevante medarbejdere, der beskæftiger sig med området, herunder personer med nøglefunktioner, modtager relevant uddannelse inden for it-risici, herunder it-sikkerhed, minimum én gang om året.

20) Direktionen skal sikre, at der bliver identificeret og tildelt centrale roller og ansvarsområder samt rapporteringskanaler for at sikre, at rammerne for it-risikostyring er effektive. Dette skal integreres fuldt ud i og tilpasses virksomhedens overordnede risikostyring.

21) Direktionen skal sikre, at it-risici bliver identificeret og styret. Den eller de it-funktioner, der er ansvarlig(e) for it-systemer, -processer og -sikkerhedsforanstaltninger, skal have passende processer og kontrolforanstaltninger til at sikre, at alle risici identificeres, analyseres, måles, overvåges, styres, rapporteres og ligger inden for virksomhedens it-risikotolerance, jf. nr. 6, litra a.

Identifikation af funktioner, processer og aktiver

22) Direktionen skal sikre identificering af forretningsfunktioner, roller og understøttende processer for at kunne vurdere betydningen af de enkelte elementer og deres indbyrdes afhængighed i forhold til it-risici og sikre, at kortlægningen holdes opdateret.

23) Direktionen skal sikre, at der udarbejdes og vedligeholdes en opdateret oversigt over it-aktiver, som understøtter forretningsfunktioner og understøttende processer. Dette skal som minimum sikre, at de it-aktiver, der understøtter kritiske forretningsfunktioner og -processer, håndteres tilstrækkeligt. Med forretningsfunktioner og understøttende processer forstås bl.a. it-systemer, it-tjenester, medarbejdere, konsulenter, tredjeparter og afhængigheder af andre interne og eksterne systemer og processer.

Klassificering og risikovurdering

24) Direktionen skal sikre, at de identificerede forretningsfunktioner, understøttende processer og it-aktiver klassificeres på basis af, hvor kritiske de er. Der skal være en klar ansvarsfordeling ift. it-aktiver.

25) For at definere hvor kritiske de identificerede forretningsfunktioner, understøttende processer og it-aktiver er, skal der som minimum tages hensyn til fortroligheds-, integritets- og tilgængelighedskrav.

26) Direktionen skal sikre, at det vurderes, om klassificeringen af it-aktiver og den relevante dokumentation er tilstrækkelig, når der foretages risikovurderinger.

27) Direktionen skal sikre, at it-risici, der påvirker de identificerede og klassificerede forretningsfunktioner, understøttende processer og it-aktiver, identificeres i overensstemmelse med deres kritikalitet. Risikovurderingerne skal foretages og dokumenteres minimum én gang om året. Sådanne risikovurderinger skal også foretages i forbindelse med større ændringer i infrastruktur, processer eller forretningsgange, der påvirker forretningsfunktionerne, de understøttende processer eller it-aktiverne. På baggrund heraf skal den samlede eksisterende risikovurdering, jf. nr. 13, af virksomheden opdateres.

28) Direktionen skal sikre, at trusler og sårbarheder, der er relevante for forretningsfunktioner, understøttende processer og it-aktiver, løbende overvåges. Desuden skal de risikoscenarier, der kan påvirke disse forretningsfunktioner, understøttende processer og it-aktiver, regelmæssigt gennemgås.

Mitigering af it-risici

29) På grundlag af risikovurderingerne skal direktionen sikre, at der træffes beslutninger om, hvilke foranstaltninger der skal implementeres for at mitigere identificerede it-risici til et acceptabelt niveau, og om det er nødvendigt at foretage ændringer i eksisterende forretningsprocesser, kontrolforanstaltninger, it-systemer og it-tjenester. Er det nødvendigt at foretage ændringer, skal det sikres, at risici i den mellemliggende periode mitigeres ved at træffe de nødvendige komplementerende foranstaltninger med henblik på at holde sig inden for virksomhedens it-risikotolerance jf. nr. 6, litra a.

30) Direktionen skal sikre, at der udarbejdes og implementeres foranstaltninger til at mitigere de identificerede it-risici samt beskytte it-aktiver i overensstemmelse med klassificeringen.

Rapportering

31) Direktionen skal sikre, at risikovurderinger i relevant omfang rapporteres tydeligt og rettidigt til direktionen og bestyrelsen.

Implementering af it-sikkerhedspolitikken

32) Direktionen skal sikre, at virksomhedens it-sikkerhedspolitik efterleves, og at denne uddybes i forretningsgange m.v.

33) Direktionen skal sikre, at der udarbejdes og implementeres forretningsgange, som understøtter, at ansvar, herunder ejerskab til it-processer og ressourcer, er placeret.

34) Direktionen skal sikre, at der udarbejdes og implementeres forretningsgange, som understøtter, at funktionsadskillelsen løbende bliver overvåget og revurderet.

35) Direktionen skal sikre, at der udarbejdes og implementeres forretningsgange, som understøtter, at der er kontrol med opretholdelse af det ønskede it-sikkerhedsniveau samt håndtering af eventuelle svagheder.

36) Direktionen skal sikre, at der udarbejdes og implementeres forretningsgange, som understøtter, at der er tilstrækkelige it-ressourcer.

Logisk sikkerhed

37) Direktionen skal sikre, at der bliver defineret, dokumenteret og implementeret forretningsgange for logisk adgangskontrol (identitets- og adgangsstyring). Forretningsgangene skal også omfatte kontrolforanstaltninger, som sikrer overvågning af uregelmæssigheder. Disse forretningsgange skal sikre, at virksomheden har en betryggende risikobaseret bruger- og rettighedsstyring, og som minimum indeholder følgende elementer, hvor udtrykket "bruger" også omfatter brugerkonti, der ikke er tildelt personer:

    a) "Need to know"-princippet, "least privilege"-princippet og "funktionsadskillelse": Virksomheden skal forvalte adgangsrettigheder til it-aktiver og deres støttesystemer efter "need to know"-princippet. Brugerne skal tildeles

minimumsadgangsrettigheder, der er strengt nødvendige for udførelsen af deres opgaver ("least privilege"-princippet), så virksomheden sikrer, at en bruger ikke tildeles kombinationer af adgangsrettigheder, som kan anvendes til at omgå kontrolforanstaltninger (princippet om "funktionsadskillelse"). Funktionsadskillelse i systemer og i tekniske miljøer skal være dokumenteret.

b) Brugeransvar: Virksomheden skal begrænse brugen af generiske og delte brugerkonti og sikre, at brugerne, som har udført handlinger i it-systemerne, kan identificeres.

c) Privilegerede adgangsrettigheder: Virksomheden skal sikre løbende kontrol og overvågning samt gennemføre stærke kontrolforanstaltninger i forhold til privilegeret systemadgang. For at opnå sikker kommunikation og reducere risikoen skal fjernadgang til kritiske it-systemer kun tildeles efter "need to know"-princippet, og når der anvendes stærke autentifikationsløsninger.

d) Logning af brugeraktiviteter: Alle relevante aktiviteter, og som minimum de aktiviteter der udføres af privilegerede brugere, skal logges og overvåges. Adgangslogs skal sikres, så uautoriseret ændring eller sletning forhindres, og skal opbevares i en periode, der står i et rimeligt forhold til kritikaliteten af de identificerede forretningsfunktioner, understøttende processer og it-aktiver. Virksomheden skal bruge disse oplysninger som led i identifikationen og undersøgelsen af uregelmæssige aktiviteter.

e) Adgangsstyring: Adgangsrettigheder skal gives, slettes, trækkes tilbage eller ændres rettidigt i overensstemmelse med foruddefinerede forretningsgange, som involverer dataejeren af de informationer, der gøres tilgængelige (ejeren af it-aktivet). Ved ophør af ansættelse skal adgangsrettighederne omgående trækkes tilbage.

f) Periodisk gennemgang af adgangsrettigheder: Adgangsrettighederne skal gennemgås regelmæssigt for at sikre, at brugerne ikke har for brede rettigheder, og at adgangsrettighederne slettes, når der ikke længere er behov for dem. Identificeres der ved gennemgangen uhensigtsmæssige eller risikofyldte adgange, skal det sikres, at der gennemføres kontrol- og opfølgningstiltag af, om adgangene har været anvendt uhensigtsmæssigt.

g) Autentifikationsmetoder: Virksomheden skal have tilstrækkeligt effektive autentifikationsmetoder. Autentifikationsmetoderne skal modsvare kritikaliteten af de it-systemer, oplysninger eller den proces, der gives adgang til. Dette skal som minimum omfatte komplekse passwords eller stærkere autentifikationsmetoder baseret på den relevante risiko.

h) Klassifikation: Virksomheden skal identificere og klassificere kritiske systemer og data i relation til rettighedsstyringen samt synliggøre risici herved. Ligeledes skal systemer og data løbende klassificeres, kritiske adgange på tværs af systemer skal identificeres, og kritiske systemadgange skal logges for at sikre en effektiv overvågning og rettidig sporing af uautoriseret aktivitet.

i) Kombination af roller og rettigheder: Virksomheden skal identificere roller, rettigheder og kombinationer heraf samt synliggøre risici forbundet hermed, herunder i hvilket omfang adgangstildelingen skal underlægges løbende kontrol og overvågning samt ansvaret herfor.

38) Applikationers adgang til data og it-systemer skal begrænses til det minimum, der er nødvendigt for at levere den relevante tjeneste.

Fysisk sikkerhed

39) Direktionen skal sikre, at fysiske sikringsforanstaltninger bliver defineret, dokumenteret og implementeret for at beskytte ejendomme, datacentre og følsomme områder mod uautoriseret adgang og klima- og miljøfarer.

40) Direktionen skal sikre, at fysiske adgange til it-systemer kun tillades for autoriserede personer. Tilladelse skal gives i overensstemmelse med den enkeltes opgaver og ansvarsområder samt begrænses til personer, der er tilstrækkeligt uddannet og overvåget. Fysiske adgangsrettigheder skal regelmæssigt gennemgås.

41) Foranstaltninger til beskyttelse mod klima- og miljøfarer skal stå i et rimeligt forhold til bygningernes betydning og kritikaliteten af den drift eller de it-systemer, der er placeret i bygningerne.

It-driftssikkerhed

42) Direktionen skal sikre, at der implementeres forretningsgange for at forebygge og minimere it-sikkerhedsproblemer. Disse forretningsgange skal omfatte alle relevante foranstaltninger for at modvirke sandsynlige risici under hensyn til virksomhedens størrelse, karakter og risikoprofil. Forretningsgangene skal som minimum, hvor relevant, forholde sig til nedenstående:

    a) Identifikation af potentielle sårbarheder, som skal vurderes og afhjælpes ved at sikre, at software og firmware er opdateret, herunder software, der anvendes af virksomhedens interne og eksterne brugere.

    b) Implementering af sikre standardkonfigurationer for alle netværkskomponenter og relevante systemer.

    c) Implementering af netværkssegmentering, systemer til at forebygge datatab (data loss prevention systems) og kryptering af netværkstrafik.

    d) Beskyttelse af enheder, hvormed brugere har adgang til systemer, herunder servere, arbejdsstationer og mobile enheder. Ligeledes skal det vurderes, om enhederne opfylder de sikkerhedsstandarder, der er fastlagt, før enhederne tilsluttes virksomhedens netværk.

    e) Sikring af at der er indført mekanismer til kontrol af software-, firmware- og dataintegritet.

    f) Kryptering af data ved opbevaring og overførsel.

43) Direktionen skal sikre, at det løbende vurderes, om ændringer i produktionsmiljøer påvirker sikkerhedsforanstaltningerne eller kræver, at yderligere foranstaltninger implementeres for at mitigere de hermed forbundne risici tilstrækkeligt. Disse ændringer skal indgå i virksomhedens formelle ændringsstyringsproces, som skal sikre, at ændringer risikovurderes, planlægges, testes, dokumenteres, godkendes og installeres korrekt, jf. nr. 85.

Sikkerhedsovervågning

44) Direktionen skal sikre, at forretningsgange udarbejdes og implementeres for at opdage og reagere på uregelmæssige aktiviteter, som kan påvirke virksomhedens informationssikkerhed. Som led heri skal der etableres løbende overvågning og effektive foranstaltninger for at kunne opdage og rapportere fysisk eller logisk indtrængen samt brud på fortroligheden, integriteten og tilgængeligheden af it-aktiver. Overvågningen skal som minimum omfatte:

    a) Relevante interne og eksterne faktorer, herunder forretningsfunktioner og administrative it-funktioner.

    b) Transaktioner til afsløring af tredjeparters eller andre enheders misbrug af adgang samt internt misbrug af adgang, jf. nr. 37.

    c) Potentielle interne og eksterne trusler.

45) Direktionen skal sikre, at der udarbejdes og implementeres forretningsgange og organisationsstrukturer for at identificere og løbende overvåge sikkerhedstrusler, som kan have væsentlig indflydelse på evnen til at levere tjenester. Den løbende udvikling i it-trusselsbilledet skal vurderes med henblik på at kunne identificere it-risici. Der skal implementeres opdagende kontrolforanstaltninger, og det skal kontrolleres, om der findes relevante nye sikkerhedsopdateringer for, som minimum, at identificere mulige informationslækager, skadelig kode samt andre sikkerhedstrusler og offentligt kendte sårbarheder i software og hardware.

46) Sikkerhedsovervågningen skal hjælpe virksomheden til at forstå hændelsen for at kunne identificere trends og understøtte opklaringen af hændelsen.

Test og gennemgang af it-sikkerhed

47) Direktionen skal sikre, at der udføres tests, gennemgange og vurderinger af informationssikkerheden for at sikre effektiv identifikation af sårbarheder i it-systemer og it-tjenester. Hvor det er relevant, skal der som minimum foretages gap-analyser i forhold til informationssikkerhedsstandarder samt gennemgange af overholdelse af regler. Desuden skal virksomheden ud fra en risikobaseret tilgang og best practices udføre kildekode-review, sårbarhedsvurderinger, penetrationstest, red team-øvelser, m.v.

48) Direktionen skal sikre, at der udarbejdes og implementeres krav til test af informationssikkerheden, så det sikres, at effektiviteten af informationssikkerhedsforanstaltningerne valideres. Virksomheden skal sikre, at disse krav tager højde for trusler og sårbarheder, som er identificeret gennem trusselsovervågning og risikovurderingsprocessen.

49) Kravene til test af informationssikkerheden skal sikre, at test:

    a) Udføres af uafhængige personer med tilstrækkelig viden, faglig kompetence og ekspertise i test af informationssikkerhedsforanstaltninger, og som ikke er involveret i udviklingen af virksomhedens informationssikkerhedsforanstaltninger.

    b) Omfatter sårbarhedsscanninger og penetrationstest, som står i et rimeligt forhold til det risikoniveau, der er identificeret i forretningsprocesser og -systemer.

50) Direktionen skal sikre, at der gennemføres løbende og gentagne test af sikkerhedsforanstaltningerne. Kritiske it-systemer skal testes mindst én gang om året. Ikke-kritiske systemer skal testes regelmæssigt og inden for en periode på minimum tre år.

51) Direktionen skal sikre, at der gennemføres test af sikkerhedsforanstaltninger i tilfælde af ændringer i infrastruktur, processer eller forretningsgange, og hvis der foretages ændringer på grund af større it-sikkerhedshændelser, jf. nr. 64. Der skal også gennemføres test som følge af lancering af nye eller væsentligt ændrede kritiske applikationer, der kan tilgås fra internettet.

52) Direktionen skal sikre, at resultaterne af de udførte sikkerhedstest bliver evalueret, samt at sikringsforanstaltninger opdateres i overensstemmelse hermed uden unødig forsinkelse, når der er tale om kritiske systemer.

53) For institutter, som udbyder betalingstjenester, skal testrammerne også omfatte sikringsforanstaltninger, der er relevante for:

    a) Betalingsterminaler og enheder, der anvendes til betalingstjenester.

    b) Betalingsterminaler og enheder, der anvendes til at autentificere betalingstjenestebrugeren.

    c) Enheder og software, som betalingstjenesteudbyderen leverer til betalingstjenestebrugeren for at generere/modtage autentifikationskoder.

54) På basis af de observerede sikkerhedstrusler og de foretagne ændringer skal der udføres test af scenarier, som omfatter relevante og forudsigelige potentielle angreb.

It-driftsstyring

55) Direktionen skal sikre, at it-driften forvaltes på grundlag af dokumenterede og implementerede forretningsgange. Disse skal definere, hvordan virksomheden driver, overvåger og kontrollerer it-systemer og -tjenester, og skal omfatte dokumentation af kritisk it-drift og vedligeholdelse af den opdaterede oversigt over it-aktiver.

56) Direktionen skal sikre, at it-driften er i overensstemmelse med forretningsmæssige krav. Virksomheden skal vedligeholde og forbedre effektiviteten af it-driften, herunder sikre at potentielle fejl som følge af udførelsen af manuelle opgaver minimeres.

57) Direktionen skal sikre, at der implementeres lognings- og overvågningsforretningsgange for kritisk it-drift for at gøre det muligt at opdage, analysere og rette fejl.

58) Direktionen skal sikre, at der føres en opdateret oversigt over it-aktiver herunder it-systemer, netværksudstyr, databaser osv. Denne skal indeholde konfigurationen af it-aktiverne og indbyrdes afhængigheder mellem de forskellige it-aktiver for at kunne gennemføre konfigurations- og ændringsstyringsprocesser.

59) Oversigten over it-aktiver skal være tilstrækkelig detaljeret til at sikre hurtig identifikation af et it-aktiv, dets placering, sikkerhedsklassifikation og ejerforhold. Indbyrdes afhængigheder mellem it-aktiver skal dokumenteres med henblik på at bidrage til styring af it-sikkerhedshændelser, herunder cyberangreb.

60) Direktionen skal sikre, at it-aktivernes livscyklus overvåges og styres for at sikre, at de løbende opfylder og understøtter forretnings- og risikostyringskrav. Virksomheden skal overvåge, om it-aktiverne understøttes af interne eller eksterne leverandører og udviklere, og om alle relevante patches og opgraderinger er implementeret i henhold til dokumenterede processer. Ligeledes skal det overvåges, om alle relevante patches og opgraderinger installeres på grundlag af dokumenterede processer. Risici som følge af forældede eller ikke-supporterede it-aktiver skal vurderes og mitigeres.

61) Direktionen skal sikre, at der implementeres kapacitetsovervågning med henblik på rettidigt at forebygge, opdage og reagere på vigtige driftsproblemer vedrørende it-systemer og mangel på it-kapacitet.

62) Direktionen skal sikre, at forretningsgange for backup og gendannelse af data og it-systemer udarbejdes og implementeres for at sikre, at de kan gendannes som påkrævet i henhold til fastsatte krav. Omfanget og hyppigheden af backup skal fastsættes i overensstemmelse med de forretningsmæssige krav til genopretning samt data og it-systemernes kritikalitet og evalueres i overensstemmelse med risikostyringen. Test af backup- og gendannelsesforretningsgange skal foretages løbende i henhold til fastsatte krav.

63) Direktionen skal sikre, at backup af data og it-systemer opbevares sikkert og isoleret fra den primære beliggenhed, så de ikke udsættes for de samme risici.

It-sikkerhedshændelses- og problemstyring

64) Direktionen skal sikre, at der udarbejdes og implementeres en forretningsgang for it-hændelses- og problemstyring med henblik på at overvåge og logge it-sikkerhedshændelser og gøre det muligt for virksomheden at fortsætte eller genoptage kritiske forretningsfunktioner og -processer rettidigt, når der opstår driftsforstyrrelser. Virksomheden skal fastsætte passende kriterier og tærskler for at klassificere it-sikkerhedshændelser samt fastsætte tidlige varslingsindikatorer, der skal fungere som alarmer for at muliggøre tidlig opdagelse af it-sikkerhedshændelser.

65) For at minimere påvirkningen af utilsigtede it-sikkerhedshændelser og muliggøre rettidig genopretning skal der udarbejdes og implementeres passende forretningsgange og organisatoriske strukturer, som sikrer en konsekvent og integreret overvågning, styring og opfølgning på it-sikkerhedshændelser. Desuden skal de grundlæggende årsager identificeres og fjernes for at forhindre, at it-sikkerhedshændelser gentages. Forretningsgangen for it-hændelses- og problemstyring skal derudover som minimum fastlægge:

    a) Krav til identifikation, sporing, registrering, kategorisering, klassificering og rapportering af it-sikkerhedshændelser prioriteret på baggrund af forretningskritikaliteten.

    b) Roller og ansvar for forskellige hændelsesscenarier.

    c) Krav til it-problemstyring med henblik på at identificere, analysere og løse årsagen bag it-sikkerhedshændelser. It-sikkerhedshændelser, der kan påvirke virksomheden, som er blevet identificeret eller har fundet sted inden for og/eller uden for organisationen, skal analyseres. Ligeledes skal de vigtigste erfaringer tages i betragtning, og sikkerhedsforanstaltningerne skal opdateres i overensstemmelse hermed.

    d) Effektive interne kommunikationsplaner, herunder notificering om it-sikkerhedshændelser og eskalationsprocedurer, der også omfatter sikkerhedsrelaterede kundeklager, for at sikre, at

i. it-sikkerhedshændelser med potentielt stor negativ indvirkning på kritiske it-systemer og it-tjenester rapporteres til den relevante ledelse,

ii. direktionen underrettes i tilfælde af væsentlige it-sikkerhedshændelser og som minimum underrettes om konsekvenserne, opfølgningen og de yderligere kontrolforanstaltninger, der skal udarbejdes og implementeres som resultat af it-sikkerhedshændelserne, og at

iii. bestyrelsen skal underrettes i relevant omfang.

e) Krav til it-sikkerhedshændelsesstyring med henblik på at mitigere konsekvenserne som følge af it-sikkerheds-hændelserne og sikre, at tjenesten rettidigt bliver operationel og sikker.

f) Specifikke eksterne kommunikationsplaner for kritiske forretningsfunktioner og processer for at sikre

i. samarbejde med relevante interessenter for effektivt at reagere på hændelsen og reetablere driften, og

ii. levering af rettidige oplysninger til eksterne parter, alt efter hvad der er relevant og i overensstem-melse med gældende lovgivning.

66) Direktionen skal sikre, at it-sikkerhedshændelser, der medfører væsentlig reduktion i funktionaliteten som følge af brud på fortrolighed, integritet og/eller tilgængelighed til it-systemer og/eller data, uden unødigt ophold bliver rapporteret til Finanstilsynet. Rapporteringen skal omfatte it-sikkerhedshændelser, som virksomheden selv kategoriserer som alvorlige og/eller kritiske, men skal også omfatte andre afvigelser, hvis disse afdækker specielle sårbarheder i en applikation, arkitektur, infrastruktur, m.v.

Brug af leverandører

67) Direktionen skal sikre effektiviteten af mitigerende foranstaltninger, når it-tjenesters, betalingstjenesters og it-systemers operationelle funktioner outsources, herunder til koncernenheder. De mitigerende foranstaltninger skal være defineret i henhold til it-risikostyringen.

68) For at sikre kontinuitet i it-tjenesterne og it-systemerne skal direktionen sikre, at kontrakter og serviceleveranceaftaler med leverandører som minimum omfatter følgende:

a) Passende og forholdsmæssige it-sikkerhedsmål og –foranstaltninger.

b) Forretningsgange for styring af it-sikkerhedshændelser, herunder eskalering og rapportering.

69) Direktion skal sikre, at leverandørers grad af efterlevelse af it-sikkerhedsmål, sikkerhedsforanstaltninger og servicemål overvåges og rapporteres i relevant omfang.

Virksomhedens eventuelle status som operatør af en væsentlig tjeneste

70) Direktionen i et penge- eller et realkreditinstitut, der er udpeget af Finanstilsynet som operatør af væsentlige tjenester, skal sikre, at Finanstilsynet og Center for Cybersikkerhed hurtigst muligt bliver underrettet om hændelser, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningen skal indeholde oplysninger om antallet af brugere, som berøres af afbrydelse af den væsentlige tjeneste, hændelsens varighed, den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen, og om eventuelle grænseoverskridende konsekvenser af hændelsen.

It-projektstyring

71) Direktionen skal sikre, at der udarbejdes og implementeres en forretningsgang for it-projektstyring, der definerer roller og ansvar.

72) Risici, der følger af virksomhedens portefølje af it-projekter, skal overvåges og mitigeres, idet der også skal tages hensyn til de risici, der kan opstå som følge af indbyrdes afhængigheder mellem forskellige projekter, herunder når de afvikles med de samme ressourcer og/eller den samme ekspertise.

73) Forretningsgangen for it-projektstyring skal som minimum omfatte:

    a) Projektmål.

    b) Roller og ansvar.

    c) En projektrisikovurdering.

    d) En projektplan, en tidsramme og de forskellige trin.

    e) Vigtigste milepæle.

    f) Krav til ændringsstyring.

74) It-projektstyringsforretningsgangen skal sikre, at informationssikkerhedskrav analyseres og godkendes af en funktion, der er tilstrækkelig uafhængig og har de rette kompetencer.

75) Direktionen skal sikre, at alle områder, der påvirkes af et it-projekt, er repræsenteret i projektteamet, og at projektteamet har den nødvendige viden til at sikre en sikker og succesfuld projektgennemførelse.

76) Etableringen og fremdriften af it-projekter og de afledte risici skal rapporteres til direktionen afhængigt af it-projekternes betydning og omfang. Rapporteringen skal ske regelmæssigt og når relevant. Projektrisici skal inddrages i risikostyringsrammerne. Rapporteringen skal tilgå bestyrelsen i relevant omfang.

Anskaffelse og udvikling af it-systemer

77) Direktionen skal sikre, at der udarbejdes og implementeres en forretningsgang for anskaffelse, udvikling og vedligeholdelse af it-systemer, som skal udformes på grundlag af en risikobaseret tilgang.

78) Direktionen skal sikre, at funktionelle og ikke-funktionelle krav, herunder krav til informationssikkerhed, defineres klart og godkendes af den relevante leder, inden it-systemer anskaffes eller udvikles.

79) Direktionen skal sikre, at der er mitigerende foranstaltninger mod utilsigtede ændringer eller bevidst manipulation af it-systemer, der er under udvikling og implementering.

80) Direktionen skal sikre, at it-systemer testes og godkendes, inden de tages i brug, og at der tages højde for forretningsprocessernes og aktivernes kritikalitet. Testmiljøer skal i tilstrækkelig grad afspejle produktionsmiljøet.

81) Direktionen skal sikre, at it-systemer, it-tjenester og foranstaltninger testes med henblik på at identificere potentielle sikkerhedsovertrædelser, -svagheder og -hændelser.

82) Direktionen skal sikre, at der etableres adskilte it-miljøer for at opnå tilstrækkelig funktionsadskillelse og forhindre ikke-verificerede ændringer til produktionssystemerne. Produktionsmiljøerne skal adskilles fra udviklings- og testmiljøerne og andre ikke-produktionsmiljøer. Samtidig skal integriteten og fortroligheden af produktionsdata, der anvendes i ikke-produktionsmiljøer, sikres. Adgang til produktionsdata skal være begrænset til autoriserede brugere.

83) Direktionen skal sikre, at der implementeres foranstaltninger til at beskytte integriteten af kildekoden til it-systemer. Udviklingen, implementeringen, driften og/eller konfigurationen af it-systemerne skal dokumenteres for at minimere unødvendig afhængighed af individer og/eller eksperter. Dokumentationen for et it-system skal, hvor det er relevant, som minimum omfatte brugerdokumentation, teknisk systemdokumentation og forretningsgange.

84) Direktionen skal sikre, at kravene for anskaffelse og udvikling af it-systemer også gælder for it-systemer, der udvikles eller håndteres af forretningsfunktionernes brugere uden for it-organisationen. Dette skal ske ud fra en risikobaseret tilgang.

It-ændringsstyring

85) Direktionen skal sikre, at der udarbejdes og implementeres en forretningsgang for it-ændringsstyring for at sikre, at alle ændringer af it-systemer registreres, risikovurderes, testes, godkendes, implementeres og verificeres på en kontrolleret måde. Haste- og nødændringer skal styres efter forudbestemte tilstrækkeligt foranstaltninger.

86) Direktionen skal sikre, at det løbende vurderes, om ændringer i eksisterende produktionsmiljøer påvirker de eksisterende foranstaltninger, eller om yderligere foranstaltninger er nødvendige. Disse ændringer skal ske i overensstemmelse med virksomhedens formelle ændringsstyringsproces.

Styring af forretningskontinuitet

87) Direktionen skal sikre, at der udarbejdes og implementeres en forretningsgang for forretningskontinuitet (Business Continuity Management, BCM) for at maksimere evnen til løbende at levere tjenester og begrænse tab i tilfælde af væsentlige it-driftsforstyrrelser.

88) Direktionen skal sikre, at en hændelse, der sætter et driftscenter ud af drift, ikke kan ramme øvrige driftscentre samtidigt. Dette skal foretages ud fra en konkret risikovurdering.

Forretningskonsekvensanalyser

89) Direktionen skal sikre, at der foretages forretningskonsekvensanalyser (Business Impact Analysis, BIA). Dette skal gøres ved at analysere eksponeringen over for væsentlige driftsforstyrrelser og vurdere potentielle konsekvenser kvantitativt og kvalitativt ved hjælp af interne og/eller eksterne data og scenarieanalyser. Der skal tages højde for fortrolighed, integritet og tilgængelighed. Forretningskonsekvensanalyserne skal også inddrage kritikaliteten af de identificerede og klassificerede forretningsfunktioner, understøttende processer, tredjeparter og it-aktiver samt deres indbyrdes afhængigheder.

90) Direktionen skal sikre, at it-systemer og it-tjenester er designet og tilpasset virksomhedens forretningskonsekvensanalyser, f.eks. ved at sikre redundans af kritiske komponenter for at undgå driftsforstyrrelser forårsaget af hændelser, der påvirker disse komponenter.

Forretningskontinuitetsplaner

91) Direktionen skal sikre, at der på grundlag af forretningskonsekvensanalyserne udarbejdes og implementeres forretningskontinuitetsplaner for at sikre driftskontinuitet (Business Continuity Plans, BCPs). Dette skal dokumenteres og godkendes af direktionen. Planerne skal tage hensyn til risici, der kan have en negativ indvirkning på it-systemer og it-tjenester. Planerne skal understøtte mål om at beskytte og genoprette fortroligheden, integriteten og tilgængeligheden af forretningsfunktioner, understøttende processer og it-aktiver. Hvor det er relevant, skal der samarbejdes med interne og eksterne interessenter under udarbejdelsen af planer.

92) Direktionen skal sikre, at der udarbejdes og implementeres forretningskontinuitetsplaner, så der kan reageres hensigtsmæssigt på potentielle nedbruds- og fejlscenarier, og at virksomheden er i stand til at genoprette kritiske forretningsaktiviteter efter nedbrud og inden for de fastsatte mål om genopretning, jf. nr. 9, litra k. Der skal som minimum tages stilling til det maksimale tidsrum, inden for hvilket et system eller en proces skal genoprettes efter en hændelse (Recovery Time Objective, RTO) og det maksimalt acceptable datatab, målt i tid (Recovery Point Objective, RPO). I tilfælde af alvorlige forretningsforstyrrelser, der udløser flere specifikke forretningskontinuitetsplaner, skal det sikres, at nødforanstaltninger prioriteres ud fra en risikobaseret tilgang.

93) Direktionen skal sikre, at forretningskontinuitetsplaner indeholder en række forskellige scenarier, herunder ekstreme, men plausible scenarier, inklusive cyberangrebsscenarier, som virksomheden kan blive eksponeret for, og skal vurdere den potentielle indvirkning, som sådanne scenarier kan have. På grundlag af disse scenarier skal det beskrives, hvordan kontinuiteten af it-systemer og it-tjenester samt informationssikkerhed sikres.

Beredskabs- og genopretningsplaner

94) På grundlag af forretningskonsekvensanalyserne, jf. nr. 89, og mulige scenarier skal direktionen sikre, at der udarbejdes og implementeres beredskabs- og genopretningsplaner (Disaster Recovery Plans, DRPs). Disse planer skal beskrive, hvilke betingelser der kan medføre aktivering af planerne, og hvilke foranstaltninger der skal træffes for at sikre tilgængelighed, kontinuitet og genopretning af, som minimum, virksomhedens kritiske it-systemer og it-tjenester. Beredskabs- og genopretningsplanerne skal sikre, at genopretningsmålene kan opnås, jf. nr. 9, litra k.

95) Beredskabs- og genopretningsplanerne skal tage højde for både kort- og langsigtede genopretningsmuligheder. Planerne skal som minimum:

    a) Fokusere på at genoprette driften af kritiske forretningsfunktioner, understøttende processer, it-aktiver og deres indbyrdes afhængigheder for at undgå negative påvirkninger på virksomheders drift og på det finansielle system, herunder på betalingssystemer og på betalingstjenestebrugere og for at sikre gennemførelse af udestående betalingstransaktioner.

    b) Dokumenteres og stilles til rådighed for forretnings- og støtteenhederne samt være let tilgængelige i nødsituationer.

    c) Opdateres i overensstemmelse med erfaringerne fra it-sikkerhedshændelser, test, nye identificerede risici og trusler samt ved ændrede genopretningsmål og -prioriteter.

96) I planerne skal der også tages stilling til alternative muligheder i tilfælde af, at det på kort sigt ikke er muligt at genoprette driften på grund af omkostninger, risici, logistik eller uforudsete omstændigheder.

97) Som led i beredskabs- og genopretningsplanerne skal direktionen tage stilling til og implementere nødplansforanstaltninger for at mitigere svigt fra leverandører, som er af afgørende betydning for den fortsatte drift af virksomhedens it-tjenester.

Test af planer

98) Direktionen skal sikre, at planerne testes regelmæssigt. Planerne for kritiske funktioner, understøttende processer, it-aktiver og disses indbyrdes afhængigheder skal testes mindst én gang om året, herunder, hvis relevant, dem der leveres af tredjeparter.

99) Planerne skal opdateres mindst én gang om året og på grundlag af testresultaterne, det aktuelle trusselsbillede og erfaringerne fra tidligere it-sikkerhedshændelser. Ændringer i genopretningsmålene (herunder RTO'er og RPO'er) og/eller ændringer i forretningsfunktioner, understøttende processer og it-aktiver skal også, hvor det er relevant, medføre opdatering af planerne.

100) Direktionen skal sikre, at test af planerne viser, at det er muligt at opretholde virksomhedens forretningsaktiviteter, indtil kritiske funktioner bliver genoprettet. Planerne skal som minimum:

    a) Omfatte test af flere alvorlige men plausible scenarier, inklusiv dem der tages i betragtning i forbindelse med udviklingen af planerne. Dette gælder også for test af tjenester udbudt af tredjeparter. Test skal også omfatte skift af kritiske forretningsfunktioner, understøttende processer og it-aktiver til virksomhedens katastrofeberedskab for at vise, at de kan fungere under disse omstændigheder i en repræsentativ periode, og at virksomheden kan tilbageføre aktiviteterne til normal drift.

    b) Være designet til at udfordre de antagelser, som planerne er baseret på, herunder governance og krisekommunikationsplaner.

    c) Omfatte krav til at efterprøve medarbejdernes, konsulenternes, it-systemernes og it-tjenesternes evne til at reagere hensigtsmæssigt på de identificerede scenarier.

101) Direktionen skal sikre, at testresultaterne dokumenteres, og at eventuelle identificerede afvigelser analyseres, adresseres og rapporteres til en relevant leder, samt direktion og bestyrelse når dette er relevant.

Krisekommunikation

102) I tilfælde af nedbrud eller nødsituationer og under gennemførelsen af forretningskontinuitetsplanerne skal direktionen sikre, at virksomheden har effektive krisekommunikationsforanstaltninger, så alle relevante interne og eksterne interessenter underrettes rettidigt og på en hensigtsmæssig måde. Dette omfatter bl.a. de kompetente myndigheder og eksterne tjenesteudbydere, leverandører og/eller koncernenheder.

Uddannelse it-sikkerhed

103) Direktionen skal sikre, at der udarbejdes og implementeres et uddannelsesprogram, herunder løbende awarenessprogrammer for alle medarbejdere og konsulenter. Det skal sikre, at de uddannes i at varetage deres opgaver og ansvar i overensstemmelse med de relevante sikkerhedspolitikker og forretningsgange for at reducere menneskelige fejl, tyveri, svig, misbrug eller tab, samt hvordan it-risici skal styres. Uddannelsesprogrammet skal tilbyde uddannelse for alle medarbejdere og konsulenter mindst én gang om året.

Efterlevelse af it-sikkerhedspolitikken

104) Direktionen skal løbende rapportere til bestyrelsen om manglende efterlevelse af it-sikkerhedspolitikken. Dette skal som minimum gøres på baggrund af tilstrækkelighed af forretningsgangene samt de implementerede tiltag.

Krav om opfølgningsproces for revisionsanbefalinger

105) Direktionen skal sikre, at der udarbejdes og implementeres forretningsgange for håndtering og efterlevelse af it-revisionsanbefalinger samt de risici, som anbefalingerne medfører.

Risikostyringsfunktionens og den risikoansvarliges opgaver på it-risikostyringsområdet

106) Risikostyringsfunktionen, jf. § 16, skal styre og overvåge overholdelsen af it-risikostyringsrammerne og sikre, at it-risici identificeres, måles, vurderes, styres, overvåges og rapporteres.

107) Rammerne for it-risikostyring skal være i overensstemmelse med IT-risikostyringspolitikken og skal som minimum omfatte processer til at:

a) Identificere og vurdere de it-risici, som virksomheden er og kan være eksponeret for, jf. nr. 6, litra b. Risicienе skal samles i et it-risikoregister, jf. nr. 13.

b) Fastlægge mitigerende foranstaltninger for at nedbringe it-risici. Der skal være en tydelig sammenhæng mellem de specifikke foranstaltninger og risici.

c) Overvåge effektiviteten af disse foranstaltninger samt antallet af it-sikkerhedshændelser.

d) Rapportere til direktionen og bestyrelsen om it-risici samt foranstaltninger og effektiviteten heraf.

e) Identificere og vurdere, om der er it-risici som følge af større ændringer i it-systemer, -tjenester, -forretningsgange og/eller processer og/eller efter væsentlige it-sikkerhedshændelser.

108) Rammerne for it-risikostyring skal dokumenteres og forbedres løbende på grundlag af erfaringer med implementering og overvågning. Rammerne skal opdateres og godkendes mindst én gang om året af direktionen.

Bilag 6. Tilrettelæggelse af arbejdet i bestyrelsen

Bestyrelsens forretningsorden

1) Bestyrelsen skal ved en forretningsorden træffe nærmere bestemmelser om udførelsen af sit hverv, jf. § 65 i lov om finansiel virksomhed, § 68 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter og § 130 i selskabsloven.
2) Ved udformningen af forretningsordenen efter nr. 1 skal bestyrelsen tage udgangspunkt i sine lovmæssigt fastsatte forpligtelser samt den finansielle virksomheds kompleksitet og forretnings- og aktivitetsområder. Forretningsorden skal som minimum indeholde:
    a) Bestemmelser om bestyrelsens konstitution, herunder anvendelse af suppleanter og krav til beslutningsdygtighed samt med hvilke intervaller, der skal afholdes møder.
    b) Bestemmelser om skriftlige og elektroniske bestyrelsesmøder, jf. nr. 19.
    c) Procedurer for fastlæggelse af arbejdsdelingen mellem bestyrelsen og direktionen, herunder bemyndigelser, ansvar for forretningsgange og tavshedspligt.
    d) Procedurer for bestyrelsens løbende stillingtagen til organisatorisk placering og bemanding af risikostyringsfunktionen beskrevet i § 16, stk. 1, og bilag 7.
    e) Procedurer for bestyrelsens tilsyn med direktionens ledelse af den finansielle virksomhed og eventuelle datterselskaber, herunder vurdering af om direktionen varetager sine opgaver på behørig måde og i overensstemmelse med den fastlagte risikoprofil, de fastlagte politikker og bestyrelsens retningslinjer til direktionen, jf. § 70, stk. 5, i lov om finansiel virksomhed og § 67, stk. 4, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.
    f) Procedurer for oprettelse og føring af bøger, fortegnelser og protokoller efter selskabslovgivningen.
    g) Procedurer for bestyrelsens løbende stillingtagen til den finansielle virksomheds forretningsmodel, risikoprofil, organisation og ressourcer.
    h) Procedurer for hvordan bestyrelsen indhenter de oplysninger, der er nødvendige for udførelse af dens opgaver herunder de forpligtelser, som bestyrelsen er pålagt i henhold til lov om finansiel virksomhed, lov om fondsmæglerselskaber og investeringsservice og –aktiviteter, lov om kapitalmarkeder m.v., lov om forebyggende foranstaltninger mod hvidvask af udbytte og terrorfinansiering og anden relevant lovgivning.
    i) Bestemmelser om bestyrelsens løbende stillingtagen til direktionens rapportering til bestyrelsen, herunder stillingtagen til den finansielle virksomheds individuelle solvensbehov, budgetter, finansielle rapporter, likviditet og kapitalbehov, væsentlige dispositioner, særlige risici og overordnede forsikringsforhold.
    j) Procedurer for bestyrelsens stillingtagen til og underskrivelse af revisionsprotokollen.
    k) Procedurer for, hvordan bestyrelsen sikrer tilstedeværelsen af det nødvendige grundlag for revision, herunder, hvis relevant, tage stilling til om der er behov for intern revision.
3) Bestyrelsen skal løbende og mindst én gang om året gennemgå forretningsordenen med henblik på at sikre, at denne afspejler den finansielle virksomheds forretnings- og aktivitetsområder.
4) Bestyrelsen skal sikre og kunne dokumentere, at samtlige bestyrelsesmedlemmer har kendskab til forretningsordenen.

Bestyrelsesmøder og bestyrelsens forhandlinger

5) Bestyrelsen skal, jf. § 74, stk. 1, i lov om finansiel virksomhed og § 69, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter mødes, når der skal træffes beslutning om forhold, der ikke er omfattet af de beføjelser, bestyrelsen har givet til direktionen, jf. § 70, stk. 2, og § 67 i henholdsvis lov om finansiel virksomhed og lov om fondsmæglerselskaber og investeringsservice og -aktiviteter. Bestyrelsen kan således ikke lovligt delegere sin beslutningskompetence for eksempel til et forretningsudvalg. Bestyrelsesformanden skal sikre, at materiale til brug for mødet udsendes i tilstrækkelig god tid før mødet.
6) Nr. 5 finder ikke anvendelse på behandling af standardiserede sager, som i henhold til vedtægter eller andet skal behandles af bestyrelsen. Sådanne sager kan henlægges til behandling og beslutning i et udvalg under bestyrelsen, hvis der på forhånd af den samlede bestyrelse er fastlagt retningslinjer for sagernes behandling. Disse retningslinjer og udvalgets behandling af de pågældende sager skal løbende evalueres af den samlede bestyrelse. Delegeringen omfatter ikke bestyrelsens ansvar for sagernes behandling og de trufne beslutninger.
7) Bestyrelsen kan beslutte, at ansatte i den finansielle virksomhed samt bestyrelsesmedlemmer og ansatte i andre selskaber i koncernen kan deltage i et bestyrelsesmøde, eventuelt alene ved enkelte punkter på dagsordenen.
8) Bestyrelsen kan ligeledes i enkeltstående tilfælde beslutte, at der kan være andre personer end de nævnte i nr. 7 til stede ved et eller flere angivne punkter på dagsordenen, eksempelvis aktionærer eller rådgivere.
9) Uanset nr. 7 og 8 må der ikke være uvedkommende personer til stede ved et bestyrelsesmøde eller ved et punkt på bestyrelsesmødets dagsorden, hvor der behandles fortrolige oplysninger, som ikke lovligt kan videregives efter reglerne

om videregivelse af fortrolige oplysninger i kapitel 9 i lov om finansiel virksomhed og kapitel 12 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.

10) Forhandlingsprotokollen i medfør af lov om finansiel virksomhed § 74, stk. 3, og § 69, stk. 3, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter skal afspejle drøftelserne på møderne, herunder skal væsentlige risikovurderinger og trufne beslutninger samt forudsætninger for disse fremgå. Det skal fremgå, hvilke medlemmer der har været til stede på et møde. Har andre personer end medlemmer af bestyrelsen været til stede, skal dette også fremgå.
11) Protokollen skal indrettes på betryggende vis, herunder så det er tydeligt, når protokollen for et møde er endelig, og at hver side i forhandlingsprotokollen er fortløbende nummereret.
12) Hvis der føres en særskilt bevillingsprotokol, skal dette fremgå af forhandlingsprotokollen. Det skal tydeligt fremgå af bevillingsprotokollen henholdsvis forhandlingsprotokollen, hvilke lån der er:
    a) Bevilget/afslået.
    b) Bevilget i henhold til § 78 i lov om finansiel virksomhed.
    c) Til orientering.
    d) Til efterbevilling (hastesager).
    e) Bevilget ved skriftlig behandling eller på et elektronisk afholdt bestyrelsesmøde.
13) Det skal udtrykkeligt anføres i bevillingsprotokollen henholdsvis forhandlingsprotokollen, når der behandles eksponeringer omfattet af § 78, stk. 1 og 4, i lov om finansiel virksomhed. De pågældende bestyrelsesmedlemmer og direktører må ikke være til stede under sagens behandling, og det skal protokolleres, at de ikke er til stede.
14) Bestemmelsen i nr. 13 er ikke til hinder for, at et bestyrelsesmedlem eller en direktør, der tillige deltager i ledelsen af et moderselskab, der ejer hele kapitalen i virksomheden, eller i et 100 pct. ejet søster- eller datterselskab, deltager i behandlingen af spørgsmål om eller eksponeringer mod dette selskab.
15) Bestemmelserne i lov om finansiel virksomhed § 78, stk. 1 og 4, er ikke til hinder for, at medarbejdervalgte bestyrelsesmedlemmer kan bevilges eksponeringer på samme vilkår som medarbejderne i den pågældende finansielle virksomhed i øvrigt.
16) Bestemmelsen i lov om finansiel virksomhed § 78, stk. 3, finder ikke anvendelse på fuldt sikrede eksponeringer eller eksponeringer af helt ubetydelig størrelse.
17) Bestyrelsen skal mindst én gang om året gennemgå eksponeringerne med de nævnte personer og selskaber i § 78, stk. 1 og 4, i lov om finansiel virksomhed og § 88, stk. 1 og 4, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, for eksempel i forbindelse med den årlige aktivgennemgang. Gennemgangen og konklusionerne herpå, skal fremgå af protokollen.

Skriftligt og elektronisk afholdte bestyrelsesmøder

18) Bestyrelsen kan afholde skriftlige og elektroniske bestyrelsesmøder i overensstemmelse med selskabsloven, i det omfang dette er foreneligt med udførelsen af bestyrelsens hverv.
19) Bestyrelsen skal beslutte, hvilke typer af sager der er egnede til behandling på et skriftligt eller elektronisk bestyrelsesmøde, for eksempel ukomplicerede og rutineprægede sager eller presserende sager, der ikke kan udsættes uden skadevirkning for virksomheden. Beslutningen skal fremgå af forretningsordenen.
20) Nr. 18 og 19 finder tilsvarende anvendelse på skriftlige bevillingsprocedurer.
21) I det omfang, hvor en bestyrelsesbeslutning træffes skriftligt eller elektronisk, kræves så vidt muligt en egentlig tilkendegivelse fra de enkelte bestyrelsesmedlemmer. Sådanne tilkendegivelser skal protokolleres. En undladelse af at reagere på fremsendt materiale er ikke tilstrækkelig tilkendegivelse.

Bilag 7. Risikostyringsfunktionen og den risikoansvarlige

Direktionens opgaver og ansvar

1) Direktionen skal, jf. § 16, stk. 1, 1. pkt., sikre, at virksomheden har en risikostyringsfunktion, og at der udpeges en risikoansvarlig.
2) Direktionen skal sikre, at det tydeligt fremgår, for eksempel af funktionsbeskrivelser og forretningsgange, hvilke opgaver der henhører under risikostyringsfunktionen, jf. nr. 4-14.
3) Direktionen skal sikre, at risikostyringsfunktionen har adgang til alle relevante oplysninger, har adgang til regelmæssig uddannelse og har tilstrækkelige ressourcer, jf. § 9, stk. 2.

Risikostyringsfunktionens og den risikoansvarliges opgaver på risikostyringsområdet

4) Den risikoansvarlige skal have et samlet overblik over virksomheden og virksomhedens risikoeksponeringer med henblik på at kunne vurdere, om der er en betryggende styring heraf.
5) Den risikoansvarlige skal tage stilling til, om direktionens og bestyrelsens beslutningsgrundlag er tilstrækkeligt, jf. nr. 6-8.
6) Den risikoansvarlige skal sikre, at alle væsentlige risici i virksomheden herunder risici, der går på tværs af virksomhedens organisation, identificeres, måles, håndteres og rapporteres korrekt.
7) Den risikoansvarlige skal sikre, at risikoeksponeringer i datterselskaber, jf. § 2, stk. 2, indgår i vurderingen af virksomhedens samlede risikoeksponeringer.
8) Den risikoansvarlige skal sikre, at risikoeksponeringer i outsourcede processer, tjenesteydelser eller aktiviteter indgår i vurderingen af virksomhedens samlede risikoeksponeringer.
9) Den risikoansvarlige skal vurdere, om der er indført de fornødne foranstaltninger til sikring af kvaliteten af data, som anvendes i styringen af risici.
10) Den risikoansvarlige skal vurdere, om der er indført de fornødne foranstaltninger til styring af modelrisiko, jf. bilag 3, nr. 13 og 14.
11) Risikostyringsfunktionen skal deltage aktivt i udviklingen af virksomhedens politikker og strategiske mål, jf. § 4, stk. 1.
12) Den risikoansvarlige skal på forhånd høres om væsentlige beslutninger, så den risikoansvarlige har mulighed for at udtale sig om risikoen forinden, herunder om væsentlige beslutninger om ændringer i strategi og forretningsmodel, risikotagning, nye produkter, nye kundegrupper, ændringer i strategi og forretningsmodel, organisatoriske ændringer, etablering af nye filialer og forretningsenheder, ændring af it-systemer, outsourcing, anvendelse af modeller, m.v.
13) Risikostyringsfunktionen skal mindst én gang om året udarbejde en rapport til bestyrelsen om virksomhedens risikostyring, jf. § 5, stk. 4. Rapporten skal indeholde den risikoansvarliges stillingtagen til forholdene anført under nr. 4-10, og 12 og skal indgå som en del af bestyrelsens samlede vurderingsgrundlag, jf. § 5, stk. 4. Virksomheden kan vælge, at rapporten indgår som en del af eller som et tillæg til vurderingen af virksomhedens solvensbehov (ICAAP). Den risikoansvarlige skal i givet fald sikre, at rapporteringen opfylder alle krav til indhold og klart fremgår af tillægget, og at bestyrelsen er orienteret om, at rapporten indgår som et tillæg.
14) Den risikoansvarlige skal hurtigst muligt give udtryk for betænkeligheder og advare bestyrelsen, hvis der sker en udvikling i specifikke risici der påvirker eller kan påvirke virksomheden, og det er relevant, at bestyrelsen tager stilling til risikoen.
15) Har virksomheden nedsat et risikoudvalg, jf. § 80 b, stk. 1, i lov om finansiel virksomhed, skal den risikoansvarliges rapport, jf. nr. 13, sendes til risikoudvalget.

Risikostyringsfunktionens organisation

16) Direktionen skal udpege en risikoansvarlig med ansvar for ledelse af risikostyringsfunktionen. Bestyrelsen kan dog beslutte, at det er bestyrelsen, der udpeger den risikoansvarlige.
17) Den risikoansvarlige skal være tilstrækkeligt uafhængig af virksomhedens funktioner til, at den risikoansvarliges opgaver kan udføres betryggende.
18) Direktionen skal sikre, at den organisatoriske placeringen af risikostyringsfunktionen er betryggende. Hvis direktionen eller bestyrelsen vælger at udpege en risikoansvarlig, der også har ansvar for andre opgaver end risikostyring, skal direktionen eller bestyrelsen sikre, at mulige interessekonflikter mellem opgaverne, som den risikoansvarlige varetager i sin egenskab af risikoansvarlig og andre opgaver, håndteres betryggende.
19) Et medlem af direktionen, som bestyrelsen ikke har udpeget som den administrerende direktør, kan udpeges som risikoansvarlig, hvis den pågældende opfylder kravene i nr. 16 og 17.
20) Direktionen i pengeinstitutter med en arbejdende kapital mindre end 12 mia. kr., mindre realkreditinstitutter og virksomheder omfattet af § 1, nr. 3 og 5-7, kan udpege en direktør, som bestyrelsen har udpeget som den administrerende direktør, som risikoansvarlig.

21) Direktionen i pengeinstitutter med en arbejdende kapital mindre end 12 mia. kr., mindre realkreditinstitutter og virksomheder omfattet af § 1, nr. 3 og 5-7 kan ligeledes vælge, at risikostyringsfunktionen udgøres af den risikoansvarlige.
22) Direktionen kan vælge at placere dele af risikostyringsfunktionens opgaver i organisatoriske enheder udenfor risikostyringsfunktionen.
23) Hvis virksomheden er et SIFI eller et G-SIFI, skal direktionen vurdere behovet for, at risikostyringsfunktionen under ledelse af den risikoansvarlige organiseres, så der oprettes bemandede risikostyringsenheder for hvert væsentligt risikoområde i virksomheden for derved at øge virksomhedens opmærksomhed på de enkelte områders risikoeksponeringer.
24) En risikoansvarlig, der er udpeget i medfør af nr. 16-21, skal sikre, at risikostyringsfunktionen udfører opgaverne, jf. nr. 4-14, betryggende.
25) Har virksomheden nedsat et risikoudvalg, jf. § 80 b, stk. 1, i lov om finansiel virksomhed, skal den risikoansvarlige på udvalgets anmodning bistå dette med information.
26) Den risikoansvarlige skal deltage i risikoudvalgets møder med henblik på forelæggelse og drøftelse af virksomhedens risikostyring, jf. nr. 4-11 og 14.
27) Den risikoansvarlige skal løbende, herunder i forbindelse med afgivelse af den risikoansvarliges rapport, jf. nr. 13, deltage i bestyrelsens møder med henblik på forelæggelse og drøftelse af virksomhedens risikostyring.

Bilag 8. Risikoen for overdreven gearing

1) Dette bilag indeholder bestemmelser om de i bekendtgørelsen omhandlede forhold, der relaterer sig til risikoen for overdreven gearing.
2) Bestyrelsen skal sikre, at virksomheden, hvor det er relevant, råder over politikker og processer til identifikation, overvågning og styring af risikoen for overdreven gearing.
3) Politikken og processerne skal afspejle virksomhedens størrelse, eksponeringer og kompleksitet.
4) Direktionen skal sikre, at bestyrelsens politik og processer indenfor risikoen for overdreven gearing efterleves.
5) Virksomheden skal have indikatorer for risikoen for overdreven gearing. Indikatorerne skal omfatte gearingsgrad, der beregnes efter artikel 429 i forordningen (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber, som ændret ved forordning (EU) 2019/876 af 20. maj 2019 om ændring af forordning (EU) nr. 575/2013 for så vidt angår gearingsgrad, net stable funding ratio, krav til kapitalgrundlag og nedskrivningsrelevante passiver, modpartskreditrisiko, markedsrisiko, eksponeringer mod centrale modparter, eksponeringer mod kollektive investeringsordninger, store eksponeringer og indberetnings- og oplysningskrav, og forordning (EU) nr. 648/2012, og mismatch mellem aktiver og passiver.
6) Virksomheden skal, hvor det er relevant, ved håndtering af risikoen for overdreven gearing udvise forsigtighed. Virksomheden skal tage behørigt hensyn til potentiel forøgelse af risikoen for overdreven gearing som følge af en formindskelse af virksomhedens kapitalgrundlag forårsaget af forventede eller realiserede tab afhængigt af de gældende regnskabsregler. Med henblik herpå skal virksomhederne i relevant omfang være i stand til at modstå forskellige stresspåvirkninger i forbindelse med risikoen for overdreven gearing.
7) Stresstest af risikoen for overdreven gearing skal afspejle virksomhedens størrelse, eksponeringer og kompleksitet.
8) Bestyrelsen skal, hvor det er relevant, i udgangspunktet én gang hvert kvartal modtage rapportering om virksomhedens risiko for overdreven gearing.
9) Direktionen skal, hvor det er relevant, mindst én gang hvert kvartal modtage rapportering om virksomhedens risiko for overdreven gearing.