DNV·GL

IKT-SIKKERHET – ROBUSTHET I PETROLEUMSSEKTOREN

Trening og Øvelse

Petroleumstilsynet

Rapportnr.: 2019-0823, Rev. 0
Dato: 2020-02-21

Prosjektnavn:	IKT-sikkerhet – Robusthet i petroleumssektoren	DNV GL AS
Rapporttittel:	Trening og Øvelse	Digital Solutions
Oppdragsgiver:	Petroleumstilsynet, P.O. Box 599	Postboks 300
	4003 Stavanger	1322 Høvik
	Norway	Norway
Kontaktperson:	Arne Halvor Embergsrud	
Dato:	2020-02-21	
Prosjektnr.:	101572712	
Org. enhet:	Cyber Security Services	
Rapportnr.:	2019-0823, Rev. 0	

Kontrakt for leveranse av denne rapport:
Avtale om IKT-sikkerhet – Robusthet i petroleumssektoren

Oppdragsbeskrivelse: Hovedmål med prosjektet er å se på ulike forhold rettet mot IKT-sikkerhet for de industrielle IKT-systemer. Robusthet til systemene samt tilhørende HMS perspektiv rettet mot menneskelig, organisatoriske og tekniske forhold. Denne rapporten ser på anvendelse av trening og øvelse rettet mot de industrielle IKT-systemene på norsk sokkel i dag og hvordan legges det til rette for trening og øving relatert til hendelser og/eller scenarioer for disse systemene.

Utarbeidet av:	Verifisert av:	Godkjent av:
Erling Håland Principal Consultant	Boye Tranum Associate Director	Trond Solberg Head of Section, Cyber Security Services

Helle Fløtaker
Senior Principal Consultant

DNV GL distribusjon:

☒ ÅPEN. Fri distribusjon, intent og eksternt.

☐ INTERN. Fri distribusjon internt i DNV GL.

☐ KONFIDENSIELL. Distribusjon som angitt i distribusjonsliste. Distribution within DNV GL according to applicable contract.*

☐ HEMMELIG. Kun autorisert tilgang.

*Distribusjonsliste:

Nøkkelord:
IKT-sikkerhet, industriell IKT, trening, øvelse, læring, beredskap, cyber-sikkerhet

Rev.nr.	Dato	Årsak for utgivelse	Utført av	Verifisert av	Godkjent av
A	2019-11-29	Første utgivelse, for kommentarer	ERHA/FUNN/HELLE	BOTRA/JJ/KKV	TROSOL
0	2020-02-21	Endelig versjon	ERHA/HELLE	BOTRA	TROSOL

Innholdsfortegnelse

1 SAMMENDRAG

Digitalisering i olje- og gass-sektoren åpner opp for effektivisering, men gjør også sektoren mer sårbar for IKT-sikkerhetshendelser. Olje- og gass-sektoren er et mål for trusselaktører på grunn av de store verdiene sektoren representerer, og for aktivister med idealistisk eller politisk motivasjon. Historisk har det vært et skarpt skille mellom industriell IKT og IT, men den teknologiske utviklingen utfordrer imidlertid dette skillet ved at disse systemene blir stadig mer integrert og dermed også mer komplekse.

Petroleumstilsynet (Ptil) gjennomfører en satsing på IKT-sikkerhet i perioden 2018-2021. Målet er å gå i dybden på en del viktige områder, innhente kunnskap om den teknologiske utviklingen og vurdere hvordan dette påvirker risikobildet. Dette prosjektet er et ledd i det å øke petroleumsnæringens fokus på IKT-sikkerhet og sikre robusthet i de industrielle IKT-systemene. Målsettingen for prosjektet har vært å samle og øke Ptils og petroleumsnæringens kunnskapsgrunnlag om IKT-sikkerhet og herunder etablering av god praksis for en systematisk tilnærming til håndtering av IKT-sikkerhetshendelser.

Denne rapporten er en av fem delleveranser i prosjektet. Denne delleveransen har fokus på anvendelse av trening og øvelse rettet mot de industrielle IKT-systemene på norsk sokkel i dag, og hvordan det legges til rette for trening og øving relatert til hendelser som omfatter disse systemene.

Trening og øvelse brukes ofte som et fellesbegrep, men for å skille læring og ferdighetstrening for enkeltindivider fra samhandling i en organisasjon, er det imidlertid i denne rapporten valgt å definere begrepene trening og øvelse hver for seg. Definisjonene benyttet i denne rapporten er i tråd med definisjoner som vist i Direktoratet for samfunnssikkerhet og beredskap (DSB) og Direktoratet for IKT-forvaltning (Difi) sine veiledere for øvelser;

- **Trening** består i å øke individers kunnskaper og kompetanse og lære de ferdigheter som er nødvendige for å fylle en gitt rolle i den organisasjonen som skal håndtere en hendelse.
- **Øvelse** består i å utvikle og forbedre en organisasjons evne til å håndtere en hendelse.

En øvelse er ikke begrenset til selve aktiviteten der et scenario utspilles, men inkluderer også planlegging av scenariet og evaluering av gjennomføringen og egnetheten til gjeldende prosedyrer og beredskapsplaner. En øvelse kan involvere en deler av en organisasjon eller hele organisasjonen, samt samhandling mellom flere organisasjoner og virksomheter.

Denne rapporten fokuserer på trening og øvelse, samt beredskap, rettet mot trusler og sårbarheter som er identifisert for de industrielle IKT-systemene. Studien har omfattet petroleumsnæringen i Norge og andre sektorer både nasjonalt og internasjonalt. Arbeidet er utført gjennom en litteraturstudie samt dybdeintervjuer med aktører i petroleumssektoren og andre industrier som opererer industrielle IKT-systemer.

Oppgaver som er vesentlige i arbeidet med trening og øvelse rettet mot en virksomhets industrielle IKT-sikkerhet og IT-sikkerhet kan gjennomføres av virksomheten selv dersom den har riktig kompetanse og tilstrekkelige ressurser. For andre virksomheter kan det være hensiktsmessig å etterspørre disse tjenestene fra spesialiserte tilbydere. Disse oppgavene inkluderer trening i bevisstgjøring av IKT-sikkerhet, rådgivning innen beredskap og øvelser, samt inntrengningstjenester og «red-team» øvelser.

Med utgangspunkt i litteraturstudien og tilbakemeldinger fra intervjuene som er gjennomført, er det identifisert og presentert 26 konkrete tiltak som samlet utgjør god praksis for håndtering av industriell IKT-sikkerhet. 23 av tiltakene er spesifikt rettet mot trening og øvelse; ett tiltak er et forslag til hvordan Ptil kan gi bedre veiledning til sektoren for arbeid med industriell IKT-sikkerhet; og to tiltak er relatert til deltakelse i fora for å få tilgang på fellesresurser, og å lære og dele informasjon og erfaring.

2 ENGLISH SUMMARY

Digitization in the oil and gas industry contributes to efficiency, but also to make the industry more vulnerable to ICT security incidents. The oil and gas industry is a target for threat actors because of the large values of the businesses involved, and for activists with idealistic or political motivation. Historically, there has been a sharp distinction between industrial ICT and IT, but this is now challenged by the technological development gradually making these systems more integrated and more complex.

The Petroleum Safety Authority (PSA) has launched an initiative on ICT security, which is being carried out during the period 2018-2021. The goal of this initiative is to gain knowledge and assess how the technological development affects the risk picture. As part of the initiative, this project is focusing on ICT security and ensuring robustness in the industrial ICT systems. The aim of the project is to gather and increase ICT security knowledge for the PSA and the petroleum industry, and to suggest measures forming basis for good practice and a systematic approach to managing ICT security risk.

This report is one of the five project deliveries. This delivery is addressing how training and exercises are applied in safeguarding the industrial ICT systems for the petroleum industry on the Norwegian Continental Shelf (NCS).

Training and exercise are often referred to as a common term. To differentiate individual learning and skills from team interaction by personnel in the organisation, the two terms training and exercise have however been given separate definitions in this report. The definitions used here are in accordance with guidelines published by the Norwegian Directorate for Civil Protection (DSB) and the [Norwegian] Agency for Public Management and eGovernment (Difi).

- **Training:** Increasing individuals' knowledge, competence and skills which are necessary to fill their given roles in the organisation, and for handling an incident/event.
- **Exercise:** Developing an organization's ability to handle an incident/event and to reveal whether the current procedures and plans are suitable for the given purpose.

An exercise is not limited to the exercise activity itself, but also includes planning the exercise scenario as well as the evaluation and follow-up activities after the exercise is performed. Exercises may be limited to the organisation itself or involve interaction with other organizations.

This study has a focus on training and exercises related to threats and vulnerabilities identified for the industrial ICT systems. The study comprises the oil and gas industry and other industries in Norway and abroad. The work has been carried out as a combination of literature review, and interviews with stakeholders within the oil and gas industry and other relevant sectors operating industrial ICT systems.

Essential tasks ensuring proper training and exercises, addressing threats to the ICT systems, have been identified. Organisations and enterprises which holds the required competence and resources may carry out these tasks by themselves. Otherwise, these tasks may be acquired from external and commercial suppliers. These tasks may comprise awareness training in ICT security, advisory services for emergency response and exercises, penetration testing and "red team" exercises.

Based on the literature review and interviews, as described above, a total of 26 measures have been identified as good practice for training, exercise, and emergency preparedness, for handling ICT security events. 23 measures are specifically dedicated to training and exercise, one measure recommending how the Norwegian petroleum safety authority (PSA) may provide better guidance to the industry within ICT security, and finally two measures addressing the benefits for organizations to participate in professional forums enabling access to common resources and to learn and share information and experience.

3 INNLEDNING

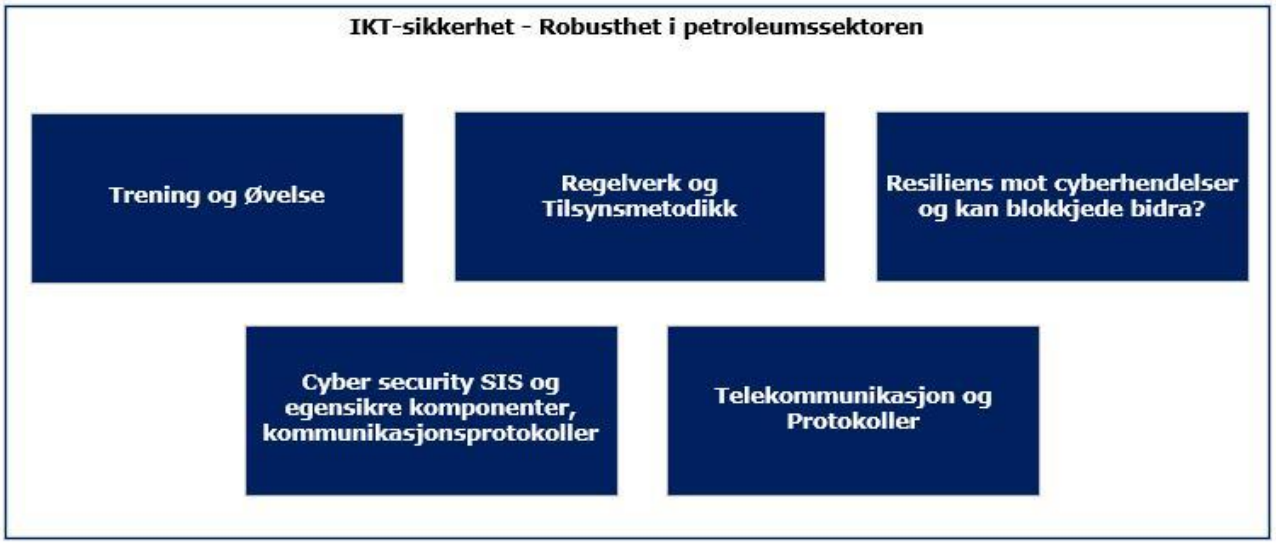
3.1 Bakgrunn

Digitalisering i olje- og gass-sektoren åpner opp for effektivisering, men gjør også sektoren mer sårbar for IKT-sikkerhetshendelser. Olje- og gass-sektoren er et mål for trusselaktører på grunn av de store verdier sektoren representerer, og for aktivister med idealistisk eller politisk motivasjon.

Utvinning, transport og distribusjon av hydrokarboner medfører en risiko for ulykker med konsekvenser for liv og helse, miljø og materielle verdier. For å redusere risiko for slike ulykker, er det installert en rekke sikkerhetssystemer. Mange av disse sikkerhetssystemene benytter IKT-teknologi og kan være sårbare for IKT-sikkerhetshendelser. Manglende eller feil funksjonalitet i sikkerhetssystemene kan få katastrofale konsekvenser. Det er et mål at IKT-sikkerhetshendelser ikke skal påvirke sikkerhetssystemene.

Petroleumstilsynet gjennomfører en satsing på IKT-sikkerhet i perioden 2018-2021. Målet er å gå i dybden på en del viktige områder, innhente kunnskap om den teknologiske utviklingen og vurdere hvordan dette påvirker risikobildet. Nylig er det publisert rapporter innen temaene «Kunnskap IKT-sikkerhet og CERT» (ref. /45/) og «Fjernarbeid og HMS» (ref. /46/). Videre pågår det en utredning om «Industriell IKT og IIoT».

Petroleumstilsynet utlyste en konkurranse for å utrede «IKT-sikkerhet – Robusthet i petroleumssektoren», som inneholder flere arbeidspakker og delleveranser, som illustrert i Figur 3-1. Dette oppdraget ble tildelt DNV GL. 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

Foreliggende rapport dokumenterer resultatene fra delleveransen **Trening og Øvelse**.

3.2 Hensikt

Hensikten med denne delleveransen er å se på anvendelse av trening og øvelse rettet mot de industrielle IKT-systemene på norsk sokkel i dag, og hvordan det legges til rette for trening og øving relatert til hendelser og/eller scenarioer for disse systemene.

Delleveransen skal omfatte:

- Beskrive hvordan man trener og øver på sikkerhetshendelser som påvirker industrielle IKT-systemer i andre sektorer nasjonalt og internasjonalt.
- Beskrive tjenestene som leveres av nasjonale og internasjonale tilbydere som er spisset mot industriell IKT.
- Beskrive de føringer dagens regelverk og Ptil har innen dette området.
- Undersøke om virksomhetene har en Definert Fare- og Ulykkeshendelse (DFU) som dekker IKT-sårbarhet og trusler.
- Identifisere og foreslå eventuelle forbedringer av systemer, regelverk, og utførelse av trening og øvelse, for å dekke inn IKT-sikkerhetsaspektet for de industrielle IKT-systemene.

3.3 Omfang

Denne rapporten gir anbefalinger til krav og beste praksis relatert til trening og øvelse (se kapittel 3.6.1), inkludert beredskap for IKT-sikkerhetshendelser (se kapittel 3.6.2) som fortrinnsvis er rettet mot industrielle IKT-systemer (se kapittel 3.6.3).

Historisk har det vært et skarpt skille mellom industriell IKT og IT, men den teknologiske utviklingen utfordrer imidlertid dette skillet ved at disse systemene blir stadig mer integrert. Et angrep på administrative IT-systemer i kontornettet kan være et springbrett inn mot de industrielle IKT-systemene.

Som følge av denne grenseflaten og koblingene mellom IT-systemer og industrielle IKT-systemer er trenden at tilgjengelighet av IT-systemer også blir stadig mer viktig. Rapporten gir derfor også anbefalinger som er rettet mot IT-systemer som indirekte vil kunne påvirke virksomhetens industrielle IKT-systemer.

3.4 Metodikk

Kunnskap er hentet inn gjennom litteratursøk og intervjuer med aktører i petroleumssektoren og andre industrier som opererer industrielle IKT-systemer.

Kunnskapen som er hentet inn gjennom dette arbeidet, danner grunnlag for anbefalte beste praksis i utarbeidelse av trening og øvelsesscenario som adresserer identifiserte trusler mot IKT-systemene som benyttes. Kunnskapen danner også grunnlag for forslag til forbedring av føringer som legges til grunn i dagens regelverk og av Ptil.

3.5 Forkortelser

Term	Definisjon/betydning
CERT	Computer Emergency Response Team (Ekvivalent med CSIRT[1])
CSF	Cyber Security Framework
CSIRT	Computer Security Incident Response Team (Ekvivalent med CERT)
DDoS	Distributed Denial of Service
DFU	Definert Fare- og Ulykkeshendelse
Difi	Direktoratet for IKT-forvaltning
DSB	Direktoratet for samfunnssikkerhet og beredskap
ENISA	European Network and Information Security Agency
ESD	Emergency shutdown
FEMA	Federal Emergency Management Agency
FKCS	Felles cyberkoordineringssenter
GDPR	General Data Protection Regulation
IADC	International Association of Drilling Contractors
IEC	International Electrotechical Commision
IKT	Informasjon- og kommunikasjonsteknologi
IKT-sikkerhet	Sikring av IKT-systemer. «Cyber Security»
ISBR	Information Security Baseline Requirement
ISO	Den internasjonale standardiseringsorganisasjonen
IT	Informasjonsteknologi
NCSC	Nasjonalt Cybersikkerhetssenter
NIST	National Institute of Standards and Technology
NOROG	Prefiks brukt der det refereres til *Norsk olje og gass* sine retningslinjer
NorSIS	Norsk senter for informasjonssikring
NSM	Nasjonal sikkerhetsmyndighet

[1] CERT er et registrert varemerke tilhørende Carnegie Mellon University. CSIRT er en fri betegnelse

Term	Definisjon/betydning
NSO	Næringslivets Sikkerhetsorganisasjon
NSR	Næringslivets sikkerhetsråd
NVE	Norges vassdrags- og energidirektorat
OFFB	Operatørenes forening for beredskap
OT	Operasjonell teknologi
PISAS	Petroleum Industry Security Alert System
PSD	Process shutdown
PST	Politiets sikkerhetstjeneste
Ptil	Petroleumstilsynet
RP	Recommended Practice
SOC	Security Operation Center
SRM	Sektorvist Responsmiljø
US / USA	United States / United States of America
VDI	Varslingssystem for digital infrastruktur

3.6 Begreper og terminologi

3.6.1 Trening og øvelse

Trening og øvelser bidrar til å trene opp virksomheters beredskapsstyrke samt å bidra til å utvikle ferdigheter, kompetanse, risikoforståelse og god sikkerhetskultur.

Trening og øvelse brukes ofte som et fellesbegrep. I US Homeland Security's kursmateriale IS-870 for krisehåndtering i damsektoren (ref. /50/), defineres for eksempel begge begreper som *trening*. For å skille på læring og ferdighetstrening for enkeltindivider og samhandling i en organisasjon er det imidlertid i denne rapporten valgt å definere begrepene trening og øvelse i tråd med definisjoner som vist i DSB (ref. /16/) og Difi (ref. /24/) sine veiledere for øvelser. Faktaboks 3-1 inneholder utklipp fra DSBs veileder (ref. /16/) og US Homeland Security's kursmateriale IS-870 (ref. /50/) som fremstiller trening og øvelse på to ulike måter.

Trening er i denne rapporten definert som å øke individers kunnskaper og kompetanse og lære de ferdigheter som er nødvendige for å fylle en gitt rolle i den organisasjonen som skal håndtere en hendelse. Merk at det er forskjell mellom behovet for generell forståelse og bevissthet og kunnskap knyttet til det å utføre spesifikke oppgaver med det industrielle IKT-systemet.

Trening omfatter blant annet;

- Bevisstgjøring om IKT-sikkerhetstrusler og -sårbarheter
- Opplæring i bruk av IKT-systemer
- Opplæring i bruk av IKT-sikkerhetssystemer
- Opplæring i roller relatert til virksomhetens beredskapsstrategi

Ref. /42/ gir følgende eksempler på tiltak rettet mot kontinuerlig og generell kompetanseheving innen IKT-sikkerhet; onboarding-programmer, phishing-kampanjer, deltakelse i sikkerhetsmåneden, e-læringskurs, lederopplæring i forbindelse med GDPR, og faglunsjer.

Øvelse er i denne rapporten definert som å utvikle og forbedre organisasjonens evne til å håndtere en hendelse. En øvelse er ikke begrenset til selve aktiviteten der et scenario utspilles, men inkluderer også planlegging av scenariet og evaluering av gjennomføringen og egnetheten til gjeldende prosedyrer og beredskapsplaner. En øvelse kan involvere en organisasjon, men også samhandling mellom flere organisasjoner og virksomheter. Evaluering av øvelser vil bidra til forbedring av virksomhetenes beredskapsplaner samt å øke krisehåndteringskompetanse. Gjennom øvelser vil man også teste og videreutvikle systemer, funksjoner og kompetanse, og påvise effekt av gjennomførte tiltak og endringer.

Øvelser omfatter blant annet:

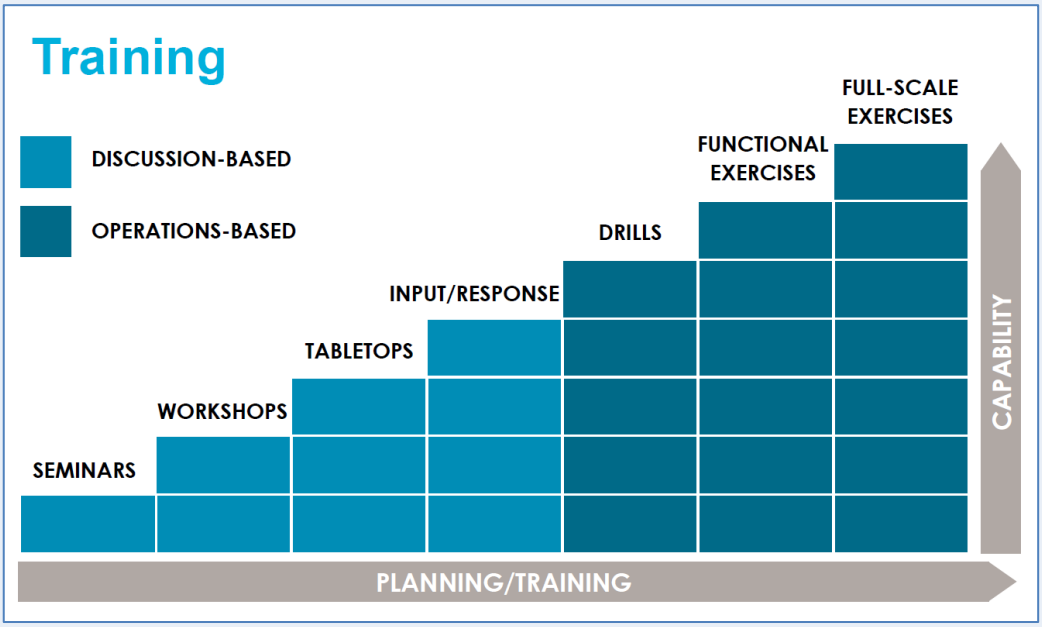
- Beredskapsøvelser
- Øvelser for å verifisere sikkerhetssystemer og prosedyrer, eksempelvis relatert til sikkerhetskopiering og gjenoppretting av systemer og data
- Øvelse på detektering av og aksjonering mot IKT-sikkerhetsangrep, for eksempel inntrengningsøvelser og «red-team»-øvelser[2]

Øvelser skal gi deltagerne kunnskap og erfaring. De skal også bidra til bedre risikoforståelse og sikkerhetskultur. Læring bør derfor vektlegges i alle øvelser.

[2] Se beskrivels av intrengningsøvelser og «red-team»-øvelser i kapittel 6.3 og Faktaboks 6-1.

Trening vs. Øvelse

Kilde: DSB Veileder i planlegging, gjennomføring og evaluering av øvelser. (ref. /16/)



Kilde: FEMA, Homeland security, Crisis Management Overview Course (ref. /50/)

Faktaboks 3-1: Begrepsbruk – trening vs. øvelse

Nasjonal IKT-øvelse 2016

Regjeringen gjennomførte en nasjonal IKT-øvelse i 2016. Formålet med øvelsen var å sette Norge i bedre stand til å håndtere et større IKT-angrep som rammer på tvers av sektorer. Øvelsen var et viktig virkemiddel for å bedre beredskapen. Læring står sterkt i fokus både i planlegging, gjennomføring og oppfølging av øvelsen. Direktoratet for samfunnssikkerhet og beredskap fasiliterte øvingsplanleggingen

Faktaboks 3-2: Nasjonal IKT-øvelse 2016

3.6.2 IKT-sikkerhet – sikkerhet og sikring

Det norske begrepet *sikkerhet* benyttes for det man på engelsk både kaller «safety» og «security». Ordet *sikkerhet* brukes noen ganger når man omtaler det som på engelske kalles «security», andre ganger brukes ordet *sikring*. Ordet *sikring* kan imidlertid også brukes når man omtaler det man på engelsk ville kategorisere under begrepet «safety», som for eksempel brannsikring, stillassikring og lignende.

Begrepet IKT-sikkerhet har grenseflater mot eller kan oppfattes synonymt med informasjonssikkerhet, cybersikkerhet og digital sikkerhet (se IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet. NOU 2018: 14 (ref. /40/)).

Typiske karakteristika for begrepene *sikkerhet* og *sikring* er presentert i Tabell 3-1. I dette dokumentet er begrepet **IKT-sikkerhet** benyttet der man på engelsk ville benyttet «cyber security». Det vil si at begrepet IKT-sikkerhet i denne rapporten fortrinnsvis er benyttet for å beskrive *sikring* av konfidensialitet, integritet og tilgjengelighet av informasjon og IKT-systemer.

Tabell 3-1: Typiske karakteristika for begrepene *Sikkerhet* og *Sikring*

Sikkerhet – Safety	**Sikring - Security**
Uønsket handling eller tilstand	Ønsket handling
Ubevisst, ikke ondsinnet	Bevisst, ondsinnet handling
Ikke planlagt	Planlagt handling

Konfidensialitet er egenskapen at informasjon og systemer bare skal være tilgjengelig for de som har behov. I en bedrift kan for eksempel deler av informasjon og systemer være åpen, andre deler kan være intern, mens andre deler igjen er hemmelig eller sensitiv som kun skal deles eller brukes av et begrenset antall personer. Integritet vil si at informasjonen eller systemene ikke blir korrumpert og at de er fremkommet gjennom gyldige forretningsmessige prosedyrer. I tillegg må systemer og informasjon være tilgjengelig for de som er rettmessige brukere, når de trenger det.

3.6.3 Industriell IKT – IT og OT

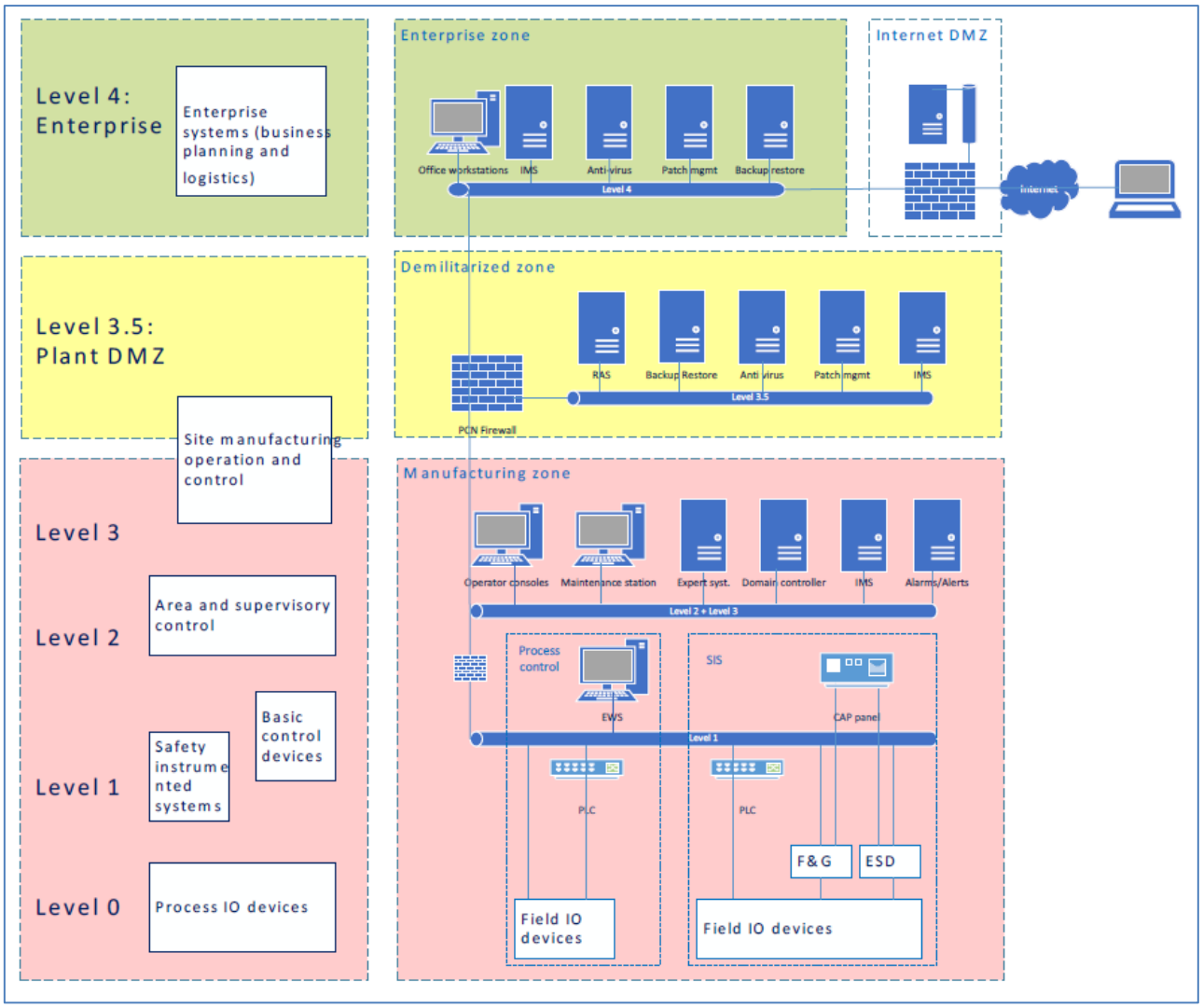
Begrepet IKT kan deles opp i Informasjonsteknologi (IT) og Operasjonell Teknologi (OT). IT fokuserer på data og kommunikasjon i kontor og administrasjonsdomene, mens OT har fokus på kontroll av fysiske prosesser på industri installasjoner. I dette dokumentet er begrepet **Industriell IKT** benyttet som en ekvivalent terminologi for OT. Purdue modellen, vist i Figur 3-2, brukes som referansemodell for å vise grensesnitt mellom IT-systemer (level 4) og industrielle IKT-systemer (level 0-3).

Ptils virksomhet har tidligere kun vært fokusert på sikkerhet i betydningen «safety», men i 2007 startet de første tilsynsaktivitetene relatert til IKT-sikkerhet. Når det gjelder programvarebaserte systemer begrenser Ptil sin virksomhet til industrielle IKT-systemer. Dette ekskluderer dermed Informasjonsteknologi (IT), også benevnt som administrative IT-systemer.

Historisk har det vært et skarpt skille mellom industriell IKT og IT, men den teknologiske utviklingen utfordrer imidlertid dette skillet ved at disse systemene blir stadig mer integrert. Konfidensialitet og integritet har tradisjonelt vært det mest dominerende innen IT, mens tilgjengelighet og det å ha kontroll

er ofte viktigst innen industriell IKT[3]. Merk at hvis integriteten svikter så har man ikke kontroll. Nå er konfidensialitet i ferd med å bli mer og mer viktig også for industrielle IKT-systemer, siden et brudd på konfidensialitet (spionasje og kompromittering), og dermed innsyn i design og operasjon av industrielle IKT-systemer, kan være forløperen for et målrettet angrep (sabotasje) som kan forårsake tap av kontroll. Et angrep på administrative IT-systemer i kontornettet kan være et springbrett inn mot de industrielle IKT-systemene, da disse i økende grad er knyttet sammen.

Et annet aspekt med den stadig tettere integrasjonen mellom IT-systemer og industrielle IKT-systemer er at IKT-sikkerhetshendelser som kun rammer IT-systemene i den administrative sonen nå også kan medføre at produksjonen vanskeliggjøres, selv om de industrielle IKT-systemene ikke er direkte rammet. På grunn av denne avhengigheten mellom IT-systemer og industrielle IKT-systemer er trenden at tilgjengelighet av IT-systemer også blir stadig mer viktig.



Figur 3-2: Purdue Modellen utvidet med level 3.5 (ref. /55/).

[3] 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.

Et eksempel på økonomisk konsekvens er IKT-sikkerhetsangrepet på Norsk Hydro våren 2019. Dette er kort beskrevet i Faktaboks 3-3.

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

Utdrag fra Q2-rapporten til Norsk Hydro:

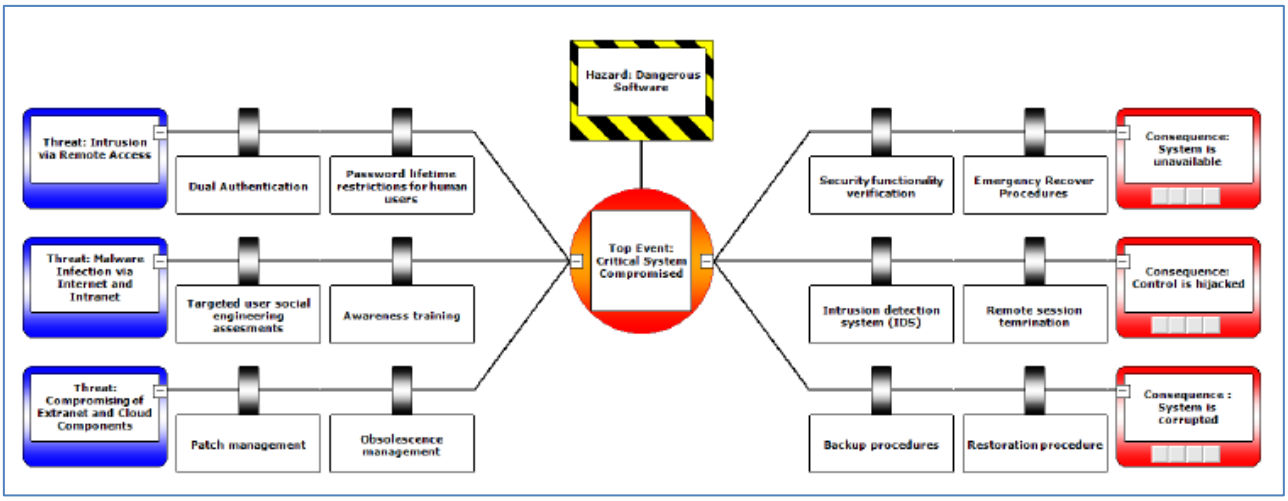
"The cyber attack on Hydro on March 19, affected our entire global organization, with Extruded Solutions having suffered the most significant operational challenges and financial losses. The financial impact of the cyber attack was around NOK 300- 350 million in the first quarter. The financial impact 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."

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

Faktaboks 3-3: IKT-sikkerhetsangrepet på Norsk Hydro

3.6.4 Definert fare og ulykkeshendelse

En definert fare og ulykkeshendelse (DFU) består av en fare og tilhørende hendelsesscenario. Et scenario er beskrevet ved en topphendelse, med tilhørende hendelsesforløp som inkluderer årsaker, potensielle konsekvenser, samt barrierer for å unngå at hendelsen inntreffer eller for å påvirke hendelsesforløpet slik at konsekvensene begrenses. Et eksempel på en DFU er presentert i Figur 3-3 i form av et Bow-Tie diagram.



Figur 3-3: Eksempel på bow-tie diagram over en DFU med tilhørende konsekvenser, årsaker/ trusler og barrierer (ref. /27/).

Mørketallsundersøkelsen 2018 utført av NSR (ref. /33/) lister opp eksempler på informasjons-sikkerhetshendelser. Disse er gjengitt i Faktaboks 3-4.

For IKT-systemer vil for eksempel skadevare være en **fare**, og tilhørende **ulykkeshendelse** vil være at systemet blir infisert. Data, informasjon, og/eller programvare kan som følge av dette bli kompromittert. Dette kan medføre at en logisk funksjon i IKT-systemet ikke klarer å håndtere en uønsket hendelse, eller at funksjonen selv skaper en uønsket hendelse.

Årsaken til en IKT-sikkerhetshendelse er en realisering av en **trussel** som eksponerer det industrielle IKT-systemets sårbarhetsflate. Dette inkluderer blant annet at systemer kan infiseres hos leverandør, under transport til installasjonen, og gjennom oppdatering av system på stedet eller via fjerntilgang.

Umiddelbar **konsekvens** av en hendelse kan være at det industrielle IKT-systemet er utilgjengelig, at kontroll av systemet er tatt over av uvedkommende, eller at systemet i seg selv er kompromittert. Videre hendelsesforløp spenner fra mindre kritiske konsekvenser som nedstengning av operasjonen, til mer kritiske konsekvenser.

Eksempler på informasjonssikkerhetshendelser, fra NSR Mørketallsundersøkelsen 2018

- Virus og/eller malwareinfeksjon
- Phishing eller andre sosial manipulerings angrep
- Forsøk på datainnbrudd/hacking
- Hendelser forårsaket av bedriftens ansatte
- DDoS angrep eller trusler om
- Bedrageri
- Dataskadeverk
- Tyveri av IT-utstyr
- Datainnbrudd/hacking
- Misbruk av IT-ressurser
- Brudd på sikring av opplysninger om f.eks. brukere, ansatte, kunder, pasienter?
- Penetrasjon av organisasjonens sikkerhetssystemer
- Hendelse forårsaket av outsourcingsleverandør
- Tapt forretningshemmeligheter gjennom informasjonstyveri/digitalspionasje

Faktaboks 3-4: Eksempler på informasjonssikkerhetshendelser (ref. /33/)

3.7 Aktører

Dette kapittelet beskriver ulike aktører som kan være relevante for en operatørs håndtering av sikkerhet i de industrielle IKT-systemene og IT-systemene. Første delkapittel viser en oversikt av hvilke typer aktører som påvirker sikkerheten i en operatørs industrielle IKT-systemer.

De to neste delkapitlene beskriver noen norske aktører som er relevante for henholdsvis industriell IKT-sikkerhet og trening og øvelse. Listen omfatter myndighetsaktører, fagmiljøer, og beredskapsressurser for datasikkerhetshendelser (CERT, CSIRT). Informasjonen gjengitt fra aktørene er i hovedsak hentet fra aktørenes egne hjemmesider.

3.7.1 Aktører som påvirker en operatørs IKT-sikkerhet

Det er mange aktører som vil påvirke og bidra til en virksomhets håndtering av sikkerheten relatert til sitt industrielle IKT-system. Aktørene nevnt under er ikke ment å være en komplett oversikt over relevante aktører, men gir eksempler på aktører som vil være relevante for å opprettholde industriell IKT-sikkerhet ved en petroleumsinnretning.

Operatør av innretningen vil ha ansvar for operasjon av innretningens produksjonssystemer som omfatter industrielle IKT-systemer. I tillegg til operatør av innretningen kan det også være separate operatører av spesifikke operasjoner. En boreoperatør vil for eksempel ha ansvar for industrielle IKT-systemer benyttet for boreoperasjoner på innretningen.

Leverandører av industrielle IKT-systemer eller komponenter til slike systemer, er en vesentlig premissleverandør for sikkerheten relatert til det industrielle IKT-systemet, både gjennom utvikling av systemet, installasjon, konfigurering og vedlikehold. Et industrielt IKT-system kan være levert av én leverandør eller satt sammen av leveranser fra ulike leverandører.

For enkelte innretninger fjernstyres en operasjon i dag fra land, eller fra en nærliggende installasjon. Dette krever et nettverk for kommunikasjon mellom kontrollrom og prosesskontroll og nødavstengnings-systemer og videre til sensorer og aktuatorer som bidrar til å monitorere og styre anlegget. Nettverket vil derfor være en integrert del av det industrielle IKT-systemet i likhet med andre systemkomponenter. Dermed vil leverandøren av nettverket og nettverkstjenester være en premissleverandør for tilgjengelig til systemet.

Noen operatører vil gjøre egne analyser av trusselbildet, men det er forventet at man også vil forholde seg til informasjon fra myndigheter og andre som analyserer og presenterer et trusselbilde for industrien. Dette er informasjon som bør legge grunnlag for beredskapsstrategier, beredskapsplaner, øvelsesdirektiver, treningsmål, og lignende. Aktører som kan bidra med å etablere eller formidle trusselbilder for en virksomhet inkluderer Politiets sikkerhetstjeneste (PST), Forsvarets etterretningstjeneste, Nasjonal sikkerhetsmyndighet (NSM), eller sektorvise responsmiljøer (SRM).

Sektorvise responsmiljøer og CERT/CSIRT'er[4] vil også kunne bistå i beredskapsarbeid og koordinert respons til IKT-sikkerhetshendelser.

Gjeldende lover og forskrifter er også en viktig premissleverandør for hvordan virksomheten håndterer IKT-sikkerhet.

[4] CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team). CERT er et registrert varemerke tilhørende Carnegie Mellon University

Leverandører av trening og øvelse omfatter for eksempel aktører som bidrar i utvikling av e-læringskurs for å øke bevisstheten rundt IKT-sikkerhet blant virksomhetens personell, aktører som gjennomfører inntrengningstester og «red-team»-øvelser[5], og aktører som bidrar til utarbeidelse, gjennomføring og evaluering av øvelser.

3.7.2 Ressurser relevante for IKT-sikkerhet

NSM – Norsk sikkerhetsmyndighet

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

Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet(sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid. Nasjonalt cybersikkerhetssenter (NCSC) ble etablert 2018. Senteret bidrar til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep.

Følgende ressurser er en del av NSM:

- *NCSC er underlagt NSM og er et samhandlingssenter mellom NSM, andre myndigheter, og aktører i næringslivet som er eier kritisk infrastruktur.*
- *NorCERT er en funksjon i NCSC.*
- *VDI er et sensornettverk som inngår i NorCERT sine verktøy.*

NCSC – Nasjonalt Cybersikkerhetssenter

https://www.nsm.stat.no/om-nsm/tjenester/nasjonalt-cybersikkerhetssenter-ncsc/

Nasjonalt cybersikkerhetssenter er etablert for å styrke Norges motstandsdyktighet og beredskap i det digitale rom. Senteret samler ressurser i NSM som har vært spredt i ulike avdelinger, og vil samarbeide tett med aktører i næringsliv, eiere av kritisk infrastruktur, og andre offentlige myndigheter som politiet og etterretningstjenesten.

- Nasjonalt cybersikkerhetssenter gir anbefalinger og rådgiving til offentlige myndigheter og næringsliv.
- Nasjonalt cybersikkerhetssenter samler nasjonal deteksjonsevne, hendelseshåndtering og cyberanalyse i det digitale rom.
- Nasjonalt cybersikkerhetssenter tilbyr en rekke tekniske tjenester for offentlige myndigheter og private virksomheter.

Nasjonalt cybersikkerhetssenter (NCSC) drifter og organiserer et nasjonalt sensornettverk på internett. Sensornettverket skal avdekke forsøk på datainnbrudd mot kritisk infrastruktur på tvers av sektorer. VDI er kort fortalt en digital innbruddsalarm for AS Norge.

[5] Se beskrivels av «red-team» i kapittel 6.3 og Faktaboks 6-1.

NorCERT – Norwegian Computer Emergency Response Team

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

Koordinerende enhet for IKT-sikkerhetshendelser, dedikert til cybersikkerhet og hendelseshåndtering i NCSC (Nasjonalt cybersikkerhetssenter). I vårt operasjonssenter håndteres alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.[7]

VDI – Varslingssystem for digital infrastruktur

https://no.wikipedia.org/wiki/Varslingssystem_for_digital_infrastruktur

VDI-samarbeidet er i stor grad basert åpenhet og tillit mellom NSM og deltagende bedrifter og etater. For den enkelte bedrift/etat er trafikkmengde, sikkerhetsmekanismer og fiendtlig aktivitet i egne datanettverk konfidensiell informasjon. Derfor blir også data fra VDI-sensorene behandlet konfidensielt.

KraftCERT

https://www.kraftcert.no/

KraftCERT jobber for bedre sikring i prosesskontroll-systemer ved å bistå kraftbransjen slik at de skal være oppdatert om relevante sårbarheter og trusler, og at de skal være i stand til å detektere og motvirke digitale angrep.

KraftCERT bistår også i håndtering av digitale sikkerhetshendelser og er med i den nasjonale beredskapsorganisasjonen. KraftCERT jobber for en god, sikker og effektiv informasjonsdeling mellom relevante selskaper nasjonalt og internasjonalt.

KraftCERT startet opp som ett av flere ulike sektorsvise responsmiljø. KraftCERT har etterhvert omfavnet aktører også utenfor kraftsektoren som det opprinnelig ble dannet for, og har i dag medlemmer fra blant annet kommunale vann- og avløpsselskaper og petroleumssektoren. Det etablert flere andre sektorsvise CERT-milljøer som også koordinerer respektive sektorer mot NorCERT.

3.7.3 Ressurser relevante for trening og øvelse

NorSIS – Norsk senter for informasjonssikring

https://norsis.no/

NorSIS er en uavhengig organisasjon som arbeider for økt kunnskap om, og forståelse for, informasjonssikkerhet. NorSIS mottar økonomisk støtte fra Justis- og beredskapsdepartementet, og er en del av myndighetenes nasjonale satsing på informasjonssikkerhet. En viktig oppgave for NorSIS er å gi råd og veiledning til befolkningen, bedrifter og offentlige virksomheter.

[7] NorCERT er en nasjonal sektorovergripende CERT. I tillegg til NorCERT eksisterer det en rekke andre CERT og CSIRT, hvorav KraftCERT er ett eksempel på et sektorvist responsmiljø for Kraftbransjen. Sektorsvise responsmiljø koordinerer respektive sektorer mot NorCERT.

3.7.4 Andre ressurser

PST – Politiets sikkerhetstjeneste

https://www.pst.no/

PSTs primære ansvar er å forebygge og etterforske straffbare handlinger mot rikets sikkerhet. Dette gjør tjenesten gjennom ulike metoder og arbeidsmåter. Sentralt står innsamling av informasjon om personer og grupper som kan utgjøre en trussel, utarbeidelse av ulike analyser og trusselvurderinger, etterforskning og andre operative tiltak, og rådgivning.

Etterretningstjenesten (e-tjenesten)

https://forsvaret.no/organisasjon/etterretningstjenesten

Etterretningstjenesten er Norges militære og sivile utenlandsetterretningstjeneste. Selv om tjenesten er en integrert del av Forsvarets organisasjon og virksomhet, løser tjenesten oppdrag for hele myndighetsapparatet og arbeider etter overordnede politiske prioriteringer.

Etterretningstjenestens ansvar er å forebygge og holde oversikt over trusler fra utlandet, mens politiet – spesielt PST og Kripos – har tilsvarende ansvar for innenlandske trusler og for å etterforske cyberkriminalitet. Etterretningstjenesten er fagmyndighet for cyberoperasjoner i Forsvaret, og har overordnet ansvar for å koordinere slike operasjoner.

NSO – Næringslivets sikkerhetsorganisasjon

https://nso.no/

NSO er tilsynsmyndighet etter sivilbeskyttelsesloven § 23 og bestemmelser gitt i medhold av denne. NSOs oppgaver er å organisere og føre tilsyn med egenbeskyttelsestiltak ved virksomheter som kommer under forskrift om industrivern.

NSR – Næringslivets sikkerhetsråd

https://www.nsr-org.no/

Næringslivets Sikkerhetsråd er en medlemsorganisasjon som har som formål å forebygge kriminalitet mot næringslivet. Arbeidet gjøres gjennom formaliserte og aktive nettverk bestående av offentlige sikkerhetsmyndigheter og medlemmer fra næringslivet, samt rådgivning, kurs og seminarer.

4 LITTERATURSTUDIE

Som en del av dette delprosjektet er det gjennomført en studie av tilgjengelig litteratur som adresserer sikkerhet relatert til industrielle IKT-systemer, med fokus på trening, øvelse og beredskap, og tilhørende tiltak. Studien dekker også en gjennomgang av litteratur som omhandler trening, øvelse og beredskap rettet mot fysiske hendelser. Dette for om mulig å identifisere tiltak som også vil kunne være relevante for trening og øvelse for IKT-sikkerhet. Litteraturstudien har omfattet lover, forskrifter, rammeverk, standarder og veiledninger, og utvalgte dokumenter som gir anbefalinger til hvordan man utfører trening og øvelse, både nasjonalt og internasjonalt. Studien er ikke begrenset seg kun til olje- og gassektoren, men inkluderer også offentlig sektor (stat/kommune), luftfart og kraftsektoren.

4.1 Lover og forskrifter

4.1.1 Lover

Lov om petroleumsvirksomhet (Petroleumsloven) (ref. /2/) gjelder for all norsk land- og havbasert petroleumsvirksomhet. Loven inneholder ingen paragrafer som henviser spesifikt til IKT-sikkerhet, ei heller trening og øvelser. Dog adresserer § 9-2 *Beredskap* og § 9-3 *Beredskap mot bevisste anslag* viktigheten av å opprettholde effektiv beredskap for å håndtere *«fare- og ulykkessituasjoner som kan medføre tap av menneskeliv eller personskade, forurensning eller stor materiell skade»* både med hensyn til ikke-planlagte og bevisste ondsinnede handlinger. Innholdet i disse to paragrafene er allikevel relevante for håndtering av IKT-sikkerhetsbrudd selv om ikke dette står eksplisitt.

Stortinget vedtok 27.02.2018 ny lov om nasjonal sikkerhet (Sikkerhetsloven) som er rettet mot å beskytte informasjon som behandles elektronisk og sikre at uvedkommende ikke får tilgang til systemer som er avgjørende for våre grunnleggende nasjonale funksjoner. Loven stiller tydelige krav om sikring av IKT-systemer. Loven omfatter forvaltningsorganer som er i besittelse av skjermingsverdig informasjon eller objekt, leverandører til disse som kan få tilgang til skjermingsverdig informasjon eller objekt, samt noen spesielt utvalgte andre virksomheter av kritisk betydning for samfunnet.

Den nye Sikkerhetsloven trådte i kraft 1.1.2019 (ref. /1/). Per november 2019 gjelder ikke Sikkerhetsloven for petroleumsnæringen, men dette er under utredning. Loven sier lite spesifikt om trening og øvelser, men § 4-3 *Plikt til å gjennomføre sikkerhetstiltak og øvelser* stiller krav om at «*Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. (...) Virksomheten skal regelmessig gjennomføre øvelser for å vurdere effekten av iverksatte sikkerhetstiltak.*» § 4-3 vil i prinsippet være relevant uavhengig om organisasjonen er underlagt Sikkerhetsloven eller ikke.

Lov om luftfart (Luftfartsloven) (ref. /3/) gjelder for sivil og militær luftfart samt luftfart i tilknytning til petroleumsvirksomhet på norsk kontinentalsokkel. Loven regulerer landingsplasser og Flysikringstjenesten. Loven inneholder ingen paragrafer som henviser spesifikt til IKT-sikkerhet. I Luftfartstilsynets arbeid med IKT-sikkerhet benyttes imidlertid i dag EU Regulering 1035/2011 som basis. I 2020 vil denne bli erstattet av EU Regulering 373/2017 hvor begrepet "Cyber Security» nevnes for første gang eksplisitt. Angående trening og øvelser sier lovens paragraf § 13-9 *Beredskap* følgende «*For å sikre nødvendig nasjonal beredskap i krig, ved krise, og i andre ekstraordinære situasjoner, kan departementet pålegge aktører innen luftfarten å yte bistand i form av (...) b) gjennomføring av eller deltagelse i øvelser og militære luftoperasjoner (...)*». I tillegg har man fra § 5-3 *Krav til tjenestegjørende på luftfartøy* at «*Den som skal gjøre tjeneste på luftfartøy, må oppfylle de vilkår departementet fastsetter med hensyn til statsborgerforhold, alder, fysisk og psykisk skikkethet, vandel, edruskap, utdanning og øvelse m.m.*».

4.1.2 Forskrifter

Ny forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften**)** trådte i kraft 1.1.2019 (ref. /4/). Forskriften er hjemlet i sikkerhetsloven og henviser i to paragrafer, § 5 *Sikkerhetsmål* og § 9 *Evaluering og øvelser*, til viktigheten av å gjennomføre og evaluere øvelser for å tilfredsstille kravet til å opprettholde et forsvarlig sikkerhetsnivå i virksomheten. I § 9 står det spesifikt «*En virksomhet skal regelmessig evaluere om kravet til et forsvarlig sikkerhetsnivå er oppfylt og minst én gang i året evaluere om styringssystemet for sikkerhet er egnet til å sørge for at kravet oppfylles, jf. §5».* Videre står det i § 9 «*Resultatet av evalueringer og øvelser skal inngå i den årlige gjennomgangen av det forebyggende sikkerhetsarbeidet i virksomheten*.»

I 2018 ble forskrift om sikkerhet og beredskap i kraftforsyningen (Kraftberedskapsforskriften**,** 2012) (ref. /10/) endret for å ta inn nye/skjerpede krav til IKT-sikkerhet (endringer, ref. /11/) og en revidert forskrift trådte i kraft 01.01.2019. Temaet øvelser er omtalt i § 2-7 *Øvelser* og § 2-9 *Evaluering*, hvor førstnevnte stiller krav om gjennomføring av øvelser og at virksomheten skal ha en flerårig øvelsesplan og gjennomføre minimum én årlig øvelse. § 2-9 stiller krav om at det skal gjennomføres en evaluering etter øvelser som skal benyttes blant annet til utvikling av beredskapskompetanse og beredskapsplaner. I 2013 ble det utarbeidet en veiledning til forskriften som var gjeldende på det tidspunktet (ref. /34/) som utdyper hvordan øvelser skal planlegges, praktisk gjennomføres og evalueres. IKT-hendelser er nevnt som et tema som det skal øves på (ref. /34/, kap. 2.7.3).

I NOU 2018:14 (ref. /40/) vurderer utvalget om organisering og regulering av nasjonal IKT-sikkerhet følgende; «Gitt det gjeldende IKT-risikobildet mener utvalget at det må utarbeides en ny lov hvor det stilles krav om forsvarlig IKT-sikkerhet til alle samfunnskritiske virksomheter og offentlig forvaltning. Den nye loven skal også gjennomføre NIS-direktivet i norsk rett. Kravene som følger av loven, må konkretiseres i forskrift og veiledning.»

Justis- og beredskapsdepartementet har i ett høringsnotat fra desember 2018 (ref. /41/) lagt frem et utkast til en ny lov som skal kunne gjennomføre EUs NIS-direktiv i norsk rett. Dette ble lagt til høring sammen med NOU 2018:14, og er ifølge Regjeringen.no (per Januar 2020) under behandling[9].

EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) trådte i kraft i EU i august 2016 (ref. /15/). Forslaget til ny forordning innebærer at EUs *European Network and Information Security Agency* (ENISA) skal få et permanent og styrket mandat. Direktivet adresserer trening og øvelser spesifikt kun ved at det sies at øvelser er viktige for å teste medlemsstatenes beredskap angående nettverkssikkerhet og sikkerhet av informasjonssystemer (security), og er et verktøy for utarbeidelse av anbefalinger og tiltak for håndtering av IKT-sikkerhetshendelser.

4.1.3 Ptils forskrifter

Forskrift om utføring av aktiviteter i petroleumsvirksomheten (Aktivitetsforskriften) er den eneste av Ptils forskrifter som eksplisitt dekker temaet trening og øvelser; § 23 *Trening og øvelser*. Andre forskriftskrav som danner et relevant grunnlag for å kunne utføre fornuftig trening og øvelser, inkluderer Aktivitetsforskriften § 21 *Kompetanse*, § 75 *Beredskapsorganisasjon* og § 76 *Beredskapsplaner* (ref. /5/), og § 19 *Verifikasjoner* i forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (Rammeforskriften) (ref. /7/).

[9] https://www.regjeringen.no/no/dokumenter/horing-nou-2018-14-ikt-sikkerhet-i-alle-ledd-og-utkast-til-lov-som-gjennomforer-nis-direktivet-i-norsk-rett/id2623252/

Ptils forskrifter og veiledninger peker generelt sett ikke på konkrete hendelsestyper. Selv om for eksempelvis IKT-sikkerhetshendelser ikke er eksplisitt nevnt i forskriftsparagrafer og veiledning så betyr ikke det at slike hendelser ikke er omfattet av forskriftene. I et brev til næringen datert september 2019 (ref. /43/) presiserer Ptil sin forståelse av hvordan paragrafer i HMS-regelverket og som er relevante i vurderingen av IKT-sikkerhet for industrielle kontroll- og sikkerhetssystemer, kan komme til anvendelse. Relatert til trening og øvelse, henviser dette brevet blant annet til § 21 *Kompetanse* og § 23 *Trening og øvelser* i Aktivitetsforskriften (ref. /5/). Tabell 4-1 presenterer utdrag fra Ptils forskrifter relevante for trening, øvelse og beredskap.

Tabell 4-1: Ptils relevante regelverk rettet mot IKT-sikkerhet samt trening og øvelse

Forskrift, paragraf og tittel	Forskriftstekst (relevant utdrag)	Veiledningstekst (relevant utdrag)
Aktivitetsforskriften § 23 Trening og øvelse	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.	For å oppfylle kravet til trening og øvelser bør a) simulatortrening brukes for overvåkings- og kontrollfunksjoner, b) de som har beredskapsfunksjoner, trene på sine beredskapsoppgaver minst én gang i løpet av oppholdsperioden. Alle som deltar i beredskapsledelse bør trene på sine beredskapsfunksjoner minst én gang i året. Det bør gjennomføres minst én årlig øvelse for beredskapsledelsen. Resultatet av øvelsen bør evalueres. **Presisering av Ptils forståelse av anvendelse for IKT-sikkerhet for industrielle kontroll- og sikkerhetssystemer** 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 § 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 til sikring av kompetansen innebærer blant annet at det stilles krav til nødvendig kompetanse, at kompetansen blir verifisert, og at den blir holdt ved like gjennom trening, øvelser, opplæring og utdanning. **Presisering av Ptils forståelse av anvendelse for IKT-sikkerhet for industrielle kontroll- og sikkerhetssystemer** Kravet om kompetanse er også relevant for de som skal håndtere faresituasjoner i forhold til IKT- hendelse med de industrielle kontroll- og sikkerhetssystemene

Forskrift, paragraf og tittel	Forskriftstekst (relevant utdrag)	Veiledningstekst (relevant utdrag)
Aktivitetsforskriften § 75 Beredskaps-organisasjon	Beredskapsorganisasjonen skal være robust slik at den kan håndtere fare- og ulykkessituasjoner på en effektiv måte.	Med beredskapsorganisasjonen menes det personellet som er knyttet direkte til enhetsressursene, områderessursene, de eksterne ressursene og de regionale ressursene. For å sikre robustheten bør det ved utvelgelse av personellet legges vekt på den enkeltes utdanning og kompetanse, erfaring, personlige egenskaper og erfaringer fra øvelser og trening. Fare- og ulykkessituasjonene som omfatter også andre fare- og ulykkessituasjoner enn de definerte, sammensatte fare- og ulykkessituasjoner, stressituasjoner og situasjoner der nøkkelpersonell faller fra eller svikter.
Aktivitetsforskriften § 76 Beredskaps-planer	Det skal utarbeides beredskapsplaner som til enhver tid beskriver beredskapen og inneholder aksjonsplaner for de definerte fare- og ulykkessituasjonene.	Beredskapsplanene bør blant annet inneholde a) en beskrivelse av formål, omfang og ansvar, b) en beskrivelse av organisering, varsling, mobilisering og kommunikasjon, c) aksjonsplaner, e) en beskrivelse av enhetsressurser, områderessurser, regionale ressurser og eksterne ressurser og utstyr, f) instrukser for beredskapspersonell, g) eventuelle samordningsprosedyrer for samordning med andre aktører h) eventuelle samarbeidsprosedyrer og avtaler Aksjonsplaner som nevnt i denne veiledningen bokstav c, bør blant annet omhandle a) beredskapsstrategi, beredskapstiltak og beslutningskriterier for beredskapsfasene.
Rammeforskriften § 19 Verifikasjoner	Den ansvarlige skal ta stilling til behov for og omfang av verifikasjoner, metode for og grad av uavhengighet i verifikasjonen for å dokumentere at	Verifikasjon kan omfatte kontroll av beregninger, tegninger og fabrikasjon ved å gå gjennom det som er gjort, samt å foreta uavhengige eller egne beregninger. Verifikasjonen kan også innbefatte prøving eller testing av produkter og systemer. Når den ansvarlige skal verifisere at krav i helse-, miljø- og sikkerhetslovgivningen

Forskrift, paragraf og tittel	Forskriftstekst (relevant utdrag)	Veiledningstekst (relevant utdrag)
	krav i helse-, miljø- og sikkerhetslovgivningen er oppfylt. Når verifikasjoner er besluttet gjennomført, skal slike verifikasjoner utføres i henhold til et helhetlig og entydig verifikasjonsprogram og verifikasjonsgrunnlag. Operatøren skal fastsette verifikasjonsgrunnlaget for den samlede virksomheten etter å ha foretatt en vurdering av omfang av, metoder for og graden av uavhengighet i verifikasjonen. Operatøren skal også foreta en samlet vurdering av resultatene fra gjennomførte verifikasjoner.	er oppfylt, omfatter dette også verifikasjon av de interne kravene som den ansvarlige setter for å konkretisere krav i helse-, miljø- og sikkerhetslovgivningen, og som skal bidra til å oppnå de målene og strategiene for helse, miljø og sikkerhet som den ansvarlige har etablert. Det er gitt krav til blant annet etablering av mål og strategier og til fastsetting av interne krav i den utfyllende styringsforskriften. Når det gjelder omfanget av verifikasjon, vil det avhenge av type krav. For eksempel vil det normalt være behov for å verifisere samsvar med krav i helse-, miljø- og sikkerhetslovgivningen på de tekniske områdene. Når det gjelder graden av uavhengighet, innebærer dette normalt at verifikasjoner skal utføres av en annen enn den som har utført arbeidet som skal verifiseres, eller den som har utarbeidet verifikasjonsgrunnlaget, samt at det er organisatorisk uavhengighet for rapportering i linjen. En viktig forutsetning er at den enheten som foretar verifikasjonen har nødvendig kompetanse og nødvendige ressurser til å utføre den.

4.2 Rammeverk og standarder

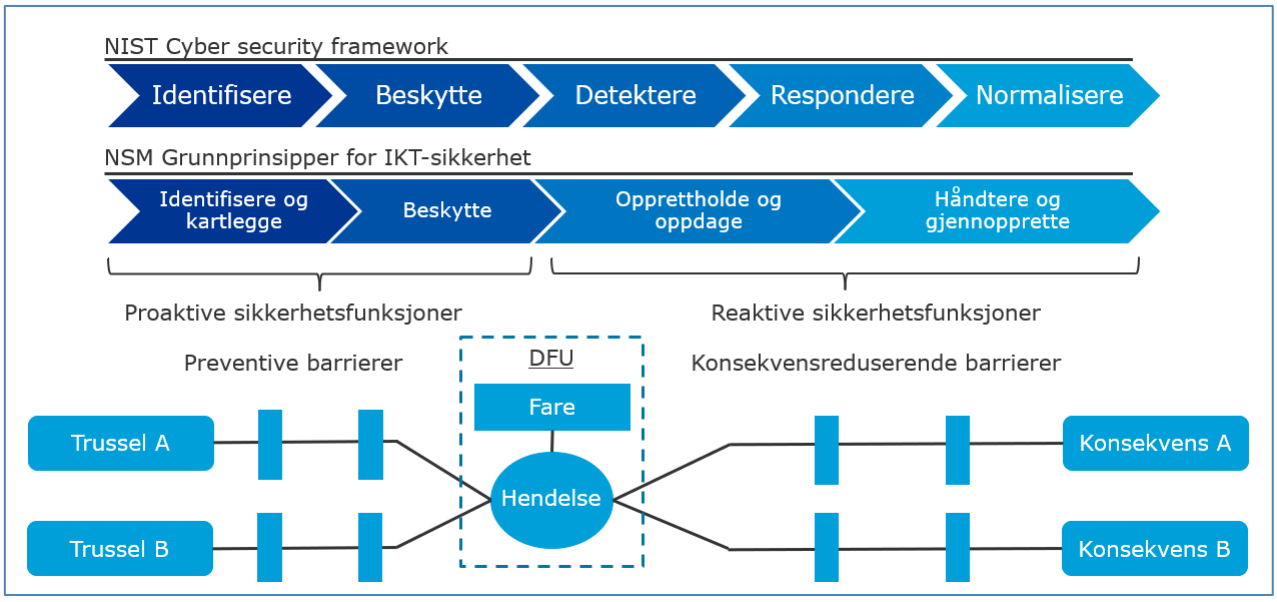
IKT-sikkerhetsrammeverk beskriver hvordan virksomheter skal jobbe med IKT-sikkerhet. Dette knytter sammen virksomhetens behov med tiltak og en struktur for implementering av disse tiltakene slik at virksomheten oppnår tilfredsstillende IKT-sikkerhet. Rammeverkene viser til standarder og veiledninger for mer utfyllende beskrivelser av hvordan tiltak kan implementeres. Trening og øvelsesaktiviteter inngår som del av tiltakene som anbefales i rammeverk og standarder for å adressere sikkerhetsfunksjonene som er spesifisert i rammeverkene.

4.2.1 Rammeverk - Sikkerhetsfunksjoner, grunnprinsipper og tiltak

National Institute of Standards and Technology (NIST, USA) har beskrevet et rammeverk for IKT-sikkerhet (Cyber Security Framework – CSF) (ref. /38/). NIST CSF er et generelt og sektorovergripende rammeverk utviklet for å gi virksomheter en risikobasert metode for å beskytte kritisk infrastruktur. I CSF har NIST definert fem overordnede IKT-sikkerhetsfunksjoner. To av funksjonene er proaktive og omfatter tiltak for å identifisere og beskytte seg mot hendelser før de inntreffer, og tre av funksjonene er reaktive og omfatter deteksjon og respons på hendelser, og normalisering av virksomhetens operasjon. Beredskap, trening og øvelse er blant tiltakene som anbefales for å opprettholde sikkerhetsfunksjonene.

NSM har beskrevet et rammeverk for håndtering av IKT-sikkerhet (ref. /29/) 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 (ref. /28/). NSM skriver her at kategoriseringen av grunnprinsippene er *«... i stor grad sammenfallende med gjeldende inndeling i «Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)» og «NIST Cyber Security Framework»»*.

Sikkerhetsfunksjonene definert av NIST og kategoriene som NSM benytter er presentert i Figur 4-1. Figuren viser også sammenhengen mellom de proaktive og reaktive sikkerhetsfunksjonene og preventive og konsekvensreduserende barrierer i et barrierediagram av en definert fare og ulykkeshendelse (DFU).



Figur 4-1: Oversikt over NIST IKT-sikkerhetsfunksjoner og NSMs kategorier av grunnprinsipper

NSM knytter en rekke konkrete tiltak opp mot hvert av grunnprinsippene som igjen er sortert under sikkerhetsfunksjonene. NIST CSF har under sine definerte sikkerhetsfunksjoner tilsvarende kategorier (grunnprinsipper) og subkategorier (tiltak). Subkategoriene som listes opp i NIST CSF er en kort beskrivelse av tiltak som anbefales, men viser også til informative referanser for mer detaljert beskrivelse av hvordan tiltaket kan implementeres. NSM gir i motsetning til NIST en mer utfyllende kontekst og beskrivelse av formålet til grunnprinsippene som tiltakene knyttes opp mot.

4.2.2 Standarder og retningslinjer

NSM skriver i ref. /28/ at *«Grunnprinsippene som har sektorovergripende fokus uthever de viktigste sikkerhetstiltakene i ISO/IEC 27002:2017.».* For de ulike subkategoriene i NIST CSF vises det til informative referanser som blant annet inkluderer ISO/IEC 27001:2013[10] og IEC 62443. ISO/IEC 27001 (ref. /12/) og IEC 62443 (ref. /14/) er sektorovergripende internasjonale standarder der den første omhandler IT-sikkerhet og inneholder krav til styringssystemer for IT-sikkerhet, og den andre definerer elementer for å etablere styringssystem for sikkerhet i industrielle automasjons og kontroll systemer.

ISO/IEC 27001:2017 stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. Annex A lister opp kontrollpunkter sortert i kategorier og subkategorier, men disse er i motsetning til NIST og NSM ikke knyttet til ulike sikkerhetsfunksjoner. Ifølge standarden skal en organisasjon selv gjøre en risikovurdering og etablere en prosess for å styre risikoen. Dette inkluderer å definere egne passende tiltak. Listen over kontrollpunkter i Annex A kan i denne sammenheng fungere som en sjekkliste for organisasjonen. ISO/IEC 27002:2017 (ref. /13/) er et beste praksis dokument som gir veiledning inkludert eksempler på tiltak for å implementere kontrollpunktene som er listet opp i ISO/IEC 27001:2017 Annex A.

IEC 62443 er en serie standarder, hvorav part 2-1 omfatter etablering av styringssystem for industriell IKT-sikkerhet, og lister opp elementer som inngår i å analysere sikkerhetsrisiko for industrielle IKT-systemer, adressere risiko gjennom styringssystemer for IKT-sikkerhet, og monitorering og forbedring av styringssystemer for IKT-sikkerhet.

Bransjeorganisasjonen *Norsk olje og gass* har utgitt en anbefalt guideline med grunnleggende krav til informasjonssikkerhet (NOROG 104, ref. /47/) spisset mot norsk petroleumsvirksomhet. NOROG 104 har adoptert IKT-sikkerhetsfunksjonene som er definert av NIST CSF, men i motsetning til NIST og NSM er de grunnleggende kravene (Information Security Baseline Requirements – ISBR) knyttet opp på tvers av funksjonene. En ISBR inneholder beskrivelse av formål og tilhørende liste av tiltak som vil kunne styrke en eller flere sikkerhetsfunksjoner.

DNVGL-RP-G108 (ref. /26/) er en guideline som beskriver hvordan IEC 62443-standardene kan implementeres for virksomheter i petroleumsindustrien. DNVGL-RP-G108 er strukturert i henhold til prosjektfaser for utvikling og operasjon av olje og gass innretninger. Denne guidelinen er utviklet gjennom et industrisamarbeidsprosjekt som involverte fire operatørselskaper, fem leverandører av industrielle IKT-systemer, Petroleumstilsynet og DNV GL.

Den internasjonale organisasjonen for drillingselskaper (IADC) har utgitt en IKT-sikkerhetsguideline (ref. /51/) 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.

[10] Tidligere versjon av ISO/IEC 27001:2017.

4.2.3 Trening og øvelse

Alle referansedokumentene som er nevnt i kapittel 4.2.1 og 4.2.2 viser til tiltak som anbefales gjennomført for å oppnå tilfredsstillende IKT-sikkerhetsnivå. Det er imidlertid få tiltak som eksplisitt beskriver trening og øvelse. To temaer som likevel går igjen, er bevisstgjøring (trening) og å gjennomføre tester (øvelser) av virksomhetens kapasitet for sikkerhetskopiering og gjenoppretting av systemer og data. I tillegg nevnes trening i risikovurderingsmetode (IEC 62443), beredskapsøvelser (NSM Grunnprinsipper og IEC 62443), og øvelser relatert til deteksjon og inntrengningstester (NSM Grunnprinsipper og NIST CSF).

Utdrag (oversatt til norsk) fra referansene beskrevet i 4.2.1 og 4.2.2 som omfatter tiltakene relatert til trening og øvelse, inkludert tiltak som viser til regelmessige tester av prosedyrer, er oppsummert i Appendix A.

4.3 Veiledere - Planlegging, gjennomføring og evaluering av øvelser

Litteraturstudiet har identifisert tre sentrale veiledere for praktisk planlegging, gjennomføring og evaluering av øvelser utarbeidet av henholdsvis DSB, Difi og NVE.

DSB sin *Veileder i planlegging, gjennomføring og evaluering av øvelser; Grunnbok: Introduksjon og prinsipper* (ref. /16/) er uavhengig av type hendelse som man ønsker å øve på. Den ble utarbeidet for å gi en helhetlig tilnærming til planlegging, gjennomføring, evaluering og oppfølging av øvelser. En felles tilnærming til arbeidet med øvelser vil bidra til at det blir enklere å øve sammen, både på lokalt, regionalt, nasjonalt og internasjonalt nivå. Veilederen gir en innføring i hva øvelser er, hvorfor er det viktig å øve, ulike typer øvelser og hvilke faser en øvelse består av. Uavhengig av øvelsestype, vil øvelsene bestå av de samme fasene og mange av de forberedende aktivitetene vil være de samme. I tillegg til selve veilederen har DSB utarbeidet supplerende metodehefter (veiledningsmateriale) som detaljerer og beskriver forskjellige øvelsestyper (ref. /17/ - /20/), anbefaling til gjennomføring og planlegging av evalueringer etter øvelser (ref. /21/), samt krav til lokal øvingsleder (ref./22/).

Difi sin *Veileder i planlegging og gjennomføring av IKT-øvelser* (ref. /24/), adresserer øvelser rettet mot IKT-sikkerhet spesifikt. Dette er en høringsutgave fra 2016 og er ikke blitt oppdatert. Veilederen viser hvordan øvelsen spiller inn i en virksomhets risikostyringssystem, og vektlegger informasjonssikkerhet og virksomhetskontinuitet. Den gir også en strukturert og generell beskrivelse av hva man ønsker å oppnå ved å øve, hva man øver på, ulike former for øvelser, og typiske steg i gjennomføringen av en øvelse. Veilederen inneholder også forslag til øvelsesdirektiv og maler for planlegging. Selv om målgruppen for veilederen er alle som har ansvar for informasjonssikkerhet i offentlig sektor, og særlig i virksomheter som ikke allerede gjennomfører minst en IKT-øvelse per år, er innholdet relevant uavhengig av sektor olje- og gass-sektoren.

NVE har utarbeidet en veileder for i hvordan planlegge og gjennomføre øvelser innen energiforsyningen (ref. /37/). Veilederen tar utgangspunkt i Kraftberedskapsforskriftens §2-7 *Øvelser* og §2-9 *Evaluering*. Denne veilederen adresserer i hovedsak de samme elementene/temaene som de to ovennevnte veilederne fra DSB og Difi innenfor planlegging, praktisk gjennomføring, evaluering og oppfølging av øvelser. NVEs veileder inkluderer en «scenariebank» som er en beskrivelse av øvelser rettet mot ulike scenarie. Scenariebanken gir eksempler på fire interne IKT-øvelser, hvorav tre er relatert til IT-systemene og ett omfatter angrep på SCADA-systemer.

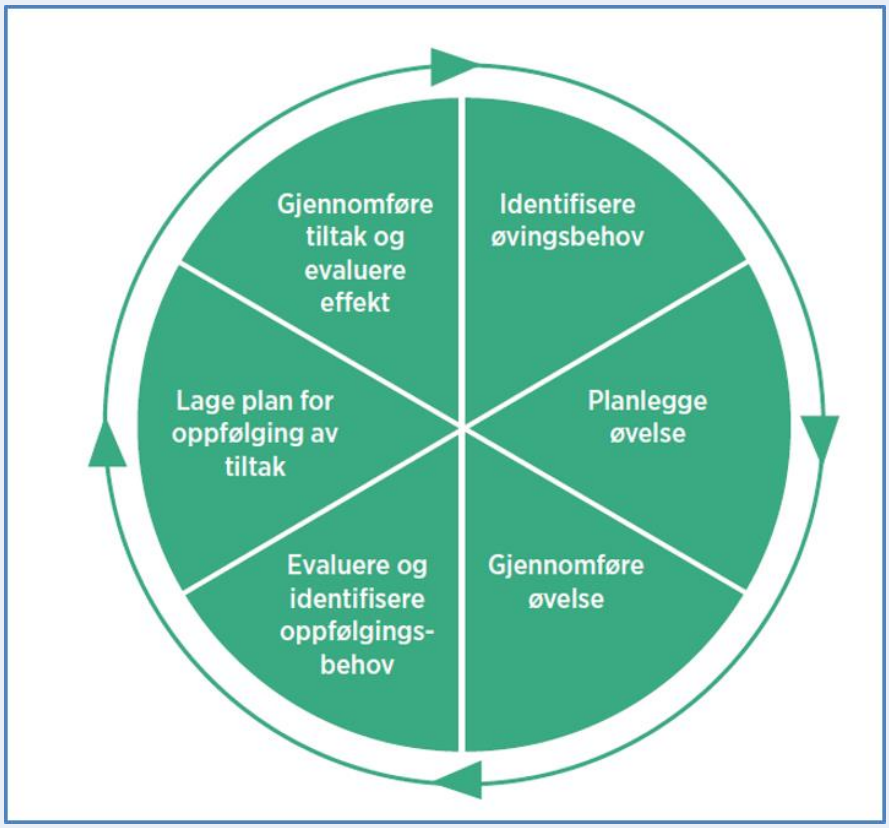
Veilederene vektlegger viktigheten av god planlegging av øvelser, hvor man blant annet skal svare på: hvorfor skal det øves (hensikt), hva er målet med øvelsen, hva skal øves (scenario), hvordan skal det øves (øvelsesform) og hvem skal øvelsen omfatte (ressurser, kompetanse). I tillegg må det besluttes om øvelsen skal favne alle eller enkelte av fasene i håndtering av en uønsket hendelse; det vil si deteksjon, varsling, respons og gjenoppretting/normalisering.

I planleggingsfasen må det også utarbeides en konkret plan for hvordan erfaringene og resultatene fra øvelsen skal evalueres og følges opp videre (evalueringsrapport, oppfølgingsplan). En evalueringsrapport skal blant annet inneholde dokumentasjon av hva som skjedde under øvelsen, analyse og vurdering av hva som kan videreføres og hva som kan endres for å bli bedre, samt identifisere læringspunkter og forslag til tiltak.

Det er vesentlig at arbeidet med beredskap og øvelser sees på som en kontinuerlig prosess. Øvelser er et virkemiddel for å teste og øve beredskapsorganisasjonen. Gjennom evaluering og oppfølging av funn kan beredskapsorganisasjon og planer forbedres, og nye aspekter som bør testes og øves identifiseres. DSB refererer i ett av sine metodehefter (ref. /21/) til *evalueringshjulet* som viser hvordan arbeid med øvelser og beredskap er en kontinuerlig prosess for forbedring av den industrielle IKT-sikkerheten. Den kontinuerlige syklusen for beredskap og øvelsesarbeid er vist i Faktaboks 4-1.

Kontinuerlig forbedring av industriell IKT-sikkerhet gjennom arbeid med øvelser og beredskap

DSB – Evalueringshjulet (ref. /21/)



Faktaboks 4-1: Kontinuerlig forbedring av industriell IKT-sikkerhet gjennom arbeid med øvelser og beredskap

For å sikre en god og strukturert gjennomføring og oppfølging av en øvelse bør det utarbeides øvingsdokumenter som tjener som konkrete hjelpemidler under og etter øvelsen. De mest sentrale dokumentene er oppsummert nedenfor (se ref. /16/ og /24/ for detaljer):

- Øvelsesdirektiv (det overordnede dokumentet som beskriver øvelsen, som gir mandat og budsjettramme for planlegging og gjennomføring av øvelsen, og som inneholder de administrative bestemmelser for gjennomføring av øvelsen)
- Gjennomføringsdirektiv
- Sambandskatalog
- Dreiebok (øvelsens «manus» og er som regel laget som en opplisting av innspill som følger øvelsens tidslinje. I dreieboken er hvert innspill nummerert og tidspunkt for når det skal spilles inn til deltagerne er angitt. Dette gir øvingsleder god og rask oversikt over øvelsens fremdrift)
- Evalueringsdirektiv og -rapport
- Oppfølgingsplan

4.4 Trening og øvelse – andre kilder

Utover ovennevnte lover, forskrifter, standarder og retningslinjer, adresserer en rekke kilder disse temaene. Spesielt kan nevnes Justis- og Beredskapsdepartementets melding til Stortinget (10, 2016 – 2017) *Risiko i et trygt samfunn – Samfunnssikkerhet* (ref. /39/) som har viet et eget kapittel om læring etter øvelser og hendelser. Her sies det blant annet at: «*Systematisk oppfølging og læring etter øvelser og hendelser er viktig for å bedre evnen til å håndtere fremtidige hendelser. Det må sikres at både individer og organisasjoner lærer, og at øvelsesvirksomhet og oppfølging av øvelser og hendelser får nødvendig oppfølging fra ledelsen*.»

Viktighet og nytte av, samt behov, for trening og øvelser er adressert eksplisitt i en rekke andre kilder som har inngått i litteraturstudien. En kort oppsummering av hva disse kildene viser er sitert nedenfor:

- Trening og øvelse er viktige elementer i oppfølging av IKT-sikkerhet.
- Øvelser er et viktig virkemiddel for å øke samfunnets evne til å håndtere kriser og styrke arbeidet med samfunnssikkerhet og beredskap.
- Øvelser skal gi deltagerne kunnskap og erfaring. De skal også bidra til bedre risikoforståelse og sikkerhetskultur.
- Det overordnede mål med øvelser er å lære. Læring bør derfor vektlegges i alle øvelser.
- Øvelser brukes til å forbedre ferdigheter og kompetanse, og til å evaluere og forbedre sikkerhetstiltak og beredskapsplaner.
- Hvordan man planlegger og gjennomfører øvelser og hvilke typer tema man øver på påvirker evnen til å håndtere uønskede hendelser.
- Erfaringer fra øvelser brukes bl.a. til å forbedre planverk, sikkerhetstiltak, og kompetansetiltak.
- Svakheter som avdekkes under øvelser bli brukt i arbeidet med å forbedre og samordne beredskapsplaner.

- Ved øvelse vil forbedringspunkter i beredskap og hendelseshåndtering avdekkes og modenheten vil øke, slik at virksomhetene er i stand til å håndtere alvorlige hendelser.
- For å undersøke om de korrekte sikkerhetsmekanismene er på plass vil det i mange tilfeller lønne seg å gjennomføre tester og øvelser hvor man forsøker å oppnå tilgang til ressurser og data som man ikke skal ha tilgang til.
- En årvåken og risikoerkjennende kultur er viktig. Arbeid i det daglige, gjennom læring etter øvelser og hendelser, er avgjørende for å lykkes.
- Avklarte ansvarsforhold, god rolleforståelse og gjennomtenkte rutiner skapes gjennom praktisk erfaring, øvelser og refleksjon over egen og andres praksis.
- Øvelser er avgjørende for å bli god på krisekommunikasjon.

5 INTERVJUER

5.1 Bakgrunn

Som en del av kunnskapsinnhentingen har totalt 11 virksomheter blitt intervjuet om deres arbeid med trening og øvelsesaktiviteter rettet mot industriell IKT og IT[11]. Følgende har blitt intervjuet; AkerBP, Vår Energi, Lundin, Equinor, Gassco, Mærsk, Transocean, Norske Shell, Avinor, Statkraft, og Statnett. Disse representerer operatører av petroleumsinnretninger til havs, petroleumsrørledninger og landanlegg, boreselskaper, samt kraftbransjen og luftfart. Flertallet av intervjuobjektene har virksomheter både i Norge og utenlands.

I intervjuene til denne studien har vi fokusert på organisering, planlegging og gjennomføring av trening og øvelse. Knytningen mellom beredskap og øvelser har gjort det naturlig å også omfatte beredskap. Studien omfatter fortrinnsvis trening og øvelser rettet mot sikkerhet for industrielle IKT-systemer. Det er likevel erkjent at IT-systemene utgjør en vesentlig del av selskapenes totale sårbarhetsflate og at trening og øvelse relatert til disse også vil påvirke sikkerheten for de industrielle IKT-systemene.

Før intervjuene ble det forberedt en intervjuguide som inneholdt en liste over spørsmål relatert til temaene trening og øvelse, under følgende kategorier:

- Generelt/strategisk
- Overordnet beskrivelse av trening og øvelser[12]
- Innhold (planer, scenarier, faser)
- Deltakere/involverte i øvelser
- Frekvens
- Gjennomføringsmetodikk
- Evaluering og oppfølging

Intervjuene ble lagt opp som samtaler. I de fleste intervjuene ble de fleste spørsmålene i intervjuguiden besvart ved at intervjuobjektene snakket og fortalte om temaene. Ved behov ble intervjuobjektene ledet inn i nye tema. Eventuelle ubesvarte spørsmål ble adressert på slutten av intervjuene.

5.2 Oppsummering

Dette kapittelet oppsummerer resultatene fra intervjuene som ble avholdt.

Trening, øvelse og beredskap. IKT-sikkerhetsarbeid inkluderer både daglig drift og oppfølging av IKT-systemene, og mer strategisk arbeid relatert til sårbarhetsvurderinger, trening av personell med tilgang til systemene, testing av systemene, og øvelser som adresserer både de tekniske løsningene og personell som håndterer disse.

[11] Fokus for studien er trening og øvelser rettet mot industriell IKT. Det er likevel erkjent at IT-systemene kan være en del av IKT-systemenes sårbarhetsflate.
[12] Her ble denne studiens definisjon av begrepene trening og øvelse presisert (se kapittel 3.6.1).

Alle aktørene har opplegg for de ansatte i virksomheten for å øke bevisstheten om IKT-sikkerhet gjennom e-læringsprogrammer og/eller phishing-kampanjer. Disse er av generell karakter og rettet i alt vesentlig grad mot IT-systemer. Lite opplæring er rettet spesielt mot IKT-sikkerhet for industrielle IKT-systemer.

Gjennom intervjuene er det avdekket betydelige forskjeller mellom aktørene når det kommer til modenhet i arbeidet med beredskapsstrategier, beredskapsorganisasjoner, samt planlegging, gjennomføring og evaluering av øvelser for å teste og øve beredskapen. Noen aktører opplyser at de nylig har begynt å legge planer for øvelser rettet mot industrielle IKT-sikkerhet, men at slike foreløpig ikke er gjennomført. I den andre enden av skalaen er det aktører som de siste årene har hatt 1-2 årlige øvelser rettet mot industriell IKT-sikkerhet.

Øvelser rettet mot industriell IKT-sikkerhet har omfattet både øvelser som tester de proaktive sikkerhetsfunksjonene i form av inntrengningstester og «red-team»-øvelser, og øvelser som adresserer de reaktive sikkerhetsfunksjonene (beredskapsøvelser). En del aktører har etablert SOC (Security Operations Center) og en aktør oppgir at SOC vil fungere som «blue-team» i en «red-team»-øvelse.

De fleste oppgir at leverandører/partnere fram til nå ikke har vært inkludert i deres øvelser, men at dette er noe man vurderer å begynne med. Blant de som er tilknyttet en CERT er det noen som har inkludert disse i sine øvelser.

En aktør adresserte problemet med å få gjennomført øvelser samtidig som man er i en 24/7-driftssituasjon.

Noen aktører oppgir å ha utført gjenopprettingsøvelser, og har erfart at dette har avdekket problemer. Dette viser at det er behov for denne typen øvelser.

Det oppgis av flere at håndtering av reelle hendelser (både egne som viser seg å ikke være ondartet, og andres) har blitt evaluert og fulgt opp på lik linje som planlagte øvelser.

En aktør nevnte at de hadde etablert ett beredskapstiltak å varsle ansatte per SMS. Dette for å unngå å måtte varsle IT-hendelser via e-post.

Definert Fare- og Ulykkeshendelse (DFU). En DFU beskriver et hendelsesscenario med tilhørende barrierefunksjoner (se kapittel 3.6.4). DFU'en definerer i så måte hvilke barrierefunksjoner og elementer som er implementert for ulike trusler, og er derfor et godt grunnlag for å vurdere hvilke funksjoner og elementer man skal verifisere tilgjengelighet og effekt av gjennom testing, trening og øvelser.

Omtrent halvparten av petroleumsaktørene har definert en egen DFU for sikkerhetshendelser i industrielle IKT-systemer. Flere aktører utaler at de synes det ville vært nyttig å ha en etablert DFU.

En utfordring relatert til DFU for sikkerhetshendelser i industrielle IKT-systemer er å sette gode ytelseskrav. Ytelseskrav er ofte begrenset til mobiliseringstid.

Beredskap. De fleste aktørene har beredskapsplaner og beredskapsorganisasjon som inkluderer industriell IKT. Noen oppgir at disse er integrert i den generelle beredskapen, mens andre oppgir å ha dedikerte beredskapsorganisasjoner for å håndtere industrielle IKT-hendelser.

Eksterne ressurser. Noen av virksomhetene bruker ressurser fra eksterne tilbydere for å utføre oppgaver som er del av virksomhetens trening og øvelsesaktiviteter rettet mot IKT-sikkerhet. Dette omfatter assistanse til etablering av beredskapsstrategier og -planer, fasilitering av øvelser (planlegging, gjennomføring og evaluering), utføring av inntrengningstester og «red-team»-øvelser. Noen få av virksomhetene har imidlertid økonomi, ressurstilgang og kompetanse til å gjennomføre dette arbeidet internt i virksomheten.

Fellestjenester. Under gjennomføring av øvelser (og reelle hendelser) benytter noen av aktørene seg av bistand fra sektorvise responsmiljøer, CERT'er/CSIRT'er, for å styrke/supplere egen kompetanse og gjennomføringsevne. De større virksomhetene har imidlertid i tillegg egne CSIRT'er (som del av 2. linje-beredskap).

Trusselbilde. De fleste virksomhetene holder seg oppdatert på det til enhver tid gjeldende trusselbildet gjennom egne vurderinger, kunnskap om reelle hendelser innen for egen virksomhet og/eller sektor, og eventuelt andre sektorer. Ellers holder de fleste seg oppdatert på de «store» bildet gjennom PST og NSM/NorCERT. De som er tilknyttet sektorvise responsmiljøer får også input fra disse. De fleste er også tilknyttet PISAS og blir varslet gjennom dette systemet.

Lover, forskrifter og rammeverk. De fleste aktører oppgir at de følger ISO 27001 for IT-systemer og IEC62443 for industrielle IKT-systemer. En rekke aktører oppgir også at de bruker NIST's rammeverk, eller har etablert egne selskapsspesifikke rammeverk. Noen av petroleumsvirksomhetene oppgir at de benytter NOROG 104. Aktører som har vært med i arbeidet som ledet til etablering av DNVGL-RP-G108 uttaler at denne er en god veiledning for implementering av IEC 62443.

I tillegg uttaler noen av petroleumsvirksomhetene at Ptils forskrifter er vage, og kunne ønske at kravene som omfatter industriell IKT-sikkerhet blir gjort mer konkrete. Flere aktører med virksomheter både i Norge og i utlandet oppgir at deres norske operasjoners arbeid med IKT-sikkerhet ligger langt framme sammenlignet med operasjoner i utlandet, og at samarbeidet med Ptil fungerer godt. Dette temaet er ytterligere belyst i rapporten «*IKT-sikkerhet – robusthet i petroleumssektoren /Regelverk og tilsynsmetodikk*» (ref. /61/).

6 TJENESTER OG TILBYDERE

Dette kapittelet tar for seg noen oppgaver som er vesentlige i arbeidet med trening og øvelse rettet mot en virksomhets industrielle IKT-sikkerhet og IT-sikkerhet. Dette er oppgaver som inkluderes i anbefalte tiltak i standarder og retningslinjer (se kapittel 4.2.2 og 4.2.3).

Virksomheter som har riktig kompetanse og ressurser tilgjengelig kan gjennomføre disse oppgavene med egne ressurser. For andre virksomheter kan det være hensiktsmessig å etterspørre disse tjenestene fra spesialiserte tilbydere.

- Trening i bevisstgjøring av IKT-sikkerhet
- Rådgivning innen beredskap og øvelser
- Inntrengningstjenester og «red-team» øvelser

6.1 Bevisstgjøring

Bevisstgjøring rundt IKT-sikkerhet er nevnt som et viktig tiltak og er definert som kontrollpunkter i en rekke standarder for IKT-sikkerhet, blant annet i;

- *ISO/IEC 27001/27002:* *A.7.2* & *A.12.2*
- *IEC 62443-2-1:* *4.3.2.4*
- *NIST CSF:* *PR.AT-1*
- *NOROG 104:* *ISBR 5*
- *DNVGL-RP-G108:* *Chapter 5.5, punkt 4*

Det er flere metoder som kan benyttes for å øke de ansattes bevissthet, for eksempel tradisjonelle kurs, e-læringskurs, og phishing kampanjer. Det er en rekke aktører i markedet som tilbyr denne typen tjenester.

Mottakere av denne typen opplæring og trening vil være alle ansatte, innleide, og eventuelle 3. part som har tilgang og brukerrettigheter til virksomhetens IKT-systemer. Det kan være hensiktsmessig å differensiere treningen slik at den blir mest mulig relevant for brukere med ulike roller i virksomheten og ulike brukerrettigheter på IKT-systemene. Dette bør dekke både de industrielle- og de administrative IKT-systemene.

6.2 Rådgivning innen beredskap og øvelser

Beredskap og øvelser er nært knyttet sammen. Gode strategier og planer for beredskap og øvelser er tiltak som anbefales blant annet i;

- *NSM Grunnprinsipper:* *4.1*
- *IEC 62443-2-1:* *4.3.4.5.11*
- *ISO/IEC 27001/27002:* *A.17.1*

NSMs grunnprinsipp 4.1 omhandler det å forberede virksomheten på håndtering av hendelser. Dette inkluderer å etablere planverk for hendelseshåndtering som ivaretar behovet for virksomhetskontinuitet

ved beredskap og krise, tildele roller for håndtering av IKT-systemene, samt teste og øve på planer jevnlig slik at de er godt innøvd.

Det finnes en rekke selskaper som tilbyr rådgivningstjenester både for å etablere beredskapsstrategier, organisasjoner og planer, og/eller tjenester relatert til planlegging, gjennomføring og evaluering av øvelser. Dette er alt fra små spesialiserte selskaper som kan tilby utvalgte tjenester, til store internasjonale selskaper som kan levere alle overnevnte tjenester.

6.3 Inntrengningstester og «red-team» øvelser

NSM har et eget grunnprinsipp (3.4) som omfatter inntrengningstester og «red-team»-øvelser. NIST CSF (DE.DP) anbefaler også å etablere, teste ut, og kontinuerlig forbedre deteksjonsprosesser. Utdrag fra NSM grunnprinsipp 3.4 er presentert i Faktaboks 6-1.

Oppgaven til et «red-team» er å identifisere og å utnytte svakheter i sikringen av IT og IKT-systemene. Formålet er å bruke denne kunnskapen til å videreutvikle forsvarsmekanismene. Gruppen som utvikler forsvars-mekanismene kalles i denne sammenhengen gjerne «blue-team»[13]. Når de to gruppene «red-team» og «blue-team» samarbeider, bruker man betegnelsen «purple-team»-øvelse.

En av angrepsmetodene som «red-team» kan benytte er inntrengningstest. Andre angrepsmetoder kan være etisk hacking og sosial manipulering. For å utføre inntrengningstester og "red-team"-øvelser kreves det spesialistkompetanse innenfor IT og IKT-sikkerhet. Det er både selskaper og organisasjoner som spesialiserer seg på denne typen øvelser. NSM skriver for eksempel på sine websider at de kan utføre inntrengningstester.

Inntrengningstest og «Red-team»-øvelse – Utdrag fra NSM Grunnprinsipp 3.4

Inntrengingstesting er et kontrollert dataangrep som prøver ut motstandskraften i IKT-systemer gjennom målrettede søk og analyser, og forsøk på utnyttelse av sårbarheter, feil og mangler som identifiseres. (...) Resultatet av en slik test vil gi dypere innsikt, gjennom en faktisk demonstrasjon av hva slags virksomhetsrisiko sårbarheter kan utgjøre. Målet med en slik test vil væreå finne de viktigste svakhetene slik at disse kan utbedres.

«Red Team»-øvelser tester virksomhetens beredskap for dataangrep gjennom simulering av faktiske angrep. Dette er en mer helhetlig tilnærming og vil utfordre virksomhetens retningslinjer, prosesser og sikringstiltak. Uavhengige «Red Team» kan bidra med verdifull og objektiv testing av effektiviteten til beredskapsprosesser og personell tilknyttet dem.

Faktaboks 6-1: Utdrag av beskrivelse av Inntrengingstesting og «Red Team»-øvelser, fra NSM Grunnprinsipp 3.4.

[13] Uttrykket «purple-team» benyttes for å beskrive sammarbeid mellom «red-team» og «blue-team».

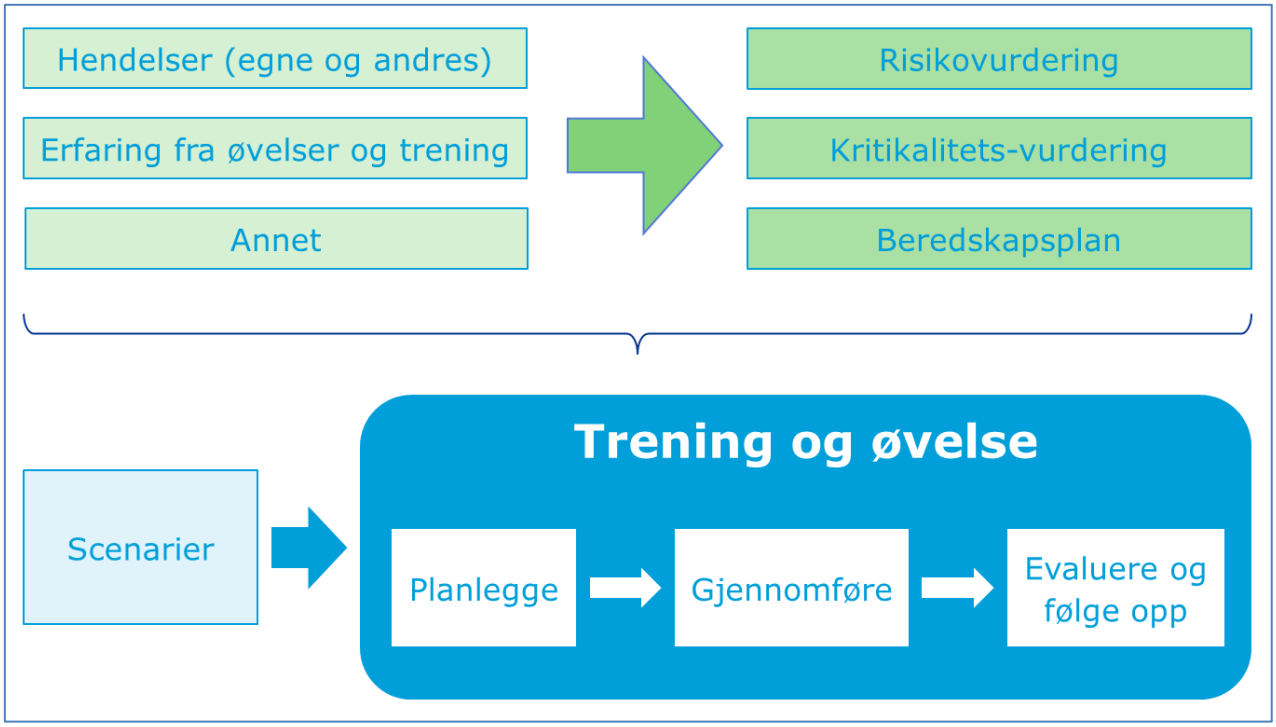
7 ANBEFALINGER – GOD PRAKSIS

Dette kapittelet sammenfatter anbefalte tiltak for god praksis for trening og øvelse i å håndtere IKT-sikkerhet og hendelser som omfatter de industrielle IKT-systemene og nærliggende systemer der det er potensiale for eskalering til de industrielle IKT-systemene. Tiltakene er basert DNV GLs vurderinger og kunnskapen som er kommet fram gjennom litteratursøk (se kapittel 4) og intervjuer med aktører (se kapittel 5). Kapittelet gir også forslag til hvordan Ptil kan gi bedre veiledning til sektoren for arbeid med industriell IKT-sikkerhet.

De anbefalte tiltakene som er oppsummert i dette kapittelet, omfatter tiltak som allerede er anbefalt i litteraturen som er gjennomgått, samt noen mer konkrete tiltak. De anbefalte tiltakene fra denne studien er sortert under *emner*, og nummerert fortløpende (ikke i prioritert rekkefølge). Tiltakene er kort oppsummert og sammenstilt i en tabell i kapittel 7.4.

7.1 Trening og øvelse

Trening og øvelse kan deles inn i tre faser som vist i Figur 7-1. Dette delkapittelet er inndelt i tre underkapitler i henhold til de tre fasene.



Figur 7-1: Input (grønn) og faser (blå) for trening og øvelse

7.1.1 Planlegging

Planlegging er helt sentralt for å ha et verdifullt trening- og øvelsesprogram. I tillegg må det foreligge en basis i form av risiko-/kritikalitetsvurderinger, beredskapsplaner og beredskapsorganisasjoner. I de følgende tiltakene dekkes ulike aspekter som er viktig å ha på plass for en god håndtering av IKT-sikkerhetshendelser i trening- og øvelsesprogrammet til en virksomhet.

Tiltak 1: Det bør ikke være egne interne krav og systemer for trening og øvelse rettet mot IKT-sikkerhetshendelser, de bør inngå i selskapets overordnede systemer

Det er ønskelig å ha et helhetlig system der det er lett å skaffe oversikt over status på utført trening og øvelse, samt hva som er planlagt av øvelser fremover:

- Trening: Det bør etableres en plan for kompetanseutvikling på området IKT-sikkerhet. Dette vil danne grunnlag for hvilke behov det vil være for trening/kurs. Status på trening/kurs for relevant personell synliggjøres i en kompetanseoversikt.
- Øvelser: Det må etableres planer for øvelser (ref. Tiltak 2). Det bør også lages en oversikt over faktisk gjennomførte øvelser. Denne oversikten gjør det mulig å i etterkant vurdere organisasjonens evne til å følge opp og gjennomføre egne planer.

Tiltak 2: Etablere årsplan over øvelser som skal utføres og som inneholder minimum én IKT-sikkerhetsrelatert øvelse

Dette bør være en del av et felles oppsett for virksomheten (ref. Tiltak 1). Denne planen bør inneholde minimum én øvelse årlig relatert til IKT-sikkerhetshendelser inkludert de industrielle IKT-systemene. Et slik krav bør også inngå i styrende dokumentasjon.

I tillegg til den årlige øvelsen relatert til IKT-sikkerhetshendelse bør det utføres 3-5 årlige øvelser som inkluderer ulike personer og ulike temaer. De fleste av disse vil kun dekke deler av et scenario. Det må lages en overordnet plan som sikrer at man i løpet av en gitt tid får øvd på alle IKT-sikkerhetsfunksjonene i et hendelsesforløp, ref. Figur 4-1. Det vil si, ikke bare for beredskapsfasen, men også øvelser med fokus på proaktive funksjoner (forhindre og detektere) for å unngå en hendelse.

Det kan vurderes å sette opp en plan som strekker seg over mer enn et år. Det kan være fornuftig i forhold til å få en bedre oversikt over hvordan man får dekket viktige områder/scenarioer over for eksempel to til tre år. Hvis man går for en slik plan bør den oppdateres årlig slik at den tar hensyn til eventuelle oppdaterte risikovurderinger, erfaringer fra øvelser, hendelser i virksomheten eller hendelser hos andre.

Tiltak 3: IKT-sikkerhetshendelser bør ha en egen DFU og eventuelt ytelsesstandard for IKT-sikkerhet

Sikkerhetshendelser for de industrielle IKT-systemene bør ha egen DFU[14] i beredskapsplanen slik at det er klare retningslinjer for hvem som har hvilke ansvar og oppgaver gitt en hendelse (se). Beredskapsplanene er styrende for hvordan øvelser gjennomføres. En IKT-sikkerhetsøvelse kan også legges inn som et element i et annet storulykkescenario.

Hver DFU skal øves på minst hvert annet år. Ved etablering av ny DFU for IKT-sikkerhetshendelser bør etablert praksis i virksomheten benyttes.

Det kan også vurderes om det er behov for en ytelsesstandard med ytelseskrav for IKT-sikkerhet. Definerte ytelseskrav kan bidra i prosessen med å definere hva det skal øves på og hva som må testes for å sikre at ytelsen opprettholdes. Eksempler på ytelseskrav kan være en fastsatt tid til mobilisering for ulike deler av beredskapsorganisasjonen.

Både DFU og ytelsesstandarder bør etableres for hendelser relatert til sikkerheten i de industrielle IKT-systemene.

14 For mer informasjon og detaljer angående DFU'er, se kapittel 3.6.4.

Tiltak 4: Beredskapsorganisasjonen må inneholde en enhet med IT/industriell-IKT-ressurser

Beredskapsorganisasjonen må inneholde et eget IKT-sikkerhetsteam med IT/industriell-IKT-ressurser slik at man har rask tilgang på definerte ressurser gitt en hendelse der den overordnede beredskapsorganisasjon må styrkes med slik kompetanse. Hvis det er etablert ulike beredskapsorganisasjoner i virksomheten basert på ulike hendelser, bør det utføres noen øvelser der det er scenarier som går på tvers av beredskapsorganisasjonene.

Hvis noen eksterne aktører/leverandører har en rolle i en IKT-sikkerhetshendelse (eksempelvis der de har en 24/7 supportfunksjon) må dette tydelig fremgå av i beredskapsplaner/beredskapsorganisasjonen.

Tiltak 5: Alle som kan bli involvert i en reell situasjon må involveres i øvelser

Det må defineres hvilke roller/enheter/virksomheter som vil bidra inn i et scenario og de må inkluderes i DFU'en og i gjennomføring av øvelser. Ut fra praktiske årsaker er det mest vanlig å gjennomføre øvelser som bare dekker en del av scenariet, og for den delen som velges ut må aktuelle aktører involveres. Basert på om det er en fullskala-øvelse eller del-øvelse må for eksempel leverandøren av SAS inkluderes gitt at de vil/kan ha en rolle i forbindelse med utvalgt innhold i øvelsen. Dette kan være relevant hvis virksomheten har en 24/7 supportavtale med leverandør av industrielle IKT-system.

Tiltak 6: Definere mål for trening og øvelse

For hver type trening og øvelse må det defineres klare mål. Dette for å sette opp et formålstjenlig trening- og øvelsesprogram og for i ettertid vurdere om målene er oppnådd. Eksempler på mål kan være:

- Overordnet mål: unngå hendelser – IT og/eller Industriell IKT
- Bli kjent med beredskapsplan
- Teste at beredskapsplanen er formålstjenlig
- Læring/kompetansebygging – utvikle ferdigheter (individnivå)
- Sikre effektiv og målrettet innsats
- Identifisere og redusere sårbarhet i systemer
- Verifisere at IKT-sikkerhetssystemer fungerer i henhold til ytelseskravene
- Forbedre sikkerhetstiltak og rutiner
- Sikre høy tilgjengelighet av viktige funksjoner/systemer

Tiltak 7: Utarbeide detaljert dreiebok for hver øvelse i god tid før gjennomføring

For å få en vellykket øvelse må den planlegges godt. Dette inkluderer Tiltak 5 og Tiltak 6 som omfatter deltakere og mål for øvelsen, samt å utarbeide detaljert dreiebok for hver øvelse. Utarbeidelse av dreiebok (og fasilitering av øvelser) kan kjøpes fra eksterne tilbydere. Relevante deler av beredskapsteamet bør likevel være involvert i utarbeidelsen av dreieboken.

Kilder til etablering av scenarier for øvelser kan være risikovurderinger, trusselvurderinger, erfaringer fra hendelser (i egen og andres virksomhet), samt erfaringer fra tidligere øvelser. Det vil normalt være mange potensielle scenarier og man vil ikke ha mulighet til å dekke alle eller nødvendigvis en fullskalaøvelse av et scenario. Det må derfor defineres hvilke scenarier som er de mest kritiske (gjerne

der det eksisterer en DFU) og så øves det på deler av scenariet. I løpet av en definert periode skal likevel hele scenariet være dekket i ulike del-øvelser.

Basert på utvalgt scenario og formål må det vurderes hvilken gjennomføringsmetodikk som er hensiktsmessig. Det finnes ulike metoder som kan utføres hver for seg eller i kombinasjon, eksempelvis tabletop med øvelser/oppgaver og prosedyre-/dokument gjennomganger, simulatortreninger, og skjulte øvelser med etisk hacker.

Tiltak 8: Varsling av hendelser til ansatte på SMS

For å sørge for at alle brukere (ansatte og innleide) med tilgang til IT og IKT-systemer blir varslet er det anbefalt å opprette SMS varsling. Ved en hendelse der det er fare for at IT-systemer er utsatt for ett angrep kan det være ønskelig at man ikke skrur på eller logger seg inn på IT-systemene. Varsling via SMS vil da være ett godt alternativ for å nå raskt ut til brukerne før de logger seg på IT-systemet.

7.1.2 Gjennomføring

Dette delkapittelet sammenfatter tiltak som omfatter gjennomføring av forskjellige typer trening og øvelse for ulike målgrupper.

Tiltak 9: Øvelser i henhold til beredskapsplan/DFU

Gjennomføre øvelser i henhold til beredskapsplan (DFU for IKT-sikkerhetshendelse) og eventuelt andre scenarier som fremgår av ulike kilder ref. Figur 7-1. Relevante tiltak for å definere gode øvelser; Tiltak 2, 5, 6 og 7.

Dette utføres eksempelvis for å vurdere at følgende fungerer i henhold til plan:

- Hvor raske er man til å identifisere at noen har kommet forbi brannmurer/inn i IT og/eller de industrielle IKT-systemene
- Hvordan sikres bevis
- Hvordan utføres vurderinger og tas beslutninger (se for eksempel Tiltak 10)
- Er alle som bør være involvert en del av beredskapsteamet/definerte kontaktpersoner

Tiltak 10: Øve på å avgrense og segregere potensielt kompromitterte IT/IKT-systemer

En DFU som dekker at IT-systemer, prosesskontrollsystemene, og etter hvert også de uavhengige sikkerhetssystemene (ref. Figur 3-2), kan være eller er kompromittert, bør inngå i beredskapsplan og øves på (ref. Tiltak 3 og Tiltak 9).

Et hovedmål med slike øvelser vil være å evaluere den etablerte beredskapsorganisasjonen og beredskapsprosessen, og vurdere om disse er hensiktsmessige for denne type alvorlige hendelser som vil involvere mange disipliner og roller (ref. Tiltak 3 og Tiltak 4). Eksempelvis kan en slik øvelse inneholde et antall alternative scenarier hvor man må ta stilling til og beslutte om man skal iverksette følgende aksjoner:

- Koble vekk kommunikasjon mellom land og hav
- Koble vekk IT fra Industrielle IKT-systemer

- Manuelt aktivere Prosesssikringssystem (PSD)
- Manuelt aktiverer Nødavstengingssystem (ESD)
- Gjennomføre nødavstenging ved hjelp av andre midler (uten bruk av programmerbare systemer) der dette er mulig.
- Evakuere innretningen eller anlegg.

Tiltak 11: Teste gjenoppretting av sikkerhetskopier

Det bør etableres prosedyrer og systemer for sikkerhetskopiering og gjenoppretting av informasjon, programvare og datasystemer. Beskyttelse av sikkerhetskopier bør etableres og benyttes. Prosedyrene bør øves på og systemene bør testes jevnlig gjennom hensiktsmessige metoder.

Tiltak 12: Utføre periodiske "Red team-øvelser"

"Red team-øvelser"[15] bør utføres for å teste virksomhetens evne til å detektere, stoppe og respondere på et angrep. Red-teamet simulerer et angrep uten at relevant IT/IKT personell og beredskapsorganisasjonen kjenner til det. Dette for å teste hvordan beredskapsplaner/-prosedyrer og beredskapsorganiseringen med tilhørende IT/IKT kompetanse fungerer ved slike hendelser.

Tiltak 13: Benytte interne eller eksterne hackere for å teste systemene (inntrengningstester)

De industrielle IKT-systemene bør testes regelmessig (eksempelvis ved endringer og større oppdateringer). Slike øvelser utføres for å avdekke om tidligere kjente svakheter er utbedret. Øvelsen utføres ved at etiske hackere prøver å hacke seg inn i systemene. Avhengig av størrelse på virksomheten, antall personer og tilgjengelig kompetanse kan dette utføres med interne ressurser eller tjenesten kan kjøpes eksternt av profesjonelle og pålitelige tjenestetilbydere.

Tiltak 14: Trening på hvordan inkludere vurdering av og krav til IKT-sikkerhet på arbeidstillatelser som gjelder arbeid på industrielle IKT-systemer

Vedlikehold og oppdateringer av industrielle IKT-systemer utføres ofte av system- og service-leverandører. Det er anbefalt at prosessen for arbeidsordre tvinger frem IKT-sikkerhetsvurderinger for arbeid som skal utføres på et IKT-system, og at de som skal utføre jobben blir gjort kjent med dette og gjeldende IKT-sikkerhetskrav. Det må trenes på hvordan slike vurderinger bør gjøres, og hvordan kontroll av at IKT-sikkerhetskravene etterleves av de som utfører arbeidet.

Tiltak 15: Introduksjonsprogram inklusiv informasjon om IKT-sikkerhet

Introduksjonsprogram/-kurs for nyansatte bør inneholde en modul om IKT-sikkerhet. Dette bør adressere sikkerhet i både IT- og industrielle IKT-systemer. De fleste aktørene i olje og gass sektoren har industriell IKT som del av sitt virke, og det anses som viktig at alle ansatte får innblikk i trusler og sårbarheter, og viktigheten av at de industrielle IKT-systemene er tilgjengelige og ikke kompromitteres.

[15] Se beskrivels av «red-team» i kapittel 6.3 og Faktaboks 6-1.

Tiltak 16: Trening på detektering i daglig arbeid

Avvik fra normaltilstand identifiseres forholdsvis ofte og er derfor en viktig del av den daglige treningen for de som skal oppdage mer alvorlige hendelser (ref. Tiltak 23). Overvåknings-systemer implementert i de industrielle IKT-systemene gir ofte mange varsler som ikke er reelle farer (falsk alarm). Det kreves trening i å operere IKT-sikkerhetssystemene for å kunne diagnostisere og håndtere alarmer og hendelser.

Følgende fire tiltak er fortrinnsvis rettet mot IT-systemer. Disse er imidlertid tatt med her fordi IT-systemene er en vesentlig del av sårbarhetsflaten mot de Industrielle IKT-systemene.

Tiltak 17: Phishing-kampanjer

De ansatte kan testes med godartede phishing e-poster. Det er en øvelse som rettes mot alle ansatte og innleide. Som en del av en slik kampanje bør resultatene evalueres og ansatte få informasjon om erfaringen og bevisstgjøring i forhold til phishing e-poster, samt få en oppfordring om å gjenta ett eventuelt opplæringskurs angående dette (ref. Tiltak 18).

Spissede phishing angrep, for eksempel mot ledelsespersoner eller personer med spesialkompetanse, kalles henholdsvis whaling og spear-phishing. Whaling-kampanjer mot spesielt viktige stillinger i virksomhetens ledelse kan gjerne være ett tema for informasjon/workshop for ledere (ref. Tiltak 19).

Tiltak 18: Bevisstgjøring i form av e-læringskurs om IKT-sikkerhet

Det bør være obligatorisk for alle ansatte og innleide med tilgang til IT- og industrielle IKT-systemer å få nødvendig opplæring, for eksempel i form av e-læringskurs. Disse kursene kan bestilles av eksterne leverandører og med mulighet for tilpassinger for den enkelte virksomhet.

For relevant personell gjelder dette også spesifikke e-læringskurs for sikring av industriell IKT. Det bør være en regelmessig repetisjon av slike kurs.

Tiltak 19: Årlig trening/workshops for virksomhetens ledelse

Årlig trening/workshops for ledelsen relatert til IKT-sikkerhet er viktig for å sikre en bred forståelse for relevante utfordringer og trusler, samt et mulig endret trusselbilde.

På slike samlinger bør det på tilsvarende måte som for øvelser defineres klare mål, innhold og oppgaver. Innholdet i slike samlinger kan omfatte gjennomgang av beredskapsplaner for IKT-sikkerhetshendelser, informasjon om sårbarheter og hvordan utenforstående kan hacke seg inn på IT-systemer, og informasjon/detaljer om alvorlige IKT-sikkerhetshendelser som har forekommet i industrien de siste årene både i Norge og internasjonalt. Det bør også fokuseres spesielt på sårbarheter i de industrielle IKT-systemene og mulige konsekvenser ved IKT-sikkerhetshendelser.

Tiltak 20: Informasjonsmøter inkl. oppgaver (tabletop)

Det bør gis informasjon til de ansatte gjennom oppslag på intranett og i ulike møter som allmøter og avdelingsmøter. I avdelingsmøter kan man også inkludere noen oppgaver/øvelser.

7.1.3 Evaluering og oppfølging

Et viktig resultat av trening og øvelse er læring, og mye av dette tilegnes gjennom evaluering og oppfølgning i etterkant. Treningen og øvelsen i seg selv har stor verdi ved at ansatte blir bedre rustet til å detektere og håndtere en IKT-sikkerhetshendelse. Trening og øvelse skal også identifisere forbedringsområder. Trening og øvelse vil verifisere at man oppnår forventet resultat (møter ytelseskrav), identifiserer mulige forbedringsområder av sikringen og identifisere forbedring av trening og øvelser (eksempelvis planlegging, gjennomføringsmetodikk, områder/scenarier som bør dekkes).

Tiltak 21: Oppdatering av beredskapsplaner etter øvelser

Hvis en øvelse viser at man ikke klarer å møte virksomhetens definerte ytelseskrav eller oppsatte mål for øvelsen, må det vurderes om beredskapsplanene skal endres og hvordan. Andre forhold som også kan føre til endring av beredskapsplaner, er eksempelvis oppdaterte risikovurderinger, endret trusselbilde eller interne/eksterne IKT-sikkerhetshendelser.

Tiltak 22: Resultater fra foregående års øvelser bør benyttes i planlegging av neste års øvelser

Resultatene fra øvelser bør legges til grunn for planlegging av nye øvelser i det påfølgende året, både med tanke på øvelsesprogrammet som helhet og valg av nye øvelses-scenarier (ref. Tiltak 2 og Tiltak 7).

Tiltak 23: Vurder hendelser der beredskapsorganisasjonen mobiliserer som «øvelser»

I tilfeller der man har mistanke om angrep (identifisert av interne ressurser eller leverandør), eller dersom andre aktører har større eller mindre hendelser (ref. Hydro- og Mærsk-hendelsene), eller at det detekteres betydelige avvik fra normaltilstand som i ettertid viser seg ikke å være ondartet, vil man mobilisere beredskapsorganisasjonen. Disse tilfellene bør i ettertid evalueres og følges opp på lik linje med planlagte øvelser, og bidra til forbedringer og eventuelt oppdatering av eksisterende beredskaps- og øvelsesplaner (ref. Tiltak 21). Evalueringen bør inkludere selve detekteringen og informasjonsprosessen og ikke kun omfatte en vurdering av hvordan beredskapsorganisasjonen har fungert etter detektering.

7.2 Føringer fra Ptil

Utover at man skal ha en robust beredskapsorganisasjon og beredskapsplaner, samt at det skal utføres nødvendig trening og nødvendige øvelser, så sier Ptils forskrifter lite konkret om hvordan man forventer at trening og øvelse skal utføres.

Tiltak 24: Utgi egne eller vise til andres eksisterende veiledere for trening og øvelse

Det anbefales at Ptil enten gir ut en egen veileder som beskriver forventinger til trening og øvelser, eller viser til eksisterende veiledere der dette er beskrevet. I kapittel 4.3 er det presentert eksempler på veiledere for trening og øvelse utgitt av DSB, Difi og NVE.

7.3 Deltakelse i fora

Sikkerhetsutfordringer relatert til industrielle IKT-systemer og IT-systemer er i stor grad like for de ulike operatørene av industrielle IKT-systemer. Man er i stor grad eksponert for de samme truslene, og har

behov for tilsvarende ressurser og støttefunksjoner, både på tvers av virksomheter i petroleums-industrien og andre industrier. Å få tilgang på fellesresurser, og å lære og dele informasjon med andre aktører, kan derfor være hensiktsmessig og kostnadsbesparende sammenlignet med at virksomheten skal tilegne seg all nødvendig kompetanse selv.

Tiltak 25: Vurdere behov for medlemskap i sektorvise responsmiljøer (CERT/CSIRT)

Sektorvise responsmiljøer og CERT/CSIRT'er[16] kan bistå i beredskapsarbeid og koordinert respons til IKT-sikkerhetshendelser. En sektorvist responsmiljø kan for eksempel bidra med sårbarhetsovervåkning, trusseletterretning, deteksjon, hendelseshåndtering, rådgivning, øvelser og kursing.

NorCERT og KraftCERT er to alternativer (se kapittel 3.7.2) der norske petroleumsvirksomheter er representert. NorCERT er sektorovergripende CERT underlagt NSM. KraftCERT er opprettet av aktører i kraftindustrien, men er også åpen for medlemmer i andre bransjer[17].

Tiltak 26: Vurdere behov for deltakelse i bransjefora

Deltakelse i bransjefora er en annen måte å dele beste praksiser, varsling av hendelser, og jobbe sammen for å finne felles løsninger på spesifikke utfordringer i bransjen.

7.4 Oppsummering av tiltak

Tiltakene beskrevet i kapittel 7.1, 7.2 og 7.3 er oppsummert i Tabell 7-1 på neste side.

[16] CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team). CERT er et registrert varemerke tilhørende Carnegie Mellon University

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

Tabell 7-1: Oppsummert liste over tiltak presentert i kapittel 7.1, 7.2 og 7.3.

Tiltak #	Tiltaksbeskrivelse (for mer detaljer se kapittelhenvisning)
Trening og øvelse – Planlegging (kapittel 7.1.1)	
Tiltak 1	Det bør ikke være egne interne krav og systemer for trening og øvelse rettet mot IKT-sikkerhetshendelser, de bør inngå i selskapets overordnede systemer
Tiltak 2	Etablere årsplan over øvelser som skal utføres og som inneholder minimum én IKT-sikkerhetsrelatert øvelse
Tiltak 3	IKT-sikkerhetshendelser bør ha en egen DFU og eventuelt ytelsesstandard for IKT-sikkerhet
Tiltak 4	Beredskapsorganisasjonen må inneholde en enhet med IT/industriell-IKT-ressurser
Tiltak 5	Alle som kan bli involvert i en reell situasjon må involveres i øvelser
Tiltak 6	Definere mål for trening og øvelse
Tiltak 7	Utarbeide detaljert dreiebok for hver øvelse i god tid før gjennomføring
Tiltak 8	Varsling av hendelser til ansatte på SMS
Trening og øvelse – Gjennomføring (kapittel 7.1.2)	
Tiltak 9	Øvelser i henhold til beredskapsplan/DFU
Tiltak 10	Øve på å avgrense og segregere potensielt kompromitterte IT/IKT-systemer
Tiltak 11	Teste gjenoppretting av sikkerhetskopier
Tiltak 12	Utføre periodiske "Red team-øvelser"
Tiltak 13	Benytte interne eller eksterne hackere for å teste systemene (inntrengningstester)
Tiltak 14	Trening på hvordan inkludere vurdering av og krav til IKT-sikkerhet på arbeidstillatelser som gjelder arbeid på industrielle IKT-systemer
Tiltak 15	Introduksjonsprogram inklusiv informasjon om IKT-sikkerhet
Tiltak 16	Trening på detektering i daglig arbeid
Tiltak 17	Phishing-kampanjer
Tiltak 18	Bevisstgjøring i form av e-læringskurs om IKT-sikkerhet
Tiltak 19	Årlig trening/workshops for virksomhetens ledelse
Tiltak 20	Informasjonsmøter inkl. oppgaver (tabletop)
Trening og øvelse – Evaluering og oppfølging (kapittel 7.1.3)	
Tiltak 21	Oppdatering av beredskapsplaner etter øvelser
Tiltak 22	Resultater fra foregående års øvelser bør benyttes i planlegging av neste års øvelser
Tiltak 23	Vurder hendelser der beredskapsorganisasjonen mobiliserer som «øvelser»
Føringer fra Ptil (kapittel 7.2)	
Tiltak 24	Utgi egne eller vise til andres eksisterende veiledere for trening og øvelse
Deltakelse i fora (kapittel 7.3)	
Tiltak 25	Vurdere behov for medlemskap i sektorvise responsmiljøer (CERT/CSIRT)
Tiltak 26	Vurdere behov for deltakelse i bransjefora

8 REFERANSER

Lover, forskrifter og standarder

/1/ Lov om nasjonal sikkerhet (sikkerhetsloven). LOV 2018-06-01-24. Ikrafttredelse 01.01.2019
https://lovdata.no/dokument/NL/lov/2018-06-01-24

/2/ Lov om petroleumsvirksomhet (petroleumsloven). LOV-2015-06-19-65 fra 01.10.2015

/3/ Lov om luftfart (luftfartsloven). LOV-1993-06-11-101. Ikrafttredelse 01.04.1994 (med retting 23.09.2016).
https://lovdata.no/dokument/NL/lov/1993-06-11-101/*

/4/ Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften). FOR 2018-12-20-2053. Ikrafttredelse 01.01.2019
https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053

/5/ Forskrift om utføring av aktiviteter i petroleumsvirksomheten (Aktivitetsforskriften). Petroleumstilsynet. Sist endret 25. januar 2019
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/aktivitetsforskriften_n.pdf

/6/ Forskrift om utforming og utrustning av innretninger med mer i petroleumsvirksomheten (Innretningsforskriften). Petroleumstilsynet. Sist endret 18. desember 2017.
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/innretningsforskriften_n.pdf

/7/ Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (Rammeforskriften). Petroleumstilsynet. Sist endret 20. desember 2018.
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/rammeforskriften_n.pdf

/8/ Forskrift om tekniske og operasjonelle forhold på landanlegg i petroleumsvirksomheten med mer (teknisk og operasjonell forskrift). Sist endret 26. april 2019
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/teknisk_og_operasjonell_forskrift_n.pdf

/9/ Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (Styringsforskriften). Petroleumstilsynet. Sist endret 26. april 2019
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_n.pdf

/10/ Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften) FOR-2012-12-07-1157. Ikrafttredelse 01.01.2013
https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

/11/ Forskrift om endring i forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften) FOR-2018-11-01-1641. Ikrafttredelse 01.01.2019
https://lovdata.no/dokument/LTI/forskrift/2018-11-01-1641

/12/ NS-EN ISO/IEC 27001:2017: Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Krav (ISO/IEC 27001:2013 innbefattet Cor 1:2014 og Cor 2:2015). Publisert 01.05.2017

/13/ NS-EN ISO/IEC 27002:2017. Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring (ISO/IEC 27002:2013 innbefattet Cor 1:2014 og Cor 2:2015). Utgitt 1. mai 2017

/14/ IEC 62443 Industrial communication networks - Network and system security

/15/ EU (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Rammeverk, veiledere, retningslinjer, presentasjoner, relevante rapporter

/16/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser. Grunnbok: Introduksjon og prinsipper, utgitt oktober 2016.
https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/grunnbok-oving/

/17/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser;
Metodehefte: Spilløvelse. Utgitt oktober 2016
https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_spillovelse.pdf

/18/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser;
Metodehefte: Diskusjonsøvelse. Utgitt oktober 2016
https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_diskusjonsovelse.pdf

/19/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser;
Metodehefte: Funksjonsøvelse. Utgitt oktober 2016
https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_funksjonsovelse.pdf

/20/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser;
Metodehefte: Fullskalaøvelse. Utgitt oktober 2016
https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_-fullskalaovelse.pdf

/21/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser;
Metodehefte: Evaluering av øvelser. Utgitt mai 2018
https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/metodehefte_evaluering_av_ovelser22.pdf

/22/ DSB Veileder i planlegging, gjennomføring og evaluering av øvelser; Metodehefte: Lokal øvingsleder. Utgitt oktober 2018. https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/tema/metodehefte_lokal_ovingsleder.pdf

/23/ Veileder i sikkerhetsstyring. Veileder til ny Sikkerhetslov. NSM, utgitt august 2019 https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-sikkerhetsstyring.pdf

/24/ Difi Veileder i planlegging og gjennomføring planlegging og gjennomføring av IKT-øvelser 2016. Hovedrapport m/vedlegg https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/veileder-planlegging-og-gjennomforing-av-ikt-ovelser

/25/ Planlegging av øvelser. Presentasjon, Håkon Styri, Difi. 2017-10-02

/26/ DNVGL-RP-G108, Cyber security in the oil and gas industry based on IEC 62443:2013. September 2017 https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

/27/ DNV GL RP-0496. Recommended practice: Cyber security resilience management https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html?utm_source=rules.dnvgl.com&utm_medium=referral&utm_campaign=RP-CyberSecurity&utm_content=Link

/28/ NSMs Grunnprinsipper for IKT-sikkerhet. Versjon 1.1. NSM, 1. november 2018. https://www.nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_for_ikt-2018.pdf

/29/ NSM, Rammeverk for håndtering av IKT sikkerhetshendelser, 07.12.2017 https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

/30/ Veiledning sikkerhets- og beredskapstiltak mot terrorhandlinger. NSM, september 2010 https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/tiltak-mot-terrorhandlinger.pdf

/31/ NSM: Risiko 2018 - Verdifulle individer, Verdifulle virksomheter, Verdifull infrastruktur https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

/32/ NSM: Risiko 2019: Krafttak for et sikrere Norge https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

/33/ NSR_Mørketallsundersøkelsen 2018. Informasjonssikkerhet, personvern og datakriminalitet https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf

/34/ NVE_Kraftberedskapsforskriften_veileder 2013_01. Juli 2013.
http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf

/35/ NVE rapport 26/2017_Regulering av IKT-sikkerhet. Mai 2017
http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

/36/ Informasjonssikkerhetstilstanden i energiforsyningen. NVE raport 74/2017.
http://publikasjoner.nve.no/rapport/2017/rapport2017_74.pdf

/37/ Øvelser. En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen. NVE rapport 39/2015. Utgitt April 2015.
http://publikasjoner.nve.no/rapport/2015/rapport2015_39.pdf

/38/ 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

/39/ Meld. St. 10 (2016 – 2017). Melding til Stortinget. Risiko i et trygt samfunn. Samfunnssikkerhet. Justis- og Bereskapsdepartementet. 09.12.2016.
https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf

/40/ NOU 2018: 14; IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet. 03.12.2018
https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

/41/ Høringsnotat fra Justis- og Beredskapsdepartementet, Høring om utkast til lov som gjennomfører NIS-direktivet i norsk rett. Saksnummer: 17/4816. 21.12.2018
https://www.regjeringen.no/contentassets/387a3609dde7484aa58bd8ae44920731/horingsnotat.pdf

/42/ Arbeidet med informasjonssikkerhet i statsforvaltningen. Kunnskapsgrunnlag. Difi rappor ISSN 1890-6583; 2018:4. 23.03.2018
https://www.difi.no/sites/difino/files/difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf

/43/ Informasjon om håndtering av IKT-sikkerhetshendelser. Brev fra Petroleumstilsynet. Dok. nr. 2019/1176/AU. Datert 18.09.2019

/44/ Tiltaksoversikt til nasjonal strategi for digital sikkerhet. Departementene. Januar 2019.
https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

/45/ SINTEF: Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten, 29.05.2018
https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf

/46/ SINTEF: IKT-sikkerhet – Fjernarbeid og HMS, 05.04.2019
https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf

/47/ Norsk olje og gass : 104 - Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer.
https://www.norskoljeoggass.no/Global/Retningslinjer/Integrerte%20operasjoner/104%20-%20Recommended%20guidelines%20for%20information%20security%20baseline%20requirements%20for%20process%20control%20safety%20and%20support%20ICT%20systems.pdf

/48/ Norsk olje og gass : 110 - Recommended guidelines for implementation of information security in Process Control, Safety and Support ICT systems during the engineering, procurement and commissioning phases
https://www.norskoljeoggass.no/contentassets/734a4ad3b5d9406f9784416a9ab61e4f/110---recommended-guidelines-for-implementation-of-information-security.pdf

/49/ Norsk olje og gass : 123 - Recommended guidelines for classification of process control, safety and support ICT systems based on criticality.
https://www.norskoljeoggass.no/en/working-conditions/retningslinjer/integrated-operations/123-recommended-guidelines-for-classification-of-process-control-safety-and-support-ict-systems-based-on-criticality/

/50/ IS-870 - Dams Sector: Crisis Management Overview Course. FEMA, Homeland security
https://emilms.fema.gov/IS870/DCM01summary.htm

/51/ IADC Guidelines for Baseline Cybersecurity for Drilling Assets, January 2018

/52/ Marine Cybersecurity Resilience. Presentasjon på Technology Week 2016. Simon Mockler DNV GL

/53/ IKT-sikkerhet «Erfaring og status fra sikringstilsyn og prosjekter innen IKT-sikkerhet. Espen Seljemo, Ptil. Presentasjon Fagdag Sikring 2018
ptil.websys.no › AdditionalContent › ExternalDownload

/54/ Robustgjøring av IKT-sikkerhet for de industrielle IKT-systemer for å kunne motstå tilsiktede og utilsiktede handlinger. Espen Seljemo, Ptil. 15.05.2019
https://www.ptil.no/contentassets/dc0fea40858645e8922818c2411ec6b0/prosjekter-innen-cybersecurity---espen-seljemo-ptil.pdf

/55/ Theodore J. Williams, 1992: The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. Research Triangle Park, NC: Instrument Society of America

/56/ Veiledning til aktivitetsforskriften
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/aktivitetsforskriften_veiledning_n.pdf

/57/ Veiledning til innretningsforskriften
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/innretningsforskriften_veiledning_n.pdf

/58/ Veiledning til rammeforskriften
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/rammeforskriften_veiledning_n.pdf

/59/ Veiledning til styringsforskriften
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_veiledning_n.pdf

/60/ Veiledning til teknisk og operasjonell forskrift
https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/teknisk_og_operasjonell_forskrift_veiledning_n.pdf

IKT-sikkerhet; DNV GL prosjektrapporter

/61/ DNVGL rapport, IKT-sikkerhet - Robusthet i petroleumssektoren, Delprosjekt 3 – Regelverk og tilsynsmetodikk, DNVGL Rapport nr 2019-0824, 29/11-2019

/62/ DNVGL rapport, IKT-sikkerhet - Robusthet i petroleumssektoren, Delprosjekt 4 – Resiliens mot cyberhendelser og kan blokkjede bidra, DNVGL Rapport nr 2019-0825, 29/11-2019

/63/ DNVGL rapport, IKT-sikkerhet - Robusthet i petroleumssektoren, Delprosjekt 5 – Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller, DNVGL Rapport nr 2019-0826, 29/11-2019

/64/ DNVGL rapport, IKT-sikkerhet - Robusthet i petroleumssektoren, Delprosjekt 6 – Telekommunikasjon og Protokoller, DNVGL Rapport nr 2019-0827, 29/11-2019

APPENDIX A
Tiltak relatert til trening og øvelse – Utdrag fra standarder og retningslinjer – Utdrag fra standarder og retningslinjer

Utdrag (oversatt til norsk) fra referansene beskrevet i 4.2.1 og 4.2.2 som omfatter tiltakene relatert til trening og øvelse, inkludert tiltak som viser til regelmessige tester av prosedyrer, er gitt i tabellen under.

Kilde/referanse	Tiltak / Kontroll
Trening – bevisstgjøring	
ISO/IEC 27001/27002 A.7.2 *Personellsikkerhet, under ansettelse*	Alle ansatte og innleide, når relevant, skal få hensiktsmessig opplæring og trening i bevisstgjøring, og regelmessige oppdateringer om organisatoriske prinsipper og prosedyrer som er relevante for deres jobbfunksjon
ISO/IEC 27001/27002 A.12.2 *Beskyttelse mot skadelig programvare*	Deteksjon, beskyttelse og gjenopprettingstiltak for å beskytte mot skadelig programvare skal implementeres i kombinasjon med hensiktsmessig bevisstgjøring av brukere.
IEC 62443-2-1 4.3.2.4 *Personellopplæring og bevisstgjøring om sikkerhet*	Alt personell (inkludert ansatte, innleide og 3. parts kontraktører) skal få adekvat teknisk trening relatert til kjente trusler og sårbarheter for hardware, software og sosial manipulering
NIST CSF – PR.AT-1 *Beskytt; Trening og bevisstgjøring*	Alle brukere skal være informert og trent i IKT-sikkerhet (viser blant annet til ISO/IEC 27001:2013 A.7.2 og A.12.2 for veiledning)
NOROG 104 – ISBR 5 *Trening og bevisstgjøring*	Brukere av IKT-systemer for prosesskontroll, prosess-sikkerhet og relevante støttesystemer, skal være trent og gjøres bevisst på informasjonssikkerhet og akseptabel bruk av IKT-systemer. (ISBR 5 er knyttet opp til NIST CSF PR.AT).
DNVGL-RP-G108 kap. 5.5, punkt 4	Påse at personell involvert i ferdigstillingsfasen er bevisst på IKT-sikkerhetsrisikoer og har nødvendig bevisstgjøringskurs.
Trening – risikoanalysemetode	
IEC 62443-2-1 4.2.3.2 *Risikoidentifikasjon, klassifisering og vurderinger*	Organisasjonen bør gi personell som skal utføre risikovurderinger hensiktsmessig trening i metode før man gjennomfører risikoidentifikasjon.
Øvelse – sikkerhetskopiering og gjenoppretting	
ISO/IEC 27001/27002 A.12.3 *Sikkerhetskopiering*	Sikkerhetskopiering av informasjon, programvare og systemoppsett skal gjennomføres og testes regelmessig i henhold til definerte prosedyrer.
ISO/IEC 27001/27002 A.17.1 *Forretningskontinuitet*	Virksomheten skal regelmessig verifisere etablerte og implementerte prosedyrer for opprettholdelse av IKT-sikkerheten.

Kilde/referanse	Tiltak / Kontroll
IEC 62443-2-1 4.3.2.5 *Forretningskontinuitetsplan*	Virksomheten skal utvikle prosedyrer for sikkerhetskopiering og gjenoppretting som støtter opp om forretningskontinuitetsplanen. Forretningskontinuitetsplanen skal testes regelmessig og oppdateres ved behov.
IEC 62443-2-1 4.3.4.3 *Systemutvikling og vedlikehold*	Prosedyrer for sikkerhetskopiering og gjenoppretting av datasystemer og beskyttelse av sikkerhetskopier skal etableres, brukes og verifiseres gjennom hensiktsmessige testmetoder.
NIST CSF – PR.IP-10 *Beskytt; Beskyttelse av informasjon, Prosesser og Prosedyrer*	Respons og gjenopprettingsplaner er testet (viser blant annet til ISO/IEC 27001:2013 A.17.1). *Å utføre respons, gjenopprettingsplaner og testing er også adressert i NIST CSF subkategori ID.SC-5 (oppfølging av forsyningskjeden), her i sammenheng med leverandører og 3.parts leverandører.*
NSM grunnprinsipp 3.6 *Etabler evne til gjenoppretting av data*	Test sikkerhetskopier regelmessig ved å utføre en gjenopprettingstest.
NOROG 104 – ISBR 7 *Forberedelse for katastrofegjenoppretting*	Katastrofegjenopprettingsplaner for kritiske IKT-systemer for prosesskontroll, sikkerhet og support skal dokumenteres, testes og vedlikeholdes, for å understøtte forretningskontinuitetsplanene.
DNVGL-RP-G108 kap. 6.5.2 *Sikkerhetskopiering og gjenoppretting*	Sikkerhetskopiering bør testes regelmessig.
Øvelse – beredskap	
NSM grunnprinsipp 4.1 *Forbered virksomheten på håndtering av hendelser*	Etabler et planverk for hendelseshåndtering som ivaretar behovet for virksomhetskontinuitet ved beredskap og krise. Tren og øv på planer jevnlig slik at disse er godt innøvd.
IEC 62443-2-1 4.3.4.5.11 *Hendelsesplanlegging og respons*	Virksomheten skal implementere en plan for hvordan man responderer på hendelser som identifiserer roller og ansvar blant personell og definerer aksjoner som skal utføres av utpekte personer. Øvelser bør gjennomføres regelmessig for å teste planen.
Øvelse – inntrenging og deteksjon	
NSM grunnprinsipp 3.4 *Gjennomfør integreringstester og «red-*	Gjennomfør jevnlige inntrengningstester for å identifisere sårbarheter og angrepsvektorer som kan brukes for å utnytte

Kilde/referanse	Tiltak / Kontroll
team» øvelser	virksomhetens systemer og ressurser. Utføre periodiske «Red Team»-øvelser[18] for å teste virksomhetens evne til å identifisere, stoppe og respondere hurtig og effektivt på dataangrep.
NIST CSF – DE.DP *Detektere; Deteksjonsprosesser*	Deteksjonsprosesser er testet. Deteksjonsprosesser forbedres kontinuerlig.

[18] Se beskrivels av «red-team» i kapittel 6.3 og Faktaboks 6-1.

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.