Oppfyller du krav og forventninger til sikring/security?

- **Kjenner du på utfordringen med nye og stadig mer omfattende krav til virksomheten din rundt sikring og security?**
- **Er det vanskelig å få oversikt over hva som kreves av deg – eller hvordan du egentlig ligger an?**
- **Har du leverandører som kanskje håndterer eller utgjør en risiko for deg innen sikring/security – men har ikke kapasitet til å følge dem opp?**

Proactima kan effektivt og kompetent hjelpe deg med dette!

I Proactima har vi en unik kombinasjon av kompetanse og erfaring innen revisjoner, tilsyn og oppfølginger, og fagkompetanse innen sikring og security. Vi kan standarder og regelverk, og har betydelig erfaring med å følge opp kontraktskrav, systemkrav og sikkerhetsforskrifter. Proactima har vært en aktiv bidragsyter i arbeidet med å oppdatere ISO 19011 – retningslinjer for å revidere styringssystemer som blant annet de nye forskriftene til sikkerhetsloven viser til.

Vi har en risikobasert tilnærming til revisjoner og tilsyn. Det vil si at revisjonene skal bidra til at negativ risiko reduseres mest mulig – med lavest mulig ressursbruk. Vi har utarbeidet og fulgt opp et stort antall sikringssystemer, gjennomført leverandørtilsyn og interne revisjoner, og kan tilby blant annet:

- En vurdering av tilstanden i virksomheten din med tanke på å oppfylle eksisterende og kommende krav til sikring
- Anbefalinger av tiltak for å oppfylle krav mest mulig effektivt
- Utarbeidelse av risikobaserte revisjonsprogrammer for interne revisjoner og/eller oppfølging av leverandører
- Gjennomføring av leverandørrevisjoner mot kontrakt og andre avtalte krav
- Gjennomføring av eller støtte til interne revisjoner
- Opplæring

Fagunderlag

Proactima har svært omfattende kompetanse og erfaring når det gjelder etablering og gjennomføring av både internrevisjon og oppfølging av og tilsyn/revisjon av leverandører. Flere av våre konsulenter er sertifiserte revisjonsledere, også for ISO 27001. Proactima har aktivt deltatt i arbeidet med å revidere ISO 19011 – retningslinjene for revisjon av styringssystemer – som kom som revidert norsk standard høsten 2018. ISO 19011 vises det blant annet til i sikkerhetslovens forskrifter, og NSMs veileder for sikkerhetsrevisjon er basert på ISO 19011.

Proactima bruker en risikobasert tilnærming ved revisjoner og tilsyn. Det vil si at revisjonene skal bidra til at negativ risiko reduseres mest mulig – med lavest mulig ressursbruk. Dette påvirker både hva som bør revideres – og hvor ofte, og hva du bør fokusere på i den enkelte revisjon. Med andre ord både hvordan du utformer virksomhetens revisjonsprogram – og hvordan du utfører og følger opp den enkelte revisjon.

Vi er opptatte av revisjonen skal gi mest mulig verdi til virksomheten, som et viktig verktøy i risikostyringen. Kartlegging og vurdering av risiko i virksomheten, vil gi god input til hvordan revisjonsprogrammet skal bygges opp for å tilføre verdi. Revisjoner bør ikke nødvendigvis gjennomføres der man tror det er sannsynlig at noe vil gå galt. Dersom kunnskap om mangler

allerede er der – er ressursene bedre utnyttet ved å etablere tiltak for å utbedre feil som er kjente. Revisjonen bør imidlertid ofte fokusere på å undersøke områder der **risikoen er høy.** Med andre ord områder som er kritiske for virksomhetens verdier og prosesser/leveranser. I dette ligger at revisjonsprogrammet bør dekke både interne og eksterne (leverandør)-revisjoner. Risikoen vår kan ofte bli høyere når aktiviteter settes ut til andre – i alle fall om den ikke følges godt opp.

Revisjonen er heller ikke bare et verktøy for å vurdere samsvar med krav, kontrakter eller forventninger. Brukt på en god måte kan revisjonsverktøyet gi betydelig innsikt i om tiltak, systemer og rutiner faktisk fungerer etter hensikten og om de er tilstrekkelige og effektive. Det er også et godt verktøy for å se hvorvidt kultur, kompetanse og struktur fungerer hensiktsmessig sammen slik at virksomheten oppnår god styring (se for øvrig også vår beskrivelse av leveranseområdene informasjonssikkerhet og sikkerhetsstyring). Internrevisjonen blir slik et veldig viktig verktøy med tanke på å skaffe ledelsen beslutningsgrunnlag. Samtidig kan revisjonen gi viktig informasjon tilbake til oppdatering av risikobildet – gjennom at det avdekkes hvorvidt barrierer og tiltak fungerer som forutsatt i risikovurderingen.

Proactimas konsulenter kan bidra i prioriteringer og valg gjennom å kombinere vår kunnskap med kundens erfaringer med egne systemer og utfordringer.

Vi har omfattende erfaring med å utarbeide og følge opp **tilsyns- og revisjonsprogrammer**. Våre konsulenter er erfarne både som tilsynsledere hos myndighetene, ansvarlige for internrevisjon i virksomheter og gjennom oppfølging av leverandører. Vi kan bistå med å:

- Etablere (intern-)revisjon i virksomheten
- Utarbeide risikobaserte kostnadseffektive revisjonsprogrammer
- Utarbeide prosedyrer, maler og andre verktøy
- Utvikle og gjennomføre kurs og opplæring.

For **gjennomføring** av revisjoner og andre samsvarsvurderinger kan vi både gjennomføre opplæring og kurs, delta som revisjonsledere og/eller fagrevisorer, og levere komplette vurderinger og revisjoner både internt og av leverandører.

I **oppfølgingsarbeidet** kan vi både anbefale og støtte gjennomføring av konkrete forbedringstiltak og gjennomføre verifiseringsaktiviteter i etterkant av revisjoner og tilsyn.

Vi har spesifikk kompetanse på sikkerhetsrevisjon både med basis i sikkerhetsloven og andre reguleringer og krav, og har også utarbeidet Statoils tilsynsmetodikk for oppfølging av leverandører med sikringsavtaler, samt der gjennomført rundt 100 tilsyn/revisjoner av leverandørene.