FINANSTILSYNET

NOTAT

Finanstilsynet

3. februar 2020

J.nr.,
/SMH

God praksis for compliance og risikostyring i kreditinstitutter

Bestyrelsen og direktionen i kreditinstitutter skal prioritere compliance og risikostyring for at opbygge en stærk kultur. Finanstilsynet har gennemført en undersøgelse, som viser, at compliance og risikostyring er tilført væsentligt flere ressourcer over de seneste ti år.

Gennem de seneste år er fokus på compliance og risikostyring i de danske kreditinstitutter vokset. Det er dels en konsekvens af skærpede regler i lyset af finanskrisen og deraf afledt øget tilsynsmæssig fokus, dels et resultat af en opprioritering i kreditinstitutterne. En række store sager, nationalt såvel som internationalt, hvor svigt i compliance og risikostyring har bidraget til store økonomiske og omdømmemæssige tab, har formentlig medvirket til det øgede fokus. Dette fokus vil fortsætte de kommende år. Både tilsynsmyndigheder, kunder og investorer vil forvente, at kreditinstitutternes compliance- og risikostyringsfunktioner er velorganiserede og i stand til at understøtte institutternes forretninger. Utilstrækkelig compliance og risikostyring er ikke samfundsmæssig acceptabelt og kan koste kreditinstitutterne dyrt - både gennem forretningsmæssige tab, tab af omdømme, kundeflugt og bøder.

Kreditinstitutterne skal naturligvis overholde lovkrav om compliance og risikostyring, som er en væsentlig del af bolværket mod, at institutter påtager sig utilsigtede risici. Vurderingen af compliance og risikostyring er derfor naturlige fokusområder i Finanstilsynets inspektionsvirksomhed, ligesom de indgår som elementer i Finanstilsynets strategi for tilsyn i gode tider.

Finanstilsynet indledte i vinteren 2018/2019 en spørgeskemaundersøgelse af compliance og risikostyring blandt pengeinstitutter i gruppe 1 og 2 samt udvalgte realkreditinstitutter. Finanstilsynet har efterfølgende været i dialog med de enkelte kreditinstitutter om deres besvarelse, og institutterne modtager individuelle skriftlige tilbagemeldinger med Finanstilsynets observationer.

Disse observationer har sammen med observationer fra inspektioner og gældende lovgivning, herunder § 16-17 og bilag 1, pkt. 25-26 og bilag 4, pkt. 14

*Kreditinstitutternes **risikostyringsfunktion** skal sikre, at alle væsentlige risici i instituttet bliver identificeret, målt, håndteret og rapporteret korrekt. Risikostyringsfunktionen skal have et samlet overblik over instituttets risikoeksponeringer for at kunne vurdere, om styringen heraf er betryggende.*

***Compliancefunktionen** skal fungere uafhængigt og kontrollere, at instituttet planlægger, organiserer og gennemfører sit arbejde indenfor gældende lovgivning, markedsstandarder og interne regler. Instituttets compliancefunktion skal have metoder og procedurer til at minimere risikoen for manglende regeloverholdelse.*

samt bilag 7 i bekendtgørelse om ledelse og styring, givet anledning til at formulere ti konkrete retningslinjer for god praksis til institutternes organisering af compliance og risikostyring.

1. Der er en klar opgave- og ansvarsfordeling mellem og indenfor forsvarslinjerne, som sikrer, at alle væsentlige risici bliver identificeret og kontrolleret. Institutterne sikrer, at både første og anden forsvarslinje udfører kontroller på kreditområdet.

2. Compliancefunktionen kontrollerer og vurderer bredt overholdelse af regler, herunder reglerne om drift af finansiel virksomhed og om risikostyringsfunktionen udfører de opgaver, som følger af lovgivningen.

3. Compliance- og risikostyringsfunktionerne har tilstrækkelige ressourcer og kompetencer til at varetage deres ansvarsområder korrekt og uafhængigt.

4. Interessekonflikter er identificeret og håndteret, så uafhængigheden i anden forsvarslinje ikke kompromitteres.

5. Rapporteringen fra den risikoansvarlige giver ledelsen et samlet og dækkende overblik over instituttets interne og eksterne risici. Rapporteringen indeholder den risikoansvarliges vurdering af, om risikostyringen er betryggende. Rapporteringen fra den complianceansvarlige giver ledelsen et klart billede af instituttets compliancerisici og eventuelle ændringsbehov og tiltag.

6. Den complianceansvarlige og den risikoansvarlige udarbejder risikovurderinger, som ligger til grund for funktionernes planlægning og udarbejdelse af flerårsplaner.

7. Den risikoansvarlige og den complianceansvarlige har en passende høj organisatorisk forankring. Den risikoansvarlige og den complianceansvarlige i SIFI virksomheder[1] er en del af eller referere direkte til direktionen. I de tilfælde, hvor den risikoansvarlige ikke er en del af direktionen, bør det direktionsmedlem, den risikoansvarlige refererer til, ikke have ansvar for væsentlige forretningsmæssige risici (medmindre der er tale om den administrerende direktør). Den risikoansvarlige og den complianceansvarlige har mulighed for at udtale sig direkte til bestyrelsen.

[1] SIFI'er omfatter gruppe 1 pengeinstitutter og realkreditinstitutter. Virksomhederne indgår i undersøgelsen på højeste konsolideringsniveau for de virksomheder (koncerner), der har flere finansielle virksomheder i koncernen.

8. Den complianceansvarlige og den risikoansvarlige bliver hørt ved væsentlige beslutninger, men må ikke være ansvarlige for forretningsmæssige projekter.

9. Den complianceansvarlige og den risikoansvarlige har betydelig erfaring fra arbejdet i et kreditinstitut, og i SIFI virksomhederne også erfaring fra arbejdet i selve funktionen.

10. Den complianceansvarlige og den risikoansvarlige har adgang til alle relevante oplysninger.

1. Opgave- og ansvarsfordeling

Undersøgelsen viser, at SIFI virksomhederne bruger, hvad der i gennemsnit svarer til 104 fuldtidsansatte pr. 1.000 ansatte til kontrolfunktioner i første forsvarslinje. De mellemstore institutter bruger, hvad der i gennemsnit svarer til 157 fuldtidsansatte pr. 1.000 ansatte. Dette skal ses i lyset af, at SIFI virksomhederne på den ene side i absolutte tal har betydeligt flere ansatte til kontrolfunktioner end de mellemstore institutter, og at SIFI virksomhederne som følge af dette bedre kan udnytte stordriftsfordele. På den anden side medfører den større kompleksitet i SIFI-virksomhedernes forretning et behov for flere ressourcer til kontrol.

I første forsvarslinje optager kontroller på kreditområdet i gennemsnit næsten halvdelen af de ansattes tid. Det næststørste tidsforbrug (i gennemsnit) i første forsvarslinje går til kontroller på hvidvaskområdet, som udgør lidt over en tredjedel af de ansattes tid, jf. figur 1.

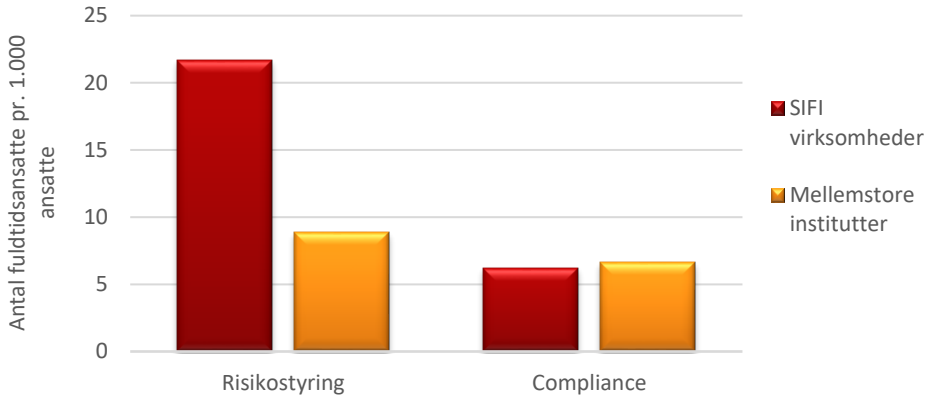
Figur 1: Opgavetyper tilknyttet kontrolfunktioner i første forsvarslinje

Note.: Fordelingen af opgavetyper der bliver udført som en del af kontrolfunktionerne i første forsvarslinje. Grafen viser et simpelt gennemsnit af undersøgelsens deltagere.

Stort set alle kreditinstitutter afsætter betydelige ressourcer i første forsvarslinje til kontrol af kreditrisici.

På hvidvaskområdet er der stor forskel på, hvor mange ressourcer der bliver afsat i første forsvarslinje. Spændvidden rækker fra et institut, der slet ikke har hvidvaskkontroller i første forsvarslinje, til institutter, hvor 80-90 pct. af kontrollerne i første forsvarslinje vedrører hvidvaskområdet. En del af forklaringen er institutternes placering af den hvidvaskansvarlige, som for enkelte institutters vedkommende er i anden forsvarslinje. Den hvidvaskansvarlige bør dog som udgangspunkt være placeret i første forsvarslinje, så kontrol af den hvidvaskansvarliges arbejde sker i anden forsvarslinje. For SIFI virksomheder skal den hvidvaskansvarlige være placeret i første forsvarslinje. Dertil kommer, at den complianceansvarlige i anden forsvarslinje skal undersøge og føre uafhængig kontrol med, at den hvidvaskansvarliges procedurer og forretningsgange er effektive.

Figur 2: Ressourcer tilknyttet compliance og risikostyring i anden forsvarslinje



Note.: Simpelt gennemsnit af undersøgelsens deltagere. Ressourcer er omregnet til antal fuldtidsmedarbejdere pr. 1.000 medarbejdere. Tallene er baseret på institutternes egne opgørelser af antal fuldtidsansatte i compliance- hhv. risikostyringsfunktionen. Der er forskelle i institutternes opgørelsesmetode af antal ansatte omregnet til fuldtidsansatte.

I anden forsvarslinje afsætter SIFI virksomhederne og mellemstore kreditinstitutter flere ressourcer til risikostyring end til compliance. Især SIFI virksomhederne bruger relativt flere ressourcer på risikostyring end de mellemstore kreditinstitutter, jf. figur 2. Ud af 1.000 ansatte bruger SIFI virksomhederne, hvad der svarer til omkring 22 fuldtidsansatte i risikostyringsfunktionen mod ca. ni fuldtidsansatte i de mellemstore institutter.

En stor del af de ansattes ressourcer i risikostyringsfunktionen bruges til styring af kreditrisici. Undersøgelsen viser, at 45 pct. af de samlede ressourcer i anden forsvarslinje bliver brugt på kreditrisici, mens markedsrisici trækker på 16 pct. af ressourcerne, jf. figur 3. Dette er ikke overraskende, da kreditrisiko udgør langt den væsentligste risiko for institutterne. Der er dog stor variation institutterne imellem. SIFI virksomhederne afsætter typisk flere ressourcer end de mellemstore institutter til kreditrisiko.

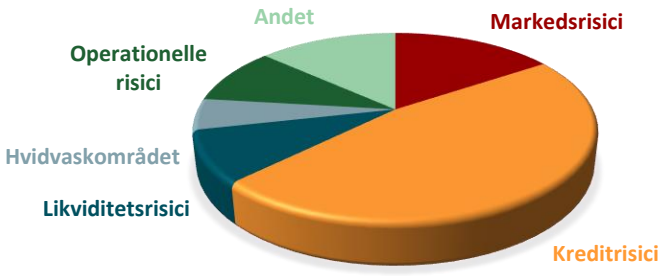
Et kreditinstitut er organiseret med tre forsvarslinjer:

<u>Første forsvarslinje</u> består af instituttets driftsfunktioner eller disponerende enheder. Det er her instituttet påtager sig risici, og disse risici skal identificeres, håndteres, måles og rapporteres. Der skal desuden ske en tilstrækkelig selvstændig kontrol af overholdelse af regler mv., så dette ikke baseres på anden forsvarslinjes kontrolindsats. Instituttet skal derfor have forretningsgange og arbejdsbeskrivelser til at sikre dette hos medarbejdere i første forsvarslinje.

<u>Anden forsvarslinje</u> består af risikostyrings- og compliancefunktionerne. Funktionerne har ansvaret for overvågning, kontrol og vurdering af risici. Funktionerne skal udarbejde en vurdering af, om arbejdet i første forsvarslinje er tilstrækkeligt i henhold til ledelsens instruktion, og stemmer overens med den valgte risikoprofil.

<u>Tredje forsvarslinje</u> er intern revision, der bl.a. har ansvaret for at vurdere, om instituttets interne kontrolsystem er hensigtsmæssigt og betryggende.

Figur 3: Ressourcer i risikostyringsfunktionen fordelt på opgavetyper

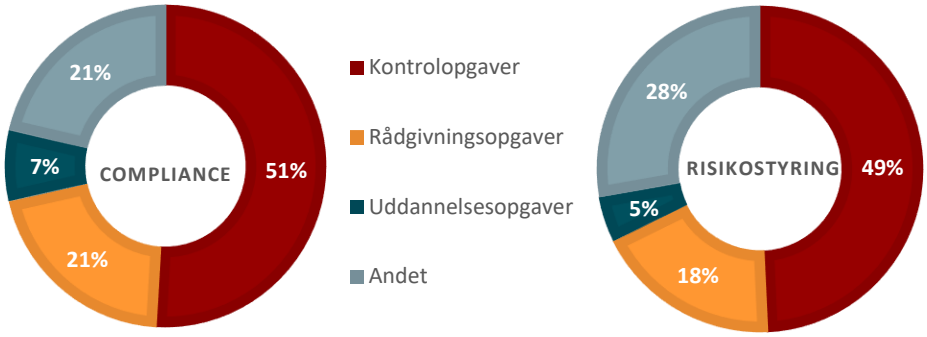


Note.: Fordelingen af ressourcer i risikostyringsfunktionen på opgavetyper. Grafen viser et simpelt gennemsnit af undersøgelsens deltagere.

I SIFI virksomhederne er omkring seks ud af 1.000 ansatte tilknyttet compliancefunktionen mod næsten syv medarbejdere i de mellemstore kreditinstitutter. Dette skal ses i lyset af, at SIFI virksomhederne i absolutte tal har betydelige flere ansatte i compliancefunktionen end de mellemstore institutter. Det giver SIFI virksomhederne nogle fordele ved stordrift, som de mellemstore institutter ikke har. Omvendt er kompleksiteten i SIFI virksomhedernes forretning større, og det medfører et behov for flere ressourcer. I absolutte tal har de mellemstore institutter mellem en og tre ansatte i compliancefunktionen.

Kontrolopgaver udgør i sagens natur en stor del af aktiviteterne i anden forsvarslinje. En oversigt over kreditinstitutternes tidsforbrug til forskellige aktiviteter viser, at såvel compliance- som risikostyringsfunktionen i gennemsnit bruger omtrent halvdelen af tiden på kontrolopgaver, jf. figur 4.

Figur 4: Compliancefunktionens hhv. risikostyringsfunktionens anslåede tidsforbrug på kontrol-, rådgivnings- og uddannelsesopgaver



Note.: Simpelt gennemsnit af undersøgelsens deltagere. "Andet" dækker over planlægning, udvikling, analyse, indberetning mv.

Institutterne bruger omkring en femtedel af tiden på rådgivningsopgaver både i compliancefunktionen og risikostyringsfunktionen. Enkelte institutter bruger

dog en væsentlig større andel af deres ressourcer på rådgivningsopgaver. Både compliancefunktionen og risikostyringsfunktionen skal udføre rådgivningsvirksomhed og eksempelvis inddrages ved udvikling af nye eller væsentlige ændringer af eksisterende produkter eller ved opstart af nye forretningsområder.

Det er dog vigtigt, at funktionernes rådgivningsvirksomhed ikke bliver så omfattende, at det går ud over ressourcerne til kontrolopgaverne.

Generelt afspejler institutternes ressourceprioritering i anden forsvarslinje, at det væsentligste risikoområde, kreditområdet, også er det højst prioriterede. Institutterne prioriterer desuden kontrolopgaverne højt. Disse er med til at sikre korrekt identifikation, måling, håndtering og rapportering af risici. Nogle institutter bruger dog relativt få ressourcer på kreditområdet i anden forsvarslinje, eller nedprioriterer kontrolopgaverne. Kreditrisiko er typisk den væsentligste risiko, og institutter, der alene bruger en lille andel af ressourcerne på denne i anden forsvarslinje, bør nøje overveje, om deres prioritering af området er tilstrækkelig. Institutterne skal sikre, at både første og anden forsvarslinje kontrollerer kreditområdet.

De fleste institutter har en kreditfunktion, som kan ligge enten i første eller anden forsvarslinje. Institutterne skal være opmærksomme på, at første forsvarslinje altid har det primære ansvar for at sikre forsvarlige bevillinger. I den forbindelse skal der i første forsvarslinje være funktionsadskillelse mellem de personer, som bevilger og etablerer, og de personer, som kontrollerer bevillingerne. Institutterne skal desuden være opmærksomme på, at der også skal ske overvågning og kontrol af bevillingsprocesserne i anden forsvarslinje.
Institutterne har også brug for en klar opgave- og ansvarsfordeling mellem og inden for forsvarslinjerne. Finanstilsynet forventer, at institutterne sikrer, at der er god kommunikation og samarbejde om opgaver og ansvar både inden for og på tværs af forsvarslinjerne. Dette skal sikre, at ingen risici bliver overset, fordi en funktion fejlagtigt tror, at en anden funktion dækker risikoen.

En klar definition af rammerne og grænsefladerne mellem enhederne i første og anden forsvarslinje kan hjælpe institutterne til mere effektivt at identificere forsvarslinjernes roller og ansvarsområder. Det er Finanstilsynets erfaring fra inspektioner, at det udførte arbejde har højere kvalitet i institutter, hvor instruksen for risikoansvarlig og complianceansvarlig klart og præcist beskriver ansvarsområder og snitflader. Ledelsen kan med en klar ansvarsfordeling bedre sikre, at risici bliver identificeret og håndteret.

Sikring af compliance og betryggende risikostyring på IT-området er en del af compliance- og risikostyringsfunktionernes ansvarsområde, men er i nogle institutter ikke tilstrækkeligt integreret i funktionernes opgave- og ansvarsfordeling. Institutterne bør derfor sikre, at IT-risici integreres i risikobilledet og

rapporteringen. Dette indebærer, at der er kompetencer til at vurdere IT-risici i anden forsvarslinje.

2. Compliancefunktionen sikrer compliance med alle områder indenfor lovgivningen

Compliancefunktionen sikrer, at instituttet udfører de opgaver, som lovgivningen kræver. Det gælder bl.a. at første forsvarslinje foretager de relevante egenkontroller, og at risikostyringsfunktionen løfter sine forpligtigelser i relation til kontrollen.

Det er erfaringen fra Finanstilsynets inspektionsvirksomhed, at nogle compliancefunktioner mest har fokus på compliance i forhold til hvidvaskområdet, forbrugerforhold og investorregler. Dette er ikke tilstrækkeligt, da compliancerisici omfatter alle væsentlige risici for manglende overholdelse af lovgivning mv., også lovkrav på kredit- og IT-området samt krav til ledelse og styring. Compliancefunktionen skal dermed også kontrollere risikostyringsfunktionens arbejde.

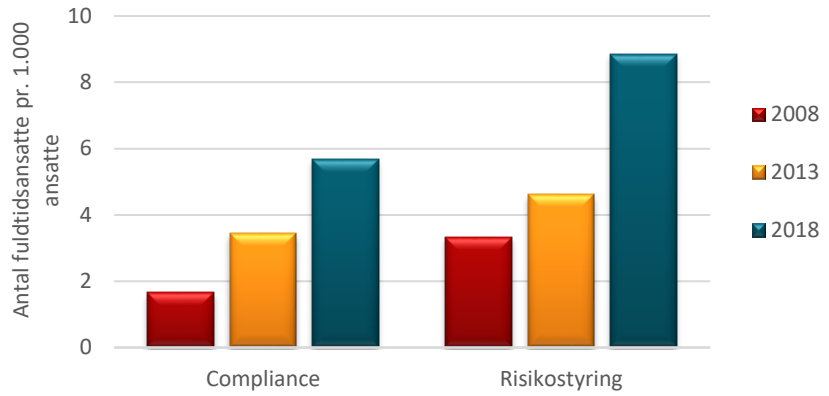
I mindre institutter, med mindre mulighed for bredde i kompetencerne i compliancefunktionen, kan denne funktion basere sig på risikostyringsfunktionens arbejde på områder, hvor risikostyringsfunktionen har en mere central rolle og derfor større kompetence. På kreditområdet kan det eksempelvis gælde kontrol af instituttets overholdelse af reglerne om likviditet i udlejningsejendomme. Hvis risikostyringsfunktionen har foretaget kontrol af området, vil det reducere behovet for compliancefunktionens kontrol. Compliancefunktionen skal dog være betrygget i risikostyringsfunktionens arbejde.

3. Tilstrækkelige ressourcer

Institutterne har de senere år fået større fokus på både compliance og risikostyring. Undersøgelsen viser, at antallet af fuldtidsansatte i compliance- og risikostyringsfunktioner er steget betragteligt over de seneste ti år. Undersøgelsen viser også, at selvom institutterne har oprustet på begge områder, så er det fra et lavt udgangspunkt. Der er samtidig stor spredning på, hvor meget de enkelte institutter har øget deres ressourcer. I undersøgelsen er det primært de større kreditinstitutter, der udviser den højeste vækst.

Undersøgelsen viser, at SIFI virksomhederne bruger næsten dobbelt så mange ressourcer på risikostyring som de mellemstore institutter. Institutterne bruger typisk i intervallet 0,5 pct. til 1,2 pct. af personale- og administrationsudgifterne til risikostyring, jf. figur 6.

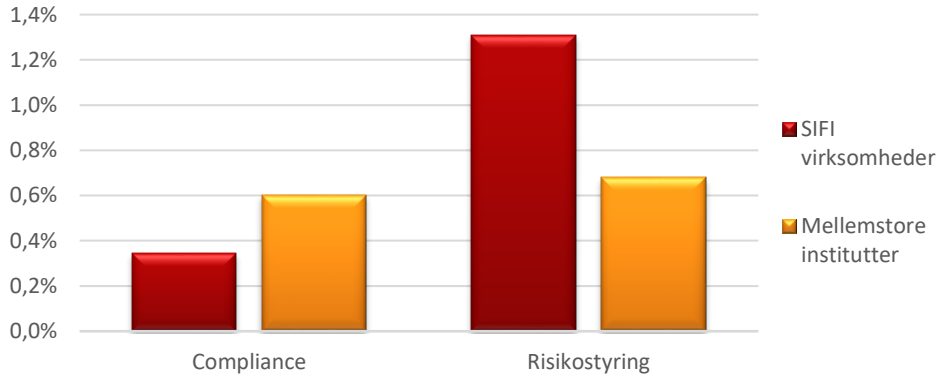
Figur 5: Udviklingen i antallet af fuldtidsansatte tilknyttet hhv. compliance og risikostyring i anden forsvarslinje



Note.: Simpelt gennemsnit af undersøgelsens deltagere. Et enkelt institut indgår ikke i grafen, da eksakte data ikke er tilgængelige. Instituttets udvikling med et voksende antal medarbejdere viser dog samme tendens som undersøgelsens øvrige deltagere. Ressourcer er omregnet til antal fuldtidsmedarbejdere pr. 1.000 medarbejdere.

Billedet er omvendt for compliancefunktionen, hvor SIFI virksomhederne bruger færre ressourcer end de mellemstore institutter. Som figur 2 viser, er forskellen noget mindre, når der alene ses på antallet af ansatte. Institutterne bruger typisk mellem 0,2 og 0,5 pct. af personale- og administrationsudgifterne til compliance.

Figur 6: Økonomisk budgetramme til hhv. compliance og risikostyring i anden forsvarslinje i procent af udgifter til personale og administration



Note.: Simpelt gennemsnit af afsatte ressourcer til compliance og risikostyring i procent af samlede udgifter til personale og administration.

Institutterne skal afsætte tilstrækkelige ressourcer til at sikre, at compliance- og risikostyringsfunktionerne kan varetage deres ansvarsområder korrekt og uafhængigt. Undersøgelsen viser, at der er stor forskel på, hvor mange ressourcer institutterne afsætter til risikostyring og compliance. Finanstilsynet

forventer, at de institutter, som ligger lavt ressourcemæssigt, er særligt opmærksomme på, om deres risikostyrings- og compliancefunktioner har tilstrækkelige ressourcer til, at funktionerne kan løfte deres opgaver.

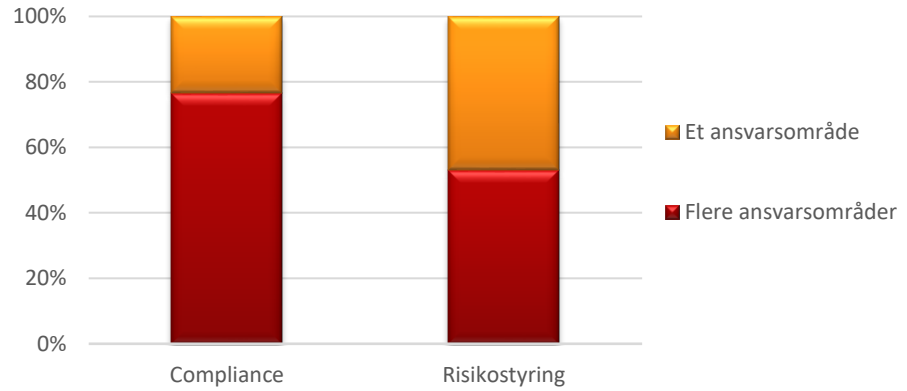
4. Uafhængighed og identifikation af interessekonflikter

I SIFI virksomheder er risikostyringsfunktionen placeret som en selvstændig enhed i organisationen lige under direktionen. I et enkelt tilfælde er den risikoansvarlige en del af direktionen. Denne organisering er også typisk tilfældet for compliancefunktionen.

I mellemstore institutter er funktionerne ofte organiserede under instituttets juridiske eller økonomiske afdeling. Det indebærer som udgangspunkt en større risiko for, at funktionerne ikke fungerer uafhængigt af resten af organisationen.

I størstedelen af institutterne er selve risikostyringsfunktionen en selvstændig enhed, der alene udfører opgaver relateret til risikostyring. Det gælder særligt kontrol og vurdering af risikostyringen, risikoanalyse og typisk også relaterede opgaver såsom udarbejdelse af ICAAP, ILAAP og overordnet risikorapportering. Alligevel har lidt over halvdelen af de risikoansvarlige andre opgaver eller ansvar for andre funktioner end risikostyringsfunktionen, jf. figur 7. Dette gælder specielt for de mellemstore institutter.

Figur 7: Den complianceansvarlige og den risikoansvarlige varetager flere ansvarsområder



Note.: Grafen viser, hvor stor en andel af de risikoansvarlige og de complianceansvarlige der også er ansvarlige for andre områder end risikostyring henholdsvis compliance.

I langt over halvdelen af institutterne har den complianceansvarlige andre ansvarsområder udover compliance, jf. figur 7. Den complianceansvarlige er i mindre institutter ofte også instituttets DPO (databeskyttelsesrådgiver) eller hvidvaskansvarlige eller har en rolle i forhold til instituttets overvågning af

f.eks. mistænkelige transaktioner, whistleblowere mv. Den complianceansvarlige er i nogle tilfælde også chef for direktionssekretariatet. I et enkelt institut er den complianceansvarlige og den risikoansvarlige samme person.

Institutterne har mulighed for at outsource deres opgaver til en ekstern part. Undersøgelsen viser, at SIFI virksomheder og de mellemstore institutter af naturlige årsager kun i begrænset omfang benytter sig af outsourcing, når det vedrører compliance og risikostyring.

Kreditinstitutternes bestyrelse er ansvarlig for, at institutterne sætter rammerne for en effektiv compliancefunktion og risikostyringsfunktion, mens det er direktionens ansvar at implementere rammerne. Både bestyrelsen og direktionen har en væsentlig rolle i forhold til at sikre en stærk compliance- og risikostyringskultur i kreditinstituttet. Der skal være klare retningslinjer for de compliance- og risikoansvarlige, og deres ansvarsområder skal være klart definerede.

Uafhængighed er et centralt krav til kreditinstitutternes compliancefunktion og risikostyringsfunktion, og institutterne skal have fokus på at sikre denne.

Er compliancefunktionen eller risikostyringsfunktionen ikke selvstændige enheder, skal instituttet udføre en grundig analyse af mulige interessekonflikter. På samme måde skal instituttet vurdere om interessekonflikten kan løses ved kompenserende foranstaltninger, så funktionerne fungerer uafhængigt af resten af organisationen. Vurderer instituttet, at de kompenserende foranstaltninger ikke er betryggende, bør organiseringen ændres. For SIFI virksomheder vil kompenserende foranstaltninger ikke være tilstrækkelige til at afdække interessekonflikterne for risikostyringsfunktioner, som ikke er selvstændige enheder. Risikostyringsfunktionen bør derfor være en selvstændig enhed lige under direktionen. Det samme gør sig i udgangspunktet også gældende for compliancefunktionen.

Finanstilsynet forventer, at den complianceansvarlige og den risikoansvarlige har henholdsvis compliance og risikostyring som hovedopgave og altså ikke har andre funktioner i et omfang, der fjerner fokus fra denne hovedopgave og dermed kan sætte uafhængigheden over styr.

Variabel aflønning

Fastsættelsen af vederlag til ansatte i en compliance- eller risikostyringsfunktion kan også bringe uafhængigheden i fare. Det følger f.eks. af aflønningsreglerne, at den risikoansvarlige og den complianceansvarlige skal udpeges som væsentlige risikotagere, da funktionerne har væsentlig indflydelse på virksomhedens risikoprofil. Væsentlige risikotagere er omfattet af aflønningsreglerne og dermed også af grænser for tildeling af variabel løn. Variabel løn, som tildeles ansatte, der udfører arbejde i forbindelse med virksomhedens

kontrolfunktioner, må ikke være afhængig af resultatet i de afdelinger, som de ansatte fører kontrol med.

Størstedelen af undersøgelsens institutter aflønner ansatte i compliance- og risikostyringsfunktionerne udelukkende med fast løn. Fire af undersøgelsens institutter giver mulighed for variabel løn til den complianceansvarlige og den risikoansvarlige, mens yderligere et institut giver mulighed for variabel løn til alle ansatte i compliance- og risikostyringsfunktionerne. Institutterne skal være opmærksomme på, at variabel løn ikke må bringe uafhængigheden i fare.

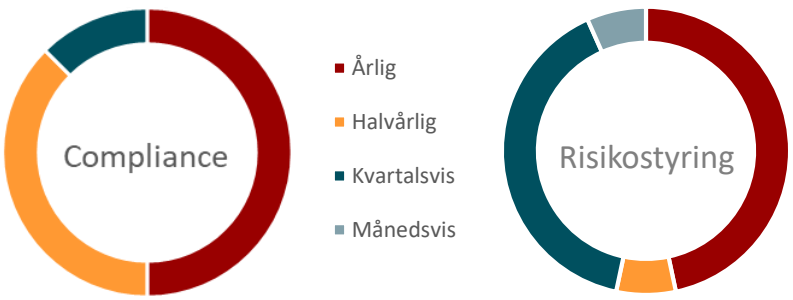
De institutter, der anvender variabel løn, anvender ofte et bonus- eller performancetillæg, som afhænger af en individuel og ekstraordinær indsats fra den enkelte medarbejder i kombination med afdelingens resultater. Den variable løn er i mindre grad baseret på instituttets samlede resultat. Udbetalingen af den variable løn sker efter en konkret vurdering af den risikoansvarliges eller den complianceansvarliges samlede indsats i deres jobfunktion.

5. Rapportering giver bestyrelsen et dækkende risikobillede

Undersøgelsen viser, at den risikoansvarlige ofte har en hyppigere rapporteringsfrekvens end den complianceansvarlige, jf. figur 8. Begge rapporterer skriftligt til både direktion og bestyrelse. Desuden deltager den complianceansvarlige og den risikoansvarlige i størstedelen af institutterne også på enten bestyrelses- eller direktionsmøder. I få institutter består den regelmæssige rapportering dog kun af en skriftlig rapport, som hverken bliver suppleret med deltagelse på bestyrelses- eller direktionsmøder.

Den complianceansvarlige i de mellemstore kreditinstitutter rapporterer typisk årligt eller halvårligt til bestyrelsen, mens frekvensen er højere i SIFI-virksomhederne.

Figur 8: Den risikoansvarliges og den complianceansvarliges rapporteringsfrekvens til bestyrelsen



Note.: Grafen viser, hvor ofte den risikoansvarlige og den complianceansvarlige rapporterer til bestyrelsen. Rapporteringen kan være gennem en skriftlig rapport eller ved deltagelse på et bestyrelsesmødet.

Den risikoansvarlige i SIFI virksomhederne har typisk en kvartalvis rapportering til bestyrelsen. I de mellemstore kreditinstitutter viser undersøgelsen, at rapporteringsfrekvensen varierer mellem en årlig, halvårlig eller kvartalsvis rapportering til bestyrelsen.

I størstedelen af institutterne har den complianceansvarlige og den risikoansvarlige en højere rapporteringsfrekvens til direktionen end til bestyrelsen. SIFI virksomhederne har en kvartalsvis afrapportering, mens frekvensen er meget forskellig i de mellemstore institutter, hvor afrapporteringer til direktionen sker alt mellem en gang om året til en gang om måneden.

Rapporteringen fra den risikoansvarlige skal give bestyrelsen et samlet og dækkende overblik over instituttets risici. Rapporteringen fokuserer særligt på de væsentlige interne og eksterne risici. Disse dækker både over finansielle og ikke finansielle risici, eksempelvis udviklingen på alle væsentlige risikoområder, reguleringsmæssige og økonomiske rammer, nye forretningsområder eller forretningsområder med høj vækst samt ændringer i forretningsmodel og strategi. Rapporteringen skal også følge op på instituttets opfyldelse af sin risikoappetit. Den skal desuden indeholde den risikoansvarliges vurdering af, om virksomhedens risikostyring er betryggende, dvs. om risikostyringen i instituttet sikrer, at alle væsentlige risici identificeres, måles, håndteres og rapporteres korrekt. Den risikoansvarlige skal sikre, at bestyrelsen får kendskab til og er opmærksom på væsentlige mangler i risikostyringen. Den risikoansvarlige skal også sikre, at bestyrelsen kender til en faktisk eller potentiel væsentlig negativ udvikling i instituttets risikoprofil.

Rapporteringen fra den complianceansvarlige skal give et klart billede af instituttets compliancerisici, ændringsbehov og tiltag for at mindske compliancerisici samt compliancefunktionens udførte arbejde. Rapporteringen bør også inddrage de compliancerisikomæssige konsekvenser af strategiske og forretningsmæssige beslutninger.

Rapporteringen fra både den risikoansvarlige og den complianceansvarlige bør indeholde anbefalinger til udbedring af identificerede mangler, bl.a. korrigerende foranstaltninger. Ledelsen skal hurtigt og effektivt følge op på disse.

Det udførte arbejde skal fremgå af rapporteringen, så bestyrelsen kan forholde sig til grundlaget for konklusionerne. Finanstilsynet finder, at det ikke er tilstrækkeligt med en erklæring fra den compliance- og den risikoansvarlige med en kortfattet konklusion om, at risikoområderne er i orden.

Rapporteringen bør omfatte de risici for identificerede mangler, som manglerne medfører. Dette involverer konsekvensanalyser, anbefalinger og korrigerende foranstaltninger fra den risikoansvarlige eller complianceansvarlige. Ledelsen skal hurtigt og effektivt følge op på konklusionerne og håndtere an-

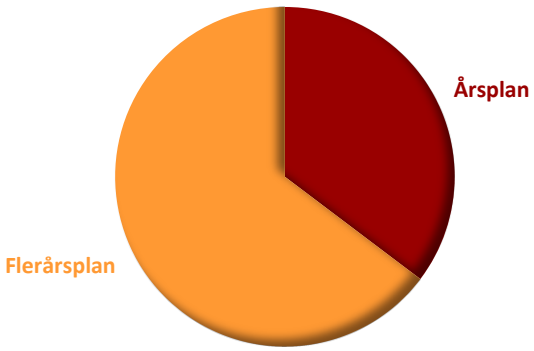
befalingerne, samt i relevant omfang gennemføre korrigerende foranstaltninger. Virksomhederne bør have klare retningslinjer for opfølgning på den complianceansvarliges og den risikoansvarliges konklusioner.

Finanstilsynet anbefaler, at rapporteringen til bestyrelsen foruden en skriftlig rapport består af en mundtlig præsentation af rapporten fra henholdsvis den risikoansvarlige og den complianceansvarlige. Dette giver bestyrelsen mulighed for at stille spørgsmål direkte til den risikoansvarlige og den complianceansvarlige.

6. Årsplaner og risikobaseret prioritering

SIFI virksomheder og mellemstore institutter arbejder alle med enten års- eller flerårsplaner for både compliance og risikostyring, jf. figur 9. Institutterne udarbejder hvert år en årsplan eller flerårsplan med opgaver og fokusområder for det eller de kommende år. Fokusområderne er udvalgt med afsæt i en risikovurdering og prioriterer de væsentlige risici først. Den risikoansvarlige og den complianceansvarlige udarbejder en risikovurdering på hvert deres område, hvorfra ledelsen prioriterer opgaver og fokusområder. Risikovurderingen og årsplanerne opdateres efter behov og som minimum en gang årligt.

Figur 9: Kreditinstitutter der arbejder med enten årsplaner eller flerårsplaner



Note.: Alle SIFI virksomheder og mellemstore kreditinstitutter bruger som minimum årsplaner. 65 pct. af institutterne bruger også flerårsplaner med opgaver og indsatsområder.

Det er Finanstilsynet erfaring fra inspektioner, at flerårsplaner medvirker til at sikre, at alle væsentlige risikoområder regelmæssigt bliver kontrolleret, og at der er overblik over og sammenhæng mellem kontrolfrekvensen på områderne og instituttets vurdering af væsentligheden. Det er med til at sikre en tilstrækkelig kontrol og vurdering af de enkelte områder. Med en flerårig tilgang mindsker instituttet risikoen for, at områder ud fra en kortsigtet prioritering helt forbigås i en længere periode.

Flerårsplanen bør være fremsynet, dække en årrække på to til fire år og blive opdateret jævnligt. Det er samtidig naturligt, at instituttet fastlægger en mere

detaljeret og præcis plan for det kommende år, der også tager bestik af ændringerne i instituttets aktuelle risikobillede.

Finanstilsynet forventer, at institutternes planer tager udgangspunkt i en risikovurdering, så de har fokus på de væsentligste risici, og så prioriteringen af opgaver bliver risikobaseret. En grundig risikovurdering sikrer samtidig et godt overblik og indsigt i alle væsentlige risikoområder. Der skal være en klar sammenhæng mellem risikovurderingen og årsplanerne.

Mere sporadisk dækning af et risikoområde bør være begrundet i en risikovurdering og er mest relevant for mindre institutter, hvor forretningsmodel og risikoprofil er mere overskuelige. Nedprioritering kan ske, så længe der ikke er tale om et væsentligt område for det enkelte institut. I mindre institutter tillades en mere overfladisk gennemgang af væsentlige områder, hvis det kan dokumenteres, at risikoen forbundet med dette er begrænset.

Institutterne må ikke nedprioritere alene med en begrundelse om begrænsede ressourcer, og de skal altid have en forsvarlig compliance og risikostyring. Institutterne skal derfor sikre sig, at de kun påtager sig overskuelige risici, som de er i stand til at styre forsvarligt med de tilgængelige ressourcer og kompetencer.

Årsplanen skal samtidig være konsistent med de tilgængelige ressourcer. Opprioriterer et institut ekstraordinært visse områder, f.eks. i relation til kreditter, hvidvask eller investorbeskyttelse, bør instituttet tilføre ressourcer til håndtering af disse risici.

7. Høj organisatorisk forankring og mulighed for at udtale sig om risici

Den risikoansvarlige og den complianceansvarlige i SIFI virksomheder er en del af eller refererer direkte til direktionen. Hvis de ikke er en del af direktionen, bør det direktionsmedlem, de refererer til, ikke have ansvar for væsentlige forretningsmæssige risici (medmindre der er tale om den administrerende direktør).

Kun i ganske få institutter rapporterer den complianceansvarlige og den risikoansvarlige til bestyrelsen uden direktionens tilstedeværelse. Specielt den complianceansvarlige har en begrænset adgang til bestyrelsen udenom direktionen.

Lovgivningen kræver, at den risikoansvarlige og den complianceansvarlige har mulighed for at henvende og udtale sig direkte til bestyrelsen uafhængigt af direktionen.

Finanstilsynet forventer, at den risikoansvarlige og den complianceansvarlige mindst en gang om året deltager på et bestyrelsesmøde. I nogle institutter

forlader direktionen bestyrelsesmødet under fremlæggelse fra den complianceansvarlige og den risikoansvarlige. Erfaringen herfra er, at det er med til at understrege den complianceansvarliges og den risikoansvarliges særlige ansvar og rolle. Bestyrelsen har samtidig en mulighed for at få et førstehåndsindtryk af nøglepersoner i organisationen med henblik på at kunne vurdere kvaliteten af arbejdet.

Undersøgelsen viser, at den risikoansvarlige i kun fire institutter i løbet af de seneste tre år har givet udtryk for betænkeligheder og advaret bestyrelsen udenom de faste rapporteringer. Det er sket i tilfælde, hvor en specifik risikoudvikling har påvirket eller kunnet påvirke virksomheden.

Det er vigtigt, at compliancefunktionen og risikostyringsfunktionen tør "sparke døren ind" til bestyrelsen, hvis de observerer væsentlige risici eller andre misforhold, der ikke er håndteret korrekt. Advarsler og betænkeligheder afgivet af risikostyringsfunktionen og compliancefunktionen skal dokumenteres, og instituttet bør have procedurer til at sikre dette.

8. Inddragelse i væsentlige beslutningsprocesser

Undersøgelsen viser, at risikostyringsfunktionen i næsten alle SIFI virksomheder de seneste tre år er blevet inddraget i alle væsentlige beslutninger, inden disse er blevet truffet. Den risikoansvarlige er også blevet hørt i forbindelse med SIFI virksomhedernes udvikling eller væsentlige ændringer af produkter og tjenesteydelser. Derudover holder den risikoansvarlige i flere af institutterne også faste møder med direktionen eller direktionsmedlemmer, hvor risici og nye tiltag bliver drøftet. Den risikoansvarlige kan desuden holde faste f.eks. kvartalsvise møder, med instituttets største risikotagere.

I de mellemstore institutter bliver risikostyringsfunktionen også inddraget i væsentlige beslutninger. Inddragelsen går fra en gang om året i nogle institutter til et par gange i løbet af kvartalet i andre. Risikostyringsfunktionen bliver f.eks. inddraget i forbindelse med nye produkter og forretningsområder, strategi, kreditændringer, etablering af nye filialer, efterstillet kapital mv.

Compliancefunktionen bliver ikke i samme omfang inddraget i forbindelse med væsentlige beslutninger. Både i SIFI virksomheder og mellemstore institutter er der stor forskel på, hvor ofte compliancefunktionen er blevet hørt de seneste tre år. For flere institutter, inklusive SIFI virksomheder, er compliancefunktionen slet ikke blevet hørt de seneste tre år. I andre institutter bliver compliancefunktionen hørt ved samtlige større beslutninger, som kan omfatte implementering af ny lovgivning, ændring af processer, produktgodkendelser, strategier, aktieudvidelser mv.

Tre af undersøgelsens deltagere har ikke udarbejdet retningslinjer for, hvilke beslutninger ledelsen skal høre risikostyringsfunktionen om og hvordan. Fem

af undersøgelsens institutter mangler klare retningslinjer for compliancefunktionen.

Den risikoansvarlige og den complianceansvarlige skal have mulighed for at udtale sig om risici forbundet med større dispositioner, som instituttet påtænker at foretage. Hvis den risikoansvarlige eller den complianceansvarlige har betænkeligheder vedrørende en disposition, skal den pågældende straks informere direktionen om dette. Den risikoansvarlige eller den complianceansvarlige skal straks informere bestyrelsen, hvis direktionen alligevel vælger at foretage dispositionen, og den risikoansvarlige eller den complianceansvarlige fortsat har betænkeligheder.

Det fremgår at ledelsesbekendtgørelsen, at den risikoansvarlige skal deltage eller som minimum høres i forbindelse med udvikling og godkendelse af nye tjenesteydelser og produkter. Den risikoansvarlige skal løbende være informeret om forløbet af godkendelsesprocessen. Den risikoansvarlige 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 skal altid kunne kræve, at en ændring af et eksisterende produkt skal behandles som et nyt produkt.

Af EBA/GL/2017/11 (Internal Governance) fremgår, at compliancefunktionen også bør have en tilsvarende rolle i forbindelse med udvikling og godkendelse af nye tjenesteydelser og produkter.

Finanstilsynet forventer, at institutternes ledelser i højere grad hører den complianceansvarlige i forbindelse med beslutningsprocesser, hvor det er relevant, eksempelvis ved vurdering af virkningen af en ny eller ændret lovgivning eller tilsynsmæssige krav. Den complianceansvarlige bør også høres om nye tjenesteydelser og produkter. Det kan f.eks. ske ved at sidde med i instituttets produktgodkendelsesudvalg. Af hensyn til uafhængigheden bør den complianceansvarlige ikke lede udvalget eller have beslutningskompetencer, men alene deltage ved at sige fra overfor produkter med for store compliancerisici.

Finanstilsynet forventer, at institutterne som minimum har procedurer for, hvornår ledelsen skal inddrage risikostyringsfunktionen og compliancefunktionen i beslutninger.

9. Den complianceansvarlige og den risikoansvarlige bør være erfarne

Undersøgelsen viser, at den complianceansvarlige og den risikoansvarlige generelt er erfarne medarbejdere med mange års indsigt fra funktionerne eller lignende stillinger. Der er tale om medarbejdere med længere videregående uddannelser og ofte med en vis grad af ledererfaring, som de har tilegnet sig

inden de fik stilling som compliance- eller risikoansvarlig. De complianceansvarlige og de risikoansvarlige har typisk 20 - 30 års erfaring indenfor den finansielle sektor.

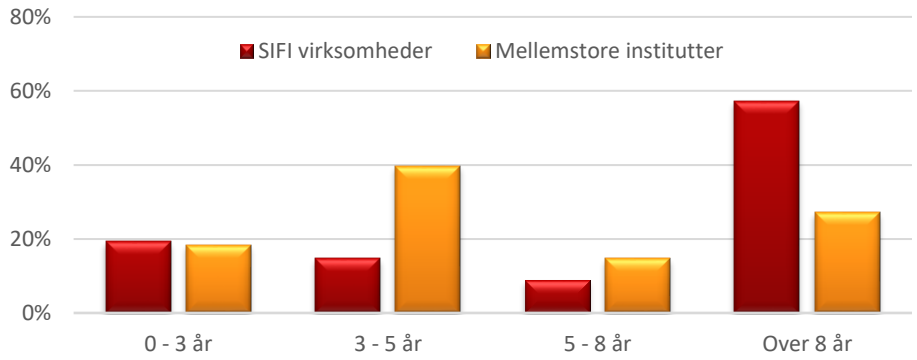
Den complianceansvarlige har typisk en juridisk baggrund, og flere har i en årrække inden ansættelsen arbejdet som advokater. Enkelte institutter har valgt en complianceansvarlig med revisorbaggrund.

De risikoansvarlige har en mere blandet uddannelsesmæssig baggrund. Fælles for dem alle er dog, at de i et vist omfang er uddannet eller efteruddannet indenfor økonomi, finansiering eller regnskab.

Den complianceansvarlige og den risikoansvarlige bør have et betydeligt kendskab til organisering og risikoområder i et kreditinstitut for at kunne varetage deres arbejde betryggende. Finanstilsynet forventer, at personer, som bliver ansat som compliance- eller risikoansvarlig, har betydelig erfaring fra arbejdet i et kreditinstitut. Hvad angår SIFI virksomheder forventer Finanstilsynet også, at de complianceansvarlige og risikoansvarlige inden ansættelsen har opnået erfaring fra arbejdet i selve funktionen eller gennem lignende funktioner.

Ansatte i compliance- og risikostyringsfunktionerne
Undersøgelsen viser, at de ansatte i compliance- eller risikostyringsfunktionerne har en gennemsnitlig ansættelsestid på lige under fire år. De ansatte har dog typisk i en årrække inden været ansat i instituttet i en anden stilling.

Figur 10: Andel af fuldtidsansatte med erfaring fra en risikostyringsfunktion eller lignende funktion i sektoren fordelt på ansættelsestid



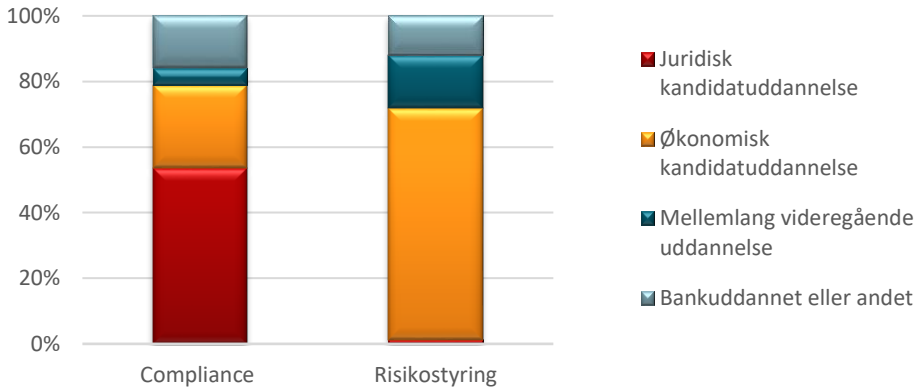
Note: Simpelt gennemsnit af undersøgelsens deltagere. Grafen viser fuldtidsansatte med erfaring fra en risikostyringsfunktion eller lignende funktion i sektoren fordelt på ansættelsestid.

Undersøgelsens resultater viser, at erfaringsgrundlaget for ansatte i en compliancefunktion spænder bredt, idet compliancefunktionerne i både SIFI-virksomhederne og mellemstore institutter beskæftiger helt nyuddannede såvel som ansatte med over otte års anciennitet.

I risikostyringsfunktionen har de ansatte i de mellemstore institutter typisk mellem tre og fem års erfaring fra en risikostyringsfunktion, mens ansatte i SIFI virksomhedernes risikostyringsfunktion har betydeligt mere erfaring med området, da de typisk har over otte års erfaring fra en risikostyringsfunktion, jf. figur 10.

I compliancefunktionen har de ansatte ofte en juridisk baggrund, mens ansatte i risikostyringsfunktionen primært kommer med en økonomisk baggrund, jf. figur 11. Kun enkelte institutter har en overvægt af økonomer ansat i deres compliancefunktion.

Figur 11: Uddannelsesmæssig fordeling for ansatte, der er tilknyttet compliance og risikostyring i anden forsvarslinje



Gennem de seneste ti år er kreditinstitutterne gået fra at have bankuddannede til at have medarbejdere med en kandidatgrad ansat i funktionerne. Der er specielt sket en ændring i risikostyringsfunktionen, hvor institutterne i stigende grad har tendens til at ansætte medarbejdere med en lang videregående økonomisk uddannelse i stedet for bankuddannede.

10. De complianceansvarlige og risikoansvarlige har adgang til relevant viden

Direktionen skal sikre, at risikostyringsfunktionen og compliancefunktionen har adgang til alle relevante oplysninger, og direktionen har ansvar for at videregive information, som kan have betydning for funktionernes arbejde.

Finanstilsynet forventer, at direktionen indgår i dialog med den risikoansvarlige og den complianceansvarlige om, hvilken information der kan have betydning for deres arbejde. Direktionen bør sikre foranstaltninger, så relevant information kan tilgås af den risikoansvarlige og den complianceansvarlige i retvisende og dækkende form, så eventuelle foranstaltninger kan igangsættes uden unødigt ophold.