Norsk Standard

NS-EN ISO 22301:2019

Publisert: 2020-03-14

Språk: Norsk

Sikkerhet og resiliens
Systemer for kontinuitetsledelse
Krav
(ISO 22301:2019)

Security and resilience
Business continuity management systems
Requirements
(ISO 22301:2019)

Referansenummer:
NS-EN ISO 22301:2019 (no)

2020-02-01 ble europeisk standard EN ISO 22301:2019 fastsatt som Norsk Standard NS-EN ISO 22301:2019. Engelsk versjon ble utgitt 2020-02-01.

Norsk oversettelse ble utgitt 2020-03-14.

NS-EN ISO 22301:2019 erstatter NS-EN ISO 22301:2014.

ICS: 03.100.70, 03.100.01

EUROPEISK STANDARD
EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN ISO 22301

November 2019

ICS: 03.100.01, 03.100.70

Erstatter EN ISO 22301:2014

Norsk versjon

Sikkerhet og resiliens — Systemer for kontinuitetsledelse — Krav (ISO 22301:2019)

Denne europeiske standarden ble godkjent av CEN 14.oktober 2019.

CEN-medlemmer er forpliktet til å følge «CEN/CENELEC Internal Regulations» som angir vilkårene for å gi denne europeiske standarden status som nasjonal standard uten noen endringer. Oppdaterte lister og bibliografiske referanser som gjelder tilsvarende nasjonale standarder, kan fås ved henvendelse til Sentralsekretariatet eller til et CEN-medlem.

Denne europeiske standarden foreligger i de tre offisielle språkversjonene (engelsk, fransk, tysk). En versjon på et annet språk som et CEN-medlem på eget ansvar har oversatt til landets eget språk, og som det har underrettet Sentralsekretariatet om, har samme status som de offisielle versjonene.

CEN- og CENELEC-medlemmer er de nasjonale standardiseringsorganisasjonene i Belgia, Bulgaria, Danmark, Den tidligere jugoslaviske republikk Makedonia, Estland, Finland, Frankrike, Hellas, Irland, Island, Italia, Kroatia, Kypros, Latvia, Litauen, Luxembourg, Malta, Nederland, Norge, Polen, Portugal, Romania, Serbia, Slovakia, Slovenia, Spania, Storbritannia, Sveits, Sverige, Tsjekkia, Tyrkia, Tyskland, Ungarn og Østerrike.

Den europeiske standardiseringsorganisasjonen
Europäisches Komitee für Normung
European Committee for Standardization
Comité Européen de Normalisation

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

NS-EN ISO 22301:2019

Innhold

NS-EN ISO 22301:2019

NS-EN ISO 22301:2019

Forord

ISO (Den internasjonale standardiseringsorganisasjonen) er et verdensomspennende forbund av nasjonale standardiseringsorganer (ISO-medlemsorganer). Arbeidet med å utarbeide internasjonale standarder utføres vanligvis gjennom tekniske ISO-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 komité) i alle saker som gjelder elektroteknisk standardisering.

Prosedyrene som er 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 noen av eller alle disse patentrettighetene. Detaljer om eventuelle patentrettigheter som identifiseres under utviklingen av dokumentet, finnes i 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 www.iso.org/iso/foreword.html.

Dette dokumentet ble utarbeidet av den tekniske komiteen ISO/TC 292, *Security and resilience*.

Denne andre utgaven opphever og erstatter den første utgaven (NS-EN ISO 22301:2014), som har gjennomgått teknisk revisjon. De viktigste endringene sammenlignet med den forrige utgaven er som følger:

— ISOs krav til ledelsessystemstandarder, som er blitt utviklet siden 2012, er lagt til grunn.
— Krav er tydeliggjort, men ingen nye krav er tilføyd.
— Disiplinspesifikke krav til virksomhetskontinuitet ligger nå nesten i sin helhet i punkt 8.
— Punkt 8 er omstrukturert for å gi en bedre forståelse av de viktigste kravene.
— En rekke disiplinspesifikke termer for virksomhetskontinuitet er endret for å gjøres tydeligere og gjenspeile dagens tankegang.

Alle tilbakemeldinger eller spørsmål om dette dokumentet bør rettes til brukerens nasjonale standardiseringsorgan. En fullstendig liste over disse organisasjonene finnes på www.iso.org/members.html.

NS-EN ISO 22301:2019

Orientering

0.1 Generelt

Dette dokumentet angir strukturen for og kravene til implementering og vedlikehold av et system for kontinuitetsledelse (BCMS – business continuity management system) som utvikler virksomhetskontinuitet i henhold til hvor stor og hva slags type virkning en organisasjon kan eller ikke kan godta etter en forstyrrelse.

Resultatene av å vedlikeholde et BCMS formes av organisasjonens juridiske, forskriftsmessige, organisasjonsmessige og bransjespesifikke krav, produktene og tjenestene som leveres, prosessene som brukes, størrelsen og strukturen på organisasjonen og kravene fra organisasjonens interesseparter.

Et BCMS understreker viktigheten av:

— å forstå organisasjonens behov og nødvendigheten av å etablere policyer og mål for virksomhetskontinuitet;
— å drive og vedlikeholde prosesser, evner og responsstrukturer for å sikre at organisasjonen vil kunne tåle forstyrrelser;
— å overvåke og gjennomgå prestasjonen til og virkningen av BCMS;
— kontinuerlig forbedring basert på kvalitative og kvantitative tiltak.

Et BCMS består, i likhet med andre ledelsessystemer, av følgende komponenter:

a) en policy;
b) kompetente personer med definerte ansvarsområder;
c) ledelsesprosesser knyttet til:

    1) policy;
    2) planlegging;
    3) implementering og drift;
    4) prestasjonsvurdering:
    5) ledelsens gjennomgåelse;
    6) kontinuerlig forbedring;

d) dokumentert informasjon som støtter driftskontroll og muliggjør prestasjonsevaluering.

0.2 Fordeler ved et system for kontinuitetsledelse

Formålet med et BCMS er å forberede, stille til rådighet og opprettholde nødvendige kontrollmekanismer og evner, slik at organisasjonen er bedre i stand til å fortsette driften under forstyrrelser. Ved å oppnå dette vil organisasjonen:

a) fra et virksomhetsperspektiv:

    1) støtte sine strategiske mål;
    2) skape et konkurransefortrinn;
    3) beskytte og forbedre sitt omdømme og sin troverdighet;
    4) bidra til organisasjonens resiliens;

b) fra et økonomisk perspektiv:

    1) redusere juridisk og økonomisk risiko;
    2) redusere direkte og indirekte kostnader ved forstyrrelser;

NS-EN ISO 22301:2019

c) fra interessepartenes perspektiv:

1) beskytte liv, eiendom og miljøet;
2) ta hensyn til interessepartenes forventninger;
3) inngi tillit til organisasjonens evne til å lykkes;

d) fra et perspektiv basert på interne prosesser:

1) forbedre sin evne til å opprettholde effektiviteten ved forstyrrelser;
2) vise proaktiv styring av risikoer på en virkningsfull og effektiv måte;
3) identifisere og håndtere sårbarheter ved driften.

0.3 Planlegg-Utfør-Kontroller-Korriger (PDCA)-syklusen (Plan-Do-Check-Act)

Dette dokumentet anvender syklusen Planlegg (etablering), Utfør (implementering og drift), Kontroller (overvåking og gjennomgåelse) og Korriger (vedlikehold og forbedring) (PDCA) for å implementere, vedlikeholde og kontinuerlig forbedre organisasjonens BCMS.

Dette sikrer en grad av samsvar med andre ledelsessystemstandarder, som NS-EN ISO 9001, NS-EN ISO 14001, SN ISO/IEC 20000-1, NS-EN ISO/IEC 27001 og ISO 28000, som dermed støtter integrert implementering og drift i samsvar med andre tilsvarende ledelsessystemer.

I samsvar med PDCA-syklusen dekker punkt 4 til 10 følgende komponenter.

— Punkt 4 innfører kravene som er nødvendige for å etablere konteksten til det BCMS som passer for organisasjonen, i tillegg til behov, krav og omfang.
— Punkt 5 oppsummerer kravene som gjelder spesielt for den øverste ledelsens rolle i BCMS, og hvordan ledelsen gir uttrykk for sine forventninger til organisasjonen gjennom en policyerklæring.
— Punkt 6 beskriver kravene til etablering av strategiske mål og retningsgivende prinsipper for helhetlig BCMS.
— Punkt 7 støtter BCMS-aktiviteter knyttet til etablering av kompetanse og kommunikasjon med interesseparter på et gjentakende grunnlag eller etter behov, samtidig som nødvendig dokumentert informasjon dokumenteres, kontrolleres, vedlikeholdes og oppbevares.
— Punkt 8 definerer behov for virksomhetskontinuitet, bestemmer hvordan disse behovene skal identifiseres og håndteres, og utvikler prosedyrer for å lede organisasjonen gjennom en forstyrrelse.
— Punkt 9 oppsummerer kravene som er nødvendige for å måle virksomhetskontinuitetens prestasjon og BCMSs samsvar med dette dokumentet, og for å utføre ledelsens gjennomgåelse.
— Punkt 10 identifiserer og beskriver BCMS-avvik og kontinuerlig forbedring gjennom korrigerende tiltak.

0.5 Innholdet i dette dokumentet

Dette dokumentet overholder ISOs krav til standarder for ledelsessystemer. Disse kravene omfatter en overordnet struktur, identisk kjernetekst og felles termer med kjernedefinisjoner, til nytte for brukere som skal implementere flere ISO-standarder for ledelsessystemer.

Dette dokumentet inneholder ikke krav som er spesifikke for andre ledelsessystemer, men elementene i dette dokumentet kan samordnes eller integreres med krav i andre ledelsessystemer.

Dette dokumentet inneholder krav som kan brukes av en organisasjon til å implementere et BCMS og til å vurdere samsvar. En organisasjon som ønsker å påvise samsvar med dette dokumentet, kan gjøre det ved å:

— gjennomføre egenvurdering og egenerklæring; eller

NS-EN ISO 22301:2019

— søke bekreftelse på samsvar hos parter som har en interesse i organisasjonen, for eksempel kunder; eller
— søke bekreftelse på sin egenerklæring fra eksterne parter; eller
— søke sertifisering/registrering av sitt BCMS hos en ekstern organisasjon.

Punkt 1 til 3 i dette dokumentet fastsetter omfanget, de normative referansene og termene og definisjonene som gjelder for bruken av dette dokumentet. Punkt 4 til 10 inneholder kravene som skal brukes til å vurdere samsvar med dette dokumentet.

I dette dokumentet brukes verbene nedenfor på følgende måte:

a) «skal» angir et krav;
b) «bør» angir en anbefaling;
c) «kan» (engelsk: «may») angir en tillatelse;
d) «kan» (engelsk: «can») angir en mulighet eller evne.

Informasjon merket som «MERKNAD» er veiledende for å forstå eller for å klarlegge det tilhørende kravet. «Begrepsmerknader» brukt i punkt 3 gir tilleggsinformasjon som utfyller terminologiske data, og kan inneholde bestemmelser om bruken av en term.

Norsk Standard **NS-EN ISO 22301:2019**

Sikkerhet og resiliens — Systemer for kontinuitetsledelse — Krav

1 Omfang

Dette dokumentet angir krav til implementering, vedlikehold og forbedring av et ledelsessystem for å beskytte mot, redusere sannsynligheten for forekomst av, forberede til, respondere på og gjenopprette etter forstyrrelser når de oppstår.

Kravene som er angitt i dette dokumentet, er ikke sektorspesifikke og er beregnet på å kunne brukes av alle organisasjoner, eller deler av dem, uavhengig av organisasjonens type, størrelse og art. Anvendelsesområdet for disse kravene avhenger av organisasjonens driftsomgivelser og kompleksitet.

Dette dokumentet gjelder for organisasjoner av enhver type og størrelse som:

a) implementerer, vedlikeholder og forbedrer et BCMS;
b) etterstreber å sikre samsvar med den fastsatte policyen for virksomhetskontinuitet;
c) har behov for å kunne fortsette å levere produkter og tjenester med en akseptabel forhåndsdefinert kapasitet ved en forstyrrelse;
d) etterstreber å forbedre sin resiliens gjennom virkningsfull anvendelse av BCMS.

Dette dokumentet kan brukes til å vurdere en organisasjons evne til å oppfylle sine egne behov for virksomhetskontinuitet og forpliktelser.

2 Normative referanser

Følgende refererte dokumenter inneholder tekst som helt eller delvis inngår i kravene i dette dokumentet. For daterte referanser gjelder kun den angitte utgaven. For udaterte referanser gjelder den nyeste utgaven av det refererte dokumentet (med eventuelle endringsblad).

NS-EN ISO 22301:2019, *Sikkerhet og resiliens — Terminologi*

3 Termer og definisjoner

I dette dokumentet gjelder termene og definisjonene gitt i NS-EN ISO 22300 i tillegg til de følgende.

ISO og IEC fører terminologidatabaser til bruk ved standardisering på følgende adresser:

— ISO Online browsing platform: tilgjengelig på https://www.iso.org/obp
— IEC Electropedia: tilgjengelig på http://www.electropedia.org/

MERKNAD Termene og definisjonene som er gitt nedenfor, erstatter de som er gitt i NS-EN ISO 22300:2018.

NS-EN ISO 22301:2019

3.1
aktivitet
samling av én eller flere oppgaver med et definert resultat

[KILDE: NS-EN ISO 22300:2018, 3.1, modifisert – definisjonen er erstattet, og eksemplet er slettet.]

3.2
revisjon
systematisk, uavhengig og dokumentert *prosess* (3.26) for å framskaffe revisjonsbevis og bedømme det objektivt for å bestemme i hvilken grad revisjonskriteriene er oppfylt

Begrepsmerknad 1: En revisjon kan være en intern revisjon (førsteparts) eller en ekstern revisjon (andre- eller tredjeparts), og den kan være en kombinert revisjon (som kombinerer to eller flere disipliner).

Begrepsmerknad 2: En intern revisjon gjennomføres av *organisasjonen* (3.21) selv eller av en ekstern part på vegne av organisasjonen.

Begrepsmerknad 3: «Revisjonsbevis» og «revisjonskriterier» er definert i NS-EN ISO 19011.

Begrepsmerknad 4: De grunnleggende elementene i en revisjon omfatter bestemmelse av *samsvar* (3.7) for et objekt i henhold til en prosedyre gjennomført av personell som ikke er ansvarlig for objektet som revideres.

Begrepsmerknad 5: En internrevisjon kan være tilknyttet ledelsens gjennomgåelse eller andre interne formål og kan utgjøre grunnlaget for en organisasjons samsvarserklæring. Uavhengighet vises ved frihet fra ansvar for den *aktiviteten* (3.1) som revideres. Eksternrevisjoner omfatter andre- eller tredjeparts revisjoner. Andreparts revisjoner utføres av parter som er interessert i organisasjonen, for eksempel kunder, eller av andre personer på deres vegne. Tredjeparts revisjoner utføres av eksterne uavhengige organisasjoner for revisjon, som de som framskaffer sertifisering/registrering av samsvar, eller myndighetsorganer.

Begrepsmerknad 6: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder. Den opprinnelige definisjonen har blitt modifisert ved at begrepsmerknad 4 og 5 er tilføyd.

3.3
virksomhetskontinuitet
en *organisasjons* (3.21) evne til å fortsette å levere *produkter* og *tjenester* (3.27) innenfor akseptable tidsrammer med forhåndsdefinert kapasitet ved en *forstyrrelse* (3.10)

[KILDE: NS-EN ISO 22300:2018, 3.24, modifisert – definisjonen er erstattet.]

3.4
kontinuitetsplan
dokumentert informasjon (3.11) som veileder en *organisasjon* (3.21) til å respondere på en *forstyrrelse* (3.10) og gjenoppta, gjenvinne og gjenopprette levering av *produkter og tjenester* (3.27) i samsvar med sine mål (3.20) for *virksomhetskontinuitet* (3.3)

[KILDE: NS-EN ISO 22300:2018, 3.27, modifisert – definisjonen er erstattet, og begrepsmerknad 1 er slettet.]

3.5
analyse av virksomhetsmessige virkninger
prosess (3.26) med å analysere *effekten* (3.13) på *organisasjonen* (3.21) over tid ved en *forstyrrelse* (3.10)

Begrepsmerknad 1: Resultatet er en erklæring og begrunnelse for *krav* (3.28) til *virksomhetskontinuitet* (3.3).

NS-EN ISO 22301:2019

[KILDE: NS-EN ISO 22300:2018, 3.29, modifisert – definisjonen er erstattet, og begrepsmerknad 1 er tilføyd.]

3.6
kompetanse
evne til å bruke kunnskaper og ferdigheter for å oppnå tiltenkte resultater

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.7
samsvar
oppfyllelse av et *krav* (3.28)

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.8
kontinuerlig forbedring
gjentatt *aktivitet* (3.1) for å forbedre *prestasjon* (3.23)

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.9
korrigerende tiltak
tiltak som skal eliminere årsaken(e) til et *avvik* (3.19) og forhindre at det oppstår på nytt

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.10
forstyrrelse
episode (3.14), enten forventet eller uventet, som forårsaker et uplanlagt, negativt avvik fra den forventede leveringen av *produkter og tjenester* (3.27) i henhold til en *organisasjons* (3.21) *mål* (3.20)

[KILDE: NS-EN ISO 22300:2018, 3.70, modifisert – definisjonen er erstattet.]

3.11
dokumentert informasjon
informasjon som det kreves at en *organisasjon* (3.21) styrer og vedlikeholder, og mediet den er lagret på

Begrepsmerknad 1: Dokumentert informasjon kan være i ethvert format og på ethvert medium og fra enhver kilde.

Begrepsmerknad 2: Dokumentert informasjon kan vise til:

- *ledelsessystemet* (3.16), innbefattet tilhørende *prosesser* (3.26);
- informasjon som utarbeides for å drive organisasjonen (dokumentasjon);
- bevis på resultater som er oppnådd (registreringer).

Begrepsmerknad 3: Begrepsmerknad 3: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

NS-EN ISO 22301:2019

3.12
virkning
i hvilket omfang planlagte *aktiviteter* (3.1) blir gjennomført og planlagte resultater oppnås

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.13
effekt
resultat av en *forstyrrelse* (3.10) som påvirker *mål* (3.20)

[KILDE: NS-EN ISO 22300:2018, 3.107, modifisert – definisjonen er erstattet.]

3.14
episode
situasjon som kan være eller kan føre til en *forstyrrelse* (3.10), et tap, en nødsituasjon eller en krise

[KILDE: NS-EN ISO 22300:2018, 3.111, modifisert – definisjonen er erstattet.]

3.15
interessepart (foretrukket term)
interessent (tillatt term)
person eller *organisasjon* (3.21) som kan påvirke, bli påvirket av eller oppfatte seg selv som påvirket av en beslutning eller *aktivitet* (3.1)

EKSEMPEL Kunder, eiere, personell, leverandører, bankierer, forskriftsmyndigheter, fagforeninger, partnere eller samfunn som kan omfatte konkurrenter eller opponerende pressgrupper.

Begrepsmerknad 1: En beslutningstaker kan være en interessepart.

Begrepsmerknad 2: Berørte lokalsamfunn og lokale befolkningsgrupper anses som interesseparter.

Begrepsmerknad 3: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder. Den opprinnelige definisjonen har blitt modifisert ved å tilføye et eksempel og begrepsmerknad 1 til 2.

3.16
ledelsessystem
sett av beslektede eller samvirkende elementer i en *organisasjon* (3.21) for å etablere *policyer* (3.24) og *mål* (3.20) og *prosesser* (3.26) for å nå disse målene

Begrepsmerknad 1: Et ledelsessystem kan ta hensyn til en enkelt disiplin eller flere disipliner.

Begrepsmerknad 2: Systemelementene omfatter organisasjonens struktur, roller og ansvarsfordeling, planlegging og drift.

Begrepsmerknad 3: Omfanget av et ledelsessystem kan omfatte hele organisasjonen, bestemte og identifiserte funksjoner i organisasjonen, bestemte og identifiserte deler av organisasjonen eller én eller flere funksjoner på tvers av en gruppe av organisasjoner.

Begrepsmerknad 4: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.17
måling
prosess (3.26) for å bestemme en verdi

NS-EN ISO 22301:2019

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.18
overvåking
bestemme statusen til et system, en *prosess* (3.26) eller en *aktivitet* (3.1)

Begrepsmerknad 1: Det kan være nødvendig å kontrollere, overvåke eller kritisk observere for å kunne bestemme statusen.

Begrepsmerknad 2: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.19
avvik
manglende oppfyllelse av et *krav* (3.28)

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.20
mål
resultat som skal oppnås

Begrepsmerknad 1: Et mål kan være strategisk, taktisk eller driftsmessig.

Begrepsmerknad 2: Mål kan ha forbindelse med forskjellige disipliner (for eksempel finansielle mål, mål for helse og sikkerhet eller miljø) og kan gjelde på forskjellige nivåer (for eksempel på strateginivå, for hele organisasjonen eller for et prosjekt, et produkt eller en *prosess* (3.26)).

Begrepsmerknad 3: Et mål kan uttrykkes på andre måter, for eksempel som et tiltenkt resultat, et formål, et driftskriterium eller et mål for *virksomhetskontinuitet* (3.3), eller ved å bruke andre ord med lignende betydning (for eksempel siktemål, målsetning eller hensikt).

Begrepsmerknad 4: Når det gjelder *ledelsessystemer* (3.16) for virksomhetskontinuitet, settes målene for virksomhetskontinuitet av *organisasjonen* (3.16), i samsvar med *policyen* (3.24) for virksomhetskontinuitet, for å oppnå definerte resultater.

Begrepsmerknad 5: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.21
organisasjon
person eller gruppe av personer som har egne funksjoner med ansvar, myndighet og relasjoner som er nødvendige for å nå organisasjonens *mål* (3.20)

Begrepsmerknad 1: Begrepet organisasjon omfatter, men er ikke begrenset til, selvstendig næringsdrivende, aksjeselskap, konsern, firma, foretak, myndighet, partnerskap, veldedig organisasjon eller institusjon, eller en del eller en kombinasjon av slike, enten det er en egen juridisk person eller ikke, offentlig eller privat.

Begrepsmerknad 2: For organisasjoner med mer enn én driftsenhet kan en driftsenhet defineres som en organisasjon.

Begrepsmerknad 3: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder. Den opprinnelige definisjonen har blitt modifisert ved at begrepsmerknad 2 er tilføyd.

NS-EN ISO 22301:2019

3.22
utkontrahere, verb
lage en ordning der en ekstern *organisasjon* (3.21) utfører deler av en organisasjons funksjon eller *prosess* (3.26)

Begrepsmerknad 1: En ekstern organisasjon er utenfor omfanget av *ledelsessystemet* (3.16), selv om den utkontraherte funksjonen eller prosessen inngår i omfanget.

Begrepsmerknad 2: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.23
prestasjon
målbart resultat

Begrepsmerknad 1: Prestasjon kan ha sammenheng med enten kvantitative eller kvalitative funn.

Begrepsmerknad 2: Prestasjon kan ha sammenheng med styring av *aktiviteter* (3.1), *prosesser* (3.26), produkter (inkludert tjenester), systemer eller *organisasjoner* (3.21).

Begrepsmerknad 3: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.24
policy
intensjon og retning for en *organisasjon* (3.21) slik organisasjonens øverste *ledelse* (3.31) formelt uttrykker den

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.25
prioritert aktivitet
aktivitet (3.1) som gis prioritet for å unngå uakseptable *effekter* (3.13) på virksomheten ved en forstyrrelse (3.10)

[KILDE: NS-EN ISO 22300:2018, 3.176, modifisert – definisjonen er erstattet, og begrepsmerknad 1 er slettet.]

3.26
prosess
sett av beslektede eller samvirkende *aktiviteter* (3.1) som omsetter inngangsfaktorer til resultater

Begrepsmerknad 1: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.27
produkt og tjeneste
utgangsfaktor eller resultat levert av en *organisasjon* (3.21) til *interesseparter* (3.15)

EKSEMPEL Produserte produkter, bilforsikring, hjemmesykepleie.

[KILDE: NS-EN ISO 22300:2018, 3.181, modifisert – termen «produkt og tjeneste» har erstattet «produkt eller tjeneste», og definisjonen er erstattet.]

NS-EN ISO 22301:2019

3.28
krav
behov eller forventning som er angitt, vanligvis underforstått eller obligatorisk

Begrepsmerknad 1: «Vanligvis underforstått» betyr at det er vanlig eller normal praksis for *organisasjonen* (3.21) og *interessepartene* (3.15) at behovet eller forventningen det gjelder, er underforstått.

Begrepsmerknad 2: Et spesifisert krav er et krav som er uttrykt for eksempel i *dokumentert informasjon* (3.11).

Begrepsmerknad 3: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

3.29
ressurs
alle aktiva (inkludert anlegg og utstyr), personer, ferdigheter, teknologi, lokaler samt forsyninger og informasjon (enten de er elektroniske eller ikke) som en *organisasjon* (3.21) er nødt til å ha tilgjengelig ved behov for å kunne opprettholde driften og oppfylle sitt *mål* (3.20)

[KILDE: NS-EN ISO 22300:2018, 3.193, modifisert – definisjonen er erstattet.]

3.30
risiko
virkningen av usikkerhet knyttet til *mål* (3.20)

Begrepsmerknad 1: En virkning er et avvik fra det forventede – positivt eller negativt.

Begrepsmerknad 2: Usikkerhet er en tilstand der det er mangel på, eventuelt delvis mangel på, informasjon angående, forståelse av eller kunnskap om en hendelse, dens konsekvens eller sannsynligheten for at den skal forekomme.

Begrepsmerknad 3: Risiko er ofte karakterisert ved å vise til mulige «hendelser» (som definert i SN-ISO Guide 73) og «konsekvenser» (som definert i SN-ISO Guide 73), eller til en kombinasjon av hendelser og konsekvenser.

Begrepsmerknad 4: Risiko uttrykkes ofte som en kombinasjon av konsekvensene av en hendelse (inklusive endring i omstendigheter) og tilhørende sannsynlighet (som definert i SN-ISO Guide 73) for at den skal forekomme.

Begrepsmerknad 5: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder. Definisjonen er modifisert gjennom tilføyelsen av «knyttet til mål» for å være konsekvent med NS-EN ISO 31000.

3.31
øverste ledelse
person eller gruppe av mennesker som rettleder og styrer en *organisasjon* (3.21) på øverste nivå

Begrepsmerknad 1: Den øverste ledelsen har fullmakt til å delegere myndighet og skaffe *ressurser* (3.29) innenfor organisasjonen.

Begrepsmerknad 2: Hvis omfanget av *ledelsessystemet* (3.16) bare dekker en del av en organisasjon, skal den øverste ledelsen henvise til dem som rettleder og styrer den delen av organisasjonen.

Begrepsmerknad 3: Dette utgjør én av de felles termene og kjernedefinisjonene i den overordnede strukturen i ISOs ledelsessystemstandarder.

NS-EN ISO 22301:2019

4 Organisasjonens kontekst

4.1 Forstå organisasjonen og dens kontekst

Organisasjonen skal påvise eksterne og interne forhold som er relevante for organisasjonens formål, og som påvirker organisasjonens evne til å oppnå ett eller flere tilsiktede resultater av BCMS.

MERKNAD Disse forholdene vil påvirkes av organisasjonens overordnede mål, dens produkter og tjenester og mengden og typen risiko den kan eller ikke kan ta.

4.2 Forstå interessepartenes behov og forventninger

4.2.1 Generelt

Når organisasjonen fastsetter sitt BCMS, skal den bestemme:

a) hvilke interesseparter som er relevante for BCMS;
b) hvilke krav fra disse interessepartene som er relevante.

4.2.2 Rettslige krav og andre krav

Organisasjonen skal:

a) implementere og vedlikeholde en prosess for å identifisere, ha tilgang til og vurdere de gjeldende juridiske og forskriftsmessige kravene knyttet til kontinuiteten i deres produkter og tjenester, aktiviteter og ressurser;
b) sørge for at det er tatt hensyn til disse gjeldende juridiske, forskriftsmessige og øvrige kravene ved implementering og vedlikehold av dens BCMS;
c) dokumentere denne informasjonen og sørge for at den holdes oppdatert.

4.3 Bestemme omfanget av systemet for kontinuitetsledelse

4.3.1 Generelt

Organisasjonen skal fastsette grensene og anvendelsesområdet for BCMS for å fastlegge systemets omfang.

Når organisasjonen bestemmer omfanget, skal den ta hensyn til:

a) de eksterne og interne forholdene nevnt i 4.1;
b) kravene nevnt i 4.2;
c) dens oppdrag, målsetninger og interne og eksterne forpliktelser.

Omfanget skal være tilgjengelig i form av dokumentert informasjon.

4.3.2 Omfanget av systemet for kontinuitetsledelse

Organisasjonen skal:

a) fastsette de delene av organisasjonen som skal inkluderes i BCMS, hvor det tas hensyn til plassering(er), størrelse, art og kompleksitet;
b) identifisere produkter og tjenester som skal inkluderes i BCMS.

NS-EN ISO 22301:2019

Når omfanget defineres, skal organisasjonen dokumentere og forklare utelatelser. Utelatelsene skal ikke påvirke organisasjonens evne til og ansvar for å levere virksomhetskontinuitet, slik det er slått fast i analysen av virksomhetsmessige virkninger eller risikovurderingen og gjeldende juridiske eller forskriftsmessige krav.

4.4 System for kontinuitetsledelse

Organisasjonen skal opprette, iverksette, vedlikeholde og kontinuerlig forbedre et BCMS, inkludert de nødvendige prosessene og vekselvirkningen mellom disse, i samsvar med kravene i dette dokumentet.

5 Lederskap

5.1 Lederskap og forpliktelse

Den øverste ledelsen skal vise lederskap og forpliktelse med hensyn til BCMS ved å:

a) sikre at policyen og målene for virksomhetskontinuitet blir etablert og er forenlige med strategiretningen til organisasjonen;
b) sikre at kravene i BCMS integreres i organisasjonens prosesser;
c) sikre at de nødvendige ressursene for BCMS er tilgjengelige;
d) kommunisere viktigheten av effektiv virksomhetskontinuitet og av å overholde kravene i BCMS;
e) sikre at BCMS oppnår det eller de tiltenkte resultatene;
f) veilede og støtte personer for å bidra til at BCMS blir virkningsfullt;
g) fremme kontinuerlig forbedring;
h) støtte personer med andre relevante lederroller til å vise sitt lederskap og sin forpliktelse der det er aktuelt for deres ansvarsområder.

MERKNAD Henvisning til «virksomhet» i dette dokumentet kan tolkes vidt og omfatte de aktivitetene som utgjør kjernen av formålet med organisasjonens eksistens.

5.2 Policy

5.2.1 Etablere policyen for virksomhetskontinuitet

Den øverste ledelsen skal etablere en policy for virksomhetskontinuitet som:

a) er hensiktsmessig for organisasjonens formål;
b) gir en ramme for å fastsette mål for virksomhetskontinuitet;
c) omfatter en forpliktelse til å oppfylle aktuelle krav;
d) omfatter en forpliktelse til kontinuerlig forbedring av BCMS.

5.2.2 Kommunisere policyen for virksomhetskontinuitet

Policyen for virksomhetskontinuiteten skal:

a) være tilgjengelig i form av dokumentert informasjon;
b) kommuniseres innad i organisasjonen;
c) være tilgjengelig for interesseparter, der det er relevant.

NS-EN ISO 22301:2019

5.3 Roller, ansvar og myndighet

Den øverste ledelsen skal sikre at ansvar og myndighet for relevante roller tildeles og kommuniseres innad i organisasjonen.

Den øverste ledelsen skal tildele ansvar og myndighet for å:

a) sikre at BCMS er i samsvar med kravene i dette dokumentet;
b) rapportere til øverste ledelse om prestasjonen til BCMS.

6 Planlegging

6.1 Tiltak for å identifisere og håndtere risikoer og muligheter

6.1.1 Bestemme risikoer og muligheter

Ved planlegging av BCMS skal organisasjonen vurdere forholdene nevnt i 4.1 og kravene nevnt i 4.2 og bestemme risikoene og mulighetene som er nødt til å identifiseres og håndteres, for å:

a) sikre at BCMS kan oppnå det eller de tiltenkte resultatene;
b) forhindre eller begrense uønskede konsekvenser;
c) oppnå kontinuerlig forbedring.

6.1.2 Identifisere og håndtere risikoer og muligheter

Organisasjonen skal planlegge:

a) tiltak for å identifisere og håndtere disse risikoene og mulighetene;
b) hvordan:

    1) tiltakene skal integreres og implementeres i BCMS-prosessene (se 8.1);
    2) virkningen av disse tiltakene skal evalueres (se 9.1).

MERKNAD Risikoer og muligheter er knyttet til virkningen av ledelsessystemet. Risikoer knyttet til forstyrrelse av produksjonen er omtalt i 8.2.

6.2 Mål for virksomhetskontinuitet og planlegging for å nå dem

6.2.1 Etablere mål for virksomhetskontinuitet

Organisasjonen skal fastsette mål for virksomhetskontinuitet for relevante funksjoner og nivåer.

Målene for virksomhetskontinuitet skal:

a) være i overensstemmelse med policyen for virksomhetskontinuitet;
b) kunne måles (hvis det er gjennomførbart);
c) ta hensyn til gjeldende krav (se 4.1 og 4.2);
d) overvåkes;
e) kommuniseres;
f) oppdateres ved behov.

NS-EN ISO 22301:2019

Organisasjonen skal oppbevare dokumentert informasjon om målene for virksomhetskontinuitet.

6.2.2 Bestemme mål for virksomhetskontinuitet

Ved planlegging av hvordan målene for virksomhetskontinuitet kan nås, skal organisasjonen fastsette:

a) hva som skal gjøres;
b) hvilke ressurser som blir nødvendige;
c) hvem som har ansvar for utførelsen;
d) når det skal være utført;
e) hvordan resultatene skal evalueres.

6.3 Planlegge endringer av systemet for kontinuitetsledelse

Når organisasjonen bestemmer at det er nødvendig å gjøre endringer i BCMS, inklusive de som er identifisert i punkt 10, skal endringene gjennomføres på en planlagt måte.

Organisasjonen skal vurdere:

a) formålet med endringene og potensielle konsekvenser av dem;
b) integriteten til BCMS;
c) tilgjengeligheten av ressurser;
d) tildeling eller omfordeling av ansvar og myndighet.

7 Støtte

7.1 Ressurser

Organisasjonen skal bestemme og skaffe til veie ressursene som er nødvendige for å etablere, implementere, vedlikeholde, oppdatere og kontinuerlig forbedre BCMS.

7.2 Kompetanse

Organisasjonen skal:

a) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker prestasjon når det gjelder virksomhetskontinuitet;
b) sikre at disse personene har tilegnet seg nødvendig kompetanse gjennom egnet utdanning, opplæring eller erfaring;
c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet;
d) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

MERKNAD Aktuelle tiltak kan for eksempel omfatte opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.

7.3 Bevisstgjøring

Personer som utfører arbeid under organisasjonens styring, skal være bevisste på:

a) policyen for virksomhetskontinuitet;

NS-EN ISO 22301:2019

b) deres bidrag til virkningen av BCMS, inklusive fordelene ved forbedret virksomhetskontinuitet;
c) konsekvensene av å ikke overholde kravene i BCMS;
d) sin egen rolle og sitt eget ansvar før, under og etter forstyrrelser.

7.4 Kommunikasjon

Organisasjonen skal fastlegge intern og ekstern kommunikasjon som er relevant for BCMS, inklusive:

a) hva kommunikasjonen skal omhandle;
b) når det skal kommuniseres;
c) hvem det skal kommuniseres med;
d) hvordan det skal kommuniseres;
e) hvem som skal kommunisere.

7.5 Dokumentert informasjon

7.5.1 Generelt

Organisasjonens BCMS skal omfatte:

a) dokumentert informasjon som kreves i dette dokumentet;
b) dokumentert informasjon som organisasjonen har bestemt er nødvendig for virkningen av BCMS.

MERKNAD Omfanget av dokumentert informasjon for et BCMS kan være forskjellig fra organisasjon til organisasjon på grunn av:

— organisasjonens størrelse og typen aktiviteter, prosesser, produkter og tjenester og ressurser;
— kompleksiteten til prosessene og vekselvirkningen mellom dem;
— enkeltpersoners kompetanse.

7.5.2 Oppretting og oppdatering

Når organisasjonen oppretter og oppdaterer dokumentert informasjon, skal den sikre hensiktsmessig:

a) identifikasjon og beskrivelse (for eksempel en tittel, dato eller forfatter eller et referansenummer);
b) format (for eksempel språk, programvareversjon eller grafikk) og medium (for eksempel papir eller elektronisk);
c) gjennomgåelse og godkjenning av egnethet og tilstrekkelighet.

7.5.3 Styring av dokumentert informasjon

7.5.3.1 Dokumentert informasjon som kreves i henhold til BCMS og dette dokumentet, skal styres for å sikre at:

a) den er tilgjengelig og egnet for bruk, der og når det er nødvendig;
b) den er tilstrekkelig beskyttet (for eksempel mot misbruk av taushetsbelagt informasjon, uriktig bruk eller tap av helhet).

7.5.3.2 For å styre dokumentert informasjon skal organisasjonen vurdere følgende aktiviteter, avhengig av hva som passer:

a) distribusjon, tilgang, gjenfinning og bruk;
b) lagring og bevaring, inklusive opprettholdelse av leselighet;

NS-EN ISO 22301:2019

c) kontroll av endringer (for eksempel versjonskontroll);
d) opprettholdelse og avhending.

Dokumentert informasjon med eksternt opphav som organisasjonen har besluttet er nødvendig for planlegging og drift av BCMS, skal i tilstrekkelig grad identifiseres og styres.

MERKNAD Tilgang kan innebære en beslutning om tillatelse til bare å se dokumentert informasjon eller tillatelse og myndighet til å se og endre dokumentert informasjon.

8 Drift

8.1 Planlegging og styring av drift

Organisasjonen skal planlegge, implementere og styre prosessene som er nødvendige for å oppfylle krav og for å iverksette tiltakene bestemt i 6.1, ved å:

a) fastsette kriterier for prosessene;
b) implementere styring av prosessene i henhold til kriteriene;
c) ta vare på dokumentert informasjon i den grad det er nødvendig for å ha tillit til at prosessene blir utført som planlagt.

Organisasjonen skal styre planlagte endringer og gjennomgå konsekvensene av utilsiktede endringer, og der det er nødvendig, treffe tiltak for å begrense eventuelle ugunstige virkninger.

Organisasjonen skal sikre at utkontraherte prosesser og leveransekjeden styres.

8.2 Analyse av virksomhetsmessige virkninger og risikovurdering

8.2.1 Generelt

Organisasjonen skal:

a) implementere og vedlikeholde systematiske prosesser for analyse av virksomhetsmessige virkninger og vurdering av risikoene ved forstyrrelser;
b) gjennomgå analysen av virksomhetsmessige virkninger og risikovurderingen med planlagte mellomrom og når det har oppstått betydelige endringer i organisasjonen eller i konteksten den virker i.

MERKNAD Organisasjonen bestemmer i hvilken rekkefølge analysen av virksomhetsmessige virkninger og risikovurderingen skal utføres i.

8.2.2 Analyse av virksomhetsmessige virkninger

Organisasjonen skal bruke prosessen med å analysere virksomhetsmessige virkninger til å bestemme prioriteringer og krav knyttet til virksomhetskontinuitet. Under prosessen skal organisasjonen:

a) definere hvilke virkningstyper og kriterier som er relevante for organisasjonens kontekst;
b) identifisere aktivitetene som støtter levering av produkter og tjenester;
c) bruke virkningstypene og kriteriene til å vurdere virkningene av forstyrrelse av disse aktivitetene over tid;
d) identifisere innenfor hvilken tidsramme virkningene av å ikke gjenoppta aktivitetene blir uakseptable for organisasjonen;

NS-EN ISO 22301:2019

MERKNAD 1 Denne tidsrammen kan omtales som «lengste akseptable periode for forstyrrelse» (MTPD – maximum tolerable period of disruption).

e) angi prioriterte tidsrammer innenfor tidsrammen identifisert i d) for gjenopptakelse av avbrutte aktiviteter med en angitt minste akseptabel kapasitet;

MERKNAD 2 Denne tidsrammen kan omtales som «mål for gjenopptakelsestid» (RTO – recovery time objective).

f) bruke denne analysen til å identifisere prioriterte aktiviteter;
g) bestemme hvilke ressurser som er nødvendige for å støtte prioriterte aktiviteter;
h) bestemme avhengigheter, inkludert partnere og leverandører, og de prioriterte aktivitetenes gjensidige avhengighet.

8.2.3 Risikovurdering

Organisasjonen skal implementere og vedlikeholde en risikovurderingsprosess.

MERKNAD Prosessen for risikovurdering omhandles i NS-EN ISO 31000.

Organisasjonen skal:

a) identifisere risikoene ved forstyrrelse av organisasjonens prioriterte aktiviteter og nødvendige ressurser;
b) analysere og evaluere de identifiserte risikoene;
c) bestemme hvilke risikoer det er nødvendig å håndtere.

MERKNAD Risikoer i dette underpunktet er knyttet til forstyrrelse av virksomhetsaktiviteter. Risikoer og muligheter knyttet til virkningen av ledelsessystemet omtales i 6.1.

8.3 Strategier og løsninger for virksomhetskontinuitet

8.3.1 Generelt

Basert på resultatene fra analysen av virksomhetsmessige virkninger og risikovurderingen skal organisasjonen identifisere og velge strategier for virksomhetskontinuitet som vurderer alternativer for tiden før, under og etter forstyrrelser. Strategiene for virksomhetskontinuitet skal bestå av én eller flere løsninger.

8.3.2 Identifisering av strategier og løsninger

Identifisering skal baseres på i hvilken grad strategier og løsninger:

a) oppfyller kravene til å fortsette og gjenoppta prioriterte aktiviteter innenfor de identifiserte tidsrammene og med den avtalte kapasiteten;
b) beskytter organisasjonens prioriterte aktiviteter;
c) reduserer sannsynligheten for forstyrrelser;
d) forkorter perioden med forstyrrelser;
e) begrenser effekten av forstyrrelsen på organisasjonens produkter og tjenester;
f) sørger for tilgjengelighet av tilstrekkelige ressurser.

8.3.3 Valg av strategier og løsninger

Valget skal baseres på i hvilken grad strategier og løsninger:

NS-EN ISO 22301:2019

a) oppfyller kravene til å fortsette og gjenoppta prioriterte aktiviteter innenfor de identifiserte tidsrammene og med den avtalte kapasiteten;
b) tar hensyn til mengden og typen risiko som organisasjonen kan eller ikke kan ta;
c) tar hensyn til tilhørende kostnader og fordeler.

8.3.4 Ressurskrav

Organisasjonen skal bestemme hvilke ressurser som kreves for å implementere de valgte løsningene for virksomhetskontinuitet. Ressurstypene som vurderes, skal innbefatte, men ikke være begrenset til:

a) personer;
b) informasjon og data;
c) fysisk infrastruktur som bygninger, arbeidsplasser eller andre lokaler og tilhørende fasiliteter;
d) utstyr og forbruksvarer;
e) systemer for informasjons- og kommunikasjonsteknologi (IKT);
f) transport og logistikk;
g) økonomi;
h) partnere og leverandører.

8.3.5 Implementering av løsninger

Organisasjonen skal implementere og vedlikeholde de valgte løsningene for virksomhetskontinuitet slik at de kan iverksettes ved behov.

8.4 Planer og prosedyrer for virksomhetskontinuitet

8.4.1 Generelt

Organisasjonen skal implementere og vedlikeholde en responsstruktur som gjør det mulig å varsle og kommunisere med relevante interesseparter i rett tid. Den skal sørge for å ha planer og prosedyrer for å lede organisasjonen ved en forstyrrelse. Planene og prosedyrene skal brukes når det er nødvendig for å iverksette løsninger for virksomhetskontinuitet.

MERKNAD Det kan inngå ulike typer prosedyrer i planene for virksomhetskontinuitet.

Organisasjonen skal identifisere og dokumentere planer og prosedyrer for virksomhetskontinuitet basert på resultatet av de valgte strategiene og løsningene.

Prosedyrene skal:

a) være spesifikke når det gjelder de umiddelbare trinnene som skal følges ved en forstyrrelse;
b) være fleksible for å kunne respondere på endringer i interne og eksterne forhold ved en forstyrrelse;
c) fokusere på effekten av episoder som potensielt kan føre til forstyrrelser;
d) være effektive når det gjelder å minimere virkningen gjennom implementering av hensiktsmessige løsninger;
e) tildele roller og ansvar for oppgaver i prosedyrene.

8.4.2 Responsstruktur

8.4.2.1 Organisasjonen skal implementere og vedlikeholde en struktur og identifisere én eller flere grupper som skal være ansvarlige for å respondere på forstyrrelser.

NS-EN ISO 22301:2019

8.4.2.2 Rollene og ansvaret til hver gruppe og forholdet mellom gruppene skal angis tydelig.

8.4.2.3 Sammen skal gruppene være kompetente til å:

a) vurdere arten og omfanget av forstyrrelsen og den potensielle virkningen;
b) vurdere virkningen opp mot forhåndsdefinerte terskler som gir grunnlag for iverksettelse av en formell respons;
c) iverksette en hensiktsmessig respons;
d) planlegge tiltak det er nødvendig å iverksette;
e) fastsette prioriteringer (med personsikkerhet som førsteprioritet);
f) overvåke virkningene av forstyrrelsen og organisasjonens respons;
g) iverksette løsningene for virksomhetskontinuitet;
h) kommunisere med relevante interesseparter, myndigheter og media.

8.4.2.4 For hver gruppe skal det finnes:

a) identifisert personell og stedfortredere for disse med nødvendig ansvar, autoritet og kompetanse til å utføre sin tildelte rolle;
b) dokumenterte prosedyrer som gir praktisk veiledning (se 8.4.4), inkludert prosedyrer for iverksetting, drift, koordinering og kommunikasjon av responsen.

8.4.3 Varsling og kommunikasjon

8.4.3.1 Organisasjonen skal dokumentere og vedlikeholde prosedyrer for å:

a) kommunisere internt og eksternt med relevante interesseparter, inkludert hva, når, med hvem og hvordan det skal kommuniseres;

MERKNAD Organisasjonen kan dokumentere og vedlikeholde prosedyrer for hvordan og under hvilke omstendigheter organisasjonen kommuniserer med ansatte og deres nødkontakter.

b) motta, dokumentere og respondere på kommunikasjon fra interesseparter, inkludert eventuelle nasjonale eller regionale systemer for varsling eller tilsvarende;
c) sikre tilgjengelighet av kommunikasjonsmidler ved en forstyrrelse;
d) legge til rette for strukturert kommunikasjon med beredskaps- og nødetatene;
e) gi informasjon om organisasjonens mediarespons etter en episode, inkludert en kommunikasjonsstrategi;
f) registrere detaljene rundt forstyrrelsen, tiltakene som ble iverksatt, og beslutningene som ble tatt.

8.4.3.2 Der det er aktuelt, skal følgende også tas hensyn til og implementeres:

a) varsle interesseparter som potensielt kan berøres av en reell eller nær forestående forstyrrelse;
b) sikre hensiktsmessig koordinering og kommunikasjon mellom flere responsorganisasjoner.

Varslings- og kommunikasjonsprosedyrene skal utøves som en del av organisasjonens øvelsesprogram, som er beskrevet i 8.5.

8.4.4 Planer for virksomhetskontinuitet

8.4.4.1 Organisasjonen skal dokumentere og vedlikeholde planer og prosedyrer for virksomhetskontinuitet. Planene for virksomhetskontinuitet skal gi veiledning og informasjon for å bistå gruppene når de skal respondere på en forstyrrelse, og for å bistå organisasjonen med respons og gjenopptakelse.

8.4.4.2 Samlet skal planene for virksomhetskontinuitet inneholde:

NS-EN ISO 22301:2019

a) informasjon om tiltakene som gruppene kommer til å iverksette for å:

   1) fortsette med eller gjenoppta prioriterte aktiviteter innenfor forhåndsdefinerte tidsrammer;
   2) overvåke virkningen av forstyrrelsen og organisasjonens respons på den;

b) referanse til forhåndsdefinerte terskler og prosesser for iverksetting av responsen;
c) prosedyrer for levering av produkter og tjenester med avtalt kapasitet;
d) informasjon om håndtering av umiddelbare konsekvenser ved en forstyrrelse med tilbørlig hensyn til:

   1) enkeltpersoners velferd;
   2) forebygging av ytterligere tap eller utilgjengelighet av prioriterte aktiviteter;
   3) miljømessige konsekvenser.

8.4.4.3 Hver plan skal omfatte:

a) formålet, omfanget og målene;
b) rollene og ansvaret til gruppen som skal iverksette planen;
c) tiltak for implementering av løsningene;
d) støtteinformasjon som er nødvendig for å iverksette (inkludert iverksettelseskriterier), drive, koordinere og kommunisere gruppens tiltak;
e) interne og eksterne gjensidige avhengigheter;
f) ressurskravene;
g) rapporteringskravene;
h) normaliseringsprosess.

Hver plan skal kunne brukes og være tilgjengelig der og når det er nødvendig.

8.4.5 Gjenopptakelse

Organisasjonen skal ha dokumenterte prosesser for å gjenopprette og gjenoppta virksomhetsaktiviteter fra de midlertidige tiltakene som er tatt i bruk under og etter en forstyrrelse.

8.5 Øvelsesprogram

Organisasjonen skal implementere og vedlikeholde et program for øvelse og trening for å måle virkningen av strategiene og løsningene for virksomhetskontinuitet over tid.

Organisasjonen skal utføre øvelser og trening som:

a) er i overensstemmelse med målene for virksomhetskontinuitet;
b) er basert på passende scenarier som er godt planlagte og har tydelig definert hensikt og mål;
c) utvikler gruppearbeid, kompetanse, tillit og kunnskap for de som har roller å utføre i forbindelse med forstyrrelser;
d) hvis de utføres over tid, måler organisasjonens strategier og løsninger for virksomhetskontinuitet;
e) produserer rapporter etter øvelser som inneholder resultater, anbefalinger og tiltak for å iverksette forbedringer;
f) gjennomgås i forbindelse med å fremme kontinuerlig forbedring;
g) utføres med planlagte mellomrom og ved betydelige endringer i organisasjonen eller i konteksten den virker i.

Organisasjonen skal handle ut fra resultatene fra øvelsene og treningen for å iverksette endringer og forbedringer.

NS-EN ISO 22301:2019

8.6 Evaluering av virksomhetens kontinuitetsdokumentasjon og -evne

Organisasjonen skal:

a) evaluere egnetheten, tilstrekkeligheten og effektiviteten til organisasjonens analyse av virksomhetsmessige virkninger, risikovurdering, strategier, løsninger, planer og prosedyrer;
b) foreta evalueringer basert på gjennomgåelser, analyser, øvelser, trening, rapporter etter øvelser og evalueringer av prestasjon;
c) foreta evalueringer av relevante partnere og leverandørers evne til virksomhetskontinuitet;
d) evaluere samsvar med gjeldende juridiske og forskriftsmessige krav, beste praksis i bransjen og samsvar med sin egen policy og sine egne mål for virksomhetskontinuitet;
e) oppdatere dokumentasjon og prosedyrer i rett tid.

Disse evalueringene skal utføres med planlagte mellomrom, etter en episode eller iverksettelse, og når det oppstår betydelige endringer.

9 Evaluering av prestasjon

9.1 Overvåking, måling, analyse og evaluering

Organisasjonen skal bestemme:

a) hva som er nødvendig å overvåke og måle;
b) metoder for overvåking, måling, analyse og evaluering, hvis det er aktuelt, for å sikre gyldige resultater;
c) når og av hvem overvåking og måling skal utføres;
d) når resultatene fra overvåking og måling skal analyseres og evalueres, og av hvem.

Organisasjonen skal oppbevare relevant dokumentert informasjon som bevis på resultatene.

Organisasjonen skal evaluere prestasjonen til og virkningen av BCMS.

9.2 Internrevisjon

9.2.1 Generelt

Organisasjonen skal gjennomføre internrevisjoner med planlagte mellomrom for å bestemme om BCMS:

a) er i samsvar med:

   1) organisasjonens egne krav til sitt BCMS;
   2) kravene i dette dokumentet;

b) implementeres og vedlikeholdes på en hensiktsmessig måte.

9.2.2 Revisjonsprogram(mer)

Organisasjonen skal:

NS-EN ISO 22301:2019

a) planlegge, etablere, implementere og vedlikeholde et eller flere revisjonsprogrammer, inklusive hyppighet, metoder, ansvar, krav til planlegging og rapportering, som skal ta hensyn til betydningen av de aktuelle prosessene i forbindelse med og resultatene av tidligere revisjoner;
b) definere revisjonskriterier og omfang for hver revisjon;
c) velge revisorer og gjennomføre revisjoner som skal sikre objektivitet og upartiskhet i revisjonsprosessen;
d) sikre at resultatene av revisjonene rapporteres til relevant ledelse;
e) oppbevare dokumentert informasjon som bevis på implementering av revisjonsprogrammet/-programmene og revisjonsresultatene;
f) sikre at eventuelle korrigerende tiltak iverksettes uten unødig forsinkelse, for å eliminere avvik som er avdekket, og årsakene til disse;
g) sikre at aktiviteter for oppfølging av revisjon skal omfatte verifisering av de iverksatte tiltakene og rapportering av resultatene av verifiseringen.

9.3 Ledelsens gjennomgåelse

9.3.1 Generelt

Den øverste ledelsen skal gjennomgå organisasjonens BCMS med planlagte mellomrom for å sikre at det fortsetter å være egnet, tilstrekkelig og virkningsfullt.

9.3.2 Inngangsfaktorer til ledelsens gjennomgåelse

Ledelsens gjennomgåelse skal omfatte vurdering av:

a) statusen for tiltak fra tidligere gjennomgåelser som ledelsen har foretatt;
b) endringer i eksterne og interne forhold som er relevante for BCMS;
c) informasjon om prestasjonen til BCMS, inkludert trender innenfor:

   1) avvik og korrigerende tiltak;
   2) resultater av evaluering av overvåking og måling;
   3) revisjonsresultater;

d) tilbakemeldinger fra interesseparter;
e) behovet for endringer i BCMS, inkludert policyen og målene;
f) prosedyrene og ressursene som kan brukes i organisasjonen for å forbedre prestasjonen til og virkningen av BCMS;
g) informasjon fra analysen av virksomhetsmessige virkninger og risikovurderingen;
h) resultat av evalueringen av dokumentasjon av og evne til virksomhetskontinuitet (se 8.6);
i) risikoer eller forhold som ikke er dekket tilstrekkelig i tidligere risikovurderinger;
j) lærdom og tiltak som følger av nestenuhell og forstyrrelser;
k) muligheter for kontinuerlig forbedring.

9.3.3 Utgangsfaktorer fra ledelsens gjennomgåelse

9.3.3.1 Resultatene av ledelsens gjennomgåelse skal omfatte beslutninger om muligheter for kontinuerlig forbedring og ethvert behov for endringer i BCMS for å forbedre effektiviteten og virkningen, inkludert følgende:

a) variasjoner i omfanget til BCMS;
b) oppdatering av analysen av virksomhetsmessige virkninger, strategiene og løsningene for virksomhetskontinuitet og planene for virksomhetskontinuitet;

NS-EN ISO 22301:2019

c) endring av prosedyrene og kontrollene for å respondere på interne eller eksterne forhold som kan påvirke BCMS;
d) hvordan virkningen av kontrolltiltakene skal måles.

9.3.3.2 Organisasjonen skal oppbevare dokumentert informasjon som bevis på resultatene fra ledelsens gjennomgåelse. Den skal:

a) kommunisere resultatene fra ledelsens gjennomgåelse til relevante interesseparter;
b) iverksette hensiktsmessige tiltak knyttet til disse resultatene.

10 Forbedring

10.1 Avvik og korrigerende tiltak

10.1.1 Organisasjonen skal bestemme muligheter for forbedring og implementere nødvendige tiltak for å oppnå de tilsiktede resultatene av BCMS.

10.1.2 Når det oppstår avvik, skal organisasjonen:

a) reagere på avviket og, hvis aktuelt:

   1) treffe tiltak for å styre og korrigere det;
   2) håndtere konsekvensene;

b) evaluere behovet for tiltak for å eliminere årsaken(e) til avviket, slik at det ikke gjentar seg eller oppstår et annet sted, ved å:

   1) granske avviket;
   2) bestemme årsakene til avviket;
   3) bestemme om lignende avvik finnes eller kan tenkes å oppstå;

c) iverksette eventuelle nødvendige tiltak;
d) gjennomgå virkningen av eventuelle korrigerende tiltak som er iverksatt;
e) foreta endringer i BCMS, om nødvendig.

Korrigerende tiltak skal være hensiktsmessige med tanke på virkningene av de avdekkede avvikene.

10.1.3 Organisasjonen skal oppbevare dokumentert informasjon som bevis på:

a) avvikenes art og eventuelle tiltak som blir truffet som følge av dem;

b) resultatene av eventuelle korrigerende tiltak.

10.2 Kontinuerlig forbedring

Organisasjonen skal kontinuerlig forbedre egnetheten, tilstrekkeligheten og virkningen av BCMS, basert på kvalitative og kvantitative tiltak.

Organisasjonen skal vurdere resultatene av analyse og evaluering, samt utgangsfaktorene fra ledelsens gjennomgåelse, for å bestemme om det finnes behov eller muligheter, knyttet til virksomheten eller til BCMS, som det skal tas hensyn til som et ledd i kontinuerlig forbedring.

NS-EN ISO 22301:2019

MERKNAD Organisasjonen kan bruke prosessene i BCMS, som lederskap, planlegging og prestasjonsevaluering, til å oppnå forbedring.

NS-EN ISO 22301:2019

Litteratur

[1] NS-EN ISO 9001, *Ledelsessystemer for kvalitet — Krav*
[2] NS-EN ISO 14001, *Ledelsessystemer for miljø — Spesifikasjon med veiledning*
[3] NS-EN ISO 19001, *Retningslinjer for revisjon av ledelsessystemer*
[4] ISO/IEC/TS 17021-6, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems*
[5] NS-ISO/IEC 20000-1, *Informasjonsteknologi — Tjenesteledelse — Del 1: Krav til ledelsessystemer for tjeneste*
[6] NS-EN ISO 22313, *Samfunnssikkerhet — Systemer for kontinuitetsplanlegging — Veiledning*
[7] ISO 22316, *Security and resilience — Organizational resilience — Principles and attributes*
[8] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
[9] ISO/TS 22318, *Societal security — Business continuity management systems — Guidelines for supply chain continuity*
[10] SN-ISO/TS 22330, *Sikkerhet og resiliens — Ledelsessystem for forretningskontinuitet — Retningslinjer for omsorgsbevisst forretningskontinuitet*
[11] SN-ISO/TS 22331, *Sikkerhet og resiliens — Ledelsessystem for forretningskontinuitet — Retningslinjer for å velge strategi for forretningskontinuitet*
[12] NS-EN ISO/IEC 27001, *Informasjonsteknologi — Sikringsteknikker — Ledelsessystemer for informasjonssikkerhet — Krav*
[13] NS-ISO/IEC 27031, *Informasjonsteknologi — Sikringsteknikker — Retningslinjer for informasjons- og kommunikasjonsteknologiberedskap for forretningskontinuitet*
[14] ISO 28000, *Specification for security management systems for the supply chain*
[15] NS-ISO 31000, *Risikostyring — Retningslinjer*
[16] NS-ISO/IEC 31010, *Risikostyring — Metoder for risikovurdering*
[17] SN-ISO Guide 73, *Risikostyring — Terminologi*

- 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