FINANSTILSYNET

N O T A T

Finanstilsynet

29. november 2022

J.nr.
/KLAS

Inspektioner af styring af operationel risiko i kreditinstitutter

I 2021 og 2022 har Finanstilsynet gennemført inspektioner af styringen af operationel risiko i store danske pengeinstitutter. Inspektionerne er afsluttet med rapportering til det enkelte pengeinstitut og offentliggørelse af Finanstilsynets redegørelser.

På baggrund af inspektionerne i de store danske pengeinstitutter og af det ordinære tilsyn med kreditinstitutterne finder Finanstilsynet anledning til i dette notat at dele nogle observationer og erfaringer, som i forskelligt omfang er relevante for kreditinstitutter, og som de bør tage i betragtning i deres tilrettelæggelse af styringen af operationel risiko.

Der er krav til styringen af operationel risiko i bilag 3 til bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. (ledelsesbekendtgørelsen, bekendtgørelse nr. 1103 af 30. juni 2022).

> Nr. 1 i bilag 3 til ledelsesbekendtgørelsen:
>
> 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.

Notatet er ikke en generel vejledning i styring af operationel risiko.

1. Styringen af operationel risiko tilrettelægges typisk inden for fem hovedaktiviteter

Operationel risiko er som risikotype karakteriseret ved at spænde over meget forskelligartede risici, hvad angår potentielle tabshændelsers årsager, hvor de kan opstå, og hvad konsekvenserne af dem kan være.

De store pengeinstitutter tilrettelægger typisk styringen af operationel risiko inden for fem hovedaktiviteter, som blandt andet dækker udførelsen af kravene i nr. 5 i bilag 3 til ledelsesbekendtgørelsen om identifikation og nedbringelse af risici samt registrering, kategorisering og rapportering af tabshændelser.

> Nr. 5 i bilag 3 til ledelsesbekendtgørelsen:
>
> 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.
>
> …
>
> 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.

De følgende afsnit i notatet omhandler Finanstilsynets observationer og erfaringer inden for hver af de fem hovedaktiviteter, som er:

- Identifikation af risici: Hvordan institutterne sikrer sig, at de er opmærksomme på, hvilke tabshændelser de kan blive udsat for.
- Vurdering af risici: Hvad sandsynligheden er for, at en tabshændelse indtræffer, og hvad konsekvenserne kan være af den.
- Nedbringelse af risici: Hvilke foranstaltninger institutterne kan have for at nedbringe sandsynligheden for, at en tabshændelse indtræffer, eller nedbringe konsekvensen af den.
- Overvågning af risici: Hvordan institutterne sikrer, at de for hver identificeret risiko har opdateret viden om sandsynligheden for, at en tabshændelse indtræffer, og konsekvenserne ved den, og at de har samlet overblik over de identificerede risici.

- Risikorapportering og strategiske mål: Hvordan institutterne sikrer, at de relevante ledelseslag har tilstrækkelig information til at vurdere, om risikoniveauet er acceptabelt i forhold til instituttets strategiske mål, eller der er behov for yderligere nedbringelse af en eller flere risici.

Ved ordinære inspektioner har Finanstilsynet observeret, at mindre og mellemstore institutter ofte mangler metoder, der sikrer en systematisk tilgang til en eller flere af de fem hovedaktiviteter. Risikostyringen bliver ofte orienteret imod løsning af specifikke enkeltopgaver, mens andre opgaver ikke løses eller kun løses overfladisk. Finanstilsynet ser for eksempel, at nogle institutter har stor fokus på overvågning af risici i form af registrering af faktiske tabshændelser, mens de i mindre omfang sikrer en systematisk identifikation, vurdering og nedbringelse af risici. Nogle institutter har opmærksomhed på styring af bestemte typer af operationelle risici, mens andre operationelle risici kun håndteres overfladisk eller slet ikke.

For at holde rede på de forskelligartede risici, som er omfattet af operationel risiko, foretager de store institutter ofte en inddeling af risiciene med udgangspunkt i et internationalt sektordrevet klassifikationssystem (ORX Reference Taxonomy), som de tilpasser til instituttets egne forhold.

Det er vigtigt, at institutterne tilrettelægger deres styring af operationel risiko, så de har en systematisk tilgang til alle væsentlige aktiviteter i risikostyringen, herunder de fem hovedaktiviteter, som er nævnt ovenfor. Udeladelse eller nedprioritering af dele af risikostyringen vil medføre, at institutterne mangler overblik over deres risici og kan overse et behov for at foretage risikoreducerende eller andre korrigerende handlinger.

De store pengeinstitutter har stor opmærksomhed på at indføre en systematisk tilgang til alle dele af risikostyringen. Det sker med brug af metoder, som gør det muligt at kæde informationer sammen igennem hele risikostyringsprocessen fra risikoidentifikation til risikoovervågning og rapportering. Derved sikres det, at de kan foretage målrettede indsatser, når de konstaterer en uønsket udvikling. De implementerer ofte IT-værktøjer, som muliggør behandling og samkøring af informationer om risikoidentifikation, risikovurderinger, risikonedbringende kontroller og faktiske tabshændelser. Samling af informationerne et sted har åbenlyse fordele for blandt andet overvågning og rapportering af risiciene.

For eksempel bør et stigende omfang af tabshændelser på et konkret område give anledning til, at instituttet genovervejer risikovurderingen for at sikre et opdateret risikobillede og tilpasser de risikonedbringende kontroller for at nedbringe omfanget af tab fremadrettet. For at opnå det skal instituttet kunne kæde oplysninger om tabshændelser sammen med de relevante risikovurderinger og tilhørende kontroller og have procedurer for regelmæssig vurdering og tilretning af kontrollerne. Hvis instituttet ikke har overblik over sine kontrol-

ler eller mangler forretningsgange for regelmæssig tilretning af dem, er der risiko for, at et forhøjet niveau af tabshændelser blot rapporteres til ledelsen, uden at der foretages passende skridt til at nedbringe niveauet.

Finanstilsynet lægger vægt på, at risikostyringen er tilpasset det enkelte institut under hensyntagen til instituttets størrelse og forretningsmodel. Risikostyringen skal dog altid indrettes, så den sikrer overblik og giver instituttet mulighed for aktiv risikostyring. Mindre institutter har normalt mindre avancerede eller håndholdte måder at samkøre informationer. Det forudsætter dog altid en systematisk tilgang i risikostyringen.

2. Identifikation af risici tager udgangspunkt i kortlægning af processer

Det er er beskrevet i afsnit 1, at operationel risiko som risikotype er karakteriseret ved at spænde over meget forskelligartede risici. Det indebærer blandt andet, at det kan være vanskeligt for institutterne at sikre, at alle risici bliver identificeret i overensstemmelse med nr. 5, litra a, i bilag 3 til ledelsesbekendtgørelsen.

> Nr. 5 i bilag 3 til ledelsesbekendtgørelsen:
>
> 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.
> …

Kreditinstitutter baserer ofte deres risikoidentifikation på, at udvalgte medarbejdere med en samlet bred viden om instituttets drift indkaldes regelmæssigt (ofte en gang årligt) for at dele informationer om eventuelle nye eller ændrede risici. Informationerne kan blandt andet være baseret på erfaring fra tabshændelser, der er indtruffet, og på viden om ændringer i interne eller eksterne forhold, som kan tænkes at påvirke instituttets operationelle risiko. Informationerne indgår i en opdatering af instituttets risikovurderinger og overblik over dets operationelle risici.

Finanstilsynet er enig i, at opsamling af ekspertviden er en værdifuld kilde til identifikation af nye og ændrede risici. Finanstilsynet finder dog, at en mere metodisk tilgang i væsentlig grad kan bidrage til at sikre, at institutterne får identificeret og vurderet alle risici.

De store pengeinstitutter baserer typisk identifikation af operationelle risici på en kortlægning af deres processer. Med et detaljeret procesoverblik har insti-

tutterne mulighed for at gennemføre en systematisk vurdering af, hvor og hvordan der kan opstå fejl, som kan medføre operationelle tab. Suppleret af opsamling af ekspertviden øger det sandsynligheden for, at institutterne får identificeret deres risici.

Mindre og mellemstore institutter har typisk en mere enkel forretningsmodel end de store institutter og mere enkle og overskuelige processer. Som udgangspunkt vil en kortlægning af processerne derfor være nemmere at gennemføre i de mindre og mellemstore institutter.

Når direktionen træffer principielle eller væsentlige beslutninger, jf. nr. 10 i bilag 3 til ledelsesbekendtgørelsen, indebærer det i særlig grad sandsynlighed for, at der kan opstå nye eller ændrede operationelle risici.

> Nr. 10 i bilag 3 til ledelsesbekendtgørelsen:
>
> 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.

Mange institutter mangler helt eller delvist forretningsgange, som sikrer, at der bliver foretaget forhåndsvurderinger af, om beslutninger medfører nye eller ændrede operationelle risici. Nogle institutter har forretningsgange om forhåndsvurdering ved særlige typer af beslutninger. Det kan f.eks. være ved beslutninger om nye produkter eller nye systemer.

Finanstilsynet vurderer, at institutter, som har en procesmæssig tilgang til identifikation af operationelle risici, har særligt gode forudsætninger for at vurdere, i hvilket omfang beslutninger påvirker processerne og derfor har risikomæssige konsekvenser.

Operationelle risici, hvor tabshændelser sker med lav sandsynlighed, men hvor konsekvenserne kan være store (halerisici), kan være vanskelige at identificere og vurdere, fordi institutterne i sagens natur har begrænset eller ingen praktisk erfaring med dem. Samtidig er det netop de risici, som i særlig grad kan påvirke institutternes robusthed, og hvor der er særlig grund til at analysere risiciene og overvåge relevante risikoindikatorer.

Nr. 7 i bilag 3 til ledelsesbekendtgørelsen peger på scenarieanalyse som en metode til at vurdere halerisici. Scenarieanalyse er en metode til at identificere, analysere og kvantificere risici under forskellige omstændigheder. Scenarieanalyse indebærer typisk en bred involvering af fageksperter og ledere på forskellige områder i at fastlægge og analysere de forhold, som i scenarierne påvirker dels sandsynligheden for tabshændelser, dels konsekvenser af tabshændelserne. Scenarieanalyse er særligt velegnet til at identificere og analysere halerisici.

> Nr. 7 i bilag 3 til ledelsesbekendtgørelsen:
>
> Bestyrelsens retningslinjer til direktionen, jf. §§ 6 og 7, skal indeholde følgende:
>
> …
>
> 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.
> …

Institutterne bruger kun i begrænset omfang scenarieanalyser til at identificere og vurdere halerisici. De store pengeinstitutter bruger typisk scenarieanalyser til at vurdere risici inden for IT-området. De har ofte planer om at udvide brugen af dem til andre risikoområder.

Finanstilsynet opfordrer institutterne til at bruge scenarieanalyser i større omfang til identifikation og vurdering af halerisici. En bred involvering af fageksperter og ledere i analyse af konkrete scenarier vil ofte i sig selv føre til en mere nuanceret identifikation og vurdering af risiciene. Særligt i mindre og mellemstore institutter kan selv simple og afgrænsede analyser medvirke til at øge forståelsen af risiciene.

3. Vurdering af risici omfatter både iboende risiko og restrisiko

I nogle institutter er det uklart, hvilke operationelle risici der forelægges bestyrelsen til vurdering, og hvad bestyrelsen konkret forholder sig til ved vurderingen af virksomhedens enkelte og samlede risici som krævet i nr. 3 i § 3, stk. 1, i ledelsesbekendtgørelsen.

§ 3, stk. 1, i ledelsesbekendtgørelsen:

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

…

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,
…

En af udfordringerne er, at operationelle risici kan være vanskelige at kvantificere. Tabshændelser har ikke altid umiddelbart en finansiel konsekvens, som kan sammenholdes med et beløbskriterium for, hvornår bestyrelsen skal involveres. For mange operationelle tabshændelser overstiger de ikke-finansielle konsekvenser som for eksempel påvirkning af kundetilfredshed, påvirkning af omdømme og regelefterlevelse langt det umiddelbart konstaterbare finansielle tab.

For at bestyrelsen kan vurdere instituttets enkelte og samlede risici, skal instituttet sikre en systematisk vurdering af de identificerede operationelle risici.

De store pengeinstitutter bruger typisk en metode, hvor hver enkelt identificerede operationelle risiko vurderes dels for sandsynligheden for, at en tabsbegivenhed indtræffer, dels for de mulige konsekvenser af en begivenhed. Da konsekvenserne kan være vidt forskellige, vurderer de store pengeinstitutter typisk konsekvenserne på flere områder. Det kan for eksempel være økonomiske konsekvenser, konsekvenser for kundetilfredshed, konsekvenser for instituttets omdømme og konsekvenser for overholdelse af regler. Risikovurderingen angives typisk på en væsentlighedsskala for henholdsvis sandsynlighed og konsekvens, som gør det muligt at vægte og aggregere risici for eksempel i en matrix med 'trafiklys'-markering af, hvordan risikoen vurderes i forhold til instituttets strategiske mål for operationel risiko.

De store pengeinstitutter bruger typisk metoden til at vurdere risikoen både uden hensyntagen til effekten af risikonedbringende foranstaltninger (iboende risiko) og med hensyntagen til dem (restrisiko). Institutter bør vurdere den iboende risiko for at kunne tage stilling til behovet for risikonedbringende foranstaltninger. De store pengeinstitutter revurderer regelmæssigt både den iboende risiko og restrisikoen for at sikre, at de har en opdateret vurdering af effektiviteten af de risikonedbringende foranstaltninger. Særligt for risici med høj iboende risiko og lav restrisiko kan institutter, der alene vurderer restrisikoen, risikere at overse betydningen af at sikre, at de risikonedbringende foranstaltninger reelt har den effekt, som de er antaget at have ved vurdering af restrisikoen.

I nogle institutter får bestyrelsen desuden kun forelagt risici til vurdering, når restrisikoen overskrider en fastsat grænse. Derved får bestyrelsen ikke mulighed for at forholde sig til, om den er tryg ved vurderingen af effekterne af de kontroller og øvrige foranstaltninger, som har bragt risikoen ned under grænsen. Det finder Finanstilsynet utilstrækkeligt, og særligt for halerisici, hvor det kan have store negative konsekvenser for instituttets robusthed, hvis kontrollerne eller de øvrige foranstaltninger svigter.

4. Operationel risiko nedbringes ved brug af kontroller

Aktiv styring af operationel risiko indebærer brug af metoder til at nedbringe risici, som ligger ud over, hvad instituttet finder acceptabelt.

> Nr. 5 i bilag 3 til ledelsesbekendtgørelsen:
>
> 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:
>
> …
>
> b) Stillingtagen til, hvordan virksomhedens operationelle risici nedbringes til et acceptabelt niveau.
>
> …

Mange institutter mangler en systematisk tilgang til, hvordan de nedbringer operationelle risici til et acceptabelt niveau. Med de mange forskelligartede former for operationel risiko kan det være vanskeligt for institutterne at tage generel stilling til, hvordan operationelle risici skal nedbringes.

De store pengeinstitutter har typisk indført en kontroltilgang, hvor de etablerer specifikke kontroller til at nedbringe konkrete risici. Kontrollerne kan have til formål at reducere sandsynligheden for, at der indtræffer tabshændelser, ved at forebygge eller opdage tabshændelser, eller de kan reducere konsekvensen af, at en tabshændelse indtræffer. Nogle kontroller kan også være indrettet til at korrigere opståede fejl. Tilgangen kræver som regel, at instituttet etablerer en beskrivelse af de typer af kontroller, som den bruger, og hvordan effektiviteten af dem skal overvåges.

Instituttet har et godt grundlag for at vurdere restrisikoen, og om der er behov for yderligere risikonedbringende foranstaltninger, når det har:

- etableret et overblik over sine væsentlige processer

- identificeret og vurderet de risici, som er knyttet til hver enkelt proces
- overblik over de kontroller, som er etableret til at reducere hver enkelt risiko.

Ud over nedbringelse af tabshændelsers sandsynlighed og konsekvens ved brug af kontroller kan institutterne også nedbringe operationelle risici ved at ændre i forretningsmodellen, så f.eks. risikobehæftede processer ophører eller omlægges til mindre risikofyldte processer.

5. Ved overvågningen af operationel risiko er registrering og analyse af tabshændelser væsentlige elementer

Registrering og kategorisering af tabshændelser, jf. nr. 5, litra e, i bilag 3 til ledelsesbekendtgørelsen, er lige så vigtig for analyse og styring af operationel risiko, som registrering og analyse af misligholdte eksponeringer er det for styring af kreditrisiko.

> Nr. 5 i bilag 3 til ledelsesbekendtgørelsen:
>
> 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:
>
> …
>
> e) Overordnede principper for, hvordan virksomheden skal registrere og kategorisere tabshændelser.
>
> …

Institutterne er som regel opmærksomme på vigtigheden af at identificere og registrere tabshændelser med henblik på at begrænse det enkelte tab og opmærksomme på at følge og rapportere udviklingen i de samlede tab.

De store pengeinstitutter tilstræber som regel, at tabshændelser registreres og klassificeres på en måde, så de kan kædes sammen med de processer, risici og kontroller, som de vedrører. Med den gennemsigtighed har institutterne et bedre analytisk grundlag for at bruge informationer om tabshændelserne til at vurdere, om kontrollerne er tilstrækkelige, og om der er behov for at revurdere de enkelte risici.

I afsnit 1 er det beskrevet, at de store pengeinstitutter ofte implementerer IT-værktøjer, som muliggør behandling og samkøring af informationer på tværs af risikostyringens hovedaktiviteter. Mindre institutter har normalt mindre avancerede eller håndholdte måder at samkøre informationer. Det er især vigtigt, at institutternes erfaringerne fra faktiske tabshændelser kan bidrage til at

sikre identifikation og vurdering af risiciene og til at vurdere, om kontrollerne er tilstrækkeligt effektive.

6. Risikorapporteringen tilpasses de strategiske mål for operationel risiko

Ligesom på andre risikoområder skal institutternes styring af operationel risiko også tage udgangspunkt i overordnede strategiske mål.

> § 4, stk. 1, i ledelsesbekendtgørelsen:
>
> 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.

På grund af det store spænd af forskellige former for operationelle risici er det en udfordring for mange institutter at formulere overordnede strategiske mål, som dækker alle typer af operationel risiko, og som samtidig er tilstrækkeligt konkrete til at være retningsgivende for styringen af de enkelte typer. Det fremgår af afsnit 1, hvordan operationelle risici kan inddeles i hovedgrupper.

Enkelte store pengeinstitutter har valgt at fastsætte strategiske mål for hovedgrupper af operationel risiko i stedet for et samlet overordnet mål. Hovedgrupper af operationel risiko kan for eksempel være:

- IT-risiko
- risiko for økonomisk kriminalitet
- compliancerisiko
- outsourcingrisiko
- modelrisiko
- anden operationel risiko.

Inden for hver hovedgruppe er de omfattede risici mere ensartede, og det giver bestyrelsen bedre muligheder for at fastlægge mål, som er konkrete og i højere grad er retningsgivende for styringen af risiciene i overensstemmelse med bestyrelsens anvisninger. Når målene er konkrete, kan bestyrelsen mere præcist vurdere, om målene nås.

Når et institut fastlægger sine strategiske mål for hovedgrupper af operationel risiko, indebærer det, at bestyrelsen skal tage stilling til risikoprofilen på et mere detaljeret niveau. Det stiller større krav til bestyrelsen og til udformningen af den rapportering, som bestyrelsen lægger til grund for sin vurdering.

Ulemperne skal vejes op imod fordelene ved, at bestyrelsen bliver i stand til at give mere konkrete mål og anvisninger.

§ 20, stk. 1, i ledelsesbekendtgørelsen:

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.

…

I de store institutter modtager ledelsen typisk en rapport hvert kvartal, som giver ledelsen mulighed for at vurdere, om instituttets samlede risici og tab ligger inden for de mål, som er fastlagt, og om der behov for yderligere tiltag til at reducere risikoen. En samlet rapportering er mulig på grund af institutternes ensartede metoder til identifikation, klassifikation og vurdering af risiciene. Rapporteringen indeholder også udviklingen i tabshændelser og konstaterede tab.

Ud over den regelmæssige rapportering modtager ledelsen i de store institutter typisk løbende rapportering om væsentlige ændringer i enkelte risici og væsentlige tabshændelser, så ledelsen kan revurdere risikovurderingen og behovet for yderligere risikoreducerende kontroller. Vurderingen af væsentlighed inddrager både den iboende risiko og restrisikoen, og for tabshændelser inddrages konstaterede tab og mulige tab på hændelser, der kan eller kunne have medført tab.