



Temaark risikostyring

B.1 Risikoappetitt 2025



Virksomhetsstyring

Kombinasjonen av prosesser og strukturer, fastsatt av styret for å informere, lede, styre og følge opp de aktivitetene virksomheten gjennomfører for å nå sine mål.

I virksomhetsstyring er risikostyring, etterlevelse og internrevisjon viktige elementer, som sammen kan bidra til god styring og verdiskapning.



Risikostyring

En prosess for å identifisere, vurdere, håndtere og følge opp potensielle endringer, hendelser eller situasjoner, for å gi rimelig grad av sikkerhet for at virksomheten kan nå sine mål på alle nivåer.



Etterlevelse

Styring og kontroll med at virksomheten overholder lover, forskrifter, kontrakter, retningslinjer, prosedyrer og andre krav.



Internrevisjon

En uavhengig og objektiv bekreftelses- og rådgivningstjeneste, som har til formål å tilføre verdi og forbedre virksomheten.



Innhold

Om temaarkene fra IIA Norge	4
Om dette temaarket.....	5
Prinsipper for risikoappetitt	6
Risikoappetitt vs. risikotoleranse	6
Fastsettelse av risikoappetittprofilen	6
Rammeverket.....	7
Periodisk rapportering for videre risikostyring	7
Oppsummering.....	8
Kilder:.....	9



Om temaarkene fra IIA Norge

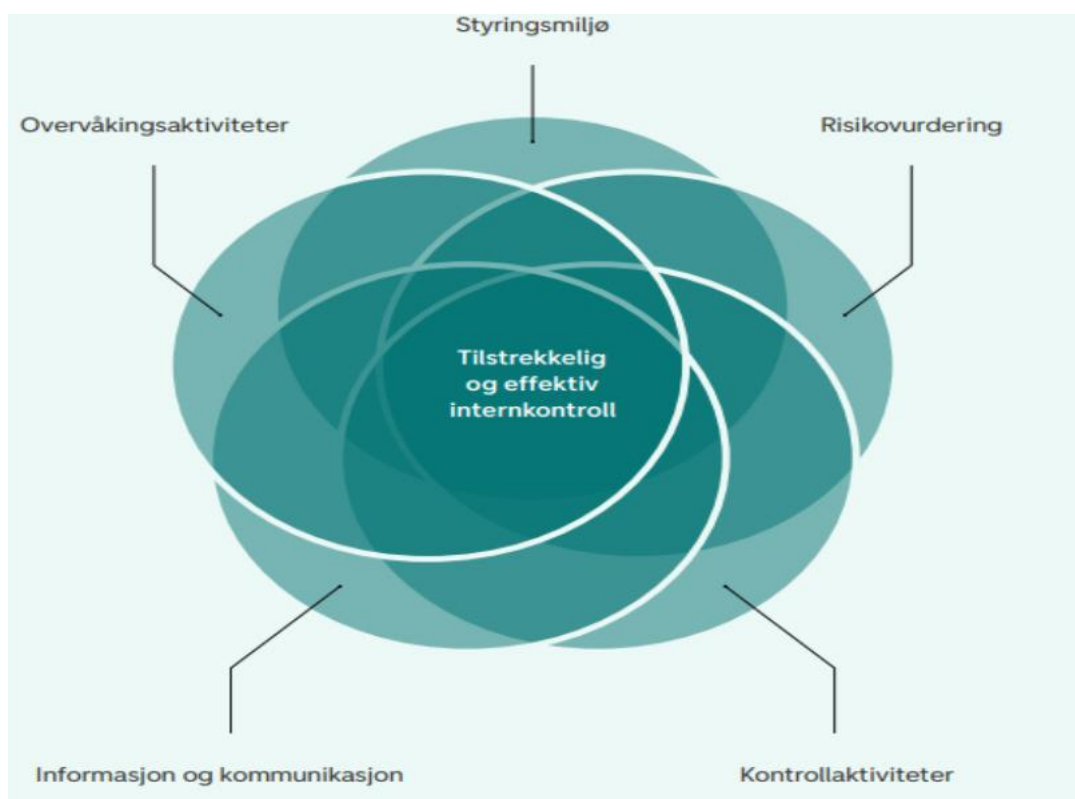
Temaarkene er utviklet for å belyse viktige faglige emner innen virksomhetsstyring, risikostyring, compliance og internrevisjon. Hensikten er å gi en kortfattet og lett tilgjengelig innføring i utvalgte temaer som er relevante for fagmiljøet.

- **Kort og konsist:** Hvert temaark er utformet med fokus på klarhet og lesbarhet, slik at innholdet raskt kan tas i bruk.
- **Faglig fordypning:** Temaarkene inneholder henvisninger til relevante kilder og litteratur for videre studier og fordypning.
- **Dynamisk innhold:** Temaarkene er ikke ment å være det siste ordet om temaet. De vil kunne oppdateres og videreutvikles i takt med faglig utvikling og innspill fra brukerne. Den til enhver tid siste versjonen vil være tilgjengelig på IIA Norge sin nettside.
- **Din tilbakemelding teller:** Som en del av vårt kontinuerlige forbedringsarbeid setter vi stor pris på dine innspill. Har du forslag til endringer eller tillegg, send gjerne en e-post til post@iia.no.



Om dette temaarket

Virksomheter opererer innenfor regulerte miljøer som stiller krav til god risikostyring og internkontroll. Kjernen i risikostyring er å kontinuerlig identifisere, vurdere, overvåke og rapportere risikoer som er relevante for virksomhetenes mål. Risikoappetitt er et sentralt begrep innen risikostyring. I denne sammenhengen er det viktig å forstå at risiko ikke nødvendigvis er negativt. Virksomheter må ta risiko for å oppnå sine taktiske og strategiske mål. Likevel er det avgjørende å ha en bevisst tilnærming til risiko. Dette innebærer å definere klare grenser for hva som er akseptabel risiko, samt å etablere mekanismer for å overvåke og håndtere den. Dette temaarket har som mål å gi innsikt i beste praksis for risikoappetitt. Dokumentet kan brukes av virksomheter på tvers av bransjer og størrelse.



Figur 1: Internkontroll- Kilde: DNB BANK ASA

Dette temaarket for risikoappetitt er utviklet av IIA Norge og Nettverk risikostyring ved:

- Michael Ismail Kilic, DNB
- Mohamad Janeed Azeem, DNB
- Nahid Dadkarimi Naroei, IIA Norge
- Petter Kapstad, Equinor



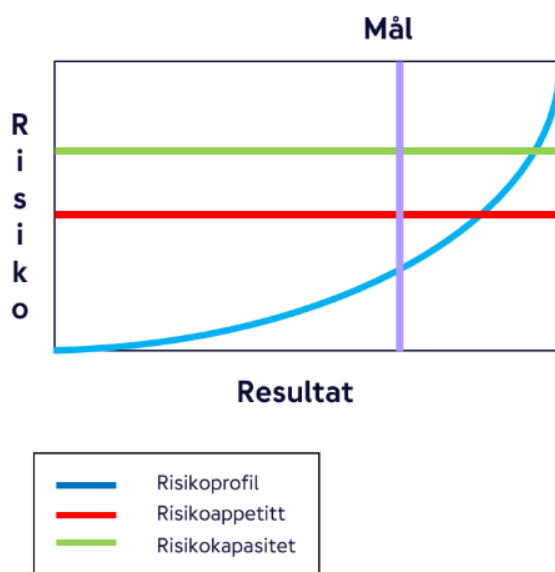
Prinsipper for risikoappetitt

Risikoappetitt kan defineres som «Den type og mengde risiko virksomheten er villig til å akseptere for å gjennomføre sine strategier og nå sine mål» (IIA 2024). Den utgjør således en integrert del av virksomhetens strategiske styring og omfatter prinsipper for vurdering av vesentlig risikotyper innenfor virksomheten. Styret bruker risikoappetitt til å fastsette virksomhetens langsiktige risikoprofil og optimalisere balansen mellom inntjening og risiko. Rammeverket for risikoappetitt gir en omfattende oversikt over risikoer virksomheten er villig til å akseptere for å nå sine mål, og er dermed en forutsetning for kontinuerlig prestasjon over tid.

Risikoappetitt vs. risikotoleranse

Risikoappetitt representerer nivået av usikkerhet en virksomhet er villig til å akseptere for å gjennomføre sine aktiviteter og oppnå sine mål. Risikoappetitt bør alltid ligge innenfor virksomhetens kapasitet til å tolerere risiko, ofte uttrykt som risikotoleranse. Risikotoleranse kan defineres som «Den variasjon i resultater en virksomhet er villig til å akseptere for å nå sine mål» (IIA 2024). Det er altså nivået av risiko en virksomhet kan tåle uten betydelige negative konsekvenser for evnen til å oppnå sine strategiske mål. Risikotoleranse må være i samsvar med virksomhetens risikoappetitt.

COSO forklarer hva de legger i risikoappetitt gjennom figur 2 her:



Figur 2: Risikoappetitt etter illustrasjon i COSO ERM

Fastsettelse av risikoappetittprofilen

Utformingen av virksomhetens risikoappetitt avhenger av hvilke typer risiko den har til hensikt å påta seg.

Kvantitativ risikoappetitt kan uttrykkes som en prosentandel av kapitalen eller inntektene som virksomheten er villig til å risikere. For eksempel ikke mer enn x % av Y million i potensielt lånetap pr. type kredittsegment eller ikke mer enn x % av potensielt tap på virksomhetens årlige investeringer i bestemte markeder. Et annet eksempel er at en virksomhet kan beslutte at den



ikke er villig til å akseptere noe vesentlig brudd på personvernlovgivningen (GDPR), men kan akseptere 10 mindre brudd på samme regelverk.

Kvalitativ risikoappetitt beskriver risikotoleransen i mer generelle termer, for eksempel «moderat», «lav» eller «høy» risikoappetitt. Et selskap kan for eksempel beslutte nulltoleranse for korrupsjon fordi en korrupsjonssak kan ha en vesentlig innvirkning på hele virksomheten. Legg merke til at nulltoleranse betyr ikke at korrupsjon ikke forekommer, men virksomheten har signalisert hva de kan akseptere, hva som er deres risikoappetitt når det gjelder korrupsjon.

Risikoappetitt utgjør en integrert del av virksomhetens strategiske styring og refererer til virksomhetens vilje til å påta seg risiko for å oppnå verdier. Risikoappetitt består av grunnprinsipper og overordnede rammer for risikostyring i en virksomhet. Prinsipper og rammer bør knyttes opp mot risikokategorier som anses å være særlig vesentlige for en virksomhet. Styret bruker risikoappetitt til å fastsette virksomhetens langsiktige risikoprofil og optimalisere balansen mellom inntjening og risiko. Risikoappetitt skal gi en helhetlig og balansert oversikt over risikoen en virksomhet er villig til å akseptere for å realisere sine målsettinger, og er dermed en forutsetning for kontinuerlig prestasjon over tid.

Risikoappetitt er et sentralt styringsprinsipp i en virksomhets risikostyring og internkontroll. Det bør være rød tråd mellom virksomhetens risikoappetitt og;

- rammeverk for risikostyring og internkontroll
- utarbeidelse av strategi og planer
- periodisk rapportering.

Rammeverket

Rammeverket for risikostyring og internkontroll består av risikoerklæringer med tilhørende akseptgrenser innenfor virksomheten. Disse erklæringene og grensene er knyttet til nøkkelrisikokategorier som anses som særlig betydningsfulle for virksomheten, inkludert lønnsomhet og kapasitet til å absorbere tap, virksomhetsrisikostyring, strategiskrisiko, IT og cyberrisiko, operasjonell risiko, omdømmerisiko og etterlevelsrisiko.

Risikokategorier, erklæringer og akseptgrenser bør gjennomgås årlig og besluttes av styret.

Innenfor hver risikokategori kan flere dimensjoner vurderes, hver med spesifiserte grenser og/eller vurderingsprinsipper som definerer akseptable risikogrenser. En utpekt koordinator i virksomhetens andre forsvarslinje er ansvarlig for å etablere oppfølgingstiltak og overvåke endringer i bruken av disse grensene.

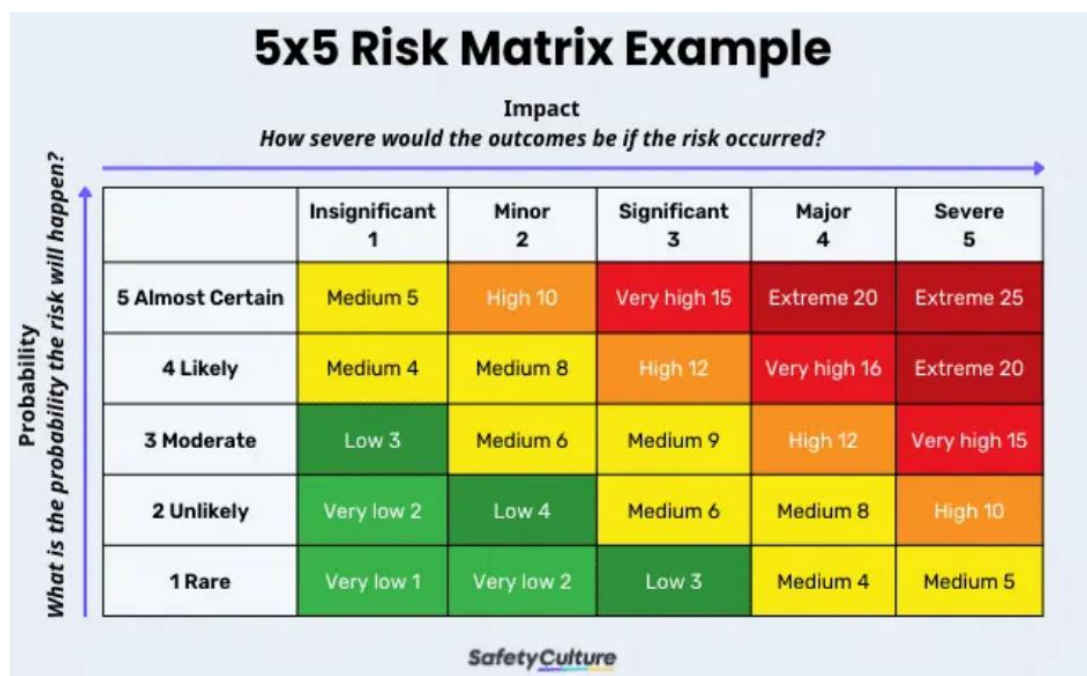
Periodisk rapportering for videre risikostyring

Ledere er ansvarlige for å drive virksomheten i samsvar med etablerte prinsipper for risikoappetitt, inkludert sikring av tilstrekkelige tiltak for internkontroll. Ledere bør rapportere risikoappetitt til styret gjennom periodisk rapportering, mens ledergruppen bør monitorere risikoappetitten oftere. Virksomhetens status vurderes opp mot grensene i rammeverket for risikoappetitt, indikert av en grønn, gul og oransje eller rød statusindikator. (se figur 3). Hver indikator har en tydelig definert betydning, og forhåndsdefinerte handlingsregler eksisterer for brudd på grenseverdier.

Virksomhetens risikoappetitt vurderes minst årlig i en fornyelsesprosess initiert av "Chief Risk Officer" (CRO). Rammeverket for risikostyring og internkontroll godkjennes av styret og



fungerer som grunnlaget for risikorapportering gjennom året. Revidering/oppdatering av rammeverket bør gjennomføres med nåværende risikoappetitt som referansepunkt for virksomhetens strategiske og finansielle planer og uavhengig av strategiske og finansielle planleggingsprosesser.



Figur 3: Risikomatrise for kvalitative evalueringer -Kilde: safetyculture.com

Oppsummering

Dette temaarket fremhever viktigheten av effektiv styring av risikoappetitt og styrets tilsynsansvar sett fra et risikostyringsperspektiv. Ved å følge prinsipper og prosesser skissert i dette dokumentet, kan virksomheter styrke sin praksis for risikostyring og slik sikre harmonisering med strategiske mål. Praksis som er beskrevet basert på virksomhetens rammeverk gir et solid grunnlag for å håndtere risiko i et dynamisk forretningsmiljø.

**Kilder:**

- COSO ERM-Helhetlig Risikostyring 2017
- DNB BANK ASA
- Globale standarder for internrevisjon 2024
- www.safeyculture.com: What is a 5x5 Risk Matrix & How to Use it?