DNV·GL

IKT-SIKKERHET – ROBUSTHET I PETROLEUMSSEKTOREN

Regelverk og tilsynsmetodikk

Petroleumstilsynet

Rapport nr.: 2019-082, Rev. 0
Dato: 2020-02-24

Prosjekt navn:	IKT-sikkerhet – Robusthet i petroleumssektoren	DNV GL AS
Rapport tittel:	Regelverk og tilsynsmetodikk	Digital solutions
Kunde:	Petroleumstilsynet, P.O. Box 599	Postboks 300
	4003 Stavanger	1322 Høvik
	Norway	Norway
Kontaktperson:	Arne Halvor Embergsrud	
Dato:	2020-02-24	
Prosjekt nr.:	101572712	
Organisation unit:	Cyber Security Services	
Rapport nr.:	2019-0824 Rev. B	
Dokument nr.:		

Kontrakt for leveranse av denne rapport:

Avtale om IKT sikkerhet – Robusthet i petroleumssektoren

Hensikt: Hovedmål med prosjektet er å innhente kunnskap om risiko, trusler, sårbarheter samt viktigheten av IKT-sikkerhet for de industrielle systemer. Denne rapporten tar for seg regelverk og tilsynsmetodikk for sikkerhet i industrielle IKT-systemer.

Utarbeidet av:

Kenneth Kvinnesland
Senior Principal Consultant

Håvard Grindheim
Principal Consultant

Sindre Trandum
Consultant

Rolf Lervik
Senior Principal Consultant

Verifisert av:

Boye Trantum
Associate Director

Godkjent av:

Trond Solberg
Head of Section, Cyber Security Services

DNV GL Distribution:

☒ Unrestricted distribution (internal and external)
☐ Unrestricted distribution within DNV GL
☐ Limited distribution within DNV GL after 3 years
☐ No distribution (confidential)
☐ Secret

Keywords:
Cybersecurity, Digitalisation, Oil & Gas, Regelverk, Tilsyn

Rev. Nr.	Dato	Formål	Utarbeidet av	Verifisert av	Godkjent av
A	2019-11-29	Utkast sendt PTIL for gjennomgang	KKV, HAVGRI, SINTRA, RLER	BOTRA	TROSOL
0	2020-02-24	Oppdatert etter PTILs gjennomgang	KKV, SINTRA	RLER	TROSOL

INNHOLD

1 SAMMENDRAG

Denne rapporten gir en vurdering av om Ptils regelverk, slik det fremstår i dag, er hensiktsmessig i forhold til temaet IKT-sikkerhet og trusselbildet innenfor dette området. Videre vurderes det om metodikken Ptil anvender for å utføre tilsyn med IKT-sikkerheten er hensiktsmessig.

Ptils regelverk er i hovedsak et funksjonsbasert regelverk, men med noen preskriptive elementer. Dette er en målbasert tilnærming som sier hva som skal oppnås men i liten grad hvordan. Ptil har utarbeidet egne veiledninger til forskriftene som viser hvordan bestemmelser i en forskrift kan oppfylles. Veiledningene viser på enkelte områder til industristandarder, som en anbefalt måte å oppfylle forskriftens krav på. Veiledningene til forskriftene er ikke rettslig bindende, og aktørene kan derfor velge andre løsninger. Hvis aktøren velger andre løsninger, som for eksempel andre standarder eller selskapsspesifikke løsninger, må de kunne dokumentere at den valgte løsningen er minst like god som, eller bedre enn, den anbefalte.

Denne rapporten drøfter fordeler og ulemper med funksjonsbasert versus preskriptivt regelverk. Et særlig viktig moment er at et funksjonsbasert regelverk krever at det er tillitt mellom Ptil og de forskjellige aktørene. Ptil gir aktørene frihet under ansvar, og modellen fungerer bare så lenge aktørene vil ta dette ansvaret og evner å gjøre det. Et funksjonsbasert regelverk kreve større faglig kunnskap både hos dem som skal etterleve regelverket og blant dem som skal håndheve det, enn et preskriptivt regelverk. Intervjuer med aktører i bransjen, utført i dette prosjektet, indikerer at arbeidet med å forbedre IKT-sikkerheten prioriteres, noe som igjen indikerer at et funksjonsbasert regelverk kan fungere etter intensjon også for beskyttelse mot IKT-hendelser.

Ptils regelverk og tilsynsvirksomhet fokuserer først og fremst på sikkerhet for menneskers liv og helse samt miljø, og ikke på at systemene skal være tilgjengelige for produksjon. Den overordnede sikkerhetsfilosofien ved alvorlige uønskede hendelser, er å gå til sikker tilstand, noe som i mange tilfeller betyr å stoppe produksjon og prosessering. En større driftsstans forårsaket av en IKT-hendelse vil kunne få store økonomiske konsekvenser, og i noen tilfeller også følgekonsekvenser for gasskjøpere, men DNV GL har ikke tatt stilling til om Ptil sitt overordnede mandat bør endres som en konsekvens av dette. Rapporten antar derfor at Ptil fortsett vil ha samme fokus i sitt arbeide.

Villede handlinger er bare en av truslene som kan true integriteten og tilgjengelighet til kritiske systemer som brukes til kontroll og overvåking. Ptils regelverk adresserer denne problemstillingen gjennom en barrierefilosofi basert på bruk av uavhengige sikkerhetssystemer. Regelverkets veiledninger refererer til norske og internasjonale standarder hvor det stilles strenge krav til analyse, utvikling, verifikasjon, validering og operasjon av slike systemer. DNV GLs samlede vurdering er at denne delen av regelverket fungerer godt med tanke på å hindre at tekniske problemer i kritiske systemer skal føre til ulykker, men at regelverket trengs å styrkes tatt i betraktning det totale trusselbildet knyttet til IKT-sikkerhet. I rapporten har DNV GL foreslått oppdateringer for å få et mer tydelig regelverk når det gjelder IKT-sikkerhet, herunder utarbeiding av en egen veileder til relevante paragrafer.

Ptil fører tilsyn av IKT-sikkerhet på et stort omfang installasjoner innen olje- og gassnæringen. Alle aktører i næringen, både operatører, entreprenører og redere i virksomheten er omfattet. Arbeidet med IKT-sikkerhet omfatter blant annet: revisjoner og verifikasjoner på innretninger og landanlegg, dialog og møter med næringen, datainnsamling om risiko, ulykker og hendelser, gransking av hendelser, og enkelte tilfeller behandling av samtykkesøknader for nye typer løsninger.

Ptil sin tilsynsmetodikk er basert på anerkjente standarder for revisjon noe som også benyttes av øvrige tilsynsorgan i Norge. Den største forskjellen vi ser mellom tilsynene er at bruken av detaljerte krav og detaljerte veiledere varierer. Dette fører i noe grad til forskjeller i hvor krevende det er å gjennomføre

tilsyn. Et viktig funn er at kapasitet til å utføre tilsyn, og å følge opp etterpå, er begrenset i forhold til mengden av tilsynsobjekter. Dette er ikke spesifikt for Ptil, men er noe vi ser hos de fleste tilsyn i Norge. Et annet funn er at regelverket krever høy og bred kompetanse fra ressursene som skal gjennomføre tilsynet.

Basert på innhentet informasjon og intervju med aktørene i markedet om hvordan Ptil gjennomfører tilsyn for IKT-sikkerhet anbefaler DNV GL et sett med endringer presentert i denne rapporten. Anbefalingene omfatter blant annet av å tydeliggjøre mandat og tilsynskriterier gjennom oppdatering av regelverket, økning av kapasitet for tilsyn, og ta i bruk verktøy som sikrer korrekt håndtering av aktørenes informasjon.

2 ENGLISH SUMMARY

This report provides an assessment of whether PSA's regulations, as of today, are suitable when it comes to protection against cyber security related threats. The methodology used by the PSA when conducting revisions and supervision on cyber security has also been assessed.

The PSA's regulatory framework is function based, but with some prescriptive elements. It has a target-based approach which describes what should be achieved, but to a lesser extent how it should be achieved. The PSA has produced guidelines to the regulations, providing a more in-depth description of the purpose of the regulation. In some areas, the guidelines references industry standards as a recommended way to ensure compliance with the regulations. The guidelines are not mandatory, and each company may select alternative solutions to achieve the level of safety described in the regulations. If they select an alternative approach, they must be able to document that their method is as strong, or better, then the recommended approach from the guidelines.

This report evaluates the pros and cons of function-based regulations compared to more prescriptive regulations. One critical point is that function-based regulations requires a relationship of trust between the PSA and the companies under supervision. The companies are given freedom with responsibility, and the model only works when each player has the motivation and capability to accept that responsibility. A function based regulatory framework requires more detailed domain knowledge from both the supervisory authority and the companies subject to the regulations, compared to a more prescriptive regulatory framework. Interviews with operators indicate that the work to improve cyber security is a priority for them, further indicating that function-based regulations can work as intended for cyber incidents.

The PSA's regulations and supervisory activities mainly focus on safety of life and the environment, and not on the systems availability for production. The overall safety-philosophy for handling of serious unwanted events is to go to a safe state, which in many cases means to shut down the production and the processing. A lengthy stop in production following a cyber security incident can have large economic consequences and may in some cases affect other countries. However, DNV GL has not taken a position on whether the PSA's overall mandate should be changed as a consequence of this. Thus, this report assumes that the PSA will maintain the same focus also in the future.

Malicious actions are just one of the threats which may compromise the integrity and availability of critical systems used for control and surveillance. The PSA's regulations address this problem using a barrier-philosophy based on use of independent safety systems. The guidelines to the regulations refer to both Norwegian and international standards for such safety systems, in which stringent requirements to development, verification, validation, and operation are detailed. DNV GLs overall assessment of the regulations is that it works well in preventing technical problems in critical systems from contributing to major accidents, but that is needs to be strengthened with respect to cyber threats. In the report DNV GL has proposed updates to make the regulations clearer, and also proposed to write a dedicated guideline for the clauses in the regulations considered relevant for cyber security.

The PSA conducts supervision of ICT-security management on a broad selection of installations within the oil & gas industry. All organisations in the industry, including operators and entrepreneurs, are subject to the supervision. The work with ICT-security comprises of: revisions and verifications of installations and onshore facilities, dialog and meetings with the industry, gathering of data on risks, investigation of incidents, and evaluating applications for consent for new types of solutions.

The PSA's methodology for supervision is based on recognized standards for revision also used by other supervisory authorities in Norway. The biggest observed difference between the authorities relates to the

use of detailed requirements and detailed guidelines. This leads to differences in how challenging it is to conduct an audit. One important finding is that the capacity to conduct audits, and to follow up afterwards, is limited compared to the number of objects subjected to supervision. This is not unique for the PSA, but something that is observed for most supervisory authorities in Norway. Another finding is that the current regulations require a high degree of competence from the resources conducting the supervisions.

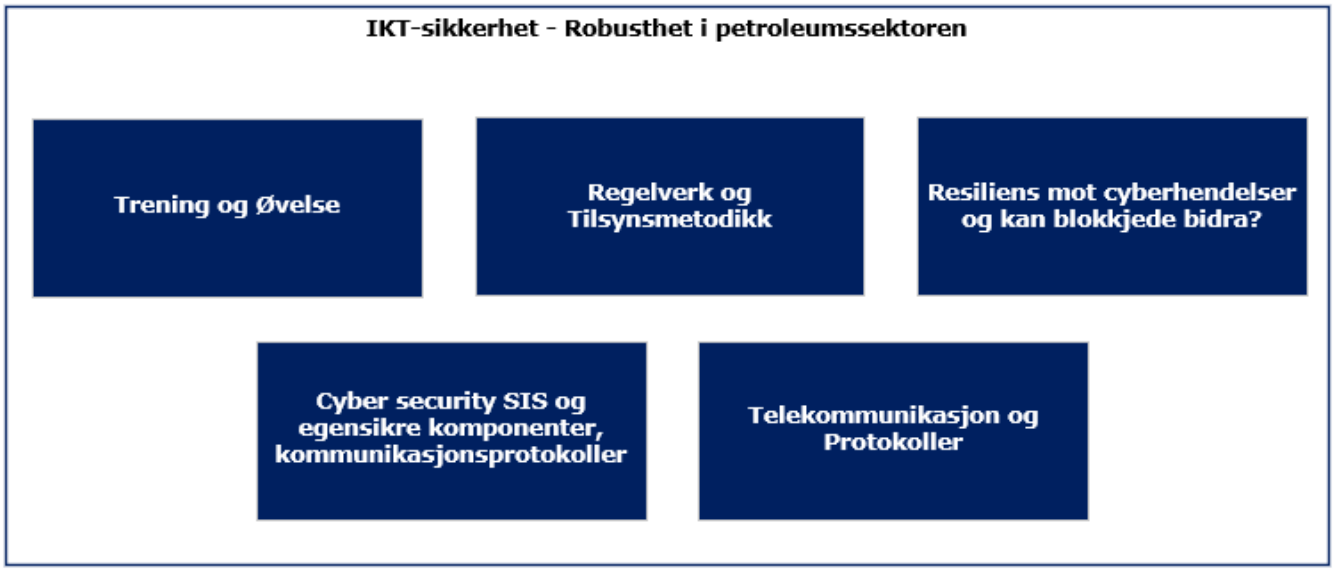
Based on gathered information and interviews with key stakeholders in the industry on how the PSA conducts supervisions for ICT-security, DNV GL recommends a set of changes in this report. The recommendations include clarifying the mandate and criteria for supervision through an update of the regulations, an increase of the capacity for supervision, and the implementation of tools in order to ensure correct handling of collected information.

3 INNLEDNING

3.1 Bakgrunn

Utviklingen av industriell kontroll- og sikkerhetssystemer og tilhørende industriell teknologi har ført til at disse systemene har blitt mer integrerte og dermed også mer komplekse. Tidligere proprietære systemer er nå i ferd med å bli integrert og koblet sammen i et større system både vertikalt og horisontalt. Digitalisering setter krav om mer programvarebaserte løsninger i de fleste segmentene også på instrumentnivå.

Rapporten er utarbeidet i et prosjekt som inneholder flere arbeidspakker og delleveranser, som illustrert i figuren under. Alle arbeidspakker har gjennomført intervjuer og innhentet informasjon fra aktørene i bransjen, samt innhentet erfaringer med tilsyn av IKT-sikkerhet i andre sektorer.



Figur 3-1 Delleveranser i prosjektet

3.2 Hensikt

Hensikten med dette delprosjektet har vært å vurdere om Ptils regelverk, slik det fremstår i dag, er hensiktsmessig i forhold til temaet IKT-sikkerhet og trusselbildet innenfor dette området. Tilsvarende om metodikken Ptil anvender for å utføre tilsyn med IKT-sikkerheten er hensiktsmessig gitt omfang av tilsynsobjekter og trusselbilde.

3.3 Omfang

Rapporten ser på dagens regelverk, forskrifter og veiledninger for sektoren, og vurderer dette mot beste praksis og kjente standarder, som IEC 62443 /15/, NIST Cybersecurity Framework (CSF)/14/, DNVGL-RP-G108 /13/, NVEs Kraftberedskapsforskrift (Kbf) /4/, IADC Cyber Security Committee guidelines /16/, samt NSMs grunnprinsipper for IKT-sikkerhet /11/.

Rapporten omhandler også tilsynsmetodikken som benyttes for å gjennomføre tilsyn og revisjoner mot industrielle IKT-systemer. Tilsynsmyndigheter fra andre sektorer har blitt intervjuet for å se om det er

noen relevante forskjeller i tilnærming og utførelse av tilsyn for IKT-sikkerhet. Relevante deler og funksjoner i IT-systemer er inkludert i den grad disse påvirker OT (operasjonell teknologi).

3.4 Metodikk

For å etablere et bilde av hvordan aktørene ser på dagens status og fremtidige behov har DNV GL i dette delprosjektet utført intervjuer med Ptil og aktørene Vår Energi, Equinor, ConocoPhilips, Norske Shell, Lundin, Aker BP og Maersk som representanter for bransjen. I tillegg er det innhentet informasjon fra leverandører via andre delprosjekter utført innenfor dette oppdraget. Videre har det vært gjennomført intervjuer i kraftbransjen og i luftfartssektoren for å sammenligne med andre bransjer som opererer svært kritiske systemer. I relasjon til dette har det vært gjort en gapanalyse mellom Ptils regelverk og NVEs kraftberedskapsforskrift. DNV GL har også trukket på egne erfaringer med sertifisering av skip og systemer etter det maritime regelverket, sertifisering av styringssystemer i henhold til ISO 9001 /63/, håndheving av standarder knyttet til IKT-sikkerhet f.eks. ISO 27001 /44/, og funksjonell sikkerhet f.eks. IEC 61508 /3/, samt kvalifisering av ny teknologi innenfor områder der eksisterende standarder og regelverk ikke er fullt ut dekkende for å kunne håndtere risikoen knyttet til teknologien.

3.5 Forkortelser og definisjoner

Term	Definisjon/betydning
AF	Aktivitetsforskriften
CERT	Computer Emergency Response Team
DMZ	Demilitarisert sone – grense mellom subnett
FSA	Functional Safety Assessor
IF	Innretningsforskriften
ISAC	Information Sharing and Analysis Center
ISMS	Information Security Management System
IT	Informasjonsteknologi
Kbf	Kraftberedskapsforskriften
KBO	Kraftforsyningens beredskapsorganisasjon
NKOM	Nasjonal kommunikasjonsmyndighet
NOROG 104	Norsk Olje og Gass (NOROG) 104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OT	Operasjonell teknologi eller industriell IKT
PLC	Programmable Logic Controller

Term	Definisjon/betydning
RF	Rammeforskriften
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SF	Styringsforskriften
SIL	Safety Integrity Level
TOF	Teknisk og operasjonell forskrift

3.6 Sikkerhet, «safety» og «security», IT og OT

På engelsk er det et skille mellom begrepene «safety» og «security». På norsk benyttes begrepet sikkerhet i begge betydninger. Ptils virksomhet har tidligere kun vært fokusert på sikkerhet i betydningen safety, men i 2007 startet de første aktivitetene relatert til IKT-sikkerhet. Når det gjelder programvarebaserte systemer begrenser Ptil sin virksomhet til Operasjonell Teknologi (OT), også benevnt som Industrielle IKT-systemer, både når det gjelder det tradisjonelle sikkerhetsbegrepet og for IKT-sikkerhet. Dette ekskluderer dermed Informasjonsteknologi (IT), også benevnt som administrative IT-systemer. Den teknologiske utviklingen utfordrer imidlertid dette skillet.

Innen IKT-sikkerhet er man opptatt av å sikre konfidensialitet, integritet og tilgjengelighet av informasjon og systemer. **Konfidensialitet** er egenskapen at informasjon og systemer bare skal være tilgjengelig for de som har behov. I en bedrift kan f.eks. noe informasjon og systemer være åpen, noe kan være intern, mens noe er beskyttelsesverdig som kun skal deles eller brukes av et begrenset antall personer. **Integritet** vil si at informasjonen eller systemene ikke er korrumpert og at de er fremkommet gjennom gyldige forretningsmessige prosedyrer. Til slutt må systemer og informasjon være **tilgjengelig** for de som er rettmessige brukere, når de trenger det.

Et viktig emne er samspillet mellom **Informasjonsteknologi (IT)** og **Operasjonell Teknologi (OT)**. IT fokuserer på data og kommunikasjon i kontor- og administrasjonsnettverk, mens OT (eller industrielle IKT-systemer) har fokus på kontroll av fysiske prosesser. Tradisjonelt er konfidensialitet og integritet det mest prominente innen IT, mens tilgjengelighet og det å ha kontroll er ofte viktigst innen OT[1]. Merk at hvis integriteten svikter, har man ikke kontroll. Historisk har det vært et skarpt skille mellom OT og IT, men grensene mellom disse to domenene utfordres. Et angrep på administrative IT-systemer i kontornettet kan være et springbrett inn mot de tekniske OT-systemene, da disse i økende grad er knyttet sammen. Et annet aspekt med den stadig tettere sammenknytningen mellom IT og OT er at IKT-sikkerhetshendelser som kun rammer IT-systemene i den administrative sonen også kan medføre at produksjonen vanskeliggjøres, selv om OT-systemene ikke er direkte rammet. På grunn av denne avhengigheten mellom IT og OT er trenden at tilgjengelighet av IT-systemer også blir stadig mer viktig.

Et eksempel på økonomisk konsekvens fra annen industri er IKT-sikkerhetsangrepet på Hydro våren 2019.

Følgende er sakset fra Q2-rapporten til Hydro:

"The cyber attack on Hydro on March 19, affected our entire global organization, with Extruded Solutions having suffered the most significant operational challenges and financial losses. The financial impact of the cyber attack was around NOK 300- 350 million in the first quarter. The financial impact for the second quarter is estimated at around NOK 250-300 million. Operations and sales have recovered successively during the quarter, reducing the incremental financial impact accordingly. Hydro has a robust cyber insurance in place with recognized insurers. Hydro has not yet recognized any insurance compensation. This will be recorded when deemed virtually certain." /52/

I tillegg til det økonomiske trusselbildet, vil IKT-sikkerhetsangrep kunne true både helse, miljø, sikkerhet og renommé, dersom uavhengige sikkerhetssystemer, i ytterste konsekvens, skulle bli kompromittert gjennom et slikt angrep.

[1] Denne sammenligningen er satt noe på spissen, da det er enkelte IT-systemer som også har svært høye krav til tilgjengelighet. Et eksempel er bank og finanssystemer.

4 REGELVERK

Dette kapitlet beskrives Ptil sitt regelverk og resultatene fra en gapanalyse mellom kravene til IKT-sikkerhet i NVEs kraftberedskapsforskrift og Ptil sitt regelverk. I tillegg beskrives hvordan aktørene i olje- og gassbransjen benytter de delene av Ptils regelverk som er relevante for IKT-sikkerhet. Avslutningsvis inneholder kapitlet DNV GL sine forslag til oppdatering av regelverket.

4.1 Dagens regelverk, forskrifter og veiledninger for sektor

Ptils regelverk er i hovedsak et såkalt funksjonsbasert regelverk, men med noen preskriptive elementer. Dette er en målbasert tilnærming som sier hva som skal oppnås, men i liten grad hvordan. De fem forskriftene som regelverket består av er beskrevet i 4.1.1 nedenfor.

Ptil har utarbeidet egne veiledninger til forskriftene som viser hvordan bestemmelser i en forskrift kan oppfylles. Veiledningene viser på enkelte områder til industristandarder, som en anbefalt måte å oppfylle forskriftens krav på. Veiledningene til forskriftene er ikke rettslig bindende, og aktørene kan derfor velge andre løsninger. Hvis aktøren velger andre løsninger, som for eksempel andre standarder eller selskapsspesifikke prosedyrer, må de kunne dokumentere at den valgte løsningen er minst like god som, eller bedre enn, den anbefalte.

Ptils funksjonsbaserte regelverk er typisk for mange bransjer, men står i kontrast eksempelvis til det preskriptive regelverket som DNV GL håndhever innenfor den maritime industrien. Det er klare fordeler og ulemper med begge modeller, noe som har blitt belyst i en rekke rapporter, se f.eks. /43/. I noen tilfeller søker man å adressere svakheter i begge modellene gjennom å lage hybrider, eksempelvis er NVEs kraftberedskapsforskrift også funksjonsbasert, men den er mer preskriptiv enn Ptil sitt regelverk når det gjelder IKT-sikkerhet.

Et preskriptivt regelverk har først og fremst den fordelen at det er lett å forstå og isolert sett relativt lett å håndheve. Viktige ulemper er at et slikt preskriptivt regelverk kan føre til at aktørene som skal etterleve det fraskriver seg ansvar gjennom å konsekvent legge seg på tillatte minimumsløsninger. I tillegg er et slikt regelverk lite fleksibelt, og aktørene kan unnlate å ta et helhetlig perspektiv på risiko.

I et historisk perspektiv var Ptils overgang fra preskriptiv til funksjonsbasert regelverk motivert av storulykker på 1970 og 80 tallet, hvor bl.a. granskingen etter Piper Alpha ulykken konkluderte med at det å etterleve et preskriptivt regelverk ikke var tilstrekkelig til å hindre en storulykke. Ifølge Ptil, er hensikten bak den funksjonsbaserte tilnærmingen blant annet å unngå detaljstyrende bestemmelser og synliggjøre aktørenes ansvar for å finne løsningene, og gjennom dette legge til rette for fleksibilitet i valg av metoder, fremgangsmåter og teknologiutvikling.

Et funksjonsbasert regelverk krever at det er høy tillit mellom Ptil og de ulike aktørene. Ptil gir aktørene frihet under ansvar, og modellen fungerer når aktørene tar dette ansvaret. Et funksjonsbasert regelverk krever større faglig kunnskap både hos dem som skal etterleve regelverket, og blant dem som skal håndheve det, enn et preskriptivt regelverk.

Et funksjonsbasert regelverk krever også høy organisatorisk modenhet når det gjelder risikohåndtering. En organisasjon som skal tilpasse seg et funksjonsbasert regelverk for første gang vil trenge modningstid til å finne praktisk løsninger som tilfredsstiller regelverket.

Når det kommer nye krav og/eller teknologier vil hele industrien trenge modningstid og samarbeid for å finne gode løsninger. Eksempler på denne type samarbeide hvor mange aktører har deltatt har vært utviklingen av Norsk Olje og Gass sin veiledning til informasjonssikkerhet (NOROG 104) /12/, som refereres i regelverket, og utviklingen av DNV GL's anbefalte praksis for cyber sikkerhet (DNVGL-RP-G108) /13/ basert på IEC 62443 /15/.

Intervjuer med aktørene i bransjen, viser at det fortsatt et stort behov for videre samarbeide og modning innenfor fagfeltet IKT-sikkerhet. Det kommer inn mindre og nye aktører på sokkelen, ny teknologi blir introdusert, og trusselbildet er i stadig endring. Bransjens fokus på problemstillingene er også av relativt ny dato, eksempelvis har man først nylig etablert et spesielt bransjeforum (CDS forum) for dette fagfeltet.

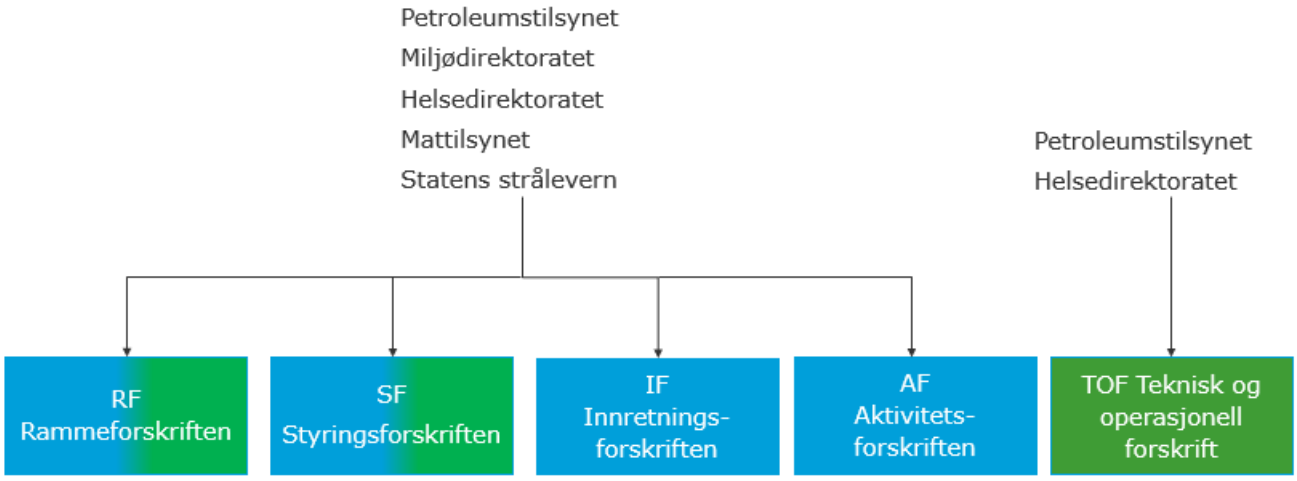
4.1.1 Oversikt over forskrifter

Ptil er delegert myndighet til å fastsette og håndheve følgende fem forskrifter:

RF	Rammeforskriften	Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg
SF	Styringsforskriften	Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg
IF	Innretningsforskriften	Forskrift om utforming og utrustning av innretninger med mer i petroleumsvirksomheten
AF	Aktivitetsforskriften	Forskrift om utføring av aktiviteter i petroleumsvirksomheten
TOF	Teknisk og operasjonell forskrift	Forskrift om tekniske og operasjonelle forhold på landanlegg i petroleumsvirksomheten med mer

Til hver forskrift er det en veiledning med mer utførlig forklaring rundt de enkelte paragrafer. Forskrifter og tilhørende veiledninger er referert i /17/-/26/. I den videre diskusjonen vises det kun til AF og IF. TOF ivaretar de delene av AF og IF som er relevante for landanlegg og kommentarene må også forstås inn i denne forskriften.

Forskriftene er også underlagt andre etater, slik figuren under viser.



Figur 4-1– Figur som viser hvilke etater de ulike forskriftene er underlagt. Blå farge indikerer at forskriften gjelder til havs, grønn farge at den gjelder til lands. RF og SF omfatter begge områdene.

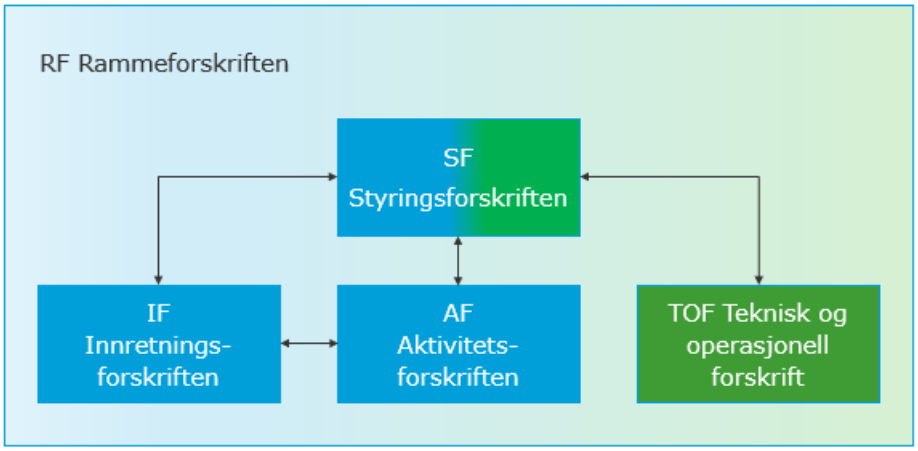
Regjeringen skriver følgende om Petroleumstilsynet i en oversikt over tilsynsmyndigheter i Norge (20.12.2016):

«Petroleumstilsynet har myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på kontinentalsokkelen og på visse petroleumsanlegg på land. Etaten er underlagt Arbeids- og sosialdepartementet. Petroleumstilsynet fører tilsyn etter petroleumsloven, brann- og eksplosjonsvernloven, el-tilsynsloven og arbeidsmiljøloven samt underliggende forskrifter.

Flere varegrupper faller inn under Petroleumstilsynets ansvarsområde, bl.a. maskiner, produkter for anvendelse i eksplosjonsfarlig område, elektrisk utstyr, trykkpåkjent utstyr og klassifisering og merking av kjemikalier.»

Ref /47/

Flere detaljer om hvilke lover og paragrafer forskriftene bygger på er redegjort innledningsvis i hver forskrift. Forholdet mellom de ulike forskriftene er illustrert i figuren under.



Figur 4-2– Rammeforskriften og styringsforskriften er overordnet de tre andre.

Det er stort fokus på helse, miljø og sikkerhet (i betydningen «safety»), men i veiledningen til Rammeforskriften § 1 /22/ står det også følgende: *«Forskriften omfatter sikkerhet, arbeidsmiljø, helse, ytre miljø og økonomiske verdier (deriblant produksjons- og transportregularitet). Tiltak iverksatt på ett av disse områdene vil normalt også ha positiv virkning på de andre områdene. I den grad tiltak skulle komme i konflikt, må hensynet til menneskers liv og helse veie tyngst.»*

4.1.2 Regelverkets håndtering av programmerbare systemer

Ptils regelverk fokuserer først og fremst på sikkerhet for menneskers liv og helse samt miljø. Den overordnede sikkerhetsfilosofien ved alvorlige uønskede hendelser, uansett årsak, er å gå til sikker tilstand, noe som i mange tilfeller betyr å stoppe produksjon og prosessering. På dette punktet vil olje & gass skille seg ut fra enkelte andre industrier slik som kraftforsyning, luftfart, og maritim, der det å stoppe systemene i mange tilfeller vil være svært uønsket også av hensyn til menneskers liv og helse.

Denne filosofien gjenspeiles ved at det stilles få krav til hvordan kontroll og overvåkningssystemene skal designes, utvikles, verifiseres, valideres og opereres, men desto strengere krav til de separate sikkerhetssystemene som i mange tilfeller representerer den siste barriere mot en ulykke.

Ptil har en praksis med å skrive funksjonskrav på et relativt høyt nivå, mens veiledningene henviser til norske og internasjonale standarder som bør anvendes innenfor det enkelte tema. I hovedsak vil det være disse standardene som stiller de detaljerte kravene til de tekniske systemene, både de som er programmerbare og andre typer systemer.

For sikkerhetssystemer henvises til standarder som IEC 61508 /3/, IEC 61511 /2/ og NOROG070 /60/ og NORSOK S-001 /61/. I sum gir disse standardene strenge krav til hvordan overvåkningssystemene skal designes, utvikles, verifiseres, valideres og opereres. Dette er beskrevet i mer detalj i rapporten «Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller» /49/.

Ptils regelverk fokuserer i liten grad på at systemene skal være tilgjengelige for produksjon. Eksempelvis finnes det ikke krav om at kontroll og overvåkningssystemene skal være redundante for å sikre oppetid. Det refereres heller ikke til standarder som sier noe om hvordan slike systemer bør designes og utvikles. Siden slike systemer utgjør en angrepsflate for IKT-sikkerhetshendelser som også kan ha betydning for sikkerheten, henviser imidlertid innretningsforskriften § 34a til NOROG 104 /12/ og sier at denne bør legges til grunn for beskyttelse mot IKT-relaterte farer.

Regelverket er begrenset til såkalt Operasjonell Teknologi (OT). Det stilles ingen krav til aktørenes IT-systemer og beskyttelse av slike systemer.

4.1.3 Ptils vurdering av paragrafer som er relevante for IKT-sikkerhet

I brevet «Informasjon om håndtering av IKT-sikkerhet» /40/ av 18.9.2019 henviser Ptil til følgende paragrafer i forskriftene:

Tabell 4-1 - Paragrafer i forskriftene som ifølge Ptil er relevante for IKT-sikkerhet

Paragraf	PtilS forståelse av anvendelse for IKT-sikkerhet
Styringsforskriften § 4 Risikoreduksjon: den ansvarlige [skal] velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.	Dette innebærer at det velges løsninger for IKT- sikkerhet som reduserer sannsynligheten for IKT- angrep som forårsaker skade, feil eller faresituasjoner.
Styringsforskriften § 8 Interne krav: Den ansvarlige skal sette interne krav som konkretiserer krav i regelverket, og som bidrar til å nå målene for helse, miljø og sikkerhet.	Det må settes krav til hvordan IKT-sikkerhet håndteres, både teknisk, operasjonelt og organisatorisk.
Innretningsforskriften § 32-34 Sikkerhetssystemer: Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer. Veiledning: systemet kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av systemsvikt, feil eller enkelthendelser i disse systemene.	Kravet om at grensesnitt mot andre systemer ikke skal påvirke negativt innebærer at heller ikke IKT- angrep skal hindre at systemene kan utføre tiltenkte funksjoner.
Innretningsforskriften § 34a Kontroll- og overvåkingssystem: Veiledning: I tillegg bør Norsk olje og gass retningslinje nr. 104 legges til grunn for beskyttelse mot IKT-relaterte farer.	Veiledningen viser til anerkjent retningslinje, men også andre standarder kan benyttes.

Paragraf	PtilS forståelse av anvendelse for IKT-sikkerhet
Aktivitetsforskriften § 21 Kompetanse: Den ansvarlige skal sikre at personellet til enhver tid har den kompetansen som er nødvendig for å kunne utføre aktivitetene i henhold til helse-, miljø- og sikkerhetslovgivningen. I tillegg skal personellet kunne håndtere fare- og ulykkessituasjoner.	Kravet om kompetanse er også relevant for de som skal håndtere faresituasjoner i forhold til IKT- hendelse med de industrielle kontroll- og sikkerhetssystemene.
Aktivitetsforskriften § 23 Trening og øvelser: Den ansvarlige skal sikre at det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte	Kravet om trening og øvelser er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhetssystemene og samhandle med responsmiljøer.
Aktivitetsforskriften § 45 Vedlikehold: Den ansvarlige skal sikre at innretninger eller deler av disse holdes ved like, slik at de er i stand til å utføre sine krevde funksjoner i alle faser av levetiden.	Oppdatering og patching av programvare når det oppdages sikkerhetssvakheter er å forstå som vedlikehold.
Aktivitetsforskriften § 48 Planlegging og prioritering: Det skal utarbeides en samlet plan for utføring av vedlikeholdsprogram og korrigerende vedlikeholdsaktiviteter	Kravet om planlegging innebærer en systematikk for hvordan selskapet har kontroll på hvilke oppdateringer som er relevante og hvilke utstyrskomponenter som må ha vedlikeholdsprogram.
Styringsforskriften § 29 Varsling og melding: Veiledning: situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse).	Melding om IKT-hendelse slik det framkommer i veiledningen er en informasjon til oss om situasjonen. Dersom det er knyttet sensitiv informasjon til hendelsen, må teksten merkes slik at denne delen kan unntas for innsyn. NSM sitt rammeverk som er omtalt ovenfor beskriver hvordan hendelser i kritisk infrastruktur / kritiske samfunnsfunksjoner skal håndteres.

Som det fremgår av tabellen ovenfor, er det kun i veiledningen til innretningsforskriften § 34a Kontroll og overvåkingssystemer, og i veiledningen til SF § 29 Varsling og melding, at IKT-sikkerhet er nevnt eksplisitt. Ptil har formidlet til industrien at andre paragrafer er relevante for IKT-sikkerhet, også før /40/ ble sendt ut i september. Dette har skjedd i møter med aktørene og på konferanser, hvor Ptil har holdt foredrag om IKT-sikkerhet.

4.2 Sammenligning av Ptils forskrifter mot Kraftberedskapsforskriften

For å identifisere forbedringspunkter har dagens forskrifter og veiledninger for petroleumssektoren blitt vurdert opp mot NVEs kraftberedskapsforskrift (Kbf). Regelverket som er lagt til grunn fra petroleumssektorens side er rammeforskriften, styringsforskriften, innretningsforskriften, aktivitetsforskriften samt teknisk og operasjonell forskrift. Innretningsforskriften peker på NOROG 104 som også er inkludert. Sammenligningen danner grunnlag for en drøfting av dagens regelverk og forslag til endringer og tillegg.

4.2.1 Spesielt om kraftberedskapsforskriften

Kraftberedskapsforskriften ble benyttet som basis i analysen grunnet at sektorene som regelverkene gjelder for er på et overordnet nivå sammenlignbare, med mange aktører i varierende størrelse, høye krav til sikkerhet og modne tilsynsorgan.

Selv om mye er sammenlignbart er det også noen viktige forskjeller i forskriftenes virkeområde. Kbf gjelder for: *forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi eller fjernvarme.* Dette gir et annet fokus enn PTILs regelverk som først og fremst fokuserer på å hindre skade og ulykker knyttet til produksjon, prosessering og overføring av olje & gass. I en IKT-sammenheng betyr dette at PTILs regelverk har et noe smalere virkeområde, samt en forskjellig tilnærming når det gjelder håndtering av alvorlige hendelser, det siste er videre diskutert i kapittel 4.2.3.

NVE har en rolle som overordnet beredskapsmyndighet innenfor kraftsektoren, mens Ptil ikke har en tilsvarende rolle innen petroleumssektoren. Dette gjenspeiler at kraftforsyning, i motsetning til olje og gass produksjon, er ansett som en samfunnskritisk funksjon, se eksempelvis DSBs oversikt over samfunnskritiske funksjoner /62/. Dette påvirker innholdet og omfanget av Kbf.

Begge regelverkene er i stor grad funksjonsbaserte, men Kbf anses å være mer preskriptiv med mer detaljerte krav. For regulering av IKT-sikkerhet er det ulike tilnærminger mellom regelverkene, noe som gjør sammenligningen interessant.

I NOU 2018:14, ref. /7/ i boks 6.1, side 33 står følgende å lese:

«To ytterliggående eksempler på variasjonen i tilnærming til regulering av IKT-sikkerhet er regelverkene for henholdsvis petroleumssektoren og kraftsektoren. Kravene om IKT-sikkerhet i disse regelverket er ulikt utformet.

På den ene side har olje- og gassindustrien et funksjonsbasert regelverk innenfor helse, miljø og sikkerhet. Petroleumsloven stiller krav om sikkerhet og forsvarlig petroleumsvirksomhet, men regelverket har lagt til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak. Dette gjøres gjennom risiko- og beredskapsanalyser i de enkelte selskapene. Næringen har selv utarbeidet spesifikke retningslinjer for IKT-sikkerhet i prosesskontroll-, sikkerhets- og støttesystemer som legges til grunn for arbeidet basert på ISO 27000-serien.

På den andre siden stiller NVEs revidert forskrift for beredskap i kraftforsyningen relativt omfattende krav om sikring av alle digitale informasjonssystemer hos virksomheter som er underlagt forskriften. Den digitale grunnsikringen innebærer at virksomheter plikter å sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Grunnsikringen skal være i henhold til anerkjente standarder og normer, deriblant å identifisere og dokumentere, sikre og oppdage, håndtere og gjenopprette. I tillegg er det krav om risiko- og sårbarhetsanalyse og sikkerhetskrav ved tjenesteutsetting i forskriften.»

Vår vurdering er at NVE fremdeles har et funksjonsbasert regelverk, men at kravene er på et mer detaljert nivå.

Nedenfor følger en kort beskrivelse av Kraftberedskapsforskriften (Kbf). Vi kommenterer noen sentrale paragrafer under hvert kapittel.

Kapittel 1. Innledende bestemmelser (§§ 1-1 - 1-5)

Det viktigste fra et samfunnsikkerhetssynspunkt er at kraftforsyningen opprettholdes. Dette gjenspeiles i § 1-1 Formål:

> *Innenfor formålene i energiloven § 1-2, skal forskriften sikre at kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene.*

Videre er den en plikt for virksomheter som er omfattet av forskriften å ha beredskap og beredskapsplaner. Dette er beskrevet i § 1-5.

Kapittel 2. Generelle krav for KBO-enheter (§§ 2-1 - 2-10)

§ 2-3 Risikovurdering og § 2-4 Beredskapsplanlegging er viktige forutsetninger for beredskap. § 2-6 Rapportering, inneholder detaljerte kriterier for hva som skal rapporteres til beredskapsmyndigheten. Flere av punktene fra a til h berører direkte eller indirekte IKT-sikkerhet:

> *a. Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS).*
>
> *c. Ved begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter.*
>
> *d. Situasjoner hvor kraftsensitiv informasjon er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette.*
>
> *h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer*

Kapittel 3. Kraftforsyningens beredskapsorganisasjon (KBO) (§§ 3-1 - 3-7)

Her beskrives beredskapsorganisasjonen hvor beredskapsmyndigheten (NVE) og Statnett SF har særskilte roller. Det er også beskrevet et sektorvist responsmiljø for IKT-sikkerhetshendelser (§ 3-6)

> *Beredskapsmyndigheten er sektorvist responsmiljø for IKT-sikkerhetshendelser i kraftforsyningen. Beredskapsmyndigheten kan delegere oppgaver innenfor varsling, informasjonsdeling og analyse for IKT-sikkerhetshendelser i kraftforsyningen til en eller flere KBO-enheter.*

Kapittel 4. Ressurser og reparasjonsberedskap (§§ 4-1 - 4-7)

Kanskje spesielt verdt å merke seg er § 4-1. Reparasjonsberedskap, første ledd:

> *KBO-enheter skal planlegge for og etablere en organisasjon med nødvendig personell, kompetanse, utholdenhet og ressurser til å holde driften gående, gjenopprette funksjon og gjennomføre oppgaver som kreves under alle ekstraordinære situasjoner på en sikker og effektiv måte.*

Dette stiller sterke krav til en organisasjons evne til å håndtere kriser. Det peker også på utholdenhet, noe som er vesentlig ved langvarige kriser.

Kapittel 5. Klassifisering og sikringstiltak (§§ 5-1 - 5-11)

Dette kapitlet omfatter klassifisering av ulike anlegg og krav til fysisk sikring av anleggene.

Kapittel 6. Informasjonssikkerhet (§§ 6-1 - 6-10)

Her er begrepet kraftsensitiv informasjon svært viktig. I § 6-2 er dette definert som

> *Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.*
> *Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen, herunder:*

Deretter følger ti punkter med eksempler/detaljer om hva dette er.

Det stilles også krav til beskyttelse og tilgangskontroll, sikkerhetsinstruks, personkontroll, osv. Dessuten stilles det krav til informasjonssystemer:

I § 6-9.Digitale informasjonssystemer heter det at

> *Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.*

Videre er det beskrevet grunnsikring i form av Identifisere og dokumentere, Risikovurdering, Sikre og oppdage, Håndtere og gjenopprette. Dette er aktiviteter i tråd med NSMs grunnprinsipper og også med NIST.

Kapittel 7. Beskyttelse av driftskontrollsystem (§§ 7-1 - 7-17)

Dette går på krav til beskyttelse av driftssentraler og kontrollanlegg, for eksempel SCADA-systemer, RTUer, dvs. typiske OT-systemer som ligger i den/de mest kritiske sonen(e). Det er blant annet krav til redundans og krav angående fjernaksess.

Kapittel 8. Avsluttende bestemmelser (§§ 8-1 - 8-9)

Dette kapittel beskriver kontroll (tilsyn), og hvilke reaksjonsmuligheter beredskapsmyndigheten har så som pålegg, dispensasjon, tvangsmulkt, overtredelsesgebyr og straff. I § 8-1 Kontroll, heter det

> *Beredskapsmyndigheten fører kontroll med at bestemmelser gitt i eller i medhold av denne forskriften overholdes.*

Avslutningsvis i kraftberedskapsforskriften finnes vedlegg som stiller mer detaljerte krav. De tre ulike klassene av anlegg er blant annet definert ut ifra hvor mye energi som produseres/overføres og hvor høy spenning det er i ledningene/kablene. Dette sier indirekte noe om den samfunnsmessige betydningen i tilfelle utfall.

Vedlegg 1 til § 5-4: Særlige krav til sikring for anlegg klassifisert i klasse 1

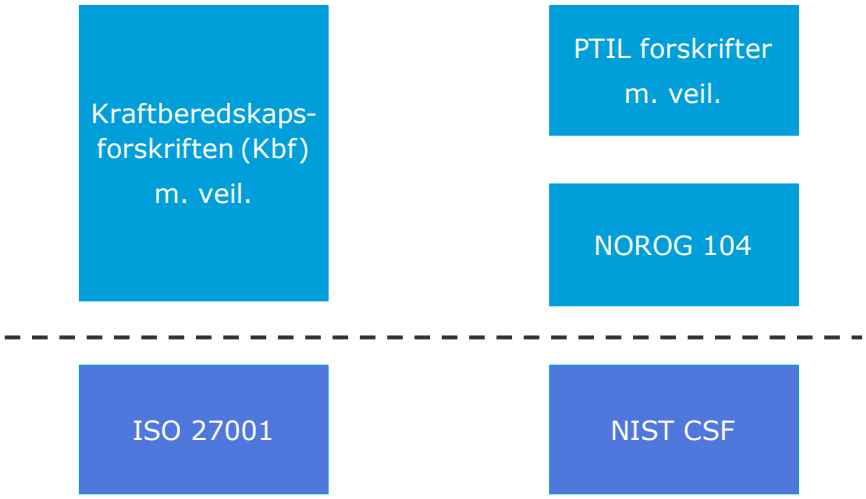
Vedlegg 2 til § 5-5: Særlige krav til sikring for anlegg klassifisert i klasse 2

Vedlegg 3 til § 5-6: Særlige krav til sikring for anlegg klassifisert i klasse 3

Vedlegg 4: Henvisning til normer og standarder i forskriften

4.2.2 Rammene for gap-analysen

Figuren nedenfor illustrerer rammene for gap-analysen. DNV GL har tatt utgangspunkt i kraftberedskapsforskriften (Kbf) og undersøkt i hvor stor grad Ptils forskrifter med tilhørende veiledning dekker relevante punkter i Kbf med hensyn på industriell IKT-sikkerhet. Siden Ptils forskrifter henviser til NOROG 104 for IKT-sikkerhet, er denne også tatt med i gapanalysen. NOROG 104 henviser videre til NIST CSF (Cybersecurity Framework), mens Kbf bygger på ISO 27001. De detaljerte kravene i disse dokumentene er ikke tatt med i gapanalysen.



Figur 4-3 – Omfang av gap-analyse – Det er gjort en gap-analyse mellom Kraftberedskapsforskriften og Ptils forskrifter utvidet med NOROG 104.

4.2.3 Strategi for håndtering av alvorlige hendelser.

Kbf og Ptils forskrifter representerer ulike strategier ved alvorlige hendelser, uavhengig av årsak. Kbfs fokus er å unngå svikt i den nasjonale kraftforsyningen, mens de mest alvorlige konsekvensene av en hendelse i olje & gass-bransjen er knyttet til ulykker, eksempelvis brann og eksplosjon. I situasjoner hvor det er fare for ulykker er strategien i olje & gass at operasjonen skal stoppes, enten av operatør eller av et automatisk sikkerhetssystem. Dette betyr bl.a. at det i olje & gass-næringen ikke er like aktuelt å:

- Skille på store og små aktører slik det blir gjort i Kbf. § 5-2, siden ulykkepotensialet kan være like stort hos små aktører som hos store.
- Stille krav som eksplisitt tar sikte på å unngå nedetid slik det eksempelvis blir gjort i Kbf. Kapittel 7, siden uønsket nedetid først og fremst vil ha økonomiske konsekvenser for den enkelte aktør. Ett mulig unntak her er Gassco som koordinerer leveransene til det Europeiske markedet for gass. Det er betydelig lagerkapasitet i leveransekjeden, men en langvarig stans kan få konsekvenser for dem som blir rammet.

Kbf § 7-11 – Systemredundans i driftskontrollsystemet er et eksempel på forskjellen i filosofi. Der Kbf fokuserer på oppetid, har Ptil en sikkerhetsfilosofi i sitt regelverk som går på stenge ned ved alvorlige hendelser, og det er ikke et krav til systemredundans i hovedkontrollsystemet. Derimot er det krav om at det skal finnes uavhengige systemer for prosessavstenging og nødavstenging, og at disse skal utvikles i henhold til strenge internasjonale standarder. Dette er også et eksempel på at PTILs regelverk på noen områder er mer preskriptivt enn Kbf. Systemredundans vil ikke være et effektivt mottiltak mot alle typer problemer som kan oppstå, eksempelvis i programvare, og det er en av årsakene til kravet om uavhengige nødsystemer. I Kbf § 7-11h står følgende: «*Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil*

ikke rammer alle dublerte system samtidig, jf. § 7-7», uten å angi spesifikke føringer for hvordan dette skal håndteres.

4.2.4 Gap som ansees som relevante for petroleumssektoren

Kraftberedskapsforskriften omhandler forebyggende sikkerhet og beredskap, hvor IKT-sikkerhet er et viktig aspekt av dette. Gapanalysen fokuserer på gap relatert til IKT-sikkerhet, og paragrafer som er vurdert som ikke relevante for petroleumssektoren er ikke inkludert i denne analysen. Det er funnet følgende punkter i Kbf som ikke er tilsvarende dekket eller detaljert i Ptils forskrifter:

Tabell 4-2 Relevante gap

Kraftberedskapsforskriften	Ptils forskrifter
Kbf § 2-2 stiller eksplisitte krav om at det skal finnes en beredskapsleder, beredskapskoordinator og en IKT-sikkerhetskoordinator.	Ptils AF § 73 – 77 omhandler beredskap, men IKT-hendelser er ikke nevnt. Fokus er på storulykker og miljørelaterte hendelser.
Kbf § 2-4 krever at beredskapsplanlegging skal samordnes med myndighetene, og spesifiserer at informasjonssikkerhet er omfattet av paragrafen.	SF § 17 og AF § 73 - 76 omhandler beredskap men er veldig rettet mot miljøberedskap. Det stilles ikke krav til samordning med berørte myndigheter eller andre relevante virksomheter. Det er ingen henvisning til IKT-sikkerhet.
Kbf § 2-6 er konkret på hvilke typer hendelser, eller potensielle hendelser, som skal varsles til myndighetene samt tidsfrist.	SF § 29 punkt d, «alvorlig svekking eller bortfall av sikkerhetsrelaterte funksjoner eller barrierer (..)», kan være relevant, men gjelder sikkerhetssystemer (safety) og ikke produksjonskontroll. I veilederen til styringsforskriften § 29, punkt i, defineres IKT-hendelser som forstyrrer kontroll- eller sikkerhetssystemer som en fare- og ulykkessituasjon som skal rapporteres til tilsynsmyndigheten. Disse punktene beskriver hendelser som fører til forstyrrelser i normal drift, dermed vil ikke sikkerhetsbrudd uten direkte konsekvenser, «nesten-ulykker», nødvendigvis rapporteres.
Kbf § 2-7 stiller krav om en flerårig øvelsesplan.	NOROG 104 - ISBR 5 stiller krav til «training and awareness», men nevner ikke øvelser. Aktivitetsforskriften har fokus på aktiviteter som kan forstyrre operasjonell drift. AF § 23 stiller krav til årlige øvelser, men mangler krav til øvelsesplan – og nevner ikke IKT-hendelser spesifikt.

Kraftberedskapsforskriften	Ptils forskrifter
Kbf § 2-8 stiller eksplisitte krav til informasjonsplan.	NOROG 104 - ISBR 16 stiller krav til intern rapportering, men har bør-krav når det kommer til rapportering til eksterne aktører. For myndigheter (Ptil) gjelder SF § 29 - Varsling og melding til tilsynsmyndighetene av fare- og ulykkessituasjoner, som plikter en initiell varsling. Denne nevner ikke informasjonsberedskap.
Kbf § 2-9 krever evaluering etter ekstraordinære situasjoner og øvelser. Inkluderer bruk av evalueringer til å oppdatere risikovurderinger og beredskapsplaner.	SF § 19 og 20 dekker innsamling og bearbeiding av data med betydning for HSE. Uklart om dette oppfattes til å omfatte IKT-hendelser. NOROG 104 - ISBR 16 - Reporting information security events – har bør krav til samling og håndtering av rapporter for oppfølging og læring.
Kbf § 3-6 definerer sektorvis responsmiljø for IKT-hendelser. I veiledningen til Kbf står det at hensikten er å spesifisere at NVE er beredskapsmyndighet for sektoren, samt å gjøre det forutsigbart hvilke oppgaver NVE kan delegere i en beredskapssituasjon.	Det finnes ikke tilsvarende beredskapsmyndighet innenfor petroleumssektoren. Flere aktører i petroleumssektoren tilknytter seg CERT-miljøer for varsling, analyse og informasjonsdeling.
Kbf § 5-7 gir beredskapsmyndighet mandat til å kreve ytterliggere sikringstiltak uavhengig av aktørenes egen vurdering.	Det finnes ingen tilsvarende paragraf i Ptils regelverk.
Kbf § 5-9 pålegger aktørene meldeplikt om sikringstiltak når man planlegger å bygge, endre eller utvide anlegg, system eller annet, før arbeidet starter.	Styringsforskriften § 25 - Krav om samtykke til enkelte aktiviteter, sier at dersom forutsetninger for et gitt samtykke endres, kan Ptil kreve at operatør innhenter nytt samtykke.
Kbf § 5-11 legger føringer for restriksjoner for adgang til steder og områder.	NOROG 104 fokuserer på logisk tilgangsstyring og nevner ikke fysisk adgang. SF § 17 omhandler risikoanalyser og SF § 5 omhandler barrierer. Det er mulig å tolke det slik at dette også dekker fysisk sikring, men det er ikke eksplisitt nevnt. Ptil nevner ikke SF § 5 som relevant for IKT-sikkerhet i sin oversikt (Tabell 4-1).
Kbf § 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere.	Det finnes ikke tilsvarende begrep for petroleumssektoren, men noe informasjon vil være sensitiv for aktører, og kan potensielt benyttes av angripere for planlegging og gjennomføring av angrep.

Kraftberedskapsforskriften	Ptils forskrifter
Kbf § 6-5 ansvarliggjør KBO-enheter for at informasjonssikkerhet ivaretas i anskaffelser, og at leverandører følger bestemmelsene for informasjonssikkerhet og taushetsplikt.	NOROG 104 - ISBR 8- Information security in engineering, procurement and commissioning processes – stiller krav til dokumentasjon av leverandørers etterlevelse av informasjonssikkerhets-krav. Mangler krav om oppfølging utover anskaffelsesfasen, og sikring av rett til revidering av leverandører.
Kbf § 6-7 stiller krav til gjennomføring av bakgrunnssjekk av personer før ansettelse.	Det finnes ingen tilsvarende krav i Ptils regelverk.
Kbf § 6-8 Sikkerhetskopier. Stiller krav til sikker og tilgjengelig fjernlagring av oppdaterte sikkerhetskopier.	NOROG 104 stiller ikke krav til hvor ofte man skal ta sikkerhetskopi, hvilke typer systemer man skal sikkerhetskopiere, hvor det skal lagres, eller hvordan den skal sikres. ISBR 7 - Preparedness for disaster recovery – henviser til aktørens egne mål for gjenopprettelse av data.
Kbf § 6-9 Digitale informasjonssystemer skal sikres for å ivareta C, I, A (konfidensialitet, integritet og tilgjengelighet), og inkluderer også revisjoner av sikringstiltak.	Styringsforskriften stiller krav til sikkerhet, inkludert barrierer for å unngå uønskede tilstander. NOROG 104 definerer anbefalte krav til IKT-sikkerhet – men et overordnet samlekrav til C, I, A i digitale informasjonssystemer mangler. I Ptils regelverk er det fokus på integritet og tilgjengelighet, men lite fokus på konfidensialitet.
Kbf § 7-13 – Beskyttelse mot elektromagnetisk puls og interferens.	Mangler krav til beskyttelse mot EMP / EMI. Det finnes ikke tilsvarende krav på forskriftsnivå fra Ptil, men slik beskyttelse kan være dekket gjennom tekniske standarder.

Alle identifiserte gap er ikke nødvendigvis relevante å dekke, da regelverkene har ulikt omfang og sikkerhetsfilosofi. De som ansees som relevante er tatt inn i forslag til regelverksendringer i Tabell 4-3.

4.3 Aktørenes tilnærming til regelverk og IKT-sikkerhet

Dette kapittelet oppsummerer hvordan aktørene innenfor olje & gass i praksis bruker regelverket. Dette er basert på intervjuene som har vært gjennomført.

4.3.1 Bruk av rammeverk for IKT sikring.

Alle aktørene er kjent med at veiledningen til innretningsforskriften § 34a for kontroll og overvåkningssystemer peker på NOROG 104 /12/ for IKT-sikkerhet. Likevel benyttes NOROG 104 i større grad som et veiledningsverktøy fremfor å bli benyttet som et sett som funksjonskrav.

De fleste av aktørene har interne rammeverk som er basert på ISO 27001 /44/ for IT siden, og IEC 62433 /15/ for OT siden. Noen aktører forholder seg også til NIST /14/. Internasjonale IKT-sikkerhetsstandarder av denne typen inneholder mer detaljerte krav, men er ikke referert til direkte i Ptil sitt regelverk med veiledere. Dette er til forskjell for hva som gjøres for teknisk sikkerhet, hvor regelverket eksplisitt referer til anerkjente internasjonale standarder, som IEC 61508 /3/ og IEC 61511 /2/.

En av aktørene pekte først og fremst på petroleumsloven kapittel 9, som basis for det arbeidet man gjør innenfor IKT-sikkerhet.

Mange av aktørene er godt kjent med DNVGL-RP-G108 fra 2017 /13/. Dette dokumentet inneholder anbefalt praksis for IKT-sikkerhet innenfor olje og gass-industrien basert på IEC 62443 /15/. Denne ble utarbeidet i et «Joint Industry Project» (JIP), der flere av aktørene som har vært intervjuet deltok. Flere av aktørene ser det som en fordel om denne også blir referert til i regelverket, spesielt for å kunne støtte seg mer på regelverket når man stiller sikkerhetskrav ved anskaffelser, samt ved innføring av ny teknologi.

4.3.2 Regelverkets omfang

Aktørene ser Ptils regelverk som kun relevant for OT og ikke for IT. Det er imidlertid en klar utvikling i retning av at aktørene tar et mer helhetlig perspektiv på IKT-sikkerhet. Historisk begynte man å arbeide med problemstillingen på IT siden, deretter har man fokusert på OT, og i dag arbeides det med å skape helhetlige løsninger. Flere av aktørene har uttrykt at man er på «en reise» innenfor dette området, og hvor det ses på løsninger som favner om både IT og OT.

Skillet mellom IT og OT utfordres bl.a. av:

- Økt press på å få etablert løsninger for fjernaksess for OT komponenter fra IT domenet.
    - Eksempel: Leverandører som ønsker å levere «Ytelse som en tjeneste» og som ønsker å justere eget utstyr basert på loggede data. Aktørene er i dag forsiktige med å bruke denne type tjenester.
- Håndtering av konfidensiell informasjon skjer ofte i IT domenet.
- Man vil i fremtiden ønske å fortløpende kunne justere prosessparametere basert på maskinlæring o.l.
- Et økende behov for logging av driftsdata fra OT domene inn i systemer i IT domene.
- Et økende behov for informasjonsflyt inn og ut av OT domene. Det være seg informasjon om personell på installasjonene, meteorologidata, radar, synkronisering av klokke, patch og antivirus oppdateringer, eller programvareoppdateringer.

Det er ulike oppfatninger blant aktørene med hensyn til Ptils rolle og regelverkets omfang. Noen mener at Ptils naturlige virkeområde er på OT siden, mens andre mener at Ptil også bør ha mandat til å gjennomføre tilsyn på større deler av IT siden, men har gitt utrykk for at det er utfordrende å definere hvilke deler.

4.3.3 Krav til leverandører

Når aktørene setter ut kontrakter til leverandører, er det gjerne krav knyttet til IKT-sikkerhet i anbudsforespørselen:

- Større selskaper har interne dokumenter som definerer selskapets tilnærming til ISO 27001 /44/ og IEC 62433 /15/, som igjen blir benyttet mot leverandører.
- Noen selskaper peker på NOROG 104 /12/ med flere, og forventer at leverandørene oppfyller dette med egnede IKT-sikkerhet løsninger.

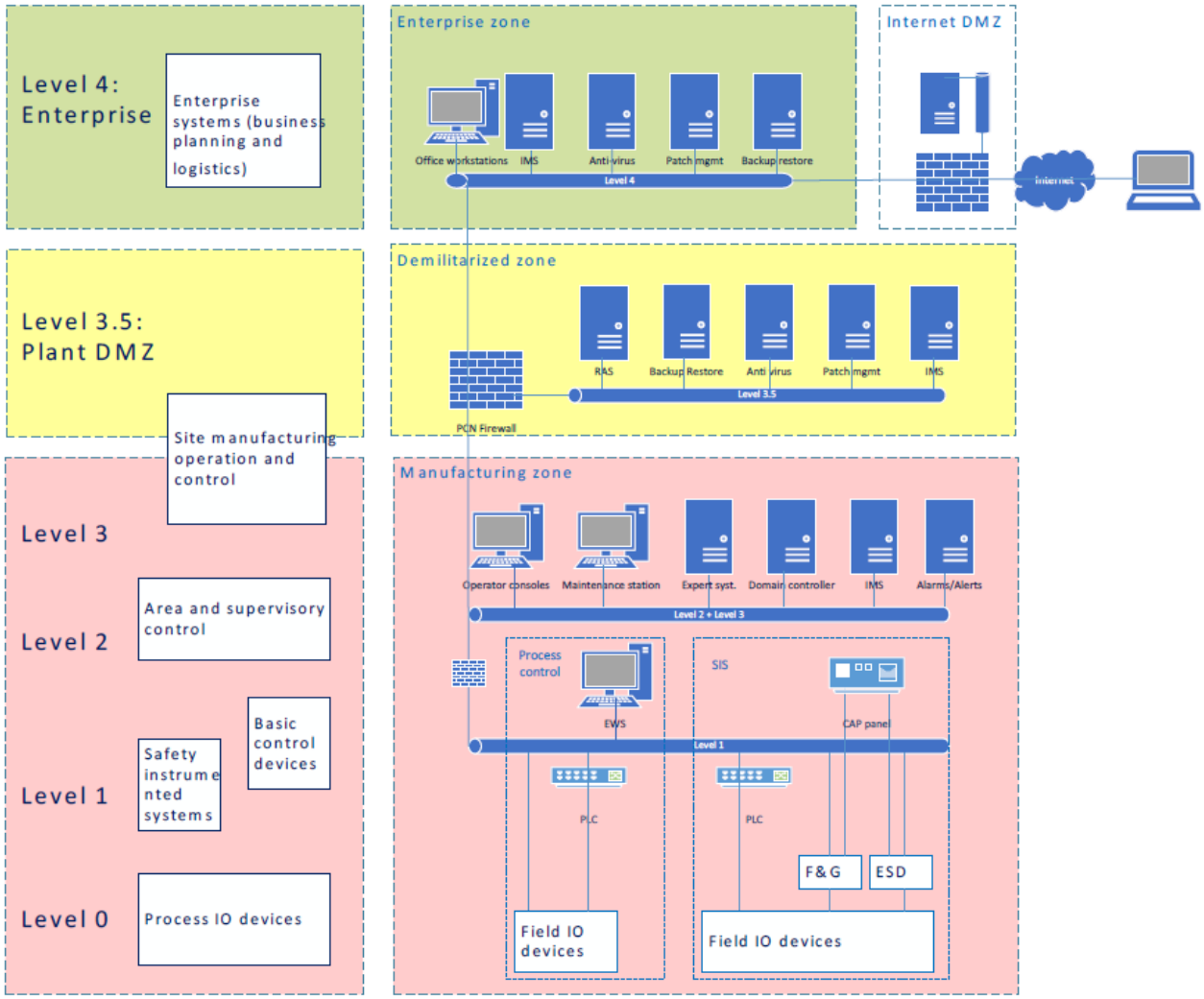
Noen leverandører har fjernaksess til OT komponenter for å kunne gjøre vedlikehold og ivareta produksjon. De ulike løsningene for fjernaksess varierer i stor grad hos aktørene. Noen krever at leverandørene skal gjennomføre aksessen fra aktørens eget nett på dedikerte maskiner, mens andre aktører tillater fjernaksess direkte fra leverandøren, men med restriksjoner. Eksempelvis ved bruk av definerte løsninger for aksesskontroll og i godkjente rom. De fleste aktører har, eller er i ferd med å ta i bruk anerkjente fjernaksessløsninger.

Praksis for patching av OT-systemer varierer også i stor grad. Noen tillater dette via fjernaksess etter et sett med kriterier, mens andre krever at dette gjøres på lokasjon med aktørens representanter tilstede.

Leverandører forventes i varierende grad å ha en rolle ved en hendelse. Noen mindre aktører forventer stor bistand fra leverandører, mens andre større aktører baserer seg på bruk av interne ressurser i størst mulig grad.

4.3.4 Segmentering og Sonemodeller

Alle aktørene som ble intervjuet segmenterer sine nettverk, i henhold til en sonemodell. I grove trekk legges Purdue-modellen til grunn for soneinndeling, se eksempel under hentet fra DNVGL-RP-G108.



Figur 4-4 – Forenklet segmentering av nettverk

Ptils regelverk krever at sikkerhetssystemer som utfører prossessavstenging og nødavstenging skal være tilstrekkelig uavhengig av kontrollovervåkingssystemene, ref. Innretningsforskriften § 32 til § 34. For oppfyllelse av kravene tillates det å benytte logisk nettverksseparasjon og bruk av en felles HMI. Dette kan medføre en økt sårbarhet i form av en større angrepsflate. Dette er belyst mer i detalj i rapporten «Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller» /49/.

Samtlige aktører informerer om at det benyttes brannmurer mellom IT og OT. I mange tilfeller er det egne dedikerte nettverk for safety systemer.

Det er også et antall systemer som er etablert utenfor de definerte sonene, men som har en relasjon til både IT- og OT-systemer. Eksempler på dette er systemer knyttet til radar, helikopternavigasjon og værdata. Noen aktører informerer om at de også har egne servicenettverk definert utenom IT- og OT-nettverkene, som benyttes for overvåking og vedlikehold av disse komponentene. Flere aktører opplyser at det arbeides med å forbedre arkitekturen for disse systemene.

4.3.5 Barrierer

Barrierefilosofi står svært sentralt i tenkningen rundt sikkerhet generelt innenfor olje og gass. I diskusjoner med aktørene kommer det frem at barrierebegrepet, naturlig nok, også benyttes knyttet til IKT-Sikkerhet, og at Ptil har en forventning om at barrierefilosofien skal være gjeldende også her. Dette antydes i Ptil sitt barrierenotat fra 2017 /42/. Kapitlet om sikring fokuserer mye på fysisk sikring, men det påpekes avslutningsvis at det også er relevant for IKT-sikkerhet. Det er ikke åpenbart for aktørene hvordan de definerer uavhengige barrierer for IKT-sikkerhet, og det foregår en dialog mellom Ptil og aktørene om dette temaet.

4.3.6 Rapportering til tilsynet

Aktørene informerte at de utelukkende rapporterer hendelser som fører til driftsforstyrrelser i OT-systemene, dette er tråd med SF §29. Hendelser i IT-systemene rapporteres ikke, dette medfører at hendelser av den typen som Hydro opplevde i 2019 der et løsepengevirus førte til omfattende problemer, ikke vil bli rapportert til Ptil dersom problemet er begrenset til bedriftens IT-systemer.

Antall hendelser som berører OT-systemene så langt antas å være lavt, men siden det ikke innhentes informasjon om hendelser som ikke påvirker drift, finnes ikke en god oversikt over dette. Dette betyr at man ikke har tilgang til god statistikk for IKT-hendelser sammenlignet med HMS-relaterte hendelser.

4.3.7 Samtykke fra tilsynet

Samtykke fra tilsynet som omfatter IKT-løsninger er blitt innhentet i forbindelse med fjerndrift av plattformer og fullautomatisering av boredekk. Når det gjelder endringer av rene IKT-løsninger, som også kan påvirke OT-systemene, informerer de fleste aktørene imidlertid om at det ikke vil være nødvendig å innhente samtykke fra Ptil. Et mulig eksempel brukt i intervjuene er optimalisering av produksjon ved bruk av algoritmer i en skyløsning. Ingen av aktørene tillater dette i dag, men det jobbes med å ta frem sikre løsninger for dette. De fleste aktørene informerer om at de tolker regelverket slik at de selv kan bestemme når en slik løsning er tilstrekkelig sikker og kan tas i bruk. Bare en av aktørene ga utrykk for at det er nødvendig å innhente samtykke fra Ptil i et slikt tilfelle.

Det er et behov for å klargjøre om § 25 i Styringsforskriften kommer til anvendelse i forbindelse med IKT-systemer, og i tilfelle når.

4.3.8 Beredskap, trening og øvelser

Intervjuer med aktørene viser at det er bevissthet rundt behovet for å ha god beredskap, trening og øvelser knyttet til IKT-sikkerhet. Det varierer hvor langt aktørene har kommet i dette arbeidet, men inntrykket er at man har kommet lengre på IT-siden enn på OT-siden. Særlig virker det å være et behov for å se på beredskap, trening og øvelser for hendelser som inntreffer på tvers av IT- og OT-systemene, da den ordinære beredskapsorganisasjonen for en installasjon ikke nødvendigvis er hensiktsmessig i et slikt scenario. Dette er videre beskrevet i to andre DNV GL-rapporter, henholdsvis «Trening og øvelse» /50/ og «Resiliens mot cyberhendelser og kan blokkjede bidra» /51/.

4.3.9 Evaluering av trusselbilde og bruk av CERT/CSIRT

De fleste virksomhetene holder seg oppdatert på det til enhver tid gjeldende trusselbildet gjennom egne vurderinger, kunnskap om reelle hendelser innenfor egen virksomhet og/eller sektor, og eventuelt andre sektorer. Det foregår blant annet endel uformelt samarbeide, der aktørene varsler hverandre dersom man får kjennskap til nye trusler.

Ellers holder de fleste seg oppdatert gjennom informasjon fra:

- NorCert som er en del av Nasjonal Sikkerhetsmyndighet (NSM). NorCert er koordinerende enhet for IKT-sikkerhetshendelser, dedikert til cybersikkerhet og hendelseshåndtering i NCSC (Nasjonalt cybersikkerhetssenter) som ble opprettet høsten 2019.
- Politiets Sikkerhetstjeneste (PST)
- Petroleum Industry Security Alert System (PISAS), som eies og administreres av Norsk olje og gass.

Når det gjelder bruk av responsmiljøer viser intervjuene at aktørene ser et behov for å være tilknyttet et CERT (Computer Emergency Response Team) eller CSIRT (Cyber Security Incident Response Team).

Noen store aktører har egne CERT/CSIRT miljøer, enkelte av disse er lokalisert utenfor Norge.

Det er noen aktører som har meldt seg på KraftCERT som illustrert nedenfor, mens andre aktører overveier medlemskap.

Aker BP tar cybergrep – allierer seg med kraftbransjen

Oljeselskapet blir medlem av kraftbransjens eget sikkerhetsselskap, KraftCERT, for å få tilgang til bedre trussel- og sårbarhetsinformasjon.

E24, 21.6.2019, /45/

SINTEF har i sin rapport, Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten /31/ anbefalt at KraftCERT utvides til også å håndtere IKT-hendelser i petroleumssektoren. På den ene side vil dette kunne være svært krevende for KraftCERT hvis det inntreffer en IKT-hendelse som rammer både kraftsektoren og petroleumssektoren. På den annen side vil et slikt sektorovergripende CERT lettere kunne oppdage at det er den samme hendelsen som rammer flere aktører på tvers av de to industriene.

Fra SINTEFs rapport, Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten /31/:

«SINTEF anbefaler opprettelse av "Olje-ISAC", samt styrking av KraftCERT som en del av et nasjonalt cybersikkerhetssenter, for håndtering av IKT-sikkerhetshendelser i petroleumsnæringen. IKT-sikkerhetskompetansen i Norge er så begrenset at det ikke er rom for å lage en egen olje-CERT. Et styrket*

KraftCERT kan bli en viktig ressurs for petroleumsnæringen. Det vil også være lettere å styrke et eksisterende fagmiljø enn å starte et nytt sektorvist responsmiljø innenfor IKT-sikkerhet for petroleum. En Olje-ISAC vil redusere avhengigheten av personlige nettverk for informasjonsdeling, noe som vil være en fordel for de mindre aktørene, og for virksomheter som ikke har bygget opp interne fagmiljø på IKT-sikkerhet.

Vi ser et sterkt behov for at alle aktørene, både oljeselskaper og CERT-aktører, samordner tilnærmingen til IKT-sikkerhet i IT- og OT-systemer siden det i dag er betydelige forskjeller i begrepsbruk, modenhet i tekniske løsninger, og kultur.

Ptils dialog- og tillitsbaserte tilsynsmetodikk innen IKT-sikkerhet synes egnet til å skape oppmerksomhet og spre læring på tvers i næringen. Etaten bør vurdere å konkretisere ytterligere hvilke IKT-relaterte hendelser som omfattes av plikten til å varsle driftsforstyrrelser, samt etablere et mer formelt kunnskapsgrunnlag om IKT-sikkerhet i næringen som grunnlag for risikobasert tilsyn.»

*ISAC: "An Information Sharing and Analysis Center or (ISAC) is a nonprofit organization that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector."

Ref. /48/

Som beskrevet i 4.3.8 varierer det hvor langt de forskjellige aktørene har kommet i arbeide med å etablere beredskap, trening og øvelser knyttet til IKT-sikkerhetshendelse, og det anbefales at dette temaet adresseres tidligere i veiledningene til paragrafene i regelverket som omhandler beredskap. Se også 4.5. som inneholder en liste med forslag til oppdateringer.

I denne sammenhengen bør det også vurderes å stille krav til bruken av CSIRT og CERT-miljøer for å sikre rask respons og tilgang på kompetente ressurser når en hendelse inntreffer, samt til overvåking og deling av relevant informasjon og erfaringer mellom relevante aktører.

4.3.10 Ny teknologi som utfordrer sonemodellen

Aktørene som har vært intervjuet har påpekt at automatisk oppdatering av prosesstyringsparametre i OT-systemer fra algoritmer som ligger i IT-systemene eller i skyen er noe som etter hvert vil komme, selv om ingen av aktørene tillater dette i dag.

Sonemodellen blir alt i dag utfordret av leverandører som vil levere «ytelse som tjeneste» (Performance as a Service).

Det vil være behov for å etablere en Anbefalt Praksis for hvordan slike teknologier kan tas i bruk på en måte som ikke påvirker sikkerheten negativt.

4.4 Forhold til sikkerhetsloven

Foreløpig er det ikke besluttet i hvilken grad sikkerhetsloven av 1.1.2019 skal gjøres gjeldende for petroleumssektoren.

4.5 Forslag til oppdatering av regelverket

Intervjuene med aktørene indikerer at det arbeides godt med å forbedre IKT-sikkerheten i bransjen. I så måte virker forutsetningene for å benytte et funksjonsbasert regelverk, som diskutert i 4.1, fortsatt å være tilstede.

Generelt sett bør imidlertid IKT-sikkerhet adresseres mer tydelig i regelverket, som i denne sammenheng omfatter Ptils forskrifter med tilhørende veiledninger. Dette kapitelet inneholder forslag til hvordan dette kan gjøres.

Regelverket er bygd opp slik at RF, SF og innledende kapitler i IF og TOF inneholder overordnede krav som gjelder for mange systemer/forhold, mens kapittel III og påfølgende kapitler i IF og TOF har paragrafer for spesifikke systemer/forhold. Relevante nasjonale og internasjonale standarder identifiseres i veilederne til forskriftene, og disse vil typiske inneholde omfattende sett med langt mer detaljerte krav enn det som finnes i selve regelverket. Foreslåtte enderinger er tilpasset denne oppbyggingen.

Når man arbeider i et spesifikt prosjekt, eksempelvis en systemendring, vil det være åpenbart hvilke paragrafer for spesifikke systemer/forhold som gjelder, men det kan være mer krevende å identifisere alle overordnede krav som også kommer til anvendelse i prosjektet. Relatert til dette har Ptil i et brev til næringen identifisert et antall paragrafer som anses å være relevante for IKT-sikkerhet, se Tabell 4-1. I de fleste av disse paragrafene er ikke IKT-sikkerhet nevnt, og brevet begrunner kort hvorfor IKT-sikkerhet likevel er relevant for disse paragrafene.

I tillegg til de paragrafer Ptil selv har identifisert, har DNV GL identifisert et antall andre paragrafer som også anses relevante. Disse er listet opp i Tabell 4-3 med en kort redegjørelse for hvorfor de anses relevante. Tabell 4-3 inneholder også paragrafene PTIL selv har indentifisert, slik at denne tabellen inneholder alle paragrafer i regelverket som anses relevante for IKT-sikkerhet. For hver paragraf i tabellen er det lagt på anbefalinger, se pkt. 2 nedenfor.

Vi foreslår som et minimum følgende oppdateringer:

1. Det foreslås å lage en egen veileder for IKT-sikkerhet, for de paragrafene i regelverket som anses relevante for IKT-sikkerhet, etter mal fra NVEs veileder til Kraftberedskapsforskriften. Tabell 4-2, og Tabell 4-3, kan brukes som utgangspunkt for arbeidet med en slik veileder. En slik veileder bør også drøfte hvordan konfidensialitet og integritet av OT-data og systemer skal klassifiseres og ivaretas. For noen utvalgte temaer kan det vurderes å lage særskilte veiledere.

2. Anbefalingene i Tabell 4-3 foreslår i mange tilfeller både å legge til en presisering i de eksisterende veilederne til regelverket, samt å utdype temaet i den foreslåtte separate IKT veilederen. For mange av de overordnede kravene i regelverket er imidlertid abstraksjonsnivået i eksisterende veiledere så høyt at det ikke er naturlig å peke på IKT-sikkerhet spesielt, uten også peke på andre tema. I slike tilfeller foreslås temaet kun adressert i den separate IKT veilederen.

3. Generelt foreslås det å referere tydeligere til anerkjente standarder som NIST CSF og IEC 62443, samt peke på bransjestandarder som NOROG 104, NOROG 110, NOROG 123 og DNVGL-RP-G108. Det vil være ekvivalent med måten Ptils regelverk referer til IEC 61508 og IEC 61511, med bransjestandarder som NOROG 070 og NORSOK S-001.

4. Det foreslås at veiledningene til regelverket referere til ISO 27000-serien for IKT-sikkerhet for IT-systemer som potensielt kan påvirke de industrielle systemene negativt.

5. Aktørene som har vært intervjuet har påpekt at automatisk oppdatering av prosesstyringsparametre i OT-systemer fra algoritmer som ligger i IT-systemene eller i skyen er noe som etter hvert vil komme, selv om ingen av aktørene tillater dette i dag. Sonemodellen blir alt i dag utfordret av leverandører som vil levere «ytelse som tjeneste» (Performance as a Service). Det anbefales å etablere et prosjekt sammen med industrien som ser spesifikt på behovet for regelverk og anbefalte praksiser for dette.

Tabell 4-3 - Paragrafer i forskriftene som DNV GL anbefaler å tydeliggjøre i forhold til IKT-sikkerhet

Pgf.	Tittel	Redegjørelse og anbefaling
SF § 4	Risikoreduksjon	Presisering fra Ptil: Dette innebærer at det velges løsninger for IKT- sikkerhet som reduserer sannsynligheten for IKT-angrep som forårsaker skade, feil eller faresituasjoner. Anbefaling relatert til SF § 4 Det anbefales at Ptils presisering tas inn i foreslått separat IKT-sikkerhet veileder til regelverket.
SF § 5	Barrierer	Det refereres til SF § 5 fra SF § 4, slik at dette implisitt er dekket i Ptils anbefaling i SF §4. Imidlertid er barrieretankegang en svært sentral del av IKT-sikkerhet og bør framheves eksplisitt. Anbefalinger relatert til SF § 5: 1. Det foreslås at IKT-sikkerhet nevnes som en barriere, og at relevante standarder for dette nevnes i veilederen til SF § 5 på samme måte som det er gjort for sikkerhetssystemer i dagens veileder. 2. I tillegg foreslås det å beskrive barrierefilosofi for IKT-sikkerhet i foreslått separat veileder til regelverket.
SF § 8	Interne krav	Presisering fra Ptil: Det må settes krav til hvordan IKT-sikkerhet håndteres, både teknisk, operasjonelt og organisatorisk. Anbefaling relatert til SF § 8 Det anbefales at Ptil sin presisering ang IKT-sikkerhet tas inn i foreslått separat veileder til regelverket.

Pgf.	Tittel	Redegjørelse og anbefaling
SF § 14	Kompetanse	I veiledningen står det følgende: «*Kompetanse som nevnt i første ledd, omfatter både individuell kompetanse og gruppekompetanse, deriblant fagkompetanse, systemkunnskap og helse-, miljø- og sikkerhetskompetanse*» Anbefalinger relatert til SF § 14: 1. Det foreslås å presiseres at sikkerhetskompetanse, som nevnt i dagens utgave av veilederen til styringsforskriften, også omfatter funksjonell sikkerhet og IKT-sikkerhetskompetanse. 2. Det foreslås at temaet IKT-sikkerhetskompetanse inkluderes i foreslått separat veileder til regelverket.
SF § 17	Risikoanalyser og beredskaps-analyser	IKT trusler og sårbarheter vil være et område som er gjenstand for risikoanalyse. Kanskje også med egne trussel og risikoanalyser som dekker både IT og OT, som må gjennomføres jevnlig. IKT utvikler seg fort og det tilkommer stadig nye trusler og sårbarheter. Dessuten kjennetegnes spesielt OT-systemer av mangel på programvareoppdateringer og sikkerhets-patching. Anbefaling relatert til SF § 17: Det foreslås at temaet risikoanalyser inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
SF § 25	Samtykke	Aktørene i bransjen har forskjellig oppfatning om når samtykke fra Ptil vil være relevant for IKT relaterte løsninger. Anbefaling relatert til SF § 25 Det er et behov for å klargjøre om § 25 i Styringsforskriften kommer til anvendelse i forbindelse med IKT-systemer, og i tilfelle når.

Pgf.	Tittel	Redegjørelse og anbefaling
SF § 29	Varsling og melding til tilsynsmyndighetene av fare- og ulykkessituasjoner	Ifølge SF § 29 skal alt som forstyrrer driften varsles til Ptil. I veiledningen punkt i) pekes det spesielt på IKT-hendelser: «*i) situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse)*». Ptil har ikke mer detaljerte kriterier for hva som skal rapporteres av IKT-hendelser. Anbefaling relatert til SF § 25 1. Det foreslås å oppdatere veiledningen til SF § 25 til å si at IKT-sikkerhetshendelser i OT-domenet som ikke fører til driftsforstyrrelser, men som har potensiale for å skape slike situasjoner også rapporteres. Det samme gjelder alvorlige hendelser i IT-domenet. 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 21	Kompetanse	Presisering fra Ptil: Kravet om kompetanse er også relevant for de som skal håndtere faresituasjoner i forhold til IKT- hendelse med de industrielle kontroll- og sikkerhetssystemene. Anbefaling relatert til AF § 21 1. Det foreslås å oppdatere veiledningen til AF § 21 i henhold til Ptils presisering ovenfor 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 23	Trening og øvelse	Presisering fra Ptil: Kravet om trening og øvelser er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhetssystemene og samhandle med responsmiljøer. Anbefaling relatert til AF § 23 1. Det foreslås å oppdatere veiledningen til AF § 21 i henhold til Ptils presisering ovenfor 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet

Pgf.	Tittel	Redegjørelse og anbefaling
AF § 26	Sikkerhetssystemer	Også IKT-sikkerhetsbarrierene kan svekkes ved avvikssituasjoner Anbefaling til AF §26 1. Veilederen til AF § 26 Bør synliggjøre at IKT-sikkerhet også er relevant for å ivareta barrierefunksjon ved avvikssituasjoner. 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 45	Vedlikehold	Presisering fra Ptil Oppdatering og patching av programvare når det oppdages sikkerhetssvakheter er å forstå som vedlikehold. Anbefaling til AF § 45 Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 46 TOF § 59	Klassifisering	AF: *«Innretningers systemer og utstyr skal klassifiseres med hensyn til konsekvensene for helse, miljø og sikkerhet av potensielle funksjonsfeil.»* TF: *«Systemer og utstyr skal klassifiseres med hensyn til konsekvensene for helse-, miljø- og sikkerhet av potensielle funksjonsfeil.»* Også IKT-systemer bør klassifiseres med tanke på hvor kritiske de er. At OT-systemer er kritiske er ofte selvsagt, men også mer administrative IT-systemer som inngår i leveransekjeden, kan vise seg å være svært kritiske. Hvis et slikt system blir rammet av en hendelse, kan det ha store konsekvenser, selv om OT-systemene fungerer som de skal. Det finnes en retningslinje for klassifisering av systemer, NOROG 123, ref. /35/. Denne er ikke referert noe sted i Ptils forskrifter eller veiledninger. Anbefalinger til AF § 46 og TOF § 59 1. Det foreslås at NOROG 123 refereres i veiledningen til disse paragrafene 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet

Pgf.	Tittel	Redegjørelse og anbefaling
AF § 47	Vedlikeholdsprogram	Behovet for å vedlikeholde IKT-systemer i kontekst IKT-sikkerhet bør synliggjøres. Eksempelvis patching, antivirusoppdatering m.m. Anbefaling til AF § 47 1. I veiledningen til AF § 47 foreslås å legge til en referanse til relevante IKT-sikkerhetsstandarder på lik linje med det som er gjort for sikkerhetssystemer, der det henvises til IEC 61508 og NOROG 070. 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 48	Planlegging og prioritiering	Presisering fra Ptil Kravet om planlegging innebærer en systematikk for hvordan selskapet har kontroll på hvilke oppdateringer som er relevante og hvilke utstyrskomponenter som må ha vedlikeholdsprogram. Anbefaling til AF § 48 Det anbefales at Ptils presisering tas inn i foreslått separat IKT-sikkerhet veileder til regelverket.
AF § 73 TOF § 64	Beredskapsetablering	Det bør være et obligatorisk krav å ha etablert beredskap som er i stand til å reagere ved IKT-sikkerhetshendelser i både IT og OT domenet. Det bør også vurderes å stille krav til bruken av CSIRT og CERT-miljøer for å sikre rask respons og tilgang på kompetente ressurser når en hendelse inntreffer, samt til overvåking og deling av relevant informasjon og erfaringer mellom relevante aktører. Tilsvarende bør det vurderes hvordan leverandører best kan utnyttes i en beredskapssituasjon. Anbefaling til AF § 73 1. Behovet for å involvere personell or organisasjoner som har kunnskap om IKT-sikkerhet foreslås synligjort veilederen til AF § 73 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet

Pgf.	Tittel	Redegjørelse og anbefaling
AF § 74	Felles bruk av beredskapsressurser	*«Ved samarbeid om felles bruk av ulike operatørers beredskapsressurser skal samarbeidet avtalefestes.»* Anbefaling til AF § 74 1. I veiledningen til til AF § 74 anbefales det å presisere at denne paragrafen også er gjeldende for IKT-sikkerhet. 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 75 TOF § 65	Beredskapsorganisasjon	Beredskapsorganisasjonen må også kunne håndtere IKT-sikkerhetshendelser på en effektiv måte. IKT må utgjøre en del av operatørens beredskapsorganisasjon. Anbefaling til AF & 75 1. I veiledningene til paragrafene evnes eksempler på nødvendige funksjoner. Det foreslås at IKT-sikkerhet legges til listen. 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet
AF § 76 TOF § 66	Beredskapsplaner	IKT-sikkerhetshendelser bør utgjøre noen av de definerte situasjonene/scenariene med tilhørende aksjonsplaner. Scenarioer hvor prosesskontrollsystemene, og etter hvert også de uavhengige sikkerhetssystemene kan være eller er kompromittert, bør inngå i beredskapsplan. Anbefaling til AF § 74 og TOF § 66 1. IKT-hendelser foreslås inkludert på listen over hva beredskapsplaner skal inneholde i veiledningen til paragrafene. 2. Det foreslås at temaet inkluderes i foreslått separat veileder til regelverket for IKT-sikkerhet. For input til denne når det gjelder beredskap se også DNV GL-rapportene «Trening og øvelse» /50/ og «Resiliens mot cyberhendelser og kan blokkjede bidra» /51/.

Pgf.	Tittel	Redegjørelse og anbefaling
AF § 77 TOF § 67	Håndtering av fare- og ulykkessituasjoner	Også alvorlige IKT-sikkerhetshendelser bør håndteres som en farlig situasjon og integreres i aktørens ordinære krisehåndteringsplaner. Anbefaling til AF § 77 og TOF § 67 Det anbefales at håndtering av fare- og ulykkessituasjoner som skyldes IKT-hendelser, tas inn i foreslått separat IKT-sikkerhet veileder til regelverket.
IF § 8 TOF § 10	Sikkerhetsfunksjoner	Det bør synliggjøres at IKT-sikkerhet også er relevant for sikkerhetsfunksjonene. Anbefalinger til IF § 8 og TOF §10 1. I veiledningen til disse paragrafene foreslås det referere tydeligere til anerkjente standarder som NIST og IEC 62443, samt peke på bransjestandarder som NOROG 104, NOROG 110, NOROG 123 og DNVGL-RP-G108. 2. Det anbefales at IKT-hendelser knyttet til sikkerhetssystemer adresseres i foreslått separat IKT-sikkerhet veileder til regelverket
IF § 9 TOF § 9	Kvalifisering og bruk av ny teknologi og nye metoder.	Behovet for å ivareta IKT-sikkerhet i et miljø hvor ny teknologi introduseres i et stadig økende tempo bør synliggjøres Anbefaling til IF § 9 Det anbefales at håndtering av IKT-hendelser, tas inn i foreslått separat IKT-sikkerhet veileder til regelverket.
IF § 18 TOF § 22	Systemer for intern og ekstern kommunikasjon	Det bør synliggjøres at IKT-sikkerhet også er relevant for interne og eksterne kommunikasjonssystemer. Anbefalinger til IF § 18 og TOF §22 1. I veiledningen til disse paragrafene foreslås det referere tydeligere til anerkjente standarder som NIST og IEC 62443, samt peke på bransjestandarder som NOROG 104, NOROG 110, NOROG 123 og DNVGL-RP-G108. 2. Det anbefales at IKT-hendelser knyttet til kommunikasjonssystemer adresseres i foreslått separat IKT-sikkerhet veileder til regelverket.

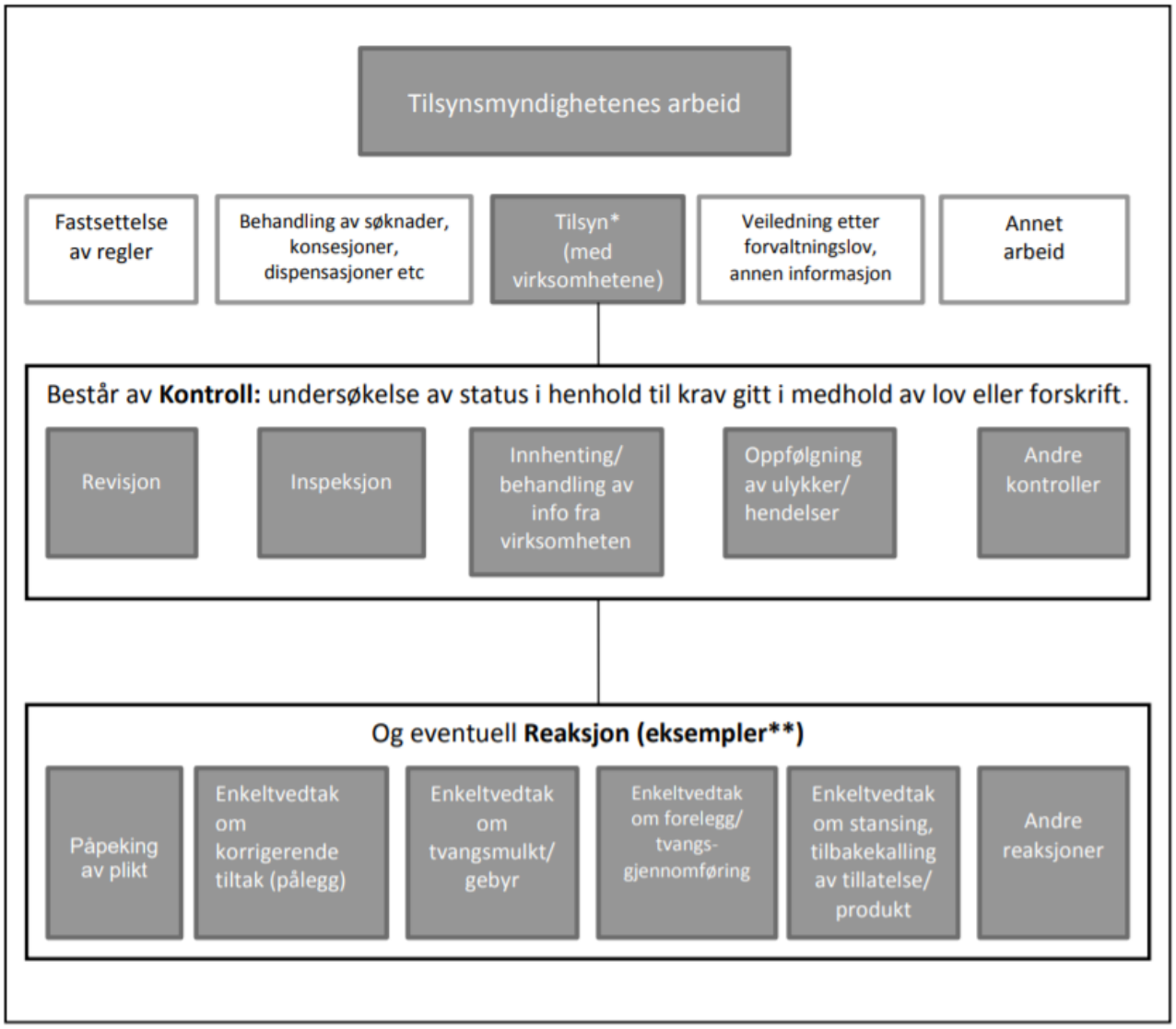
Pgf.	Tittel	Redegjørelse og anbefaling
IF § 32-34 TOF § 32-34	Sikkerhetssystemer	Presisering fra Ptil Kravet om at grensesnitt mot andre systemer ikke skal påvirke negativt innebærer at heller ikke IKT-angrep skal hindre at systemene kan utføre tiltenkte funksjoner. Anbefaling til IF §32-34 og TOF § 32-34 3. I veiledningen til disse paragrafene foreslås det referere tydeligere til anerkjente standarder som NIST og IEC 62443, samt peke på bransjestandarder som NOROG 104, NOROG 110, NOROG 123 og DNVGL-RP-G108. 4. Det anbefales at IKT-hendelser knyttet til sikkerhetssystemer adresseres i foreslått separat IKT-sikkerhet veileder til regelverket
IF § 34a TOF §33a	Kontroll og overvåkingssystemer	Presisering fra Ptil Veiledningen viser til anerkjent retningslinje, men også andre standarder kan benyttes. Anbefaling til IF § 34a og TOF § 33a 1. I veiledningen til disse paragrafene foreslås det referere tydeligere til anerkjente standarder som NIST og IEC 62443, samt peke på bransjestandarder som NOROG 104, NOROG 110, NOROG 123 og DNVGL-RP-G108. 2. Det anbefales at IKT-hendelser knyttet til kontroll og overvåkingssystemer er adresseres i foreslått separat IKT-sikkerhet veileder til regelverket

5 TILSYNSMETODIKK

Dette kapitlet beskriver dagens tilsynsmodell og diskuterer alternative tilsynsmodeller. Det inneholder også informasjon om hvordan andre relevante tilsynsmyndigheter gjennomfører sitt oppdrag. Avslutningsvis inneholder kapitlet DNV GL sine forslag til endringer knyttet til tilsynsmetodikken.

5.1 Tilsyn

Med referanse til figuren under hentet fra *Tilsynsmyndighetenes retningslinje for samordnet tilsyn og felles tilsynsprofil* /28/ består et tilsyn av «***Kontroll: undersøkelse av status i henhold til krav gitt i medhold av lov eller forskrift***.». Retningslinjen er utarbeidet av Arbeidstilsynet, DSB, Mattilsynet, Miljødirektoratet, Næringslivets sikkerhetsorganisasjon, Ptil, Statens helsetilsyn og Statens Strålevern i samarbeid.



Figur 5-1 – Grafisk fremstilling av begreper brukt i tilsyn (fra /28/)

**Tilsyn med virksomhetene i planleggings-, prosjekterings-, drifts- og eventuelt i avviklingsfasen.*
***Figuren viser kun eksempler på reaksjoner. Regelverket inneholder bestemmelser for hvilke reaksjoner de ulike etatene kan benytte seg av.*

Med kontroll menes revisjon, inspeksjon, innhenting/behandling av informasjon fra virksomheten, oppfølging av ulykker/hendelser og andre kontroller.

I tråd med dette skriver Ptil selv følgende om tilsyn:

«Tilsyn omfatter alle aktiviteter som gir oss grunnlag for å vurdere om, og følge opp at selskapene driver virksomheten sin forsvarlig og i tråd med regelverket.»

Tilsyn omfatter blant annet:

- Revisjoner og verifikasjoner på innretninger, landanlegg og byggeplasser
- Dialog og møter med næringen
- Datainnsamling om risiko, ulykker og hendelser
- Gransking av ulykker
- Behandling av samtykkesøknader
- Vurdering av utbyggingsplaner
- Samsvarsuttalelser (SUT) for flyttbare innretninger
- Aktørvurdering og konsesjonstildelinger
- Bruk av reaksjonsmidler

5.2 Dagens praksis

Gjeldende regelverk er funksjonsbasert og gir også en stor frihetsgrad for operatørene til å etablere løsninger de selv anser som best egnet, og som har endret seg i takt med hvilke løsninger som er tilgjengelige til enhver tid. Kombinasjonen med et funksjonsbasert regelverk med lav andel preskriptive krav, og stor variasjon i hvordan de tekniske løsningene er etablert innen regelverket, medfører store krav til både bredde- og dybdekompetanse knyttet til alle momenter hos tilsynsobjektet for at tilsynsoppgaven skal kunne gjennomføres med nødvendig kvalitet.

Tilsyn knyttet til IKT-sikkerhet er basert på samme metodikk og verktøy som Ptil gjør for øvrige sikkerhetsløsninger, og i noen sammenhenger er det slått sammen med øvrig tilsyn. Selve metodikken er i tråd med Figur 5-2 - Steg i et tilsyn.

Figur 5-2 - Steg i et tilsyn

5.2.1 Omfang av tilsyn forbundet med IKT-sikkerhet

Ptils ansvarsområde er illustrert i Figur 5-3. Ved årsskiftet 2018/19 var det 83 felt i produksjon på norsk sokkel. Det er 14 operatører som driver produksjon på sokkelen, i tillegg er det Gassco som koordinerer leveransene av gass til Europa, og operatører som driver med boring.

Figur 5-3– Ptils ansvarsområde (ref. /27/)

Ptil fører tilsyn med alle aktører i næringen, både operatører, entreprenører og redere i virksomheten. DNV GL har gjennomgått med Ptil hvordan tilsyn med IKT-sikkerhet utføres. Som underlag er også et brev om varsel om tilsyn benyttet /29/. Ptils tilsyn med fokus på IKT blir gjennomført som revisjoner og verifikasjoner. Noen hovedpunkter er:

- I 2007, begynte Ptil med en kartlegging for å få en oversikt over status på utvalgte kontroll og sikkerhetssystemer og sikring av disse. I samarbeid med SINTEF ble det den gang sendt ut en spørreundersøkelse som man ba selskapene besvare. Senere, i 2012, ble selskapene bedt om å fylle ut regnearket, NOROG 104 Self assessment ISBR /12/. Ptil ba dem om å kommentere resultatene, beskrive eventuelle tiltak og oversende oppsummeringsarket (ISBR Summary). IKT-sikkerhet har vært delelement i noen tverrfaglige tilsyn i perioden 2012 til 2019. Kontroller hos leverandørene med hovedfokus på IKT-sikkerhet startet opp i 2017.
- Ptil har hovedfokus på OT, og ikke på IT. Med OT forstås typisk SCADA, PLC/RTU og aktuatorer/ sensorer. Avgrensningen for Ptils fokusområde går i DMZ mellom kontornett (IT) og prosessnett (OT).
- Det er 60 rigger/innretninger og 8 landanlegg. Det gjennomføres få IKT-tilsyn i året. Det er planlagt fire slike revisjoner i 2020. Dette er lite når man ser på antall innretninger og anlegg innenfor Ptils ansvarsområde. For IKT-tilsyn har Ptil derfor konsentrert seg om å dekke flest mulig operatører og gamle og nye installasjoner som anses representative for de andre. Det er i dagens situasjon langt fra mulig å dekke alle installasjoner. Relaterer til dette forventer PTIL at operatørene korrigerer avvik fra en spesifikk kontroll på alle relevante installasjoner, noe operatørene i intervjuer har bekreftet at de vil gjøre. Avvik som måtte være unike for installasjoner og anlegg som ikke blir kontrollert vil ikke bli fanget opp med denne tilnærmingen. Hvor stor grad av variasjon det er mellom installasjonene, varierer fra operatør til operatør.
- Ptil planlegger ikke å gjennomføre egne IKT-tilsyn av leverandører. Det er særlig to store leverandører i det norske markedet som er representert i de fleste installasjoner. Disse har i

større eller mindre grad fjerntilgang til sine systemer for ulike formål. Operatørene er spesielt avhengige av sine leverandører for å rydde opp etter en IKT-hendelse. Leverandører er ikke med i beredskapsøvelser, men ved en skarp hendelse, er man avhengig av dem. Selv om det er operatørene som sitter med ansvaret, anbefales det å gjennomføre kontroller også hos leverandører.

- Ptil har en intern prosedyre for revisjon /33/. Denne gjelder generelt for alt tilsynsarbeid. Det er også laget en veileder til denne /34/. I Ptils prosedyre for revisjoner /33/ står det at den bygger på prinsippene i ISO 19011:2018.
- I tillegg er Ptil i ferd med å utarbeide en intern ytelsesstandard for IKT-revisjon. En slik standard vil gjøre IKT-revisjonene mer enhetlige og mindre personavhengig.

Andre typer løpende aktiviteter som Ptil utfører:

- Endringer og høringer av regelverk/direktiver.
- Samler inn data / foretar granskning av hendelser. Det har til nå vært svært få IKT-hendelser.
- Ptil promoterer IKT-sikkerhets-fagområdet i bransjen (eksempel eget CDS-forum).

5.2.2 IKT-tilsyn

Den generelle metoden for tilsyn er basert på systemrevisjon som beskrevet i det følgende. I tillegg kan Ptil gjennomføre uanmeldte inspeksjoner, men vi er ikke kjent med at dette er benyttet for IKT.

Vanligvis sender Ptil ut brev om varsel om tilsyn, der det redegjøres for revisjonsplan og hvilke paragrafer i forskriftene som er spesielt viktig med tanke på IKT.

Ptil får på forhånd tilsendt dokumentasjon fra den som er gjenstand for tilsyn. Dokumentasjonen er i form av tekniske krav til IKT-sikkerhet. Noen operatører bygger på NIST CSF, mens andre bygger på NOROG 104. Her er det bekymring fra noen av aktørene at Ptil også ber om teknisk dokumentasjon som skal og bør holdes unna offentligheten[2].

Hvem som skal intervjues plukkes ut ifra roller om bord i innretningen. Typiske roller relevant for IKT-revisjon er SAS ingeniør/tekniker, fagansvarlig automasjon og fagansvarlige for elektro, telekom, boring og brønn.

Tilsynet blir gjennomført med presentasjoner, samtaler med relevant personell, gjennomgang av dokumenter og verifikasjon av de industrielle IKT-systemer. Tilsynet hos en operatør omfatter typisk besøk på kontor på land og deretter verifikasjon på innretningen til havs eller landanlegget.

Det stedlige tilsynet gjennomføres i løpet av ca. en uke (fire dager i henhold til varselbrevet vi har sett), men med forberedelser og etterarbeid varer hvert tilsyn ca. en måned. Tilsynet gjennomføres av minimum to personer i Ptil.

På oppstartsmøtet, første dagen, får Ptil også innsyn i den mer installasjonsspesifikke dokumentasjonen.

Under verifikasjon av industrielle IKT-systemer sjekkes brannmuren mot OT-systemene, om den er konfigurert i samsvar med selskapets egne krav. Det gjennomføres stikkprøver med dump av brannmurens regelsett.

[2] Det var noe delt oppfatning blant selskapene om dette..

Avvik som blir avdekket, skal rettes opp av selskapet. Ptil godtar at selskapet selv rapporterer at avviket er lukket. Ptil vil sjekke dette ved senere tilsyn av selskapet. Dette kan ta lang tid siden det er få IKT-tilsyn per år.

5.2.3 Dialog med næringen

I forbindelse med IKT-sikkerhet jobber Ptil mot næringen på flere forskjellige måter. Med økt fokus på temaet benytter Ptil flere metoder for kommunikasjon og stimulering til tiltak for temaet IKT-sikkerhet i OT-systemer.

Herunder:

1. **Arrangement for ulike temaer knyttet til IKT-sikkerhet.**

Ptil har invitert alle relevante aktører til å delta på åpne arrangementer hvor det drøftes dagsaktuelle problemstillinger knyttet til IKT-sikkerhet. Dette gjøres ofte som halv- eller heldagsmøter med presentasjoner og diskusjoner. Topplederkonferansen 2019, for inviterte deltagere med beslutningsmyndighet, hadde et stort fokus på IKT-sikkerhet, og hvor det ble delt synspunkter og relevante erfaringer knyttet til temaet.

2. **Brev, nyhetsbrev og publikasjoner på nettsidene**

De produserer brev til næringen, samt åpne nyhetsbrev, artikler og kronikker fortløpende knyttet til aktuelle temaer. Rapporter fra IKT-tilsyn publiseres, i den grad det er mulig, på Ptils hjemmesider med delvis formål å gi andre mulighet til å forbedre sine løsninger.

3. **1 – 1 diskusjoner om IKT-sikkerhet med aktørene**

Ptil har jevnlig 1-1 møter med aktørene hvor ulike temaer drøftes. Herunder også temaer relatert til IKT.

4. **Fagfora PDS/CDS/Subesea kontroll/Sikkerhetssystemkonferansen.**

Ptil deltar aktivt i ulike fagfora knyttet til IKT-sikkerhet i OT-systemer, og holder ofte presentasjoner og innlegg hvor tilsynsrollens synspunkter synliggjøres. Næringen ønsker enda mer av denne type interaksjon med Ptil.

5. **Joint Industry Projects**

Ptil har uttalt at de stimulerer til og ønsker at sektoren går sammen for å utvikle og definere beste praksis og prosedyrer for IKT-sikkerhet tilpasset næringens behov. Og de deltar selv aktivt i arbeidet.

Samtlige aktører som ble intervjuet som del av dette prosjektet har gitt uttrykk for at de finner Ptils rolle som pådriver og stimulator til IKT-sikkerhetsarbeid nyttig og verdifullt.

5.2.4 Samtykkesøknader

Et eksempel på en IKT-endring som potensielt vil kunne kreve samtykke er en prosessoptimaliserings løsning som krever toveis kommunikasjon fra en skyløsning via IT-systemer til OT.

De fleste aktørene vurderer det slik at Ptil ikke trenger å samtykke til slike løsninger, dersom de selv anser løsningen som tilstrekkelig sikker. Kun en av operatørene vurderer at det er nødvendig å innhente samtykke fra Ptil dersom de avviker fra det som i dag er normal praksis knyttet til IKT-Sikkerhet.

Det bør avklares om samtykkeparagrafen (§ 25 i styringsforskriften) kommer til anvendelse i forbindelse med endringer i OT/IT-systemer. Se også Tabell 4-3 angående foreslåtte oppdateringer av regelverket.

5.2.5 Tilsynsorganets rolle ved alvorlige IKT-hendelser

Ifølge SF § 29 skal alt som forstyrrer driften varsles til Ptil. I veiledningen punkt i) pekes det spesielt på IKT-hendelser: «*i) situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse)*».

Ptil har ikke mer detaljerte kriterier for hva som skal rapporteres av IKT-hendelser. For eksempel er følgende hendelse ikke dekket: Administrative systemer i kontornettet på en eller flere innretninger som tilhører et selskap kan være infisert med skadevare som fører til problemer, uten at kontroll- og sikkerhetssystemer er direkte rammet.

Blant aktørene vi intervjuet var det ulikt syn på hva som skulle meldes til Ptil. Noen mente at for eksempel et løsepengevirus som lammet IT-systemene (og ikke OT) var selskapets eget problem, og ikke noe som skulle rapporteres. Andre mente at slike situasjoner også var noe som burde rapporteres.

En bekymring fra noen av aktørene er at Ptil kan offentliggjøre informasjon om IKT-hendelser. Dette kan føre til økt sårbarhet, og kan også påvirke markedsinfo/finansinfo. Varslingsskjema inneholder ingenting om at opplysninger om IKT-hendelser skal være unntatt offentligheten. Noen aktører varsler derfor kun muntlig til Ptil, for å holde dem orientert.

Ptil har ikke noen aktiv rolle ved beredskapssituasjoner som skyldes IKT-hendelser, annet enn å bli informert, og eventuelt undersøke hendelsen i etterhånd.

5.2.6 Reaksjonsmidler

I henhold til gjeldende forskrifter er det identifisert at bare RF § 72 omhandler reaksjonsmidler. Denne paragrafen inneholder følgende bestemmelse:

«Bestemmelser om straff og andre reaksjonsmidler som går fram av helse-, miljø- og sikkerhetslovgivningen gjelder ved brudd på krav som er gitt i og i medhold av denne forskriften og utfyllende forskrifter.»

Ptil opplever at operatørene gjennomfører tiltak basert på funnene i tilsynsrapportene, og det har så langt ikke vært nødvendig å ty til reaksjonsmidler angående IKT-sikkerhet.

RF § 67: *Tilsynsmyndighetene kan på sine respektive myndighetsområder pålegge operatøren å få gjennomført, eller eventuelt selv å gjennomføre verifikasjoner, jf. § 19*.

5.3 Relevante retningslinjer

Ptils interne dokument *Tilsynsmyndighetenes retningslinje for samordnet tilsyn og felles tilsynsprofil* /28/ inneholder også en kort retningslinje for tilsyn (kapittel 3) og i tillegg en veiledning for revisjon (Vedlegg II).

Relevante retningslinjer for tilsyn kan være ISO 19011:2018 /5/ og ISO/IEC 27007:2017 /6/. Disse gir retningslinjer for revisjoner. Figuren under illustrerer relasjonen mellom dem.

Figure 5-1 – Illustrasjon av forholdet mellom ISO 19011 og ISO/IEC 27007

ISO/IEC 27007 /56/ henviser til punkter i ISO 19011:2018 *Retningslinjer for revisjon av ledelsessystemer* /5/, som er generiske for revisjonsprosessen. I tillegg inneholder ISO/IEC 27007 spesifikke punkter for revisjon av et ISMS (Information Security Management System), som kan være nyttig under et tilsyn med vekt på IKT-sikkerhet.

5.4 Tilsynsmodeller

Dersom man ser på hvordan tilsyn med kritiske systemer og infrastruktur for IT blir gjennomført, kan man grovt sett snakke om tre modeller for tilsyn, hvor de tre modellene også kan kombineres i større eller mindre grad:

- Modell 1 – Tilsynsmyndigheten utfører et aktivt tilsyn
- Modell 2 – Tilsynet baseres på bruk av selvdeklarering
- Modell 3 – Tilsyn basert på bruk av tredjepart
    - Modell 3a – Samsvarsvurderingsorgan
    - Modell 3b – Uavhengig tredjepart

Modellene er beskrevet nærmere i de følgende underkapitler.

5.4.1 Modell 1 - Aktivt tilsyn

Ved aktivt tilsyn vil tilsynsmyndigheten gjennomføre og følge opp tilsyn direkte med operatøren. Denne modellen regnes som den mest omfattende og ressurskrevende for tilsynsmyndigheten. Kvaliteten av tilsynet er i stor grad avhengig av omfanget og dybden i gjennomføringen, samt frekvensen av tilsyn og detaljkompetansen til tilsynsmyndigheten.

5.4.2 Modell 2 - Selvdeklarering

Ved å benytte selvdeklarering vil operatøren være ansvarlig for å rapportere selv til tilsynsmyndigheten at de oppfyller et sett med sikkerhetskrav. Sikkerhetskravene må defineres på forhånd og det er deretter opp til operatør å bekrefte at kravene oppfylles. Hvordan kravene oppfylles kan dokumenteres på mange ulike måter, og Ptil kan selv definere hva som anses som godt nok som bevis for hvordan kravene oppfylles.

Modellen anses som mindre omfattende og ressurskrevende for tilsynsmyndigheten. Hovedoppgaven til tilsynet vil være å evaluere mottatt dokumentasjon, samt gjennomføre stikkprøver innenfor et prioritert utvalg av områder.

Mekanismen med selvdeklarering benyttes blant annet for å oppfylle sikkerhetskrav i Norm for informasjonssikkerhet Helse- og omsorgstjenesten (Normen /36/). Den benyttes også for elektronisk identitet(eID) og tillitstjenester.

Når det innføres nye kritiske kontrollsystemer innenfor eksempelvis Jernbane og Luftfart, vil det være et betydelig element av selvdeklarasjon med i bildet. Tilsynene vil akseptere at systemene tas i bruk først og fremst basert på at mottatt dokumentasjon sannsynliggjør at sikkerhetskravene er oppfylt.

Et viktig trekk ved disse to industriene er at det stilles krav til uavhengighet i teknisk verifikasjon og validering, og at kravene til uavhengighet varierer med hvor kritiske systemene er.

Et eksempel på uavhengighet i valideringsrollen er Bane NORs sluttkontrollører for signal og sikringsanlegg. Disse rapporter til uavhengig sakkyndig leder innenfor fagområdet, og det er denne lederen som gir tillatelse til å sette anlegg i drift. Merk at Jernbanen også stiller krav til Independent Safety Assessor (ISA). Denne vil som oftest være organisatorisk uavhengig.

5.4.3 Modell 3 – Bruk av tredjepart

Tilsynets hovedoppgave vil i denne modellen være å ha et eget overordnet ansvar for å verifisere og bekrefte tredjepartens konklusjoner og behandle øvrig informasjon fra operatøren.

5.4.3.1 Modell 3a – Akkreditert Samsvarsvurderingsorgan

Et samsvarsvurderingsorgan er en akkreditert[3] tredjepart som gjennomfører en uavhengig vurdering av løsninger og prosesser mot et sett med kriterier, og produserer en rapport eller sertifikat som benyttes som dokumentasjon på tilstanden til løsningen. I denne modellen er det samsvarsvurderingsorganet som innehar detaljkunnskap og kan vurdere hvor gode løsningene er. Dersom en etablerer kriterier etter anerkjente internasjonale standarder, vil en kunne benytte akkrediteringsløsninger for å sikre nødvendig kvalitet hos samsvarsvurderingsorganet.

Bruk av tredjepart er vanlig for maritime fartøy, der klassifiseringsselskaper som DNV GL opptrer på vegne av sjøfartsmyndighetene i en rekke land, også i Norge. Dette kan omfatte regler både for «flag state», hvor fartøyet er registrert, og spesielle regler for «port state», hvor fartøyet skal gå i havn.

Innenfor maritime, jernbane og mange andre industrier, har man bruk av såkalte Notified Bodies. Dette er på norsk et "kontrollorgan", og er et uavhengig organ som sikrer og verifiserer at produsenter følger EUs regelverk og direktiver innenfor spesifikke områder.

3 Kilde Norsk Akkreditering:
Akkreditering er den formelle anerkjennelsen fra et akkrediteringsorgan til et samsvarsvurderingsorgan av deres tekniske og organisatoriske kompetanse til å utføre spesifikke tjenester i henhold til standarder og normative krav slik som beskrevet i deres akkrediteringsomfang.

Tillitstjenester og eID baseres på løsninger med høye krav til sikkerhet. For utstedere/operatører har det lenge vært benyttet en selvdeklarasjonsordning. Denne er nå i stor grad erstattet med samsvarsvurderingsorgan, i stor grad fordi en ikke oppnådde nødvendig tillit ved bruk av selvdeklarasjon.

5.4.3.2 Modell 3b – Ikke-akkreditert uavhengig tredjepart

En uavhengig tredjepart kan benyttes der det ikke finnes akkrediteringsordninger for sektoren, samt i tillegg til akkrediterte ordninger, et antall eksempler er nevnt nedenfor:

Innenfor maritime utfører klassifiseringsselskaper som DNV GL sertifisering i henhold til egne regler, på oppdrag fra reder. Disse reglene tar opp i seg regler fra the International Maritime Organisation (IMO). Det finnes mange forskjellige klassenotasjoner som gjøres gjeldene avhengig av fartøyets bruksområde. Det finnes også frivillig klassenotasjoner for redere som ønsker å gå utover minimumskravene. Over tid kan bruk av spesifikke frivillige notasjoner bli så vanlig i næringen at de endrer status til å bli obligatoriske. DNV GL tilbyr i øyeblikket Cyber Class som en frivillig klassenotasjon.

Innenfor olje & gass benyttes såkalt Functional Safety Assessor (FSA) der hvor uavhengige nødsystemer brukes til å redusere risiko ned til et akseptabelt nivå. Denne rollen tilsvarer jernbanens ISA som nevnt i forrige kapittel.

- Krav om bruk av FSA kommer inn gjennom standardene IEC 61511 og IEC 61508 som refereres i veiledningene til Ptils regelverk. Formelt krever standardene bruk av FSA kun for nødsystemer hvor det stilles krav om Safety Integrity Level (SIL) 3 og høyere[4], men aktørene velger likevel ofte å benytte FSA for systemer med lavere SIL-krav.
- En person som arbeider som FSA vil ofte ha en personlig sertifisering som viser at vedkommende har tilstrekkelig kompetanse.
- I siste utgave av IEC 61511 fra 2016 stilles det krav om «security risk assessment» som en del av den totale prosessen for risikoanalyse, og det betyr at security også er blitt et relevant tema for FSA.
- For sikkerhetssystemer innenfor olje & oass er det også utstrakt bruk av komponenter som er sertifiserte som SIL kapable i henhold til IEC 61508 av organisasjoner som TÜV, Exeda, o.l. For komplekse komponenter som f.eks. «safety controllers» er dette er en svært krevende prosess.

Jernbanestandarder som EN 50126 er avledet fra IEC 61508 og har krav om Independent Safety Assessor[5] (ISA). Denne rollen tilsvarer FSA. Et akkreditert Notified Body som beskrevet i forrige kapittel vil ofte også opptre som ISA.

I luftfart benytter det amerikanske FAA (Federal Aviation Authorities) seg av såkalte «designated engineering» representatives. Se faktaboks under:

> *"These designees are private individuals who act as representatives of the FAA. Some of these designees are company employees who are authorized to act on behalf of the FAA only for their company, and some are independents who may work for any client."* /53/

4 I praksis er SIL3 det strengeste kravet som stilles til nødsystemer av den typen som brukes innenfor Olje & Gass. SIL4 krav er typisk for systemer hvor hovedkontrollfunksjonen kontinuerlig må sørge for sikker tilstand, og operatør ikke forventes å kunne avverge en ulykke dersom systemet feiler. Signal og sikringssystemer som brukes på jernbanen er et eksempel på denne type system.

5 FSA og ISA er begreper som brukes innen ulike standarder og bransjer for omtrent samme sak. For eksempel: Olje & gass, prosessindustri og bilbransjen bruker FSA; jernbane benytter ISA.

5.4.4 Vurdering av modellene

Nedenfor er en vurdering av de tre modellene oppsummert i en tabell.

Tabell 5-1 Vurdering av de tre modellene for tilsyn

Modell	Fordeler	Ulemper	Kommentarer
1. Aktivt tilsyn	Tilsynsmyndigheten kan opparbeide seg erfaring og kompetanse over lengre tid. Man slipper ulempene som er identifisert for modellene selvdeklareringer og tredjepart.	Tilsynsmyndigheten kan mangle kompetanse innen viktige områder. Kan være kostbart å vedlikeholde og fornye kompetanse over tid. Krever stor kapasitet for IKT-tilsyn	Krever høy kompetanse og tilstrekkelig med ressurser hos tilsynet. Dette er modellen som har vært brukt ved IKT tilsyn i 2018 og 2019
2. Selvdeklarering	Den enkelte aktør bør best kjenne sin egen virksomhet. Mindre omfattende og ressurskrevende for tilsynsmyndigheten. Kan medføre at Ptil får frigjort kapasitet til å gjennomføre rettede IKT-tilsyn. Man slipper ulempene som er identifisert for modellene aktivt tilsyn og tredjepart.	Kan være stor forskjell i kompetanse mellom ulike aktører innen cybersikkerhet. Basert på tillit – at aktøren er ærlig og oppriktig. Aktørene kan bli «blinde» for egne svakheter.	Krever stikkprøver og sterkt behov for reaksjons-mekanismer. Fungerer best dersom aktørene har et sterkt regime for verifikasjon og validering med tilstrekkelig uavhengighet i disse prosessene. Kan kombineres med andre modeller: Først selvdeklarering av mange aktører, deretter revisjon og verifikasjon av et mindre utvalg basert på resultatene fra undersøkelsen. PTILs bruk av NOROG 104 self-assessment, tilbake i 2012 er et eksempel på bruk av denne modellen

Modell	Fordeler	Ulemper	Kommentarer
3. Tredjepart	En tredjepart vil oppfattes som nøytral. En tredjepart kan få lettere tillit og en åpnere dialog med aktøren under tilsyn. Vil øke kapasitet på IKT-tilsyn Tilsynsmyndigheten kan fokusere på mer rettede kontroller. Tilsyn vil få tilgang på kompetanse som i dagens marked kan være vanskelig å skaffe gjennom. Man slipper ulempene som er identifisert for modellene aktivt tilsyn og selvdeklarering.	Tilsynsmyndigheten kan miste «hands on» kjennskap til viktige områder. Organisasjoner som utfører slike oppdrag kan havne i interessekonflikter, dersom de har andre typer oppdrag for aktørene som blir gjenstand for tilsyn. Tolkningsrommet i et funksjonsbasert regelverk kan være en utfordring. Bruk av tredjepart er enklere der regelverket peker på standarder som har mer detaljerte krav.	Det vil også være mulig å leie inn enkeltpersoner til å støtte tilsynets revisjonsvirksomhet
3a. Samsvars-vurderingsorgan	Mer standardisert gjennomgangen tredjepart kan få lettere tillit og en åpnere dialog med aktøren under tilsyn.		
3b. Uavhengig tredjepart	Kan skaffe ekstern ekspertise, skreddersydd for oppdraget, og som kan gå mer i dybden.En tredjepart kan få lettere tillit og en åpnere dialog med aktøren under tilsyn.		

Eksisterende modell hos Ptil er i praksis en blanding av Aktivt tilsyn og Selvdeklarering. Modeller som også innebærer bruk av tredjepart har vært diskutert i intervjuer med aktørene, men det synes å være bred enighet om at det funksjonsbaserte regelverket gjør at det ikke ligger godt til rette for at tredjepart skal håndheve det på vegne av tilsynet. Det tredjepart kan gjøre er å håndheve internasjonale standarder. Aktørene er imidlertid tvilende til om standardiseringen for de industrielle systemene er kommet langt nok til at dette i øyeblikket er farbar vei.

For å øke kapasiteten vil det være mulig for Ptil å leie inn enkeltpersoner med riktig kompetanse som ekspertrevisorer for å gi støtte til Ptils revisjonsleder, slik som for eksempel NKOM gjør i eKOM-bransjen. Da trenger ikke revisjonsleder å ha samme dybdekompetanse og det vil potensielt være flere personer hos Ptil som kan opptre som leder for IKT-orienterte revisjoner.

En utfordring med denne modellen kan være at det å arbeide for tilsynet vil kunne legge begrensninger på hva IKT-sikkerhetsekspertens organisasjon kan gjøre av rådgivningstjenester mot aktørene som er gjenstand for tilsyn. Dersom Ptil ønsker å gå videre med denne modellen, bør det undersøkes i hvilken grad det finnes eksperter som er villige til å gå inn i en slik ordning.

En åpenbar fordel men denne modellen er at tilsynet vil kunne få tilgang på kompetanse som i dagens marked kan være vanskelig tilgjengelig gjennom faste ansettelser.

5.5 Erfaringer fra andre tilsynsmyndigheter

I underkapitlene nedenfor beskrives overordnet hvordan ulike tilsynsmyndigheter utøver IKT-tilsyn i noen relevante bransjer.

5.5.1 Norges vassdrags- og energidirektorat

Fra 1.1.2019 er kravene til IKT-sikkerhet skjerpet i og med den nye kraftberedskapsforskriften. Norges vassdrags- og energidirektorat (NVE) vil begynne å føre tilsyn med informasjonssikkerhet etter de nye reglene fra høsten 2019. De har laget en spørsmålsliste om IKT-sikkerhet som vil bli brukt ved tilsyn. De skriver selv om dette på sin hjemmeside /55/:

> «NVE har laget revisjonsspørsmål til bruk i arbeidet med tilsyn på IKT-sikkerhet. Spørsmålslisten kan være et hjelpemiddel i det interne sikkerhetsarbeidet i selskapene. NVE deler derfor denne listen med aktuelle brukere.
>
> Fordi kravene til IKT-sikkerhet er skjerpet i Kraftberedskapsforskriften som trådte i kraft 1.1 2019, har NVE utarbeidet et nytt spørreskjema som vil bli brukt under tilsyn. NVE deler nå dette spørreskjemaet fordi det kan være et av flere verktøy selskapene kan bruke for å arbeide med IKT-sikkerhet internt. NVE står selvsagt fritt til å kutte eller legge til nye spørsmål når vi gjennomfører tilsyn.
>
> Det er laget en midlertidig veiledning til kraftberedskapsforskriften som dekker de viktigste endringene. I tillegg gjelder fortsatt deler av den gamle veiledningen. Tilsyn etter de nye reglene vil tidligst skje høsten 2019.»

NVE gjennomfører mellom 40 og 50 revisjoner i året angående ulike scenarier, hvorav 8-10 angående IKT. NVE får tilsendt relevant dokumentasjon på forhånd (kryptert). Tilsynet av IKT gjennomføres typisk i løpet av en dag med foreløpige funn som presenteres tilsynsobjektet. Det lages en foreløpig tilsynsrapport som selskapet kan kommentere på, og en endelig tilsynsrapport (unntatt offentlighet[6]). NVEs tilsyn er stikkprøvebasert og går ikke i detalj inn på tekniske systemer. Selskapene må informere NVE om hva de har gjort for å lukke avvik.

NVE lager mange publikasjoner og veiledninger og slik bidrar til opplysning og forbedring av sikkerheten i bransjen. Nedenfor lister vi opp noen av de nyeste dokumenter med relevans for IKT-sikkerhet.

En veiledning om øvelser, som også omfatter fire IKT-scenarier:

> Øvelser – En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen /64/

[6] Informasjon i forbindelse med revisjoner er kraftsensitiv informasjon.

En rapport fra 2017 om regulering av IKT-sikkerhet. Dette var en forstudie for den nye utgaven av kraftberedskapsforskriften (2019):

> Regulering av IKT Sikkerhet - Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor /65/.

Opplæring for ungdom:

> CyberSmart /66/.

Faktaark over ulike hendelser fra 2018, deriblant IKT-hendelser:

> Oppsummering av uønskede hendelser 2018 i energiforsyningen /67/.

Faktaark om hva man kan finne av ting koblet mot internett. Dette er en oppskrift som selskapene selv kan gjøre bruk av for å finne ut hvor eksponert de er.

> Metode for å finne kraftsensitiv informasjon på Internett /68/.

I tillegg til å være tilsynsorgan har NVE også en førende rolle ved beredskapshendelser. NVE spiller også en aktiv rolle i store beredskapsøvelser. Det var egne IKT-øvelser i 2016 og 2018.

5.5.2 Nasjonal kommunikasjonsmyndighet

Nasjonal kommunikasjonsmyndighet (Nkom) sitt overordnede mål er å legge til rette for et likeverdig tilbud av sikre og grunnleggende elektroniske kommunikasjonstjenester og posttjenester av høy kvalitet og til rimelige priser over hele landet. Nkom skriver følgende om sin rolle i arbeid med sikkerhet og beredskap i nett:

«En viktig del av arbeidet til Nasjonal kommunikasjonsmyndighet (Nkom) er knyttet til sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester.

Nkom kartlegger og gjennomfører kontinuerlig tilsyn med Norges viktigste infrastruktur for elektronisk kommunikasjon. Hensikten er å følge med på den teknologiske utviklingen og gjøre vurderinger av eksisterende nivå for sikkerhet og beredskap.

I tillegg gjennomfører Nkom risiko- og sårbarhetsanalyser (ROS-analyser) av kritisk infrastruktur med formål å identifisere konkrete tiltak som etter gjennomføring vil øke det nasjonale sikkerhets- og beredskapsnivået.

Nkom både arrangerer og deltar på øvelser i sektoren og på tvers av sektorer, for å forbedre beredskapen og samhandlingen under krise- og beredskapssituasjoner. For tverrsektorielle øvelser samarbeider Nkom nært med Norges vassdrags- og energidirektorat (NVE), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM).

For øvrig har Nkom et utstrakt samarbeid med kraftbransjen, da kraftbransjen og ekombransjen er gjensidig avhengig av hverandre. Dette gjelder blant annet samordnede tilsyn og sikring av prioritert kraftforsyning til viktige punkter i elektroniske kommunikasjonsnett.»

Ref /54/

Nkom gjennomfører flere revisjoner i året angående ulike scenarier knyttet til IKT-sikkerhet. Nkom får tilsendt relevant dokumentasjon fra aktørene på forhånd (kryptert), og har egnede verktøy for å sikre at konfidensialitet blir ivaretatt. Tilsynet gjennomføres typisk i løpet av en dag med foreløpige funn som presenteres tilsynsobjektet ved slutten av dagen. Det lages så en tilsynsrapport som selskapet kan kommentere på før en endelig tilsynsrapport utstedes.

Nkom gjennomfører flere beredskapsøvelser i løpet av året sammen med andre offentlige instanser og markedsaktørene.

For å ha tilgang til ekspertkompetanse benytter Nkom rammeavtaler med eksterne aktører, som da kan bistå ved behov.

5.5.3 Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) beskriver i korte trekk hvordan tilsyn foregår på sin hjemmeside /37/. I tillegg har NSM gitt ut en veileder for tilsyn med forebyggende sikkerhetsarbeid /38/. Denne har som målgruppe blant annet sektormyndigheter med tilsynsansvar – dvs. andre myndigheter enn NSM.

«Et departement kan tildele en eksisterende sektormyndighet ansvar for å føre tilsyn med forebyggende sikkerhetsarbeid i sin sektor. Slik tildeling skjer etter en helhetsvurdering og i samarbeid med NSM. Tildeling forutsetter at sektormyndigheten:

- *allerede har ansvar for å føre tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur*
- *har eller kan opparbeide seg nødvendig kompetanse for gjennomføring av tilsyn med at sikkerhetskrav i eller i medhold av sikkerhetsloven overholdes*

Ved å gi eksisterende sektormyndigheter ansvar for tilsyn med forebyggende sikkerhetsarbeid sikres det at tilsynsmyndigheten har bransjekunnskap gjennom kunnskap om tilsynsobjektene i sektorlovgivningen.»

Veilederen inneholder også et eget kapittel om IKT-revisjon, der det står at aktuelle revisjonskriterier er NSMs grunnprinsipper for IKT-sikkerhet og ISO 27001/27002. Tilsynsmyndigheten kan også innhente teknisk informasjon ved hjelp automatiserte metoder, dvs. dataprogrammer eller applikasjoner. Det påpekes flere steder i veilederen at nye vurderinger skal gjøres ved endringer av ulik art.

5.5.4 Luftfartstilsynet

Luftfartstilsynet har vært kontaktet mht. til omfang av IKT tilsyn og regelverk.

Når det gjelder omfang så fokuserer Luftfartstilsynet i likhet med Ptil først og fremst på sikkerheten for menneskers liv og helse. Systemer som kun påvirker kapasitet for trafikkavvikling, har så langt ikke vært fokus for tilsyn knyttet til IKT-sikkerhet.

I likhet med Ptil forankrer luftfartstilsynet i dag arbeidet med IKT-sikkerhet i regler som opprinnelig ikke var tatt frem spesifikt med dette for øyet. Per dags dato benyttes EU Regulering 1035/2011 /57/ som basis. I 2020 vil denne erstattes av EU Regulering 373/2017 /58/ som en del av Norsk lov. I denne nevnes begrepet Cyber Security for første gang eksplisitt. Videre arbeides European Aviation Safety Agency (EASA) med en ny og mer detaljert regulering for informasjonssikkerhet. Denne er på høring og forventes å tre i kraft etter 2023.

5.6 Anbefalte endringer knyttet til tilsynsmetodikk

Basert på innhenting av informasjon fra både tilsynet og tilsynsobjekter om hvordan Ptil gjennomfører tilsyn for IKT-sikkerhet i dag, samt fra tilsvarende tilsynsmyndigheter fremmer DNV GL følgende anbefalinger til endringer.

5.6.1 Tydelig og forutsigbare tilsynskriterier

Uklarheter i regelverket i forhold til IKT-sikkerhet er kjent og drøftes i kapittel 4 Regelverk.

Det anbefales å lage en veiledning til regelverket slik at det fremkommer tydelig hvilke paragrafer og krav som gjelder for IKT-sikkerhet. Dette vil medføre at man ved tilsyn kan ha en større forutsigbarhet for alle parter. For Ptil vil det medføre forenkling ved forberedelse, gjennomføring og oppfølging av et tilsyn. Se Tabell 4-1 i kapittel 4.5 for liste over relevante paragrafer.

5.6.2 Mandat

Ptil anser sitt mandat til å omfatte løsninger innenfor OT domenet, samt enkeltelementer i IT domenet som kan påvirke disse.

Utviklingen av nye løsninger og krav til optimalisering vil presse frem større interaksjon mellom IT og OT domenet, og siden en cyberhendelse i IT-nettverket kan spre seg til OT-nettverket, mener DNV GL at omfanget av Ptils tilsynsmyndighet bør utvides og klargjøres med et tilsvarende omfang som for resten av forskriftene som omhandler HMS.

5.6.3 Leverandører og andre aktører

Ptil gjennomfører i dag tilsyn med operatørene. Flere operatører informerer at de benytter eksterne leverandører og tjenester for flere aktiviteter som er del av, eller nært opptil drift og vedlikehold av OT-systemer.

DNV GL anbefaler at omfanget av tilsyn utvides slik at også leverandører og andre aktører som har en rolle knyttet til IKT-sikkerhet blir gjenstand for tilsyn

5.6.4 Kapasitet og kompetanse

I forhold til mengden av tilsynsobjekter anser vi at Ptil har begrensede ressurser til å gjennomføre og verifisere resultater etter tilsyn med vekt på IKT-sikkerhet.

For å sikre at tilsynet kan gjennomføre tilsyn og oppfølging av tilsyn med god kvalitet, anbefaler DNV GL at kapasiteten styrkes internt med ressurser som har utfyllende kompetanse. Det anbefales også å søke bistand fra ekspertmiljøer ved særskilte behov.

DNV GL anbefaler at det sees nærmere på bruk av uavhengige tredjepartskapasiteter, eksempelvis bruk av sertifiserte enkeltpersoner som kan bistå eller gjennomføre tilsyn.

5.6.5 Systematisk tilnærming

Vår oppfatning etter intervjuene er at dagens praksis bærer preg av en viss tilfeldighet i forhold til hva som er valgt som fokusområder for et tilsyn, samt at praksisen utvikles i litt for stor grad underveis. Noen aktører informerte om at de av og til undres over hvilket detaljnivå som blir prioritert og om objektiviteten ivaretas. Relatert til dette har Ptil informert at de er i ferd med å utvikle interne rutiner og retningslinjer for hva som skal anses som forventet godhet i løsninger i interne ytelsesstandarder.

DNV GL anbefaler at Ptil etablerer mekanismer som bidrar til at tilsynet gjennomføres for hvert enkelt tilsynsobjekt med korrekt prioritering, og sikrer objektiv håndtering av hver enkelt aktør.

Modenhetsanalyser[7] benyttes ofte som et startpunkt for å prioritere videre tiltak internt i en organisasjon. Tilsvarende metodikk kan vurderes benyttet som verktøy som kan bidra til tilsvarende prioritering av tilsynsområder. Analysen bør da gjennomføres i forkant per aktør og per installasjon mot et komplett sett av kriterier som dekker alt fra styring og ledelse, mennesker og sikkerhetskultur, kapasitet og evner, innovasjon og teknologi. Samtidig anbefales Ptil også å vurdere å få på plass flere og mer detaljerte veiledere til IKT-sikkerhet.

5.6.6 Verktøy og prosesser for håndtering av sensitiv informasjon

I gjennomføringen av et tilsyn vil det være behov for å kommunisere informasjon mellom tilsyn og aktør. For at Ptil skal kunne forberede seg best mulig vil det være behov for at aktørene i forkant av et tilsyn deler en stor del informasjon som av ulike årsaker anses som sensitiv og kritisk i et IKT-sikkerhetsperspektiv. Flere aktører har informert at de er ukomfortable med å dele sensitiv informasjon med tilsynet, både når det gjelder hvordan den kommuniseres med og lagres hos tilsynet, samt hvordan tilsynet ivaretar sitt ansvar i forhold til offentleglova /41/.

DNV GL anbefaler at Ptil i større grad tar i bruk tekniske verktøy og prosedyrer for kommunikasjon og lagring av informasjon som beskytter det aktørene anser som sensitiv informasjon i et IKT-sikkerhetsperspektiv mot offentlig innsyn.

DNV GL anbefaler at kapittel 3 i offentleglova /41/ benyttes for dokumentasjon som sendes fra aktørene, i tråd med hva vi ser andre tilsyn gjør.

5.6.7 Rapportering

Veiledning til SF § 29 sier at situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse) skal varsles til tilsynet. I intervjuene informerte flere av aktørene om at de var utsatt for flere IKT-sikkerhetsrelaterte hendelser enn det som ble rapportert til Ptil.

Det bør vurderes å kreve rapportering av hva aktørene er utsatt for av IKT-sikkerhetsrelaterte hendelser på både IT- og OT-siden, selv om disse ikke nødvendigvis fører til driftsforstyrrelse. Dette for å innhente statistikkgrunnlag for å kunne gjøre tiltak for kontinuerlig forbedring.

[7] https://www.difi.no/fagomrader-og-tjenester/digitalt-forstevalg/hvordan-komme-i-gang/mal-digital-modenhet

6 LISTE OVER ANBEFALINGER

Tabellen nedenfor inneholder DNV GL sine anbefalinger knyttet til regelverk og tilsynsmetodikk.

Tabell 6-1- Liste over anbefalinger

Nr.	Emne	Anbefaling	Kapittel Ref.
1	IKT relaterte paragrafer i regelverket	Tabell 4-3 i denne rapporten inneholder et antall paragrafer i regelverket som anses som relevante for IKT-sikkerhet. For hver av disse paragrafene er det gitt en anbefaling om hvordan regelverket kan presiseres mht. til IKT-sikkerhet. Dette foreslås gjort gjennom en egen veileder til regelverket for IKT-sikkerhet som dekker alle disse paragrafene, se anbefaling nr. 2 nedenfor. For et flertall av paragrafene foreslås det også i Tabell 4-3 å legge til en presisering i eksisterende veiledere til regelverket.	4.5
2	Veiledere til paragrafer i regelverket som er relevante for IKT-sikkerhet	Det foreslås også å lage en egen veileder, for de paragrafene i regelverket som anses relevante for IKT-sikkerhet, etter mal fra NVEs veileder til Kraftberedskapsforskriften. Tabell 4-2, og Tabell 4-3 i denne rapporten kan brukes som utgangspunkt for arbeidet med en slik veileder. En slik veileder bør også drøfte hvordan konfidensialitet og integritet av OT-data og systemer skal klassifiseres og ivaretas. For noen utvalgte temaer kan det vurderes å lage særskilte veiledere.	4.5 5.5.1
3	Referanse til standarder	Generelt foreslås det å referere tydeligere til anerkjente standarder som NIST og IEC 62443, samt peke på bransjestandarder som NOROG 104, NOROG 110, NOROG 123 og DNVGL-RP-G108. Det vil være ekvivalent med måten Ptils regelverk for teknisk sikkerhet referer til IEC 61508 og IEC 61511, samt bransjestandarder som NOROG 070 og NORSOK S-001.	4.3.1 4.5
4	IT-systemer som kan ha negativ påvirkning på OT	Det foreslås at veiledningene til regelverket referere til ISO 27000-serien for IKT-sikkerhet for IT-systemer som potensielt kan påvirke de industrielle systemene negativt.	4.3.2 4.5

Nr.	Emne	Anbefaling	Kapittel Ref.
5	Ny teknologi	Aktørene som har vært intervjuet har påpekt at automatisk oppdatering av prosesstyringsparametre i OT-systemer fra algoritmer som ligger i IT-systemene eller i skyen er noe som etter hvert vil komme, selv om ingen av aktørene tillater dette i dag. Sonemodellen blir alt i dag utfordret av leverandører som vil levere «ytelse som tjeneste» (Performance as a Service). Det anbefales å etablere et prosjekt sammen med industrien som ser spesifikt på behovet for regelverk og anbefalte praksiser for dette.	4.5
6	Mandat	Ptil anser sitt mandat til å omfatte løsninger innenfor OT-domenet, samt enkeltelementer i IT-domenet som kan påvirke disse. Utviklingen av nye løsninger og krav til optimalisering vil presse frem større interaksjon mellom IT- og OT-domenet, og siden en sikkerhetshendelse i IT-nettverket kan spre seg til OT-nettverket, mener DNV GL at omfanget av Ptils tilsynsmyndighet bør utvides tilstrekkelig for å kunne dekke denne problemstillingen. Dette bør sees i sammenheng med introduksjon av ny teknologi, punkt 7.	5.6.2
7	Leverandører og andre aktører	Ptil gjennomfører i dag tilsyn med operatørene. Flere operatører informerer at de benytter eksterne leverandører og tjenester for flere aktiviteter som er del av, eller nært opptil drift og vedlikehold av OT-systemer. DNV GL anbefaler at omfanget av tilsyn utvides slik at også leverandører og andre aktører som har en rolle tilknyttet IKT-sikkerhet blir gjenstand for tilsyn	5.6.3

Nr.	Emne	Anbefaling	Kapittel Ref.
8	Kapasitet og kompetanse	I forhold til mengden av tilsynsobjekter anser vi at Ptil har begrensede ressurser til å gjennomføre og verifisere resultater etter tilsyn med vekt på IKT-sikkerhet. For å sikre at tilsynet kan gjennomføre tilsyn og oppfølging av tilsyn med god kvalitet, anbefaler DNV GL at kapasiteten styrkes internt med ressurser som har utfyllende kompetanse. Det anbefales også å søke bistand fra ekspertmiljøer ved særskilte behov. DNV GL anbefaler at det sees nærmere på bruk av uavhengige tredjepartskapasiteter, eksempelvis bruk av sertifiserte enkeltpersoner som kan bistå eller gjennomføre tilsyn.	5.5.4 5.6.4
9	Systematisk tilnærming	DNV GL anbefaler at Ptil etablerer mekanismer som bidrar til at tilsynet gjennomføres for hvert enkelt tilsynsobjekt med korrekt prioritering, og sikrer objektiv håndtering av hver enkelt aktør. En mulig mekanisme som kan bidra til dette er å gjennomføre modenhetsanalyser per aktør og per installasjon mot et komplett sett av kriterier som dekker alt fra styring og ledelse, mennesker og sikkerhetskultur, kapasitet og evner, innovasjon og teknologi.	5.6.5
10	Verktøy og prosesser for håndtering av sensitiv informasjon	DNV GL anbefaler at Ptil i større grad tar i bruk tekniske verktøy og prosedyrer som sikrer at kommunikasjon og lagringen av IKT sensitiv informasjon ivaretar aktørenes behov. DNV GL anbefaler at kapittel 3 i offentleglova /41/ benyttes for dokumentasjon som sendes fra aktørene, i tråd med hva vi ser andre tilsyn gjør.	5.6.6

Nr.	Emne	Anbefaling	Kapittel Ref.
11	Rapportering til tilsynet	Veiledning til SF § 29 sier at situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse) skal varsles til tilsynet. I intervjuene informerte flere av aktørene om at de var utsatt for flere IKT-sikkerhetsrelaterte hendelser enn det som ble rapportert til Ptil. Det bør vurderes å kreve rapportering av hva aktørene er utsatt for av IKT-sikkerhetsrelaterte hendelser på både IT- og OT-siden, selv om disse ikke nødvendigvis fører til driftsforstyrrelse. Dette for å innhente statistikkgrunnlag for å kunne gjøre tiltak for kontinuerlig forbedring.	5.6.7
12	Etablering av systemer utenfor definerte soner.	Det er et antall systemer som er etablert utenfor de definerte sonene, men som har en relasjon til både IT- og OT-systemer. Eksempler på dette er systemer knyttet til radar, helikopternavigasjon og værdata. Noen aktører informerer om at de også har egne servicenettverk definert utenom IT- og OT-nettverkene, som benyttes for overvåking og vedlikehold av disse komponentene. Flere aktører opplyser at det arbeides med å forbedre arkitekturen for disse systemene. Det anbefales å etablere et prosjekt sammen med industrien som ser spesifikt på behovet for regelverk og anbefalte praksiser for dette.	4.3.4

7 REFERANSER

/1/ Petroleumsloven
https://lovdata.no/dokument/NL/lov/1996-11-29-72

/2/ IEC 61511 Functional safety - Safety instrumented systems for the process industry sector, 2016.

/3/ IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

/4/ Kraftberedskapsforskriften
https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

/5/ ISO 19011:2018 Retningslinjer for revisjon av ledelsessystemer.

/6/ ISO/IEC 27007:2017 Guidelines for information security management systems auditing.

/7/ NOU 2018:14 IKT-sikkerhet i alle ledd - Organisering og regulering av nasjonal IKT-sikkerhet
https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

/8/ Nytt regelverk knyttet til NIS-direktivet (under høring)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

/9/ Ny sikkerhetslov fra 1.1.2019
https://lovdata.no/dokument/NL/lov/2018-06-01-24

/10/ ISO 27019 Information security for process control in the energy industry.

/11/ NSM-grunnprinsipper for IKT-sikkerhet
https://www.nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf

/12/ NOROG 104 - Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems, 2016, Rev. 6
https://www.norskoljeoggass.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements.pdf

/13/ DNVGL-RP-G108, 2017, Cyber security in the oil and gas industry based on IEC 62443:2013
https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

/14/ NIST CSF Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, April 2018
https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

/15/ IEC 62443 Industrial communication networks - Network and system security.

/16/ IADC cyber security committee guidelines
https://www.techstreet.com/mss/products/preview/2021294

/17/ Aktivitetsforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/aktivitetsforskriften_n.pdf

/18/ Veiledning til aktivitetsforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/aktivitetsforskriften_veiledning_n.pdf

/19/ Innretningsforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/innretningsforskriften_n.pdf

/20/ Veiledning til innretningsforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/innretningsforskriften_veiledning_n.pdf

/21/ Rammeforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/rammeforskriften_n.pdf

/22/ Veiledning til rammeforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/rammeforskriften_veiledning_n.pdf

/23/ Styringsforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_n.pdf

/24/ Veiledning til styringsforskriften
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_veiledning_n.pdf

/25/ Teknisk og operasjonell forskrift
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/teknisk_og_operasjonell_forskrift_n.pdf

/26/ Veiledning til teknisk og operasjonell forskrift
https://www.Ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/teknisk_og_operasjonell_forskrift_veiledning_n.pdf

/27/ Espen Seljemo, Ptil, IKT-sikkerhet for industrialiserte systemer i et myndighetsperspektiv, Presentasjon, 17.6.2019, Sopra Steria, Stavanger.

/28/ Tilsynsmyndighetenes retningslinje for samordnet tilsyn og felles tilsynsprofil (6.3.2014)

Et samarbeid mellom: Arbeidstilsynet, DSB, Mattilsynet, Miljødirektoratet, Næringslivets sikkerhetsorganisasjon, Ptil, Statens helsetilsyn og Statens Strålevern.

https://www.dsb.no/globalassets/dokumenter/brann-og-redning-bre/pdfer/tilsynsmyndighetenes-retningslinje-for-samordnet-tilsyn-og-felles-tilsynsprofil--godkjent-6.mars-2014.pdf

/29/ Varsel om tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT systemene. Aktivitet 054006028. Brev fra Ptil til Aker BP ASA, Ptil 2019/155/AU.

/30/ Lotteri og stiftelsestilsynet, Metodedokument – Tilsynsmetodikk, revisjon 2, 19.12.2014 https://lottstift.no/wp-content/uploads/2015/12/Overordna-metodedokument-for-Lottstift.pdf

/31/ SINTEF: Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten, 29.5.2018. https://www.Ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf

/32/ Torkjell Jonsson Trædal, Norsk Politiforum, «En oppskrift på cyber-lapskaus?», 30.11.2018 https://www.politiforum.no/artikler/en-oppskrift-pa-cyber-lapskaus/443587

/33/ Ptil: Prosedyre for revisjoner, 17.6.2019.

/34/ Ptil: Veiledning til prosedyre for revisjoner og verifikasjoner, 19.6.2019.

/35/ NOROG 123 - Norwegian Oil and Gas Association Guideline for Classification of process control, safety and support ICT systems based on criticality, Rev. 01, 5.1.2009.

/36/ Direktoratet for eHelse, Normen. Faktaark 38 - Sikkerhetskrav for systemer v5.0 https://ehelse.no/normen/faktaark/faktaark-38-sikkerhetskrav-for-systemer

/37/ Nasjonal Sikkerhetsmyndighet, Slik foregår tilsyn fra NSM, 17.6.2014 https://www.nsm.stat.no/om-nsm/tjenester/tilsyn/slik-foregar-tilsyn-fra-nsm/

/38/ Nasjonal Sikkerhetsmyndighet, Veileder for tilsyn med forebyggende sikkerhetsarbeid, 2019, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-for-tilsyn-med-forebyggende-sikkerhetsarbeid.pdf

/39/ NSM, Rammeverk for håndtering av IKT-sikkerhetshendelser, 7.12.2017 https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

/40/ Ptil 2019/1176/AU - Informasjon om håndtering av IKT-sikkerhetshendelser.

/41/ Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova) https://lovdata.no/dokument/NL/lov/2006-05-19-16

/42/ Barrierenotat 2017 https://www.Ptil.no/contentassets/43fc402b97e64a7cbabdf91c64b349cb/barrierenotat--2017.pdf

/43/ Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet. Rapport avgitt av ekspertgruppe til arbeidsdepartementet 27.08.2013.

/44/ ISO/IEC 27001, Information technology - Security Techniques - Information security management systems.

/45/ https://e24.no/boers-og-finans/i/dOrR6j/aker-bp-tar-cybergrep-allierer-seg-med-kraftbransjen

/46/ https://www.nsm.stat.no/norcert

/47/ https://www.regjeringen.no/contentassets/be6dde2da6dd4c85a0827a423904466e/oversikt-over-markedstilsynsmyndigheter.pdf

/48/ https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center

/49/ «Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller», DNV GL, Rapport nr 2019-0826.

/50/ «Trening og Øvelse», DNV GL, Rapport nr 2019-0823.

/51/ «Resiliens mot cyberhendelser og kan blokkjede bidra», DNV GL, Rapport nr 2019-0825.

/52/ Hydro Second Quarter Report 2019 https://www.hydro.com/Document/Index?name=Report%20Q2%202019.pdf&id=105855

/53/ About the FAA designee program: https://www.faa.gov/other_visit/aviation_industry/designees_delegations/about/#q1

/54/ Nkoms arbeid med sikkerhet og beredskap i nett - https://www.nkom.no/teknisk/sikkerhet-og-beredskap/ekomsikkerhet/pts-arbeid-med-sikkerhet-og-beredskap-i-nett

/55/ NVE revisjonsspørsmål til bruk i arbeidet med tilsyn på IKT-sikkerhet – https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/er-ikt-sikkerheten-i-samsvar-med-kravene-i-kraftberedskapsforskriften/

/56/ ISO/IEC 27007, Information technology - Security techniques - Guidelines for information security management systems auditing.

/57/ COMMISSION IMPLEMENTING REGULATION (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010.

/58/ COMMISSION IMPLEMENTING REGULATION (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011.

/59/ IADC Guidelines for Baseline Cybersecurity for Drilling Assets, January 2018.

/60/ NOROG 070, Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements), 2018.

/61/ NORSOK Standard S-001, Technical Safety, 2018.

/62/ Direktoratet for samfunnssikkerhet og beredskap, samfunnets kritiske funksjoner, versjon 1.0 2016.

/63/ ISO 9001:2015, Quality Management Systems – Requiriements.

/64/ Øvelser – En veiledning i hvordan planlegg og gjennomføre øvelser innen energiforsyningen, NVE Rapport nr. 39 2015 http://publikasjoner.nve.no/rapport/2015/rapport2015_39.pdf

/65/ *Regulering av IKT Sikkerhet - Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor, NVE Rapport nr. 26/2017.* *http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf*

/66/ CyberSmart – et pilotprosjekt for opplæring av ungdom i cybersikkerhet, NVE rapport nr. 35/2019.
http://nve.impleoweb.no/Orders/Prods/Rapport,%20bokm%C3%A5l_7d919edf7a96471e8fde51efe80ed137.pdf

/67/ Oppsummering av uønskede hendelser 2018 i energiforsyningen, NVE faktaark nr. 4/2019.
http://publikasjoner.nve.no/faktaark/2019/faktaark2019_04.pdf

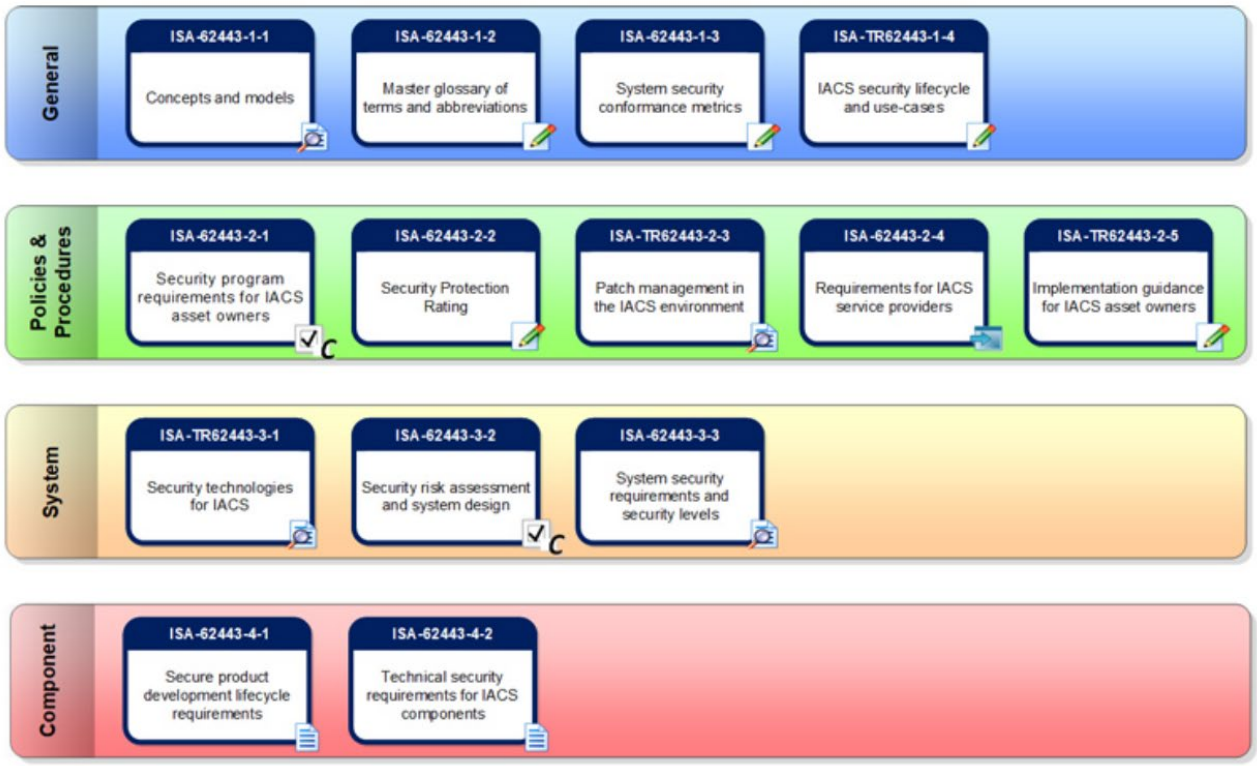
/68/ Metode for å finne kraftsensitiv informasjon på Internett, NVE faktaark nr. 11/2019.
http://publikasjoner.nve.no/faktaark/2019/faktaark2019_11.pdf

APPENDIX 1 – RELEVANTE STANDARDER

ISO/IEC 27001, Information technology – Security Techniques – Information security management systems — Requirements, er først og fremst en standard for styringssystem for informasjonssikkerhet. Denne inneholder krav mest relevant i IT-domenet. ISO 27000-familien omfatter flere standarder og guidelines og har også en standard med tekniske krav for industrielle kontrollsystemer innen energisektoren, ISO/IEC TR 27019. Denne er derfor rettet mot OT.

NIST (National Institute of Standards and Technology) har et rammeverk for cybersikkerhet (Cybersecurity Framework) for kritisk infrastruktur /15/. Rammeverket inneholder hovedfunksjonene Identify ID, Protect PR, Detect DE, Respond RS og Recover RC. Videre er det underpunkter som refererer til CIS CSC, COBIT 5, IEC 62443, ISO/IEC 27001 og NIST SP 800-53.

IEC 62443 /14/ inneholder standarder og tekniske rapporter som definerer prosedyrer for implementering av sikre industriautomatiserings – og kontrollsystemer (IACS/OT).



Figur 7-1– IEC 62443 serien.

DNVGL-RP-G108, Cyber security in the oil and gas industry based on IEC 62443, /13/ er en anbefalt praksis[8]. Denne gir retningslinjer for hvordan benytte IEC 62443-serien av standarder i olje- og gassindustrien. Selv om standarden (IEC 62443) beskriver cybersikkerhetskrav for alle typer industrier, er denne anbefalte praksis spesielt tilpasset olje og gass. Mens standarden fokuserer på hva som skal gjøres, fokuserer den anbefalte praksis på hvordan det skal gjøres.

[8] RP = Recommended Practice.

NSM har beskrevet et rammeverk for håndtering av IKT-sikkerhet /39/ som inkluderer samspillet mellom og forventinger til virksomheter, sektorvise responsmiljøer, og relevante myndigheter og etater i Norge. I tillegg til rammeverksdokumentet har NSM gitt ut et dokument der de har definert grunnprinsipper for IKT-sikkerhet. NSM skriver at kategoriseringen av grunnprinsippene er *«... i stor grad sammenfallende med gjeldende inndeling i «Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)» og «NIST Cyber Security Framework»»*.

Den internasjonale organisasjonen for drillingselskaper (IADC) har utgitt en IKT-sikkerhetsguideline (ref./59) spesifikk for drilling installasjoner. Formålet med denne guidelinen er å samle relevante standarder og beste-praksis dokumenter. Standardene som fremheves spesielt er NIST CSF, IEC 62443 og ISO/IEC 27000.

Om DNV GL

DNV GL er et internasjonalt selskap innen kvalitetssikring og risikohåndtering. Siden 1864 har vårt formål vært å sikre liv, verdier og miljøet. Vi bistår våre kunder med å forbedre deres virksomhet på en sikker og bærekraftig måte.

Vi leverer klassifisering, sertifisering, teknisk risiko- og pålitelighetsanalyse sammen med programvare, datahåndtering og uavhengig ekspertrådgivning til maritim sektor, til olje- og gass-sektoren, og til energibedrifter. Med 80,000 bedriftskunder på tvers av alle industrisektorer er vi også verdensledende innen sertifisering av ledelsessystemer.

Med høyt utdannede ansatte i 100 land, jobber vi sammen med våre kunder om å gjøre verden sikrere, smartere og grønnere.