Norsk Standard

NS-ISO 31000:2018

Publisert: 2018-11-12

Språk: Norsk

Risikostyring
Retningslinjer

Risk management
Guidelines

Referansenummer:
NS-ISO 31000:2018 (no)

Norsk forord

Den engelske versjonen av internasjonal standard ISO 31000:2018 ble fastsatt som Norsk Standard NS-ISO 31000:2018 2018-04-01.

Den norske oversettelsen ble utgitt 2018-11-12.

Denne standarden erstatter NS-ISO 31000:2009.

ICS: 03.100.01, 926

Innhold

Forord

ISO (den internasjonale standardiseringsorganisasjonen) er en verdensomspennende sammenslutning av nasjonale standardiseringsorganer (ISO-medlemsorganer). Arbeidet med å utvikle internasjonale standarder utføres vanligvis i ISOs tekniske komiteer. Hvert medlemsorgan som er interessert i et emne som det er opprettet en teknisk komité for, har rett til å være representert i den komiteen. Internasjonale organisasjoner, både offentlige og private, tar også del i arbeidet i samarbeid med ISO. ISO samarbeider nært med IEC (Den internasjonale elektrotekniske kommisjon) i alle saker som gjelder elektroteknisk standardisering.

Prosedyrene brukt ved utarbeidelse av dette dokumentet og de som skal brukes ved videre vedlikehold, er beskrevet i ISO/IEC-direktivene, del 1. Det er særlig viktig å legge merke til de forskjellige godkjenningskriteriene som er nødvendige for ulike typer ISO-dokumenter. Dette dokumentet er utarbeidet i samsvar med reglene som er gitt i ISO/IEC-direktivene, del 2 (se www.iso.org/directives).

Det er viktig å merke seg at noen av elementene i dette dokumentet kan være underlagt patentrettigheter. ISO skal ikke holdes ansvarlig for å identifisere slike patentrettigheter helt eller delvis. Detaljer om eventuelle patentrettigheter som er identifisert under utarbeidelsen av dokumentet, skal angis under punktet Orientering og/eller i ISOs liste over mottatte patentdeklarasjoner (se www.iso.org/patents).

Eventuelle handelsnavn i dette dokumentet er informasjon til brukerne og innebærer ikke en anbefaling.

For en forklaring på standardenes frivillige karakter, betydningen av ISOs spesielle termer og uttrykk i forbindelse med samsvarsvurdering så vel som informasjon om ISOs overholdelse av World Trade Organization (WTO)-prinsippene i Tekniske handelshindringer (TBT), se følgende URL: www.iso.org/iso/foreword.html.

Dette dokumentet ble utarbeidet av den tekniske komiteen ISO/TC 262, *Risk management*.

Denne andre utgaven opphever og erstatter den første utgaven (ISO 31000:2009), som har gjennomgått teknisk revisjon.

De viktigste endringene sammenlignet med den forrige utgaven er som følger:

— gjennomgåelse av prinsippene for risikostyring, som er nøkkelkriteriene for at den skal være vellykket;
— framheving av den øverste ledelsens lederskap og integrering av risikostyring, der utgangspunktet er hvordan organisasjonen styres;
— større fokus på risikostyringens gjentakende karakter, der det erkjennes at nye erfaringer, kunnskap og analyser kan føre til en revisjon av prosesselementer, tiltak og kontroller ved hvert stadium i prosessen;
— forbedring av innholdet med større fokus på å understøtte en modell som kan tilpasses flere behov og kontekster.

Orientering

Dette dokumentet er til bruk for personer som skaper og beskytter verdi i organisasjoner ved å styre risikoer, ta beslutninger, fastsette og oppnå mål og forbedre prestasjon.

Organisasjoner av alle typer og størrelser står overfor eksterne og interne faktorer og påvirkninger som gjør det usikkert om de vil oppnå sine mål.

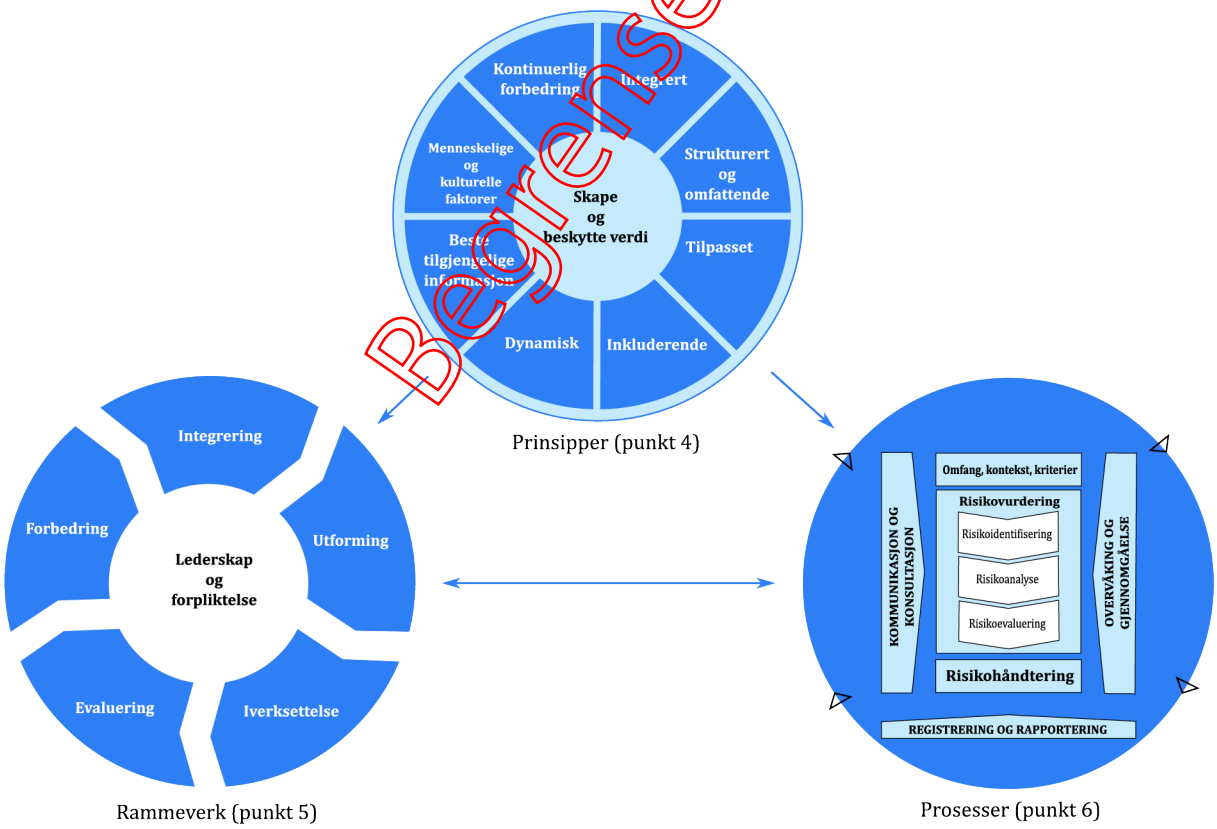
Å styre risiko er av gjentakende karakter og bistår organisasjoner i å fastlegge strategi, oppnå mål og ta veloverveide beslutninger.

Å styre risiko er en del av styring og lederskap og er avgjørende for hvordan organisasjonen ledes på alle nivåer. Risikostyring bidrar til forbedring av ledelsessystemer.

Å styre risiko er en del av alle aktiviteter som forbindes med en organisasjon, og omfatter samhandling med interessenter.

I risikostyring tas det hensyn til organisasjonens eksterne og interne kontekst, medregnet menneskelig atferd og kulturelle faktorer.

Å styre risiko er basert på prinsippene, rammeverket og prosessen beskrevet i dette dokumentet, som vist på Figur 1. Det kan hende at alle eller deler av disse komponentene allerede finnes i organisasjonen, imidlertid kan det være nødvendig å tilpasse eller forbedre dem slik at risikostyringen blir virkningsfull, effektiv og konsistent.



Figur 1 —Prinsipper, rammeverk og prosess

Risikostyring — Retningslinjer

1 Omfang

Dette dokumentet gir retningslinjer for styring av risiko som organisasjoner står overfor. Anvendelsen av disse retningslinjene kan tilpasses alle organisasjoner og deres kontekst.

Dette dokumentet gir en felles metode for å styre alle typer risiko og er ikke bransje- eller sektorspesifikk.

Dette dokumentet kan brukes i hele organisasjonens levetid og kan anvendes på enhver aktivitet, medregnet beslutningstaking på alle nivåer.

2 Normative referanser

Det er ingen normative referanser i dette dokumentet.

3 Termer og definisjoner

I dette dokumentet gjelder følgende termer og definisjoner.

ISO og IEC vedlikeholder terminologidatabaser for bruk i standardisering på følgende adresser:

— ISO Online browsing platform: tilgjengelig på http://www.iso.org/obp

— IEC Electropedia: tilgjengelig på http://www.electropedia.org

3.1
risiko
virkningen av usikkerhet knyttet til mål

Begrepsmerknad 1: En virkning er et avvik fra det forventede. Den kan være positiv, negativ eller begge deler og kan ta for seg, skape eller resultere i muligheter og trusler.

Begrepsmerknad 2: Mål kan ha forskjellige aspekter og kategorier og kan anvendes på forskjellige nivåer.

Begrepsmerknad 3: Risiko uttrykkes ofte i form av *risikokilder* (3.4), potensielle *hendelser* (3.5), deres *konsekvenser* (3.6) og *sannsynligheten* (3.7) for at de skal forekomme.

3.2
risikostyring
koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til *risiko* (3.1)

3.3
interessent
person eller organisasjon som kan påvirke, bli påvirket av eller oppfatte seg selv som påvirket av en beslutning eller aktivitet

Begrepsmerknad 1: Termen «interessepart» kan brukes som alternativ til «interessent».

3.4
risikokilde
element som alene eller i kombinasjon har et iboende potensial til å forårsake *risiko* (3.1)

3.5
hendelse
forekomst av eller endring i et bestemt sett med omstendigheter

Begrepsmerknad 1: En hendelse kan være én enkelt begivenhet eller en serie av begivenheter, og den kan ha flere årsaker og flere *konsekvenser* (3.6).

Begrepsmerknad 2: En hendelse kan også være at noe forventes, men ikke skjer, eller at noe ikke forventes, men skjer.

Begrepsmerknad 3: En hendelse kan være en risikokilde.

3.6
konsekvens
resultat av en *hendelse* (3.5) som påvirker mål

Begrepsmerknad 1: En konsekvens kan være sikker eller usikker og ha positiv eller negativ virkning på mål.

Begrepsmerknad 2: Konsekvenser kan uttrykkes kvalitativt eller kvantitativt.

Begrepsmerknad 3: Alle konsekvenser kan bli mer omfattende gjennom kjedereaksjoner.

3.7
sannsynlighet[NM1]
potensialet for at noe kan skje

Begrepsmerknad 1: I terminologi innenfor *risikostyring* (3.2) brukes ordet «sannsynlighet» om potensialet for at noe kan skje, enten det er definert, målt eller fastsatt objektivt eller subjektivt, kvalitativt eller kvantitativt, og enten det beskrives i generelle eller matematiske vendinger (for eksempel som en sannsynlighet eller en frekvens i en gitt tidsperiode).

Begrepsmerknad 2: Den engelske termen «likelihood» mangler en direkte ekvivalent på enkelte språk. Derfor brukes ofte ekvivalenten til termen «probability» i stedet. På engelsk blir imidlertid «probability» ofte avgrenset som en matematisk term. I risikostyringsterminologi brukes derfor «likelihood» med den intensjon at ordet skal ha den samme brede tolkningen som termen «probability» har på mange andre språk enn engelsk.

3.8
kontroll
tiltak som opprettholder og/eller modifiserer *risiko* (3.1)

Begrepsmerknad 1: Kontroller inkluderer, men er ikke begrenset til, enhver prosess, policy, plan og praksis eller andre forhold og/eller ordninger som opprettholder og/eller modifiserer risiko.

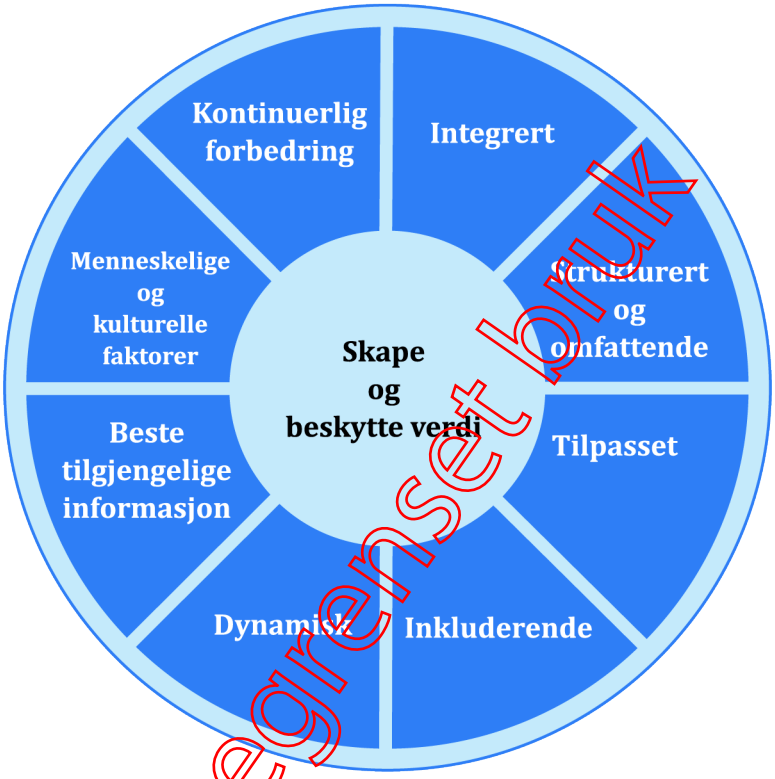
Begrepsmerknad 2: Det er ikke alltid at kontroller har den tiltenkte eller antatt modifiserende virkningen.

[NM1] Nasjonal merknad: På engelsk: Likelihood

4 Prinsipper

Formålet med risikostyring er å skape og beskytte verdi. Risikostyringen forbedrer prestasjon, oppmuntrer til innovasjon og støtter oppnåelsen av mål.

Prinsippene beskrevet på Figur 2 gir veiledning om egenskapene ved effektiv og virkningsfull risikostyring, kommuniserer dens verdi og forklarer dens hensikt og formål. Prinsippene er grunnlaget for å styre risiko og bør tas i betraktning når rammeverket og prosessene for organisasjonens risikostyring skal opprettes. Disse prinsippene bør gjøre det mulig for en organisasjon å styre virkningene av usikkerhet knyttet til sine mål.



Figur 2 — Prinsipper

Virksom risikostyring forutsetter elementene på Figur 2 og kan forklares på følgende måte.

a) Integrert

Risikostyring er en integrert del av alle organisatoriske aktiviteter.

b) Strukturert og omfattende

En strukturert og omfattende tilnærming til risikostyring bidrar til konsistente og sammenlignbare resultater.

c) Tilpasset

Rammeverket og prosessen for risikostyring er tilpasset organisasjonen og står i forhold til dens eksterne og interne kontekst som er knyttet til målene.

d) Inkluderende

Hensiktsmessig deltakelse av interessenter til riktig tid gjør det mulig å ta hensyn til deres kunnskap, synspunkter og oppfatninger. Det resulterer i forbedret bevissthet og veloverveid risikostyring.

e) Dynamisk

Risiko kan oppstå, endre seg og forsvinne etter hvert som organisasjonens eksterne og interne kontekst endres. Risikostyring forutser, avdekker, bekrefter og blir påvirket av disse endringene og hendelsene på en hensiktsmessig måte til riktig tid.

f) Beste tilgjengelige informasjon

Inngangsfaktorene til risikostyring er basert på historisk og nåtidig informasjon så vel som på framtidige forventninger. Risikostyring tar uttrykkelig hensyn til alle begrensninger og usikkerheter forbundet med slik informasjon og slike forventninger. Informasjonen bør gis til riktig tid og være klar og tilgjengelig for relevante interessenter.

g) Menneskelige og kulturelle faktorer

Menneskelig atferd og kultur påvirker i vesentlig grad alle aspekter ved risikostyring på hvert nivå og stadium.

h) Kontinuerlig forbedring

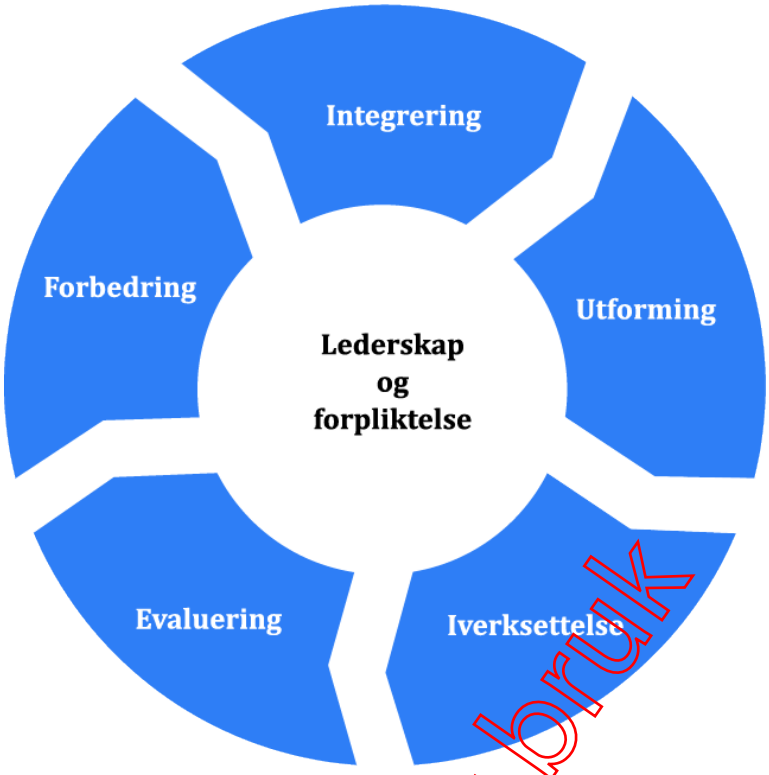
Risikostyring forbedres kontinuerlig gjennom læring og erfaring.

5 Rammeverk

5.1 Generelt

Formålet med rammeverket for risikostyring er å bistå organisasjonen i å integrere risikostyring i viktige aktiviteter og funksjoner. Hvor virkningsfull risikostyringen er, vil avhenge av hvordan den integreres i styringen av organisasjonen, medregnet beslutningstaking. Dette krever støtte fra interessentene, særlig den øverste ledelsen.

Utvikling av rammeverket omfatter å integrere, utforme, iverksette, evaluere og forbedre risikostyring gjennom hele organisasjonen. Figur 3 viser komponentene i rammeverket.



Figur 3 — Rammeverk

Organisasjonen bør evaluere sin eksisterende praksis og sine eksisterende prosesser for risikostyring, evaluere eventuelle gap og ta for seg disse gapene innenfor rammeverket.

Komponentene i rammeverket og måten de virker sammen på, bør tilpasses organisasjonens behov.

5.2 Lederskap og forpliktelse

Den øverste ledelsen og overordnede organer, der det er aktuelt, bør sikre at risikostyringen er integrert i alle organisatoriske aktiviteter, og vise lederskap og forpliktelse ved å:

— tilpasse og iverksette alle komponenter i rammeverket;
— utgi en erklæring eller policy som fastlegger en tilnærming, plan eller serie av tiltak for risikostyring;
— sikre at risikostyring blir tildelt nødvendige ressurser;
— gi myndighet, ansvarsområder og ansvarlighet på hensiktsmessige nivåer i organisasjonen.

Dette vil hjelpe organisasjonen med å:

— samordne risikostyringen med sine mål, sin strategi og sin kultur;
— erkjenne og ta for seg alle forpliktelser, så vel som sine frivillige løfter;
— fastlegge mengden og typen risiko som kan eller ikke kan tas for å veilede utviklingen av risikokriterier, og sikre at de blir kommunisert til organisasjonen og dens interessenter;
— kommunisere verdien av risikostyring til organisasjonen og dens interessenter;
— fremme systematisk overvåking av risikoer;
— sikre at rammeverket for risikostyring forblir hensiktsmessig i forhold til organisasjonens kontekst.

Den øverste ledelsen er ansvarlig for å styre risiko, mens overordnede organer er ansvarlige for å overvåke risikostyring. Det forventes eller kreves ofte at overordnede organer skal:

— sikre at det blir tatt tilstrekkelig hensyn til risikoer når organisasjonens mål skal fastsettes;
— forstå risikoene som organisasjonen står overfor, når den søker å nå sine mål;
— sikre at systemene for å styre slike risikoer blir iverksatt og drevet på en virksom måte;
— sikre at slike risikoer er hensiktsmessige i konteksten av organisasjonens mål;
— sikre at informasjon om slike risikoer og styringen av dem blir behørig kommunisert.

5.3 Integrering

Integrering av risikostyring avhenger av en forståelse av organisasjonens strukturer og kontekst. Strukturer varierer avhengig av organisasjonens formål, målsetninger og kompleksitet. Risiko styres i hver del av organisasjonens struktur. Alle i en organisasjon har ansvar for å håndtere risiko.

Styringen bestemmer organisasjonens kurs, dens eksterne og interne forhold samt regler, prosesser og praksis som trengs for å oppfylle formålet. Ledelsesstrukturene omsetter styringens retning til strategi og tilhørende mål som kreves for å oppnå ønskede nivåer av bærekraftig prestasjon og langsiktig overlevelse. Å bestemme risikostyringens ansvarlighet og overordnede roller i en organisasjon er integrerte deler av organisasjonens styring.

Å integrere risikostyring i en organisasjon er en dynamisk og gjentakende prosess og bør tilpasses organisasjonens behov og kultur. Risikostyring bør være en del av, og ikke atskilt fra, organisasjonens formål, styring, lederskap og forpliktelse, strategi, mål og operasjoner.

5.4 Utforming

5.4.1 Forstå organisasjonen og dens kontekst

Når organisasjonen skal utforme sitt rammeverk for risikostyring, bør den undersøke og forstå sin eksterne og interne kontekst.

Undersøkelse av organisasjonens eksterne kontekst kan omfatte, men er ikke begrenset til:

— samfunnsmessige, kulturelle, politiske, juridiske, forskriftsmessige, finansielle, teknologiske, økonomiske og miljømessige faktorer, enten det er internasjonalt, nasjonalt, regionalt eller lokalt;
— viktige drivkrefter og trender som berører organisasjonens mål;
— eksterne interessenters forhold, oppfatninger, verdier, behov og forventninger;
— kontraktsmessige forhold og forpliktelser;
— kompleksitet og gjensidig avhengighet i nettverk.

Undersøkelse av organisasjonens interne kontekst kan omfatte, men er ikke begrenset til:

— visjon, oppgave og verdier;
— styring, organisasjonsstruktur, roller og ansvarlighet;
— strategi, mål og policyer;
— organisasjonens kultur;
— standarder, retningslinjer og modeller som brukes i organisasjonen;
— dugelighet, forstått som ressurser og kunnskap (f.eks. kapital, tid, mennesker, åndsverk, prosesser, systemer og teknologier);
— data, informasjonssystemer og informasjonsstrømmer;
— forhold til interne interessenter, der det tas hensyn til deres oppfatninger og verdier;
— kontraktsmessige forhold og forpliktelser;
— gjensidig avhengighet og gjensidige forbindelser.

5.4.2 Formulere forpliktelse til risikostyring

Den øverste ledelsen og overordnede organer, der det er aktuelt, bør vise og formulere sin kontinuerlige forpliktelse til risikostyring gjennom en policy, en erklæring eller andre midler som klart formidler en organisasjons mål og forpliktelse til risikostyring. Forpliktelsen bør omfatte, men er ikke begrenset til:

— organisasjonens formål med risikostyring og sammenheng med dens mål og andre policyer;
— å forsterke behovet for å integrere risikostyring i organisasjonens generelle kultur;
— å integrere risikostyring i kjernevirksomheter og beslutningstaking;
— myndigheter, ansvarsområder og ansvarlighet;
— å gjøre nødvendige ressurser tilgjengelige;
— måten motstridende mål håndteres på;
— måling og rapportering innenfor organisasjonens prestasjonsindikatorer;
— gjennomgåelse og forbedring.

Forpliktelsen til risikostyring bør kommuniseres innad i organisasjonen og til interessenter, hvis hensiktsmessig.

5.4.3 Tildeling av roller, myndighet, ansvarsområder og ansvarlighet i organisasjonen

Den øverste ledelsen og overordnede organer der det er aktuelt, bør sikre at myndigheter, ansvarsområder og ansvarlighet for relevante roller når det gjelder risikostyring, blir tildelt og kommunisert på alle nivåer i organisasjonen, og bør:

— understreke at risikostyring er et kjerneansvarsområde;
— identifisere personer som har ansvarlighet og myndighet til å styre risiko (risikoeiere).

5.4.4 Tildeling av ressurser

Den øverste ledelsen og overordnede organer der det er aktuelt, bør sikre at risikostyring blir tildelt hensiktsmessige ressurser, som kan omfatte, men ikke er begrenset til:

— mennesker, ferdigheter, erfaring og kompetanse;
— organisasjonens prosesser, metoder og verktøy som skal brukes for risikostyring;
— dokumenterte prosesser og prosedyrer;
— systemer for styring av informasjon og kunnskap;
— behov for faglig utvikling og opplæring.

Organisasjonen bør vurdere dugelighet og begrensninger hos eksisterende ressurser.

5.4.5 Fastlegge kommunikasjon og konsultasjon

Organisasjonen bør fastlegge en godkjent metode for kommunikasjon og konsultasjon for å støtte rammeverket og lette den faktiske anvendelsen av risikostyring. Kommunikasjon innebærer å dele informasjon med målgruppene. Konsultasjon innebærer også at deltakerne gir tilbakemelding, med forventning om at den vil bidra til å forme beslutninger eller andre aktiviteter. Metoder og innhold i kommunikasjon og konsultasjon bør gjenspeile interessentenes forventninger, der det er relevant.

Kommunikasjon og konsultasjon bør finne sted til riktig tid, og det bør sikres at relevant informasjon samles inn, sammenholdes, forenes og deles hvis hensiktsmessig, og at det blir gitt tilbakemelding og gjort forbedringer.

5.5 Iverksettelse

Organisasjonen bør iverksette rammeverket for risikostyring ved å:

— utvikle en hensiktsmessig plan inkludert tid og ressurser;
— identifisere hvor, når og hvordan forskjellige typer beslutninger tas i hele organisasjonen, og av hvem;
— modifisere gjeldende prosesser for beslutningstaking der det er nødvendig;
— sikre at organisasjonens ordninger for å styre risiko er klart forstått og praktisert.

Vellykket iverksettelse av rammeverket fordrer at interessentene engasjerer seg og er bevisste. Dette gjør det mulig for organisasjoner eksplisitt å ta for seg usikkerhet i beslutningstaking samtidig som de sikrer at det kan tas hensyn til all ny eller etterfølgende usikkerhet etter hvert som den oppstår.

Når rammeverket for risikostyring er tilfredsstillende utformet og iverksatt, vil det sikre at risikostyringsprosessen er en del av alle aktiviteter i hele organisasjonen, medregnet beslutningstaking, og at endringer i ekstern og intern kontekst vil bli fanget opp på en egnet måte.

5.6 Evaluering

For å evaluere hvor virkningsfullt rammeverket for risikostyring er, bør organisasjonen:

— regelmessig måle prestasjonen til rammeverket for risikostyring opp mot formålet, planer for iverksettelse, indikatorer og forventet reaksjon;
— bestemme om det fortsatt er egnet for å understøtte oppnåelsen av organisasjonens mål.

5.7 Forbedring

5.7.1 Tilpasning

Organisasjonen bør kontinuerlig overvåke og tilpasse rammeverket for risikostyring slik at det tar hensyn til eksterne og interne endringer. Organisasjonen kan øke sin verdi ved å gjøre dette.

5.7.2 Kontinuerlig forbedring

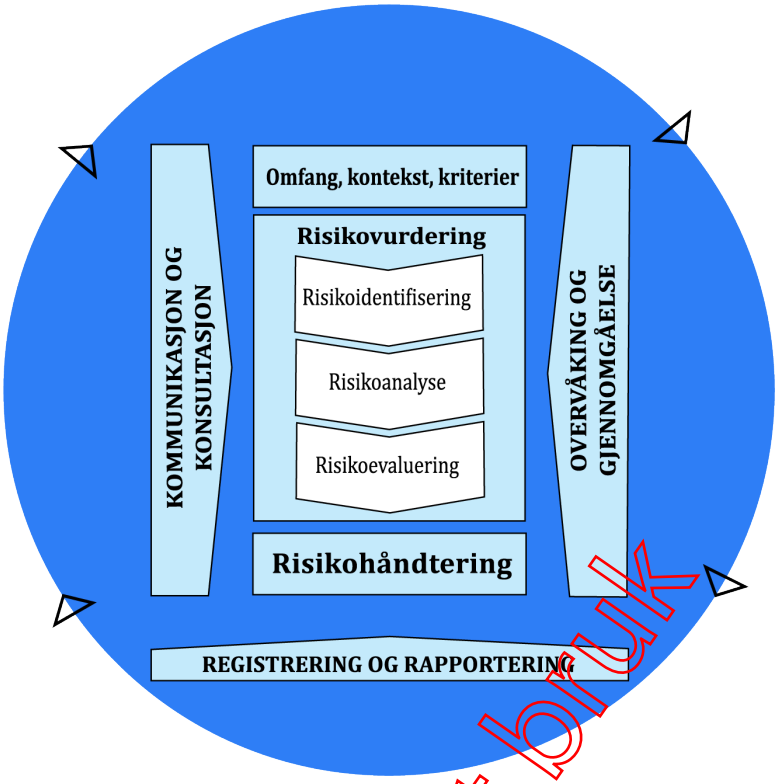
Organisasjonen bør kontinuerlig forbedre egnetheten, tjenligheten og virkningen av sin forvaltning av rammeverket for risikostyring og måten risikostyringsprosessen er integrert på.

Etter hvert som relevante gap eller forbedringsmuligheter blir identifisert, bør organisasjonen utvikle planer og oppgaver og fordele dem på de ansvarlige for iverksettelsen. Når disse forbedringene er implementert, bør de bidra til å forsterke risikostyringen.

6 Prosess

6.1 Generelt

Risikostyringsprosessen omfatter systematisk anvendelse av policyer, prosedyrer og praksis på aktivitetene kommunikasjon og konsultasjon, bestemmelse av kontekst og vurdering, behandling, overvåking, gjennomgåelse, registrering og rapportering av risiko. Denne prosessen er vist på Figur 4.



Figur 4 – Prosess

Risikostyringsprosessen bør være en integrert del av ledelse og beslutningstaking og være integrert i organisasjonens struktur, drift og prosesser. Den kan anvendes på strategisk nivå, operasjonelt nivå, programnivå eller prosjektnivå.

Risikostyringsprosessen kan anvendes på mange måter i en organisasjon, tilpasset for å oppnå mål og passe inn i den eksterne og interne konteksten som de anvendes i.

Det faktum at menneskelig atferd og kultur er dynamisk og variabel, bør vurderes gjennom hele risikostyringsprosessen.

Selv om risikostyringsprosessen ofte framstilles som sekvensiell, er den i praksis gjentakende.

6.2 Kommunikasjon og konsultasjon

Formålet med kommunikasjon og konsultasjon er å bistå relevante interessenter i å forstå risiko, grunnlaget for beslutningstakingen og årsakene til at bestemte tiltak er påkrevd. Kommunikasjon har som formål å fremme bevissthet og forståelse av risiko, mens konsultasjon omfatter innhenting av tilbakemelding og informasjon for å støtte beslutningstaking. Nært samarbeid mellom de to bør lette faktisk, relevant, nøyaktig og forståelig utveksling av informasjon til riktig tid, der det tas hensyn til personvernet.

Kommunikasjon og konsultasjon med hensiktsmessige eksterne og interne interessenter bør finne sted innenfor og gjennom alle trinn i risikostyringsprosessen.

Kommunikasjon og konsultasjon har som mål å:

— bringe forskjellige områder av ekspertise sammen for hvert trinn i risikostyringsprosessen;
— sikre at forskjellige synspunkter tas tilstrekkelig hensyn til når risikokriterier skal fastsettes, og når risikoer skal evalueres;

— gi tilstrekkelig informasjon for å lette oversikten over risiko og beslutningstaking;
— bygge en forståelse av å være inkludert og ha eierskap blant dem som er berørt av risiko.

6.3 Omfang, kontekst og kriterier

6.3.1 Generelt

Formålet med å fastlegge omfang, kontekst og kriterier er å tilpasse risikostyringsprosessen slik at virkningsfull risikovurdering og hensiktsmessig risikohåndtering muliggjøres. Omfang, kontekst og kriterier innebærer fastsettelse av omfanget av prosessen og forståelse av den eksterne og interne konteksten.

6.3.2 Fastsette omfang

Organisasjonen bør fastsette omfanget av sine aktiviteter knyttet til risikostyring.

Siden risikostyringsprosessen kan anvendes på forskjellige nivåer (for eksempel strategisk nivå, operasjonelt nivå, programnivå, prosjektnivå eller i andre aktiviteter), er det viktig å være tydelig om det aktuelle omfanget, de relevante målene som skal tas hensyn til, og samordningen av disse målene med organisasjonens mål.

Planlegging av tilnærmingen omfatter at det tas hensyn til følgende:

— mål og beslutninger som det er nødvendig å ta;
— forventede resultater av trinnene som tas i prosessen;
— tid, plassering, spesifikke innlemmelser og utelatelser;
— hensiktsmessige verktøy og teknikker for risikovurdering;
— ressursbehov, ansvarsområder og registreringer som skal tas vare på;
— forhold til andre prosjekter, prosesser og aktiviteter.

6.3.3 Ekstern og intern kontekst

Ekstern og intern kontekst er miljøet der organisasjonen søker å fastsette og oppnå sine mål.

Konteksten for risikostyringsprosessen bør fastlegges ut fra forståelsen av eksternt og internt miljø der organisasjonen driver sin virksomhet, og bør gjenspeile det spesifikke miljøet for aktiviteten som risikostyringsprosessen skal anvendes på.

Det er viktig å forstå konteksten fordi:

— risikostyring skjer i konteksten av organisasjonens mål og aktiviteter;
— organisasjonsmessige faktorer kan være en risikokilde;
— formålet med og omfanget av risikostyringsprosessen kan være gjensidig forbundet med organisasjonens mål.

Organisasjonen bør fastlegge ekstern og intern kontekst for risikostyringsprosessen ved å ta hensyn til faktorene nevnt i 5.4.1.

6.3.4 Fastsette risikokriterier

Organisasjonen bør angi mengden og typen risiko som den kan eller ikke kan ta, sett i forhold til målene. Den bør også fastsette kriterier for å evaluere betydningen av risiko og for å understøtte beslutningstakingsprosesser. Risikokriterier bør samordnes med rammeverket for risikostyring og

tilpasses det bestemte formålet og omfanget av den aktuelle aktiviteten. Risikokriterier bør gjenspeile organisasjonens verdier, mål og ressurser og være konsistente med policyene og erklæringen om risikostyring. Ved fastsettelse av kriterier bør det tas hensyn til organisasjonens forpliktelser og interessentenes synspunkter.

Selv om risikokriterier bør fastlegges i begynnelsen av risikovurderingsprosessen, er de dynamiske og bør gjennomgås og endres kontinuerlig ved behov.

Det bør tas hensyn til følgende ved fastsettelse av risikokriterier:

— arten og typen av usikkerhet som kan påvirke resultater og mål (både materielle og immaterielle);
— hvordan konsekvenser (både positive og negative) og sannsynlighet vil bli fastsatt og målt;
— tidsavhengige faktorer;
— konsistens i bruken av målinger;
— hvordan risikonivået skal bestemmes;
— hvordan kombinasjoner og rekkefølger av flere risikoer skal tas hensyn til;
— organisasjonens kapasitet.

6.4 Risikovurdering

6.4.1 Generelt

Risikovurdering er den overordnede prosessen med risikoidentifisering, risikoanalyse og risikoevaluering.

Risikovurdering bør gjennomføres systematisk, gjentakende og gjennom samarbeid, der det dras nytte av interessentenes kunnskap og synspunkter. Under risikovurderingen bør den beste tilgjengelige informasjonen brukes, supplert med ytterligere undersøkelser ved behov.

6.4.2 Risikoidentifisering

Formålet med risikoidentifisering er å finne, gjenkjenne og beskrive risikoer som kan hjelpe en organisasjon med eller forhindre den fra å nå sine mål. Relevant, hensiktsmessig og oppdatert informasjon er viktig når risikoer skal identifiseres.

Organisasjonen kan bruke en rekke teknikker for å identifisere usikkerhet som kan påvirke ett eller flere mål. Det bør tas hensyn til følgende faktorer og forholdet mellom dem:

— materielle og immaterielle risikokilder;
— årsaker og hendelser;
— trusler og muligheter;
— sårbarhet og dugelighet;
— endringer i ekstern og intern kontekst;
— indikatorer for risikoer som oppstår;
— arten og verdien av verdier og ressurser;
— konsekvenser og deres innvirkning på mål;
— begrensninger i kunnskap og informasjonens pålitelighet;
— tidsavhengige faktorer;
— fordommer, antakelser og overbevisninger hos dem som er involvert.

Organisasjonen bør identifisere risikoer, uavhengig av om den har kontroll med risikokildene eller ikke. Det bør tas hensyn til at det kan være mer enn én type resultat som kan føre til en rekke materielle eller immaterielle konsekvenser.

6.4.3 Risikoanalyse

Formålet med risikoanalyse er å forstå arten av risiko og dens kjennetegn medregnet risikonivået der det er hensiktsmessig. Risikoanalyse innebærer en detaljert vurdering av usikkerhet, risikokilder, konsekvenser, sannsynlighet, hendelser, scenarier, kontroller og deres virkning. En hendelse kan ha flere årsaker og konsekvenser og kan påvirke flere mål.

Risikoanalyse kan gjennomføres med varierende grad av detaljer og kompleksitet avhengig av formålet med analysen, informasjonens tilgjengelighet og pålitelighet og tilgjengelige ressurser. Analysemetoder kan være kvalitative, kvantitative eller en kombinasjon av disse, avhengig av omstendigheter og tiltenkt bruk.

Risikoanalyse bør omfatte vurdering av faktorer som:

— sannsynligheten for at hendelser og konsekvenser skal inntreffe;
— arten og mangfoldet av konsekvenser;
— kompleksitet og forbindelser;
— tidsavhengige faktorer og labilitet;
— virkningen av eksisterende kontroller;
— følsomhet og statistisk sikkerhet.

Risikoanalysen kan påvirkes av alle forskjeller i meninger, fordommer, oppfatninger av risiko og bedømmelser. Andre forhold som påvirker, er kvaliteten på informasjonen som brukes, antakelser og utelatelser som gjøres, alle begrensninger i metodene og hvordan de utføres. Disse påvirkningene bør vurderes, dokumenteres og kommuniseres til beslutningstakerne.

Svært usikre hendelser kan være vanskelige å kvantifisere. Det kan være tilfellet når hendelser med alvorlige konsekvenser skal analyseres. I slike tilfeller gir vanligvis en kombinasjon av metoder større innsikt.

Risikoanalyse gir innspill til risikoevaluering, beslutninger om hvorvidt risikoen trenger å håndteres, og eventuelt hvordan, og om de mest hensiktsmessige strategiene og metodene for risikohåndtering. Resultatene tilfører innsikt til beslutninger der det skal gjøres valg, og der alternativene innebærer forskjellige typer og nivåer av risiko.

6.4.4 Risikoevaluering

Formålet med risikoevaluering er å understøtte beslutninger. Risikoevaluering innebærer sammenligning av resultatene av risikoanalysen med fastlagte risikokriterier for å bestemme hvor det er nødvendig med ytterligere tiltak. Dette kan føre til en beslutning om å:

— ikke gjøre noe mer;
— vurdere alternativer for risikohåndtering;
— foreta ytterligere analyse for å forstå risikoen bedre;
— vedlikeholde eksisterende kontroller;
— vurdere målene på nytt.

Ved beslutninger bør det tas hensyn til en utvidet kontekst og de faktiske og oppfattede konsekvensene for eksterne og interne interessenter.

Resultatet av risikoevaluering bør registreres, kommuniseres og deretter valideres på hensiktsmessige nivåer i organisasjonen.

6.5 Risikohåndtering

6.5.1 Generelt

Formålet med risikohåndtering er å velge og iverksette alternativer for å ta hensyn til risiko.

Risikohåndtering innebærer en gjentakende prosess som går ut på å:

— formulere og velge alternativer for risikohåndtering;
— planlegge og iverksette risikohåndtering;
— vurdere virkningen av denne risikohåndteringen;
— beslutte om restrisikoen er akseptabel;
— hvis den ikke er akseptabel, treffe tiltak for ytterligere håndtering.

6.5.2 Valg av alternativer for risikohåndtering

Å velge det eller de mest hensiktsmessige alternativene for risikohåndtering innebærer å avveie de potensielle fordelene utledet fra måloppnåelsen mot kostnader, innsats eller ulemper ved iverksettelsen.

Det er ikke nødvendigvis slik at alternativer for risikohåndtering utelukker hverandre gjensidig eller er hensiktsmessige i alle sammenhenger. Alternativer for å håndtere risiko kan innebære ett eller flere av følgende forhold:

— unngå risiko ved å beslutte å ikke starte eller fortsette med aktiviteten som medfører risiko;
— ta eller øke risiko for å forfølge en mulighet;
— fjerne risikokilden;
— endre sannsynligheten for at risiko inntreffer;
— endre konsekvensene;
— dele risiko (for eksempel gjennom kontrakter, kjøp av forsikring);
— beholde risikoen gjennom veloverveid beslutning.

Begrunnelsen for risikohåndtering er videre enn bare økonomiske hensyn. Det bør tas hensyn til alle organisasjonens forpliktelser, frivillige forpliktelser og synspunkter hos interessentene. Valget av alternativer for risikohåndtering bør foretas i henhold til organisasjonens mål, risikokriterier og tilgjengelige ressurser.

Ved valg av alternativer for risikohåndtering bør organisasjonen vurdere interessentenes verdier, oppfatninger og potensielle engasjement og de mest hensiktsmessige måtene å kommunisere med dem og konsultere dem på. Selv om risikohåndteringen er like virkningsfull kan enkelte alternativer være mer akseptable for noen interessenter enn for andre.

Risikohåndtering kan være nøyaktig utformet og iverksatt og likevel ikke gi de forventede resultatene, og den kan få utilsiktede konsekvenser. For å kunne sikre at de forskjellige formene for behandling blir og fortsetter å være virkningsfulle, kreves det at overvåking og gjennomgåelse er en integrert del av iverksettelsen av risikohåndteringen.

Risikohåndtering kan også føre til nye risikoer som det er nødvendig å styre.

Hvis ingen alternativer for håndtering er tilgjengelig, eller hvis alternativene for håndtering ikke modifiserer risikoen tilstrekkelig, bør risikoen registreres og gjennomgås kontinuerlig.

Beslutningstakere og andre interessenter bør være klar over arten og omfanget av restrisiko etter risikohåndtering. Restrisiko bør dokumenteres og overvåkes, gjennomgås og håndteres ytterligere ved behov.

6.5.3 Utarbeidelse og iverksettelse av planer for risikohåndtering

Formålet med planer for risikohåndtering er å angi hvordan de valgte alternativene for håndtering vil bli iverksatt, slik at ordningene blir forstått av de involverte, og slik at framdriften i henhold til planen kan overvåkes. Planen for håndtering bør klart angi i hvilken rekkefølge risikohåndtering bør iverksettes.

Planene for håndtering bør integreres i planene for ledelse og prosessene i organisasjonen i samråd med relevante interessenter.

Informasjonen som gis i planen for håndtering, bør omfatte:

— begrunnelsen for valg av alternativene for håndtering, medregnet fordeler som forventes oppnådd;
— de som har ansvarlighet og er ansvarlige for godkjenning og iverksettelse av planen;
— foreslåtte tiltak;
— påkrevde ressurser, medregnet beredskap;
— tiltak for å måle prestasjon;
— begrensninger;
— påkrevd rapportering og overvåking;
— når det forventes at tiltak skal gjennomføres og fullføres.

6.6 Overvåking og gjennomgåelse

Formålet med overvåking og gjennomgåelse er å sikre og forbedre kvaliteten på og virkningen av prosessens utforming, iverksettelse og resultater. Pågående overvåking og regelmessig gjennomgåelse av risikostyringsprosessen og dens resultater bør være en planlagt del av risikostyringsprosessen med klart definerte ansvarsområder.

Overvåking og gjennomgåelse bør skje på alle stadier av prosessen. Overvåking og gjennomgåelse omfatter planlegging, innsamling og analyse av informasjon, registrering av resultater og å gi tilbakemelding.

Resultatene av overvåking og gjennomgåelse bør integreres i organisasjonens styring av prestasjon, målinger og rapporteringsaktiviteter for hele organisasjonen.

6.7 Registrering og rapportering

Risikostyringsprosessen og resultatene av den bør dokumenteres og rapporteres ved hjelp av hensiktsmessige mekanismer. Målet med registrering og rapportering er å:

— kommunisere aktiviteter knyttet til risikostyring og resultater i hele organisasjonen;
— gi informasjon for beslutningstaking;
— forbedre aktiviteter knyttet til risikostyring;
— fremme samhandlingen med interessenter, medregnet de med ansvarsområder og ansvarlighet for aktiviteter innenfor risikostyring.

Beslutninger om opprettelse, oppbevaring og håndtering av dokumentert informasjon bør tas hensyn til, men ikke begrenses til, bruken av beslutningene, informasjonens følsomhet og ekstern og intern kontekst.

Rapportering er en integrert del av organisasjonens styring. Rapporteringen bør styrke kvaliteten på dialogen med interessenter og understøtte den øverste ledelsen og overordnede organer når de skal oppfylle sine ansvarsområder. Faktorer som skal tas i betraktning ved rapportering, omfatter, men er ikke begrenset til:

— differensiering av interessenter og deres bestemte informasjonsbehov og krav;
— kostnad, hyppighet og aktualitet ved rapportering;
— rapporteringsmetode;
— informasjonens relevans for organisasjonens mål og beslutningstaking.

Litteratur

[1] NS-ISO IEC 31010, *Risikostyring – Metoder for risikovurdering*

- Norsk Standard fastsettes av Standard Norge og er varemerkebeskyttet.
- Andre leveranser fra Standard Norge, som tekniske spesifikasjoner, workshopavtaler og veiledninger, utgis etter ferdigstilling uten formell fastsetting.
- Standard Norge kan gi opplysninger om innholdet og svare på faglige spørsmål.
- Spørsmål om gjengivelse rettes til Standard Online AS.
- Inntektene fra salg av standarder utgjør en stor og avgjørende del av finansieringen av standardiserings-arbeidet i Norge.
- Mer informasjon om standardisering, standarder, kurs og andre produkter finnes på www.standard.no.

Standard Norge
Postboks 242
1326 Lysaker

Telefon 67 83 86 00

info@standard.no
www.standard.no

Standard Online AS
Postboks 252
1326 Lysaker

Telefon 67 83 87 00

salg@standard.no
www.standard.no

Besøksadresse:

Mustads vei 1
0283 Oslo