Innspill revidering av begrepsliste

Formålet med begrepslisten er at det skal være et praktisk verktøy for rapporteringsansvarlige og ansatte som skal fylle ut skjemaer og rapporter. Det er avgjørende at de som fyller ut skjema eller rapporterer angående internkontroll er kjent med betydningen av begrepene som blir brukt.

Begrepslisten er delt i tre kategorier, selve begrepet, en definisjon av begrepet, og konkrete eksempler som kan være til hjelp for å forstå hvilken kontekst man skal forstå definisjonen i.

Helhetlig internkontroll ved UiB - Begreper

Begrep	**Beskrivelse/definisjon**	**Eksempler**
Andrelinje	Linjeledere ved de fellesadministrative avdelingene har ansvar for å rådgi, støtte og påse at internkontrollen følges innenfor sine fagområder eller hovedprosesser. Andre benevnelser er Forvaltningsansvarlig, Prosessansvarlig o.l.. for det internkontrollsystemet enhetene må forholde seg til.	• Eksempelvis er HR-avdelingen ansvarlig for prosedyrer og rammer for HMS-internkontrollen. • IT-avdelingen er ansvarlig for forvaltning av overordnede rutiner rundt informasjonssikkerhet og personvern for UiB. • Økonomiavdelingen er ansvarlig for overordnede rutiner for å følge anskaffelsesregelverket og økonomiregelverket forøvrig.
Avvik	Et avvik oppstår når det foreligger en uønsket hendelse / forhold som ikke er i samsvar med myndighetskrav eller interne regler.	• Eksempelvis forhold som har ført til eller kan føre til skade på mennesker, miljø og verdier. • Et annet eksempel kan være dersom det har kommet personopplysninger på avveie fordi man ikke hadde kontroll med tilgangsstyring (brudd på informasjonssikkerheten og brudd på personopplysningssikkerheten)
Ansvar	Ansvar er en forpliktelse til å stå til rette for, gjøre rede for eller bære utgiftene for noe. En skiller mellom ansvar og oppgaver.	Ansvaret for internkontroll hviler på en enhet og en linjeleder. Oppgavene knyttet til internkontroll vil være spredt på flere personer og enheter.

		• Linjelederne ved grunnenhetene (fakultetene, avdelingene og instituttene/sentrene) har ansvar for å gjennomføre og etterleve etablert internkontroll innenfor eget ansvarsområde (førstelinje). • De fellesadministrative avdelingene har i tillegg ansvar for å rådgi, støtte og påse internkontrollen innenfor sine fagområder/hovedprosesser (andrelinje).
Førstelinje	Direkte ansvar for å gjennomføre og etterleve internkontroll innenfor sitt ansvarsområde (gjennomføringsansvarlig). Dette inkluderer linjeledere ved fakulteter, avdelinger og institutter/sentre. De har ansvar for å sikre at internkontrollen er implementert og følges opp i deres respektive enheter.	Linjeleder er ansvarlig for å følge og gjennomføre de rutinene gitt av andrelinje, eksempelvis årlig HMS-rapportering, eller verdikartlegging av informasjonssystemer.
Helhetlig internkontroll	Den samlede oversikten over virksomhetens overordnede aktiviteter. Å systematisere de overordnede aktivitetene for å sikre at universitetet oppnår sine mål på en effektiv måte, overholder lover og regler, og gjennomfører nødvendige tiltak.	Eksempelvis gjennom å sørge for at alle arbeider mot felles mål og bruker ressursene på en effektiv måte. For eksempel innen universell utforming eller enhetene sine egne virksomhetskritiske aktiviteter, BoA-, økonomi- eller HR-oppfølging
Informasjonssikkerhet	Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet • Konfidensialitet: Sikre at informasjonen og systemer kun er tilgjengelig for de som skal ha tilgang. • Integritet: Sikre at informasjonen er korrekt, oppdatert og fullstendig, og hindre uønsket endring, sletting eller manipulering. • Tilgjengelighet: Sikre at brukere har tilgang til informasjon ved behov innenfor de tilgjengelighetskrav som er satt. • Robusthet: At organisasjonen og systemene er motstandsdyktige, og at organisasjonen evner å gjenopprette normaltilstand ved hendelser	• Eksempelvis gjennom å sikre informasjon ved enhetene, og følge de rutiner og prosedyrer gitt av IT-avdelingen, for å sikre informasjonssikkerheten ved UiB. • Andre eksempler er kontroll med tilgangsstyring, trygg og sikker drift og god forvaltning av informasjonen vi behandler (holde den oppdatert og korrekt).

Informasjonseier	En informasjonseier er den øverste lederen på en enhet som har et overordnet ansvar for en spesifikk informasjonsressurs. Dette inkluderer å definere verdien av informasjonen og sikre dens konfidensialitet, integritet og tilgjengelighet (informasjonssikkerhet). Informasjonseieren er ansvarlig for å sette rammer, prioritere sikkerhetstiltak, og sikre at informasjonen brukes og behandles på en sikker og ansvarlig måte (dvs. styre risiko) i tråd med UiBs retningslinjer.	
Informasjonsverdier	Alle typer data, opplysninger og dataressurser (IT-utstyr, applikasjoner, systemer, datanettverk m.m) som har betydning for UiB sin virksomhet.	• Eksempelvis personopplysninger UiB behandler om studenter og ansatte. • Eksempelvis viktige forskningsdata som enten er personopplysninger av særlig kategori, eller øvrig informasjon som er kritisk i forskningsprosjekter.
Internkontroll	Systematiske sett av aktiviteter som skal sikre at virksomhetenes aktiviteter planlegges, organiseres, utføres, sikres og vedlikeholdes i samsvar med: • Overholdelse av krav fastsatt i eller i medhold av lovgivningen og internt regelverk • Målrettet og effektiv drift • Pålitelig rapportering og forvaltning • Gjennomføring av vedtak og tiltak	• Eksempelvis Helse-, miljø- og sikkerhetslovgivningen, deriblant Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften) og UiBs Retningslinje for systematisk HMS-arbeid • Styringssystem for informasjonssikkerhet og personvern • Styringssystem for bygg og verdier
Kontrollaktiviteter	Kontrollaktivitet inneholder også den faktiske gjennomføringen; ofte benevnt som etterlevelseskontroll.	Eksempelvis, gjennomgang og utfylling av årsrapporteringsskjema knyttet til informasjonssikkerhet eller HMS.
Kvalitetssystem	Et kvalitetssystem er også del av internkontrollen; dette er en struktur som sikrer tydelighet rundt interne prosedyrer, rutiner, oppgaver og ansvarsforhold,	Eksempelvis Kvalitetssystemet for utdanning ved UiB

	herunder avvikshåndtering for kontinuerlig forbedring. Et kvalitetssystem skal styrke internkontrollen og risikostyringen. Kan være et teknisk system, men kan også være samling av skriftlige rutiner, prosedyrer mv., eksempelvis på intranett eller i fysiske permer.	
Linjeleder	Øverste leder ved avdeling/fakultet/institutt/senter	Innen HMS: Universitetsdirektør, dekan, fakultets-/avdelingsdirektør og instituttleder, eller tilsvarende som har det overordnete HMS-ansvaret ved enheten.
Myndighetskartet	UiBs oversikt over intern fordeling av myndighet og fullmakter, samt regler for delegasjon ved institusjonen.	Myndighetskart UiB
Mål	Ønsket sluttresultat eller en framtidig tilstand som en enhet har som intensjon å oppnå.	
Målsetting	En intensjon om å nå ett mål, som er klart formulert.	
Objektverdier	Fysiske objekter, gjenstander og/eller samlinger, som hvis utsatt for en uønsket hendelse, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av dem.	Uønsket hendelse kan være brannskade, vannskade, innbrudd, hærverk, tyveri, etc.
Prosedyrer	Interne veiledninger, rutinebeskrivelser og prosessbeskrivelser. Dette er dokumenter som beskriver hvordan oppgaver løses og kan om nødvendig inneholde sjekklister.	Eksempel: Prosedyre for avhending av problemavfall.
Prosesser	Prosesser består typisk av et sett med aktiviteter som utføres for å oppnå et resultat eller virkning. Til prosessaktiviteter kan det være rutiner som definerer hvordan aktiviteter skal gjennomføres.	Eksempler på prosess kan være anskaffelse av et nytt IT-system, rekruttering av nye medarbeidere, opptak av studenter o.l.
Regelsamlingen	Samling av relevante lover, forskrifter og retningslinjer for UiB sin virksomhet.	Regelsamlingen for UiB
Retningslinjer	Dette er interne dokumenter som angir rolle, ansvar, og oppgaver, og som kan være vedtatt på ulike nivåer i organisasjonen.	Et eksempel på dette er overordnede retningslinjer for behandling av personopplysninger ved UiB, eller f.eks. UiB sine HMS-retningslinjer.
Risiko	Risiko er forhold eller hendelser som kan inntreffe, og har eller kan ha uønskede eller negative konsekvenser.	

	Konsekvensene kan være knyttet til for eksempel liv og helse, miljø, økonomiske verdier eller målsetninger.	
Risikostyring	Er aktiviteter for å håndtere og balansere risiko og kontrolltiltak for å nå mål og for å forhindre uønskede hendelser. Risikostyring binder mål og internkontroll sammen.	Risikostyring i staten | DFØ
Risikovurdering	I en risikovurdering forsøker man få innsikt i uønskede hendelser som kan oppstå, hvorfor de kan oppstå, hva konsekvensene kan være og sannsynligheten for at de oppstår.	• Eksempelvis HMS-risikovurdering og Sikkerjobbanalyse (SJA) (Typer risikovurderinger) • Et annet eksempel kan være risikovurderinger man gjør før implementering av et nytt IT-system eller en ny IT tjeneste.
Risiko- og sårbarhetsanalyse (ROS)	ROS er en type vurdering/analyse der sårbarhet er spesielt vektlagt.	Ved UiB benyttes ROS hovedsakelig i forbindelse med overordnede hendelser knyttet til sikkerhet og beredskap (Typer risikovurderinger), samt IT-tjenester, og i forbindelse med prosjekter.
Skallsikring	Sikring av byggets ytterste elementer; vegger, vinduer, dører (inkludert tekniske rom innside og utside, og i enkelte tilfeller rom rett på innsiden av bygget der inngangsparti er felles for flere brukere)	
Styringsdokumenter	Dokumenter som angir prinsipielle og overordnede rammer for virksomheten.	
Styringsprinsipper	Skal sikre en effektiv og resultatorientert virksomhet.	Eksempel på styringsprinsipp er mål- og resultatstyring.
Systemeier	Den øverste lederen ved en enhet som er ansvarlig for et IT-system eller en IT-tjeneste. Alle IT-systemer ved UiB skal ha en definert systemeier. Systemeierrollen har sitt ansvar definert i styringssystemet for informasjonssikkerhet og personvern	• Eksempelvis er Felles studentsystem (FS) tillagt avdelingsdirektør for studieavdelingen som systemeier. • Et annet eksempel er SAFE som er tillagt IT-direktør som systemeier.
Sårbarhet	Sårbarhet er svakheter som kan utnyttes til å forårsake skade.	• Et eksempel på sårbarhet kan være at et IT-system ikke har blitt oppdatert med de siste publiserte sikkerhetsoppdateringene som kommer fra en leverandør. Dette gjør at det finnes sikkerhetshull

		som kan utnyttes og gi uønskede konsekvenser for UiB. • Et annet eksempel er i situasjoner hvor man har store verdier som eksempelvis kan befinne seg i virksomheten og som kan ha dårlige sikringstiltak (eksempelvis manglende tilgangskontroll) i forhold til risikoen for at noe skal skje. Da eksisterer det en sårbarhet som kan utnyttes og føre til uønskede hendelser med uønskede konsekvenser. • Dårlig eller manglende tilgangsstyring i IT systemer er også et eksempel på sårbarhet. Dersom systemet behandler viktige verdier, kan disse havne på avveie eller noen som ikke skulle ha tilgang til disse kunne fått tilgang.
Tiltak	Med et tiltak menes en handling som reduserer gjenværende risiko.	• Tiltak kan omfatte alt fra endring av utførelsesmetoder, etablering av nye rutiner, korrigering av feil, til forbedring av eksisterende prosesser. Formålet er å sikre at virksomheten opererer effektivt, etterlever regelverket, og kontinuerlig forbedrer seg. • Tiltak kan være tekniske/fysiske eller organisatoriske. Et eksempel på fysiske tiltak kan være beskyttelse av lokaler i form av adgangskontroll og alarmsystem. Et eksempel på et organisatorisk tiltak er opplæring av ansatte, gjester og studenter.
Verdi	Virksomhetskritiske elementer ved UiB	Informasjonsverdier, immaterielle og materielle verdier for virksomheten.
Verdikartlegging	Identifisere de mest kritiske verdiene ved UiB	Verdikartlegging utføres på alle sikkerhetsområder ved UiB og dokumenteres. • Et eksempel på verdikartlegging er å skaffe oversikt over de mest kritiske forskningsdataene som behandles ved UiB.

		• Et annet eksempel er å skaffe oversikt over alt datautstyr som er verdifullt og hvor det kan være kritisk dersom noe skjer med dette.
Verdivurdering	Klassifisere og vurdere de identifiserte verdiene ved UiB	Når man har skaffet oversikt over de mest verdifulle verdiene i verdikartleggingen, utføres en verdivurdering. Da settes det en konkret verdi, samt at det gjøres en risikovurdering for å se på om verdiene er godt nok sikret i forhold til hva de kan bli utsatt for. • Eksempelvis er en del gjenstander på en enhet høyt verdsatt og krever sikringstiltak i forhold til å sikre seg mot innbrudd o.l. • Et annet eksempel er data som behandles i et forskningsprosjekt. Dersom det behandles store verdier som får store konsekvenser om det skjer noe med disse, må ha strenge sikringstiltak for å kunne ha et akseptabelt risikonivå.
Virksomhetsstyring	Virksomhetsstyring betegnes som den totale styringen av virksomheten. Denne skal sikre UiBs oppnåelse av strategiske, finansielle og operasjonelle mål, overholdelse av lover og regler, pålitelig rapportering, gjennomføring av politiske vedtak og tilstrekkelig håndtering av risiko.	Virksomhetsstyring kan gjennomføres vha. helhetlig internkontroll, langtidsbudsjettering, og UiBs strategi.

23.09.25/Runa Jakhelln, Arild Shandiz Nessen, Peter Arnold Ståhl Woldseth, Monica Nielsen Øen