TIBER-NO

Implementeringsveiledning

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn

Samfunnet er avhengig av at betalingssystemet og annen finansiell infrastruktur fungerer. Det sikrer at privatpersoner og bedrifter kan betale for varer og tjenester, at banker kan formidle finansiering og at risiko kan omfordeles. En sikker og effektiv finansiell infrastruktur er derfor en forutsetning for finansiell stabilitet. Risikoen for cyberangrep mot denne infrastrukturen er en økende utfordring for effektivitet og sikkerhet i betalingssystemet internasjonalt og i Norge.

Den europeiske sentralbanken (ECB) utarbeidet i 2018 et rammeverk for trusselbasert inntrengingstesting for finansiell sektor, TIBER-EU («Threat Intelligence-based Ethical Red Teaming»). Formålet med TIBER-EU er å legge til rette for testing og deling av erfaringer etter testing for å styrke cyberforsvaret i europeiske finanssektor[1]. TIBER-EU er innført i flere europeiske land herunder Danmark, Sverige og Finland.

TIBER-NO er utarbeidet av Finanstilsynet og Norges Bank i dialog med næringen og andre relevante myndigheter.

1.2 Hva er TIBER-EU?

TIBER-EU er retningslinjer utarbeidet av ECB for å teste finansielle institusjoners evne til å oppdage, beskytte seg mot og reagere på avanserte cyberangrep. Bruk av målrettet trusseletterretning og eksterne testspesialister («Red Team») bidrar til at testingen blir realistisk. Viktige IKT-systemer testes ved å etterligne taktikk, teknikk og prosedyrer som benyttes av reelle trusselaktører. Hensikten er å oppdage sårbarheter slik at risikoreduserende tiltak kan iverksettes. Målsettingen er at sentrale aktører i finansiell sektor skal bli bedre rustet til å oppdage, beskytte seg mot og håndtere alvorlige cyberangrep.

TIBER-EU har følgende målsettinger:

- Forbedre cyberforsvaret i finansiell sektor.
- Standardisere og harmonisere måten virksomheter i EU utfører trusselbasert inntrengingstesting på, samtidig som hvert land beholder en viss fleksibilitet til å tilpasse rammeverket til nasjonale forhold.
- Veilede myndighetene om hvordan de kan etablere, implementere og administrere denne formen for trusselbasert testing på nasjonalt og europeisk nivå.
- Legge til rette for grensekryssende, trusselbasert inntrengingstesting for multinasjonale virksomheter.

[1] Rammeverket bygger på lignende testprogram fra Storbritannia og Nederland

- Legge til rette for at ulike overvåkings- og tilsynsmyndigheter kan basere seg på hverandres vurderinger, redusere regulatorisk byrde for foretak i finansiell sektor og fremme gjensidig anerkjennelse av tester på tvers av EU.

- Opprette prosedyrer og retningslinjer for samarbeid, resultatdeling og analyser mellom myndigheter og land som deltar i TIBER-EU.

Et standardisert oppsett for testing bidrar til sammenlignbare vurderinger av sikkerhet på tvers av systemer og land og legger til rette for informasjonsdeling mellom myndigheter og virksomheter nasjonalt og internasjonalt.

En TIBER-test imiterer et potensielt angrep fra relevante trusselaktører for å teste om tiltakene foretakene har iverksatt er tilstrekkelige. Testingen er et supplement til foretakenes periodiske sikkerhetsrevisjoner, penetrasjonstester og sårbarhetsskanninger, og kan bidra til å gi et mer reelt bilde av motstandsdyktighet overfor cyberangrep.

Foretak som testes er etter TIBER-EU ansvarlig for testingen. Det innebærer at foretaket leier inn leverandører av trusseletterretning og testing, styrer risiko, gjennomfører testing og tar ansvar for oppsummering og læringspunkter. En egen gruppe hos foretaket («White Team») har ansvaret for dette.

1.3 Om TIBER-NO

TIBER-NO-rammeverket er den norske implementeringen av TIBER-EU og gjelder for finansiell sektor i Norge. Implementeringsveiledningen (dette dokumentet) fastsetter det norske rammeverket - TIBER-NO - innenfor rammene etablert av TIBER-EU, og klargjør hvilke valg som er tatt for TIBER-NO.

Europa-kommisjonen har i sitt forslag til «Digital Operational Resilience Act for the financial sector» (DORA) datert 24. september 2020, foreslått bestemmelser som stiller krav til foretakenes testing av cybersikkerhet, herunder regelmessig trusselbasert testing (TLTP) for foretak utpekt, etter regelverket, av tilsynsmyndighetene. Det er videre foreslått at de europeiske tilsynsmyndighetene for banker (EBA), forsikring og pensjon (EIOPA) og verdipapirer (ESMA), etter konsultering med ECB og hensyntatt eksisterende rammeverk, skal utarbeide forslag til regulatoriske tekniske standarder (RTS) for testrammeverk. Det antas at DORA, når regelverket blir fastsatt, vil være EØS-relevant og bli tatt inn i norsk rett. Det kan gi behov for tilpasninger av TIBER-NO.

TIBER-NO er det første nasjonale rammeverket for trusselbasert testing av cybersikkerhet i finansiell sektor i Norge.

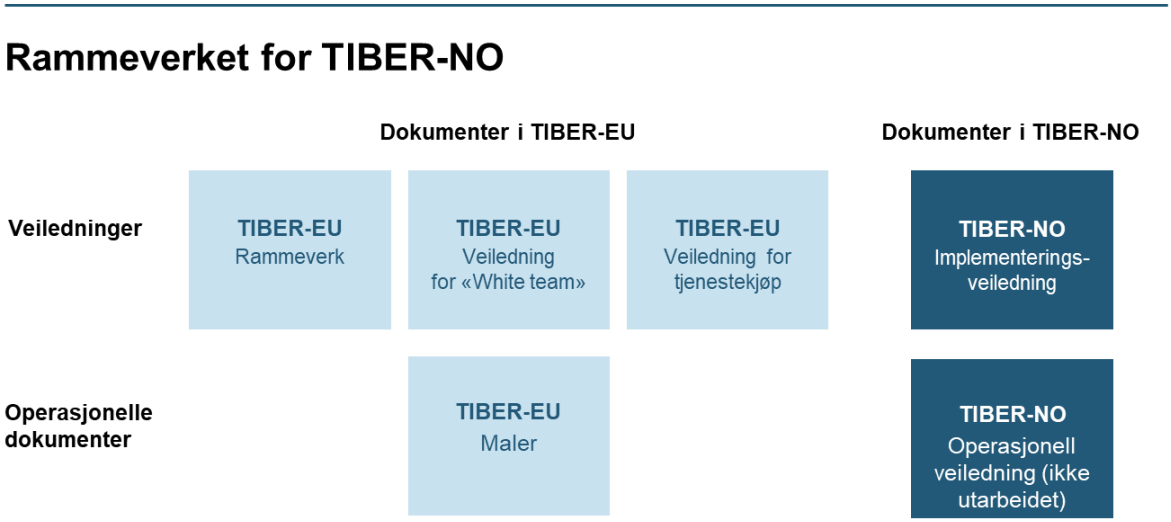
TIBER-EU åpner for at nasjonale TIBER-rammeverk kan ha ulike målsettinger med TIBER-testing. For TIBER-NO er målsettingen å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i det norske finansielle systemet. Funksjoner som er kritiske vil bli prioritert i testingen. TIBER-NO innføres ikke som et verktøy for tilsyn eller overvåking av foretak eller enkeltsystemer.

Flere store aktører i norsk finansiell sektor er del av multinasjonale konsern. En målsetting for TIBER-NO er å legge til rette for at multinasjonale konsern kan teste konsernets virksomhet i Norge etter rammeverket.

TIBER er ment for foretak i finansiell sektor som har funksjoner som er kritiske for det norske finansielle systemet. For TIBER-NO er det likevel valgt at ikke-kritiske funksjoner kan inkluderes i TIBER-testing. Det åpner for at foretak i finansiell sektor som ikke har kritiske funksjoner kan delta i TIBER-NO og gjennomføre tester, og at foretak som har kritiske funksjoner kan inkludere ikke-kritiske funksjoner i TIBER-testing.

I vurderingen av hva som er kritiske funksjoner vil det bli sett hen til kriterier fra Single Resolution Board (SRB). [2]

TIBER-rammeverket spesifiserer hva som er obligatorisk for en TIBER-test herunder retningslinjer og maler som skal følges, se figur under.



Figur 1: Veiledninger og operasjonelle dokumenter i TIBER-EU og TIBER-NO

TIBER-EU legger opp til at nasjonale myndigheter kan velge om testingen skal være frivillig eller obligatorisk. I Norge er det valgt at det skal være frivillig å delta i TIBER-testing. Alle foretak som velger å delta i TIBER-NO skal gjennomføre TIBER-tester. Foretak som velger å delta i TIBER-NO får tilgang til erfaringer fra TIBER-tester av andre foretak i Norge og andre land. Foretaket som testes «eier» informasjonen fra egen testing og bestemmer hva som kan deles og hvem de vil dele med. Erfaringen fra andre land som har innført TIBER viser at testresultater vanligvis deles på et aggregert nivå.

[2] https://www.srb.europa.eu/system/files/media/document/critical_functions_final.pdf

For TIBER-NO er det vektlagt at TIBER-testingen tilpasses norske forhold og norsk finansiell sektor. TIBER-NO er utarbeidet av Finanstilsynet og Norges Bank i dialog med næringen, med vekt på kontrollert ressursbruk, gradvis innføring, læring og tilpasning av rammeverket underveis.

1.4 Hensikten med veiledningen

Denne implementeringsveiledningen gir en overordnet beskrivelse av hva som må være oppfylt, herunder hvordan en TIBER-test skal gjennomføres, for at testen skal kunne godkjennes som en TIBER-test[3]. Veiledningen beskriver hvordan TIBER er operasjonalisert i Norge og gir oversikt over krav, roller og prosesser. Implementeringsveiledningen er det mest sentrale dokumentet i det norske TIBER-rammeverket.

For full oversikt må veiledningen leses sammen med dokumenter fra TIBER-EU-rammeverket og TIBER-NO «Operational Guide»[4]. Se oversikt over relevante dokumenter i figur 1.

1.5 Juridisk grunnlag og opphavsrett

Som del av implementeringen av TIBER-EU i Norge og utarbeidelsen av denne veiledningen, har Norges Bank vurdert rammeverket opp mot norske og EØS-relevante lover og forskrifter. Hensikten har vært å sikre at det ikke er konflikt med krav, metoder og prosesser i TIBER-EU og TIBER-NO. Vurderingen har vært foretatt for det tilfelle at ansvaret for forvaltning av rammeverket legges til Norges Bank.

Konklusjonen etter den juridiske gjennomgangen er at implementering av TIBER-EU-rammeverket kan gjennomføres i tråd med norsk lovgivning. En viktig forutsetning for konklusjonen er at alle foretak og institusjoner som deltar i TIBER-NO gjør dette frivillig.

Det vil jevnlig bli gjennomført ny gjennomgang og oppdatering av den juridiske vurderingen for å sikre at TIBER-NO fortsetter å være i tråd med norsk lovgivning. Slik oppdatering vil bli gjort så lenge rammeverket er i bruk i Norge.

Det understrekes at foretakene og tredjepartsleverandørene som testes i en TIBER-test, har ansvaret for at testen gjennomføres i henhold til gjeldende lover og forskrifter og at tilstrekkelig styring og kontroll av risiko er på plass.

Foretakene som deltar i TIBER-NO er ansvarlige for å gjennomføre en juridisk vurdering før testing gjennomføres, og kan ikke basere seg på den juridiske gjennomgangen utført av Norges Bank.

Informasjonen i veiledningen kan ikke anses som juridisk eller operasjonell rådgivning. Dokumentet inneholder elementer fra publikasjonen «TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming» som ECB eier opphavsretten til.

[3] Veiledningen er utarbeidet av Norges Bank og Finanstilsynet og publisert på de to virksomhetenes nettsider

[4] TIBER-NO «Operational Guide» er så langt ikke utarbeidet

2 Roller og ansvar i TIBER-NO

2.1 TIBER Cyber Team (TCT-NO)

Finanstilsynet og Norges Bank samarbeider om implementering og bruk av TIBER-rammeverket i Norge, og vil etablere de nødvendige fora for overordnet oppfølging, styring og involvering av næringsaktører og andre relevante myndigheter. Vurderingen av hva som er kritiske funksjoner og den overordnede styringen av hvilke foretak og funksjoner som skal testes, skal ivaretas av Finanstilsynet og Norges Bank gjennom disse foraene.

Norges Bank organiserer og bemanner et «TIBER Cyber Team» (TCT-NO) for å forvalte og operasjonalisere TIBER-NO, og har det formelle ansvaret for forvaltning av rammeverket.

TCT-NO bør ha erfaring og kunnskap om IKT-virksomheten til foretak som er kandidater for testing. Videre må TCT-NO ha kunnskap om relevante IKT-systemer, kompetanse på risikostyring, kunnskap om trusselaktørers motiver og mål, taktikker, teknikker og prosedyrer, og kompetanse på trusselutvikling og geopolitisk utvikling. TCT-NO må ha kompetanse til å gjennomgå og godkjenne alt relevant materiale utarbeidet i testprosessen.

TCT-NO er ansvarlig for å overvåke at alle TIBER-NO-tester gjøres i samsvar med TIBER-NO. TCT-NO skal følge opp at kritiske funksjoner i det finansielle systemet testes og inngår i foretaks testing.

TCT-NO følger opp at TIBER-NO-tester oppfyller kravene i TIBER-rammeverket og kan anerkjennes som TIBER-tester, og kan og bør gi råd og anbefalinger om omfang for tester. TCT-NO godkjenner endelig omfang og resultat for hver enkelt TIBER-test, og har rett til å underkjenne en TIBER-test hvis testen ikke er gjennomført i samsvar med kravene i TIBER-NO.

TCT-NO følger opp at foretakene utfører testing på en enhetlig og kontrollert måte. TCT-NO kan ikke holdes ansvarlig for handlinger utført av foretakenes «White Team», foretaket for øvrig eller tjenesteleverandører til foretaket, eller for konsekvenser TIBER-NO-testing har påført foretak som testes eller tredjepart.

TCT-NO er ansvarlig for løpende forvaltning av TIBER-NO-rammeverket i samsvar med gjennomførte tester og andre erfaringer og endringer i TIBER-EU. TCT-NO ivaretar sitt ansvar i samarbeid med deltakere i TIBER-NO og TCT i andre jurisdiksjoner.

TCT-NO deltar i kunnskapssenteret for TIBER som drives av ECB (TIBER Knowledge Centre - TKC). Deltakere i TKC er TCT-team i land som implementerer eller har implementert TIBER-rammeverket. TKC skal være en arena for samarbeid og gjensidig støtte.

2.2 Generisk trussellandskapsrapport («Generic Threat Landscape»)

Generisk trussellandskapsrapport (GTL) er en overordnet vurdering av trusselbildet mot finansielle institusjoner. GTL danner grunnlaget for de målrettede etterretningsrapportene som utarbeides og benyttes i TIBER-tester.

TCT-NO er ansvarlig for at GTL-rapporten for TIBER-NO utarbeides, vedlikeholdes og oppdateres regelmessig. Nordic Financial CERT (NFCERT) utarbeider en nordisk GTL-rapport med nasjonale vedlegg som beskriver trusselbildet mot finansiell sektor. Rapporten oppdateres minimum årlig.

Nordiske land som har innført TIBER har besluttet at GTL-rapporten fra NFCERT skal være GTL-rapport for TIBER-testing, og dette er valgt også for TIBER-NO.

TCT-NO skal sikre at relevante organisasjoner[5] er tilstrekkelig involvert i utarbeidelsen av GTL-rapporten for TIBER-NO, og at rapporten deles med foretak som deltar i TIBER-NO. TCT-NO skal videre bidra til å kvalitetssikre innholdet i GTL-rapporten.

GTL-rapporten vurderer hvordan trusselen fra statlige aktører, vinningskriminelle, aktivister og andre trusselaktører, kan ramme kritiske funksjoner i finansforetak, andre sentrale aktører i bank- og betalingssystemet og sentrale leverandører til disse. GTL-rapporten tar for seg trusselaktørenes motiver og mål, samt taktikker, teknikker og prosedyrer (TTPer) de benytter.

2.3 Samarbeid med andre og deling av informasjon

NFCERT er i samarbeid med blant annet TCT-NO ansvarlig for å utarbeide den generelle trusselrapporten (GTL-rapporten) som er et viktig utgangspunkt for all planlegging av TIBER-NO testing. Under utarbeidelsen av rapporten er NFCERT i dialog med relevante nasjonale myndigheter innenfor cybersikkerhet.

GTL-rapporten kan deles med aktuelle leverandører av trusseletterretning og Red Team-tjenester, både de som tidligere har levert oppdrag under TIBER-NO og de som ikke har det, samt med foretak som så langt ikke har blitt testet.

NFCERT støtter medlemsforetakene ved håndtering av cyberangrep og dermed også foretakenes håndtering av simulerte cyberangrep som gjøres i TIBER-testing. NFCERT deler sin oppsummering av angrep (der de har støttet foretak) med relevante nasjonale myndigheter innenfor cybersikkerhet, i møtefora etablert utenfor TIBER-NO.

Det testede foretaket er juridisk eier av alt materiale som produseres under testen. Foretaket deler resultater fra testingen med TCT-NO[6]. TCT-NO vil kun dele informasjon om testing med andre dersom foretaket gir sitt samtykke.

TCT-NO har ikke en tilsyns- eller overvåkingsrolle overfor enkeltsystemer og/eller foretak. TCT-NO skal ikke dele TIBER-NO-informasjon om tester eller annen dokumentasjon av testede foretak, med mindre foretaket har gitt samtykke. Organiseringen av TCT skal bidra til at TIBER-NO-tester kan gjennomføres i en åpen og samarbeidende form uten at myndigheter stiller krav til testede foretak som en direkte konsekvens av testingen, og utenfor den ordinære tilsyns- og overvåkingsaktiviteten. Når en TIBER-NO-test med testrapport er fullført, informerer TCT-NO norske tilsyns- og overvåkingsmyndigheter om at foretaket har gjennomført TIBER-testing.

Tilsyns- og overvåkingsmyndigheter kan som del av sin ordinære tilsyns- og overvåkings-virksomhet etterspørre informasjon om TIBER-testing direkte fra det enkelte foretak, gitt nødvendig hjemmel. For å sikre transparens i overvåking og tilsyn overfor den enkelte institusjon, skal Norges Bank og Finanstilsynet kun hente informasjon om TIBER-testing til dette formål direkte fra det enkelte testede foretak. Informasjon hentet fra TCT-NO kan i tråd med

[5] F.eks. NCSC, NC3 og Nordic Financial CERT

[6] Se mer informasjon om de testede foretakenes deling av testresultater med TCT-NO i punktene 4.4.1 (Planlegging av tiltak) og 4.4.2 (Deling av resultater)

hovedformålet med TIBER-NO brukes av de to institusjonene i et systemperspektiv, for eksempel for vurderinger av finansiell stabilitet, men da kun som grunnlag for vurderingene. Norges Bank og Finanstilsynet vil utarbeide retningslinjer og rutiner for deling av informasjon mellom de to institusjonene og internt.

2.4 Internasjonalt samarbeid

Et av målene for TIBER-EU er å standardisere og harmonisere trusselbasert inntrengingstesting slik at TIBER-testing av multinasjonale foretak på tvers av landegrenser er mulig. For å oppnå det har TCT i alle land der TIBER er innført ansvar for å ta kontakt med andre relevante TCTer når en test medfører behov for testing i flere land.

Før hver test etter TIBER-NO skal TCT-NO, sammen med foretaket som skal testes, identifisere om testen omfatter testing i andre land. Gjør den det skal TCT-NO kontakte TCT i disse landene med sikte på å etablere samarbeid om testingen og gjensidig anerkjennelse av testen.

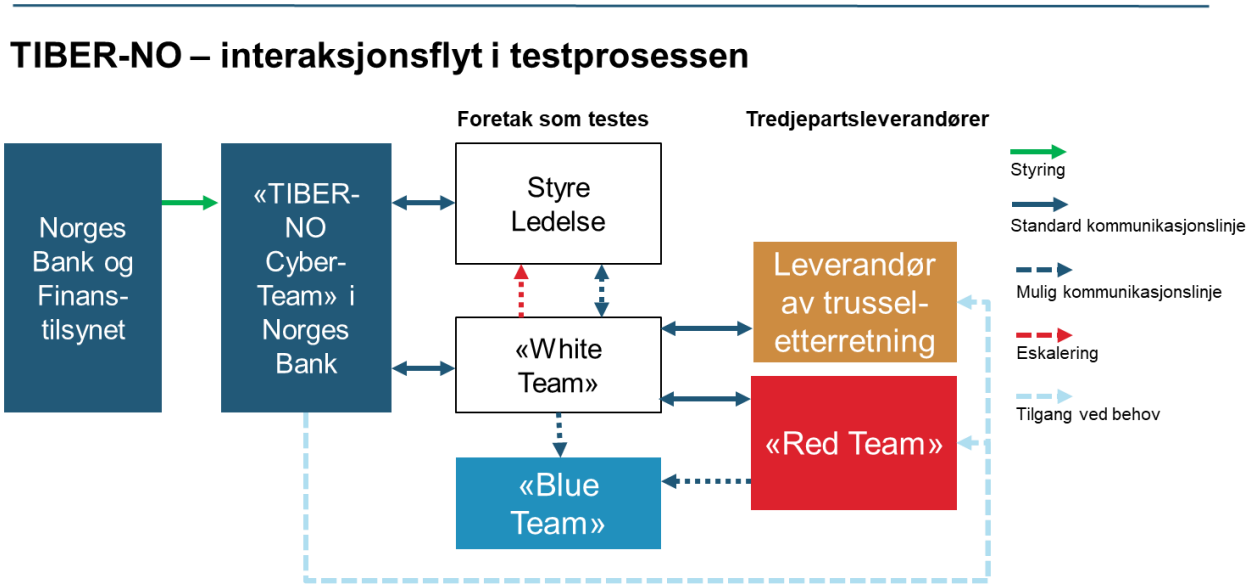
Tilsvarende kan TCT-NO samarbeide med myndigheter (TCT) i andre jurisdiksjoner når testing av foretak hjemmehørende i annen jurisdiksjon medfører behov for testing etter TIBER-NO.

Samarbeid om TIBER-testing som involverer norske foretak krever samtykke fra det norske foretaket.

3 Interessenter («stakeholders») i TIBER-NO-testprosess

De direkte interessentene involvert i en TIBER-NO-test er:

- Norges Bank
- Finanstilsynet
- «TIBER-NO Cyber Team» (TCT-NO)
- Foretaket som skal testes, organisert i «White Team» (WT) og «Blue Team» (BT)
- Tredjepartsleverandører av trusseletterretning («Targeted Threat Intelligence» - TTI) og «Red Team» (RT)-testing
- Nordic Financial CERT (NFCERT)



Figur 2: Aktører i en TIBER-NO test med forventet kommunikasjonsflyt

NFCERT vil støtte foretaket som testes på samme måte som ved et reelt angrep.

Etter TIBER-EU er det valgfritt for nasjonale rammeverk å stille krav til eventuell obligatorisk involvering av nasjonale etterretningsorgan, cybersikkerhetssentre eller relevante enheter i politiet. For TIBER-NO er det ikke stilt krav til slik obligatorisk deltakelse.

3.1 Organisering og ledelse av TIBER-tester

Foretak som tester etter TIBER-NO er selv ansvarlige for ledelse og organisering av testen. Det inkluderer kjøp av tjenester fra eksterne, implementering av kontroller, prosesser og prosedyrer for å sikre at testen etterlever krav i TIBER-rammeverket og for øvrig følger beste praksis, og styring av risiko slik at den blir holdt innenfor et akseptabelt nivå.

3.1.1 «White team» (WT)

For hver TIBER-NO-test må foretaket som skal testes opprette et White Team (WT). WT er på vegne av foretaket ansvarlig for å bestemme omfang og gjennomføring av testen, kommunisere med de andre deltakerne i testen og styre risiko under testingen.

WT skal bemannes av ledere og ansatte i foretaket med god kjennskap til foretakets kritiske funksjoner. Teamet bør ikke bestå av flere personer enn nødvendig, og færrest mulig i foretaket bør kjenne til testen. WT er ansvarlig for at planlegging og ledelse av testen er i samsvar med TIBER-NO.

«White Team» skal ha en egen leder, «White Team Lead» (WTL). WTL koordinerer all testaktivitet inkludert håndtering av leverandører av «Threat Intelligence» og «Red Team»-testing.

Mer informasjon om roller, ansvar og sammensetning av «White Team» er tilgjengelig i *TIBER-EU White Team Guidance.*

3.1.2 «Blue team» (BT)

Alle ansatte og ledere i foretaket som ikke er del av WT, er henvist til «det blå laget» («Blue Team» – BT). Det er viktig at alle medlemmer av «Blue Team» er ekskludert fra forberedelse og gjennomføring av TIBER-NO-testen og ikke på noen måte har kjennskap til testens innhold og varighet.

Ved gjennomgang av resultatet etter avsluttet testing skal «White Team» informere «Blue Team». Relevante representanter fra «Blue Team» bør delta på gjennomgang etter testing og oppfølgingen av testresultat.

3.1.3 Tredjepartsleverandører

For TIBER-NO-tester er det krav til at tredjepartsleverandører skal brukes for målrettet trusseletterretning og «Red Team»-testing. Etter TIBER-NO kan en test bare godkjennes hvis den blir utført av uavhengige tredjepartsleverandører.

Selv om testing gjennomført av interne testere (interne «Red Team») gir verdi og generelt sett bør gjennomføres, har «Red-Team»-testing gjennomført av eksterne leverandører noen klare fordeler. Eksterne har et mer uavhengig perspektiv enn interne, som ofte har bindinger til interne systemer, mennesker og prosesser og besitter kunnskap som ikke er tilgjengelig for eksterne, heller ikke for trusselaktørene. Videre har eksterne leverandører ofte mer ressurser tilgjengelig og mer oppdatert spisskompetanse.

En viktig forutsetning for vellykket gjennomføring av TIBER-NO-testing, herunder håndtering av risiko, er at leverandørene av «Threat Intelligence» og «Red Team» er kompetente, kvalifiserte og har den nødvendig erfaring. Å følge *TIBER-EU Services Procurement Guidelines* kan bidra til dette.

Ved anskaffelse av «Threat Intelligence» og «Red Team»-testleverandører skal følgende inngå i avtalen: Testens omfang og avgrensninger, risikoreduserende tiltak for gjennomføring av test, tidspunkt, tilgjengelighet for leverandørene, kontrakter og ansvar.

3.1.4 Leverandør av målrettet trusseletterretning («Targeted Threat Intelligence» - TTI)

Trusseletterretningsleverandøren («Threat Intelligence Provider» - TIP) er en ekstern tjenesteleverandør som anskaffes av «White Team». Rapporten fra TIP skal inneholde målrettet etterretning om foretaket som testes. Det skal tilsvare informasjon en avansert cyberangriper antas å ha tilgang til. Informasjonen gis til foretaket i form av en «Targeted Threat Intelligence Report» (TTIR) («Spesifikk trussel- og scenariorapport»). Det er anbefalt at tjenesteleverandøren bruker flere kilder i tillegg til GTL-rapporten i sin etterretning, for å kunne lage en etterretningsrapport som er så nøyaktig og oppdatert som mulig. «White Team» er oppdragsgiver og følger opp innhold og kvalitet i rapporten.

3.1.5 «Red team» (RT)

«Red Team»-testing leveres av en ekstern tjenesteleverandør, «Red Team-testing Provider» (RTP), anskaffet av «White Team». RTP skal prøve å bryte seg inn i foretakets IKT-systemer ved hjelp av hackingmetoder. RTP skal til enhver tid følge strenge etiske retningslinjer. «Red Team» planlegger og utfører en TIBER-NO-test av systemer og tjenester basert på scenariene utviklet av trusseletterretningsleverandøren. Etter testen lager «Red Team» en rapport som viser funn identifisert i testen.

Interne ressurser i foretaket som testes kan etter avtale med leverandør og godkjenning av TCT-NO delta i testingen og støtte ekstern «Red-Team-provider» (RTP). Slik deltakelse krever skriftlig avtale mellom RTP og foretaket.

4 TIBER-NO-testprosess

Figur 3 gir en overordnet beskrivelse av fasene for en TIBER-NO-test, herunder leveranser fra hver fase.

Figur 3: Fasene i en TIBER-test med resultater for hver fase

4.1 Oppstart («Initiation phase»)

For foretak som deltar i TIBER-NO vil «TIBER-NO Cyber Team» (TCT-NO) gjøre tilgjengelig maler, retningslinjer og andre relevante dokumenter fra TIBER-NO og TIBER-EU.

TIBER-testing for foretak som deltar i TIBER-NO kan initieres av TCT-NO eller av foretaket selv. Når det er avklart at et foretak skal gjennomføre en TIBER-test, vil TCT-NO utarbeide et utkast til

overordnet plan med milepæler. Deretter starter foretaket sin planlegging. En viktig del av planleggingen er å identifisere hvilke interessenter utover TCT-NO og tredjepartsleverandørene[7] som skal involveres. Kritiske tjenestetilbydere, herunder datasentre, er eksempler på slike interessenter.

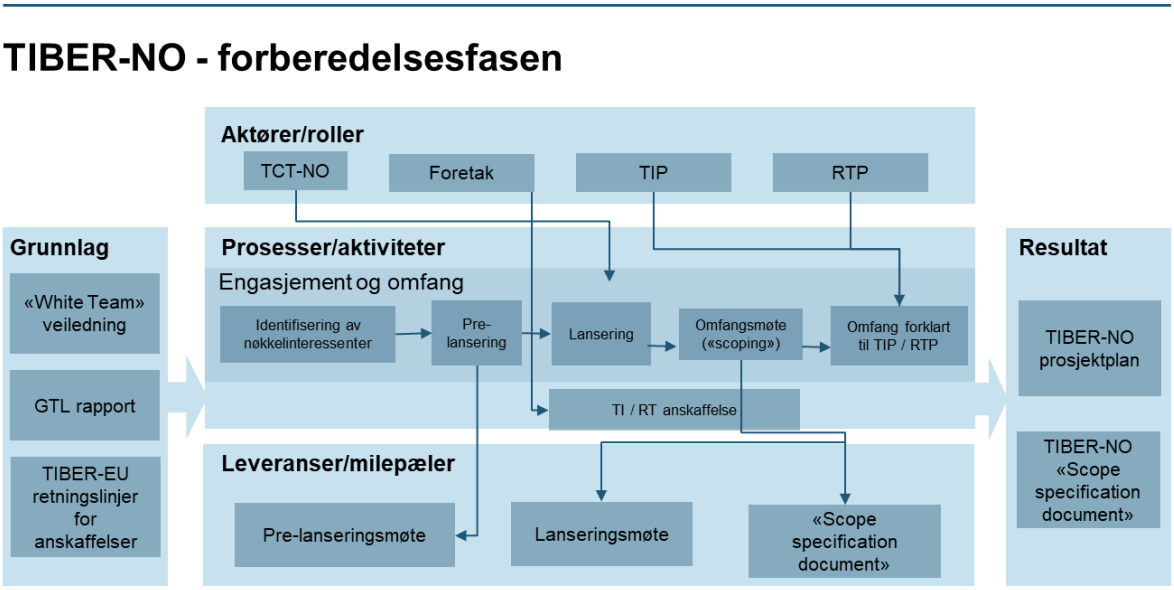
Foretakets interne organisasjon for gjennomføring av TIBER-NO testen, «White Team» (WT), etableres i oppstartsfasen. Denne innledende fasen omfatter også markedsundersøkelser for å identifisere mulige tredjepartsleverandører og identifisering av juridiske problemstillinger som må være avklart før testing.

I oppstartsfasen gjennomfører foretaket en innledende vurdering av hvilke kritiske funksjoner som skal inngå i testen («scoping») og hvilke IKT-systemer som støtter disse funksjonene. Vurderingen er basert på hvilke overordnede kritiske funksjoner TCT-NO mener skal testes og hvilke kritiske funksjoner i foretaket som støtter disse.

4.2 Forberedelser («Preparation phase»)

I den forberedende fasen går «TIBER Test Manager» (TTM)[8] i dialog med foretaket som skal testes for formelt å starte prosjektet. Fasen bør igangsettes minimum tre måneder før selve testen.

TCT-NO og foretaket skal i denne fasen bli enige om omfanget av testen og foretaket skal anskaffe cybersikkerhetsleverandør(er). Fasen er forventet å vare fire til seks uker, ekskludert foretakets anskaffelsesprosess.



Figur 4: Forberedelsesfasen med aktører, aktiviteter og leveranser

[7] Med tredjepartsleverandører menes i denne sammenheng leverandør av trusseletterretning (TIP) og leverandør av «Red-team»-testing (RTP)
[8] TTM er en del av TCT-NO-teamet

4.2.1 Forberedelsesmøter

Forberedelsesfasen starter med et møte (pre-lansering) mellom TCT-NO og «White Team» (WT). TCT-NO vil i dette møtet informere foretaket om krav til TIBER-NO-prosessen, interessentenes roller og ansvar, sikkerhetsprotokoller, og kontraktshensyn knyttet til leverandører av testing og etterretning. Videre vil TCT-NO sørge for at WT starter sine forberedelser. Det inkluderer overordnet prosjektplanlegging i tråd med avtalte datoer, anskaffelse av tredjepartsleverandører, risikostyring og vurdering av omfang for testen. Endelig beslutning om scope tas senere, se punkt 4.2.2.

Foretaket bør starte anskaffelsesprosessen umiddelbart etter pre-lanseringsmøtet.

Senere i forberedelsesfasen skal det gjennomføres et møte mellom alle interessentene i TIBER-NO-testen («Lanseringsmøte» - se figur over) hvor det gjennomføres forventningsavklaring og deltakerne sammen går gjennom testprosessen. WT lager på bakgrunn av dette et utkast til TIBER-NO prosjektplan.

4.2.2 Beslutte omfang («scoping»)

Omfanget («scope») av testen og hvilke kritiske funksjoner som skal testes, må fastsettes med utgangspunkt i vurdering av omfang gjort i Oppstartsfasen (4.1). Foretaket som skal testes vurderer hvilke interne funksjoner som støtter kritiske funksjoner som skal testes, og avklarer dette med TCT-NO. «White Team» (WT), «Red Team»-leverandør (RTP) og «Threat Intelligence» leverandør (TIP) deltar i avklaringen.

Omfanget av testen dokumenteres av «White Team» i det testede foretaket i «TIBER-EU Scope Specification document». Det skal her redegjøres for omfanget av TIBER-testen og nøkkelsystemer og tjenester som inngår. Det hjelper WT med å sette mål («flags») og definere mer overordnede målsettinger for testen. Selv om målsettingene defineres i denne fasen kan de justeres i senere faser for eksempel på bakgrunn av oppdatert informasjon fra trusseletterretning eller testing.

TCT-NO har ansvar for å sikre at kritiske funksjoner testes på en hensiktsmessig måte for å bidra til finansiell stabilitet. TCT-NO godkjenner at omfanget av testen er iht. TIBER-NO.

Omfanget forankres på styrenivå hos foretaket som skal testes. Tilgang til informasjon om testen begrenses mest mulig.

4.2.3 Innkjøp av tjenester («Services procurement»)

Etter TIBER-NO kan en trusselbasert test kun godkjennes som en TIBER-test dersom den gjennomføres ved hjelp av uavhengige tredjepartsleverandører.

To typer tredjepartsleverandører må være involvert:

- «Threat Intelligence»-tilbyderen» (TIP) leverer en «Targeted Threat Intelligence Report» (TTIR) («Spesifikk trussel- og scenariorapport») som beskriver relevante trusselaktører og foreslåtte trusselscenarier for testing.
- «Red Team»-tilbyderen (RTP) planlegger og utfører TIBER-NO testen mot systemene og tjenestene som er «scopet inn» i testen. RTP leverer etter gjennomført test en beskrivelse

av testen inkludert eventuelle problemer med gjennomføring og en «Red Team»-testrapport til foretaket.

Foretaket står selv ansvarlig for at det foreligger en gjensidig avtale med TIP og RTP. En slik avtale skal som et minimum inkludere følgende faktorer: Omfang og begrensninger for testen («scope»), periode for gjennomføring, tilgjengelighet for personell, avtalte kontrollhandlinger og testing, klausuler om ansvarlighet og relevante forsikringer. Kontrakten bør inneholde:

- Krav til sikkerhet og konfidensialitet på nivå med de generelle kravene som gjelder for foretaket.
- Klausuler for beskyttelse av personell involvert i selve testen.
- Klausuler for eventuell kompromitteringsvarsling og håndtering av ødeleggelse av data.
- Avklaring av hvilke aktiviteter og handlinger som ikke er tillatt under testen, for eksempel: Ødeleggelse av utstyr, ukontrollert endring av data/applikasjoner, sette driften av kritiske systemer i fare, utpressing, trusler og bestikkelser av ansatte, og avsløring av resultatene av testen.

Foretaket som skal testes er ansvarlig for at de valgte tjenestetilbydere oppfyller minimumsvilkårene for en slik test, jf. *TIBER-EU Services Procurement Guidelines*.

4.2.4 Risikostyring («Risk management»)

TIBER-NO-testen foregår i finansielle institusjoners og/eller deres leverandørers produksjonsmiljøer og medfører derfor elementer av risiko for foretakene. WT er ansvarlig for å implementere passende risikoreduserende kontroller, prosesser og prosedyrer, for å sikre at testen utføres med tilstrekkelig forsiktighet og at risiko er innenfor foretakets aksepterte nivå.

Risiko skal identifiseres, analyseres og håndteres (herunder reduseres, unngås, overføres eller aksepteres) i henhold til foretakets rammeverk og praksis for risikostyring. Risikovurdering og gjennomføring av tiltak for å håndtere risiko må ferdigstilles før testing starter. Ansvaret for dette ligger på WT.

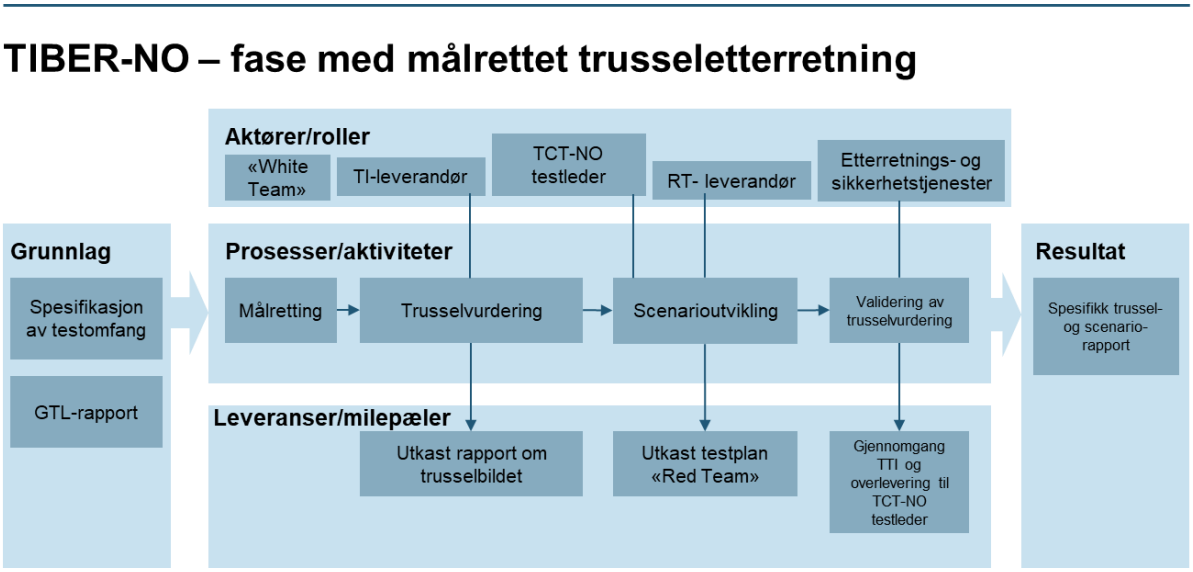
Når forberedelsesfasen er ferdig skal foretaket som testes ha produsert:

- *TIBER-EU Scope Specification document* som avklarer omfanget av testen og valgte leverandører for trusseletterretning og gjennomføring av testing.
- *TIBER-NO Prosjektplan.*

4.3 Testing («Testing phase»)

4.3.1 Målrettet trusseletterretning («Targeted Threat Intelligence»)

Formålet med fasen er å sørge for at testingen er etterretningsdrevet, det vil si basert på foretakets reelle trusselbilde. I trusselbildet inngår relevante trusselaktører, hva disse aktørene er ute etter og hvordan de opererer. Informasjonen samles, struktureres og avleveres i en «Targeted Threat Intelligence Report» (TTIR) («Spesifikk trussel- og scenariorapport»).



Figur 5: Fase med målrettet trusseletterretning - aktører, aktiviteter og leveranse

TTIR beskriver realistiske angrepsscenarier mot foretakets kritiske funksjoner som kan inngå i testen. For å gjøre det mulig å utarbeide TTIR-rapporten skal foretaket forut for denne fasen ha levert relevant informasjon til «Threat Intelligence tilbyderen» (TIP). Denne informasjonen skal omfatte overordnet og teknisk oversikt over alle systemer som understøtter kritiske funksjoner, foretakets oppdaterte trusselvurdering og trusselregister, og eksempler på nylige angrep på foretaket.

GTL-rapporten leveres til TIP som bruker den som et utgangspunkt for å identifisere konkrete trusselaktører som er relevante for testen.

TIP er ansvarlig for å gjennomføre en målrettet innsamling av informasjon fra et bredt spekter av kilder[9]. TIP gjennomfører deretter analyse av informasjonen og formidler et utkast av TTIR. Deretter gjennomfører TIP scenarioutvikling med relevante trusselaktører og sannsynlige trusselscenarier for det konkrete foretaket. TIP produserer et utkast til testplan.

Sluttproduktet fra denne fasen er en «Targeted Threat Intelligence Report» (TTIR) («Spesifikk trussel- og scenariorapport») som inneholder tre deler.

Første del er oversikt over foretaket fra et etterretningsperspektiv. Oversikten skal bidra til å skape en strategisk forståelse av virksomhetsområdene med nåværende og planlagte aktiviteter. Denne delen skal gi innsikt i forretnings- og system-konsekvenser ved eventuell kompromittering av kritiske funksjoner. For å gjøre dette så effektivt som mulig skal foretaket gjøre følgende informasjon tilgjengelig for TIP:

- En beskrivelse av foretakets kjernefunksjoner, herunder underliggende faktorer som er kritiske for kjernefunksjonene og en begrunnelse for hvorfor foretaket er kritisk for det finansielle systemet.

[9] Herunder åpne kilder, f.eks. OSINT, TECHINT og HUMINT

- En overordnet og teknisk oversikt over alle systemer som understøtter kritiske funksjoner som omfattes av testen (er «in scope»).
- Oppdatert trusselvurdering og trusselregister.
- Eksempler på tidligere trusselhendelser.

Andre del er oversikt over aktører og overordnede scenarier. I denne delen vil GTL-rapporten bli brutt ned av TIP, slik at den blir mer spesifikk for foretaket som skal testes. Det skal vurderes hva slags intensjon og kapabilitet de relevante trusselaktørene har for å angripe foretaket og deres kritiske funksjoner. Analysen skal bunne ut i en liste over de mest sannsynlige og kapable trusselaktørene.

TIP vil i andre del lage flere overordnede scenarier om hvordan et angrep fra de valgte trusselaktørene kan arte seg. Scenariene skal knyttes til trusselaktørenes motivasjon og intensjon om å angripe de konkrete kritiske funksjonene. Rapporten skal inneholde:

- De meste relevante trusselaktørene for angrep på de kritiske funksjonene til foretaket.
- En redegjørelse for motivasjonen til trusselaktørene for å gi innsikt i hvorfor de kan komme til å angripe.
- Mest sannsynlige mål for hver av trusselaktørene.
- Overordnede angrepsscenarier for hver av trusselaktørene.

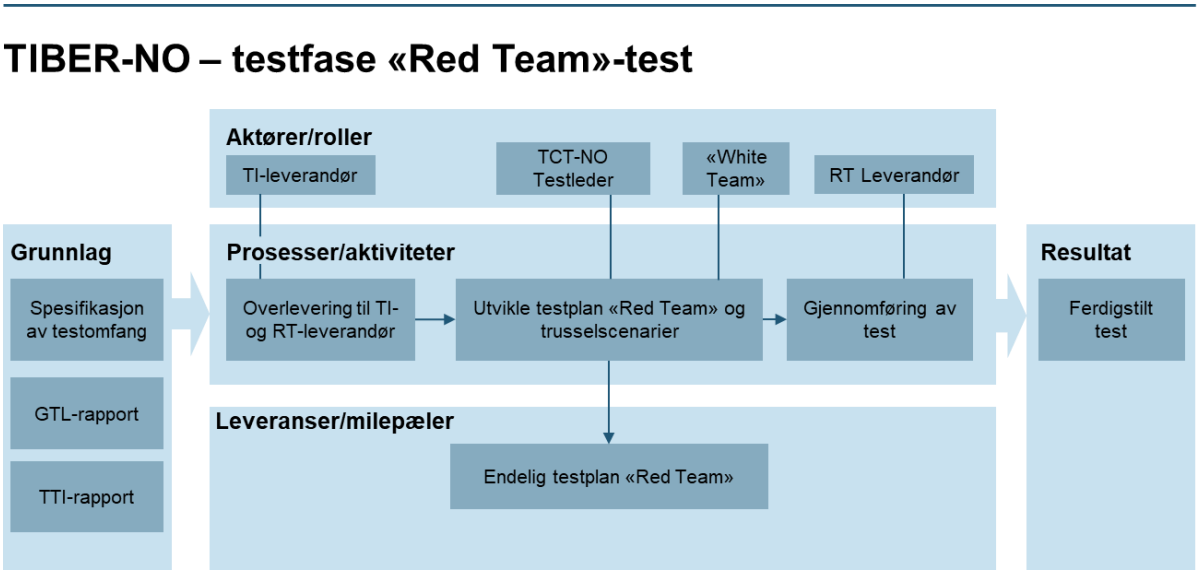
Del tre (siste del) av rapporten er etterretning om foretakets digitale tilstedeværelse (angrepsflate). TIP vil her gi «Red Team» etterretning på hva de aktuelle trusselaktørene kan ha kunnskap om vedrørende potensielle angrepsflater til foretaket. Hensikten er å være konkret på mulighetsrommet for trusselaktørene. «White Team» i foretaket kan bidra med informasjon til TIP for å fokusere søket.

Der det er hensiktsmessig og relevant er det ønskelig at nasjonale etterretnings- og sikkerhetstjenester kvalitetssikrer etterretningsinformasjonen før TTIR overleveres til TTM.

Etter TIBER-NO er det valgfritt om leverandøren av trusseletterretning for en enkelt test fortsetter engasjementet mens testingen pågår, og leverer oppdatert etterretning i denne perioden.

4.3.2 «Red team»-testing

Denne fasen starter når TIP overleverer den målrettede trusselrapporten (TTIR) til RTP. I rapporten beskrives de foreslåtte trusselscenariene for testingen.



Figur 6: Testfasen med aktiviteter, aktører og leveranser

RTP tar utgangspunkt i angrepsscenariene i TTIR og utvikler disse videre. Det skal gjøres på en slik måte at de fortsatt er trusseletterretningsstyrt. Som del av denne planleggingen foreslår RTP de konkrete målene som skal oppnås med testingen.

Foretaket som skal testes gir ved hjelp av «White Team» tilbakemelding på de foreslåtte angrepsscenariene til RTP og tar endelig beslutning på hvilke scenarier som skal testes. RTP utfører testingen basert på disse scenariene mot spesifiserte produksjonssystemer, ansatte og prosesser i foretakets kritiske funksjoner. RTP bør benytte en rekke teknikker, taktikker og prosedyrer i løpet av testen.

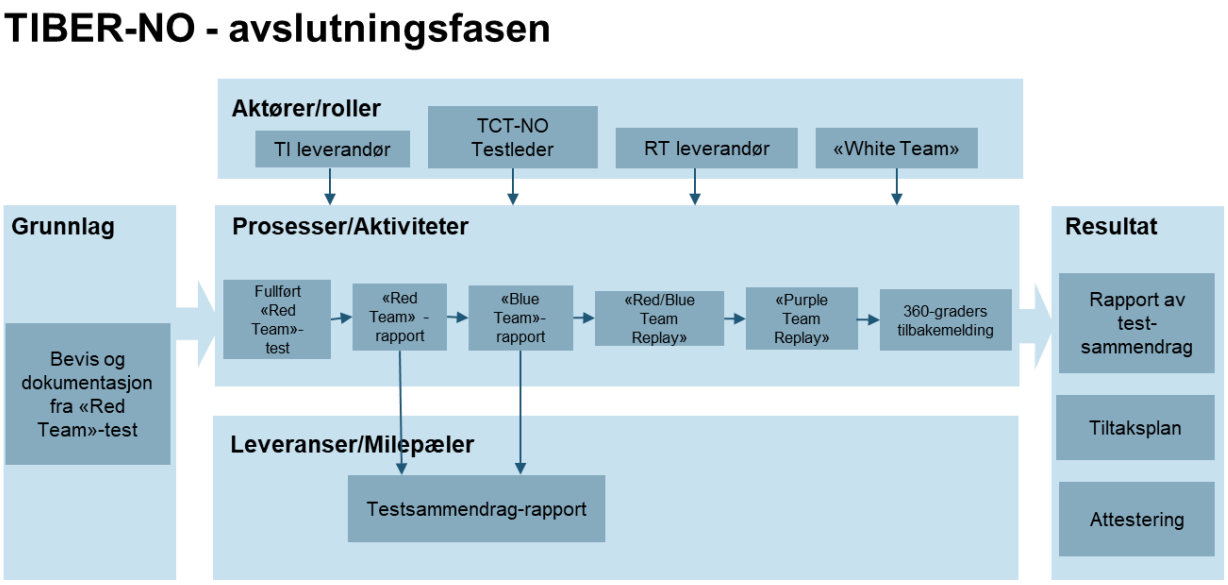
RTP skal til enhver tid følge strenge etiske retningslinjer. Testen skal gjennomføres på en kontrollert måte for alle scenarier som testes. Testingen skal ikke medføre unødig risiko for foretaket som testes og dets kritiske funksjoner, eller for annen part som er avhengig av tjenester levert av foretaket. Foretaket som blir testet, kan ved hjelp av «White Team» umiddelbart sette scenarier på vent dersom andre betydelige hendelser oppstår.

Tiden som er satt av til testingen bør være proporsjonal med omfanget av testen. Basert på erfaring forventes det at testfasen for de fleste TIBER- tester bør vare om lag 10-12 uker. Dette er kun et estimat. Tidsbruken vil variere avhengig av størrelsen på foretaket, valgte scenarier, omfang av testen herunder kritiske funksjoner som skal dekkes, og andre faktorer.

TIBER åpner for at hvert enkelt land kan velge å tillate bruk av ulike fysiske gjenstander, herunder minnepinner, komponenter knyttet til trådløse nett mv. og «plante» slike gjenstander for å få tilgang til det interne datanettverket. Det understrekes at risikovurderingen forut for hver test må inkludere en grundig vurdering av eventuell bruk av slike gjenstander.

I tillegg til de forhåndsdefinerte scenariene kan RTP teste etter såkalt «Scenario X» for å gjøre testingen enda mer virkelighetsnær og mer lik avanserte angrep. Scenario X innebærer at RTP kan teste etter scenarier som RTP selv utformer etter at testen har startet. Slik kan RTP foreslå nye veier til målet basert på erfaringer og kunnskap tilegnet i løpet av testingen. Eventuell bruk av «Scenario X» må godkjennes av WT og TCT-NO.

4.4 Avslutningsfasen



Figur 7: Avslutningsfasen med aktiviteter og leveranser

I avslutningsfasen utarbeider RTP en testrapport som beskriver gjennomført testing, funn og observasjoner. Rapporten bør inneholde forslag til tiltak for å forbedre tekniske kontroller, policyer, prosedyrer eller rutiner, og eventuelle råd for å heve kompetanse eller begrense tilgang til informasjon hos foretaket. Rapporten leveres til «White Team» i foretaket. «Blue Team» i foretaket informeres av «White Team» om den gjennomførte testen og scenariene som har blitt testet. Rapporten deles med TCT-NO.

Læring er et viktig formål for TIBER-testing. «Purple Teaming» og 360-graders tilbakemeldingsmøter kan bidra til slik læring, og er valgfrie aktiviteter i TIBER-NO. Purple Teaming» innebærer at «Red Team» og «Blue Team» bringes sammen for felles oppsummering og erfaringsoverføring.

Det er valgfritt om TCT-NO, overvåker, tilsynsmyndighet og leverandør av trusseletterretning blir invitert til oppsummeringsmøter som skal gjennomføres etter gjennomført test. Leder for «White Team» (WTL) beslutter hvem som skal inviteres.

4.4.1 Planlegging av tiltak («Remediation planning»)

Når gjennomgangen av testresultatene er ferdigstilt er det testede foretaket ansvarlig for å bearbeide funnene fra testen og utarbeide testoppsummeringsrapport og utbedringsplan.

Testoppsummeringsrapporten skal gi et bilde av den samlede testprosessen og resultater fra testingen. Rapporten skrives med grunnlag i rapporter fra hhv. «Blue Team» og «Red Team» samt TTI-rapporten. Testoppsummeringsrapporten skal ikke inneholde detaljert teknisk informasjon eller konkret informasjon om svakheter og sårbarheter. Informasjon på et slikt detaljnivå er potensielt svært sensitiv informasjon som tilhører foretaket som er testet og ikke bør deles.

Foretaket deler en aggregert versjon av testoppsummeringsrapporten med TCT-NO. TCT-NO kan gjennomgå de mer detaljerte funnene fra testen med foretaket dersom foretaket ber om det.

Utbedringsplanen er basert på testresultatene og brukes til implementering av forbedringer hos foretaket.

4.4.2 Deling av resultater («Result sharing»)

Når rapportene fra testingen er ferdigstilt, skal det testede foretaket, TIP, RTP og TCT-NO attestere om testen er utført i samsvar med TIBER-NO. Attestasjonen skal undertegnes av styret i foretaket som er testet, og av TIP og RTP. Attestasjonen godkjenner den utførte testen som en TIBER-test overfor andre relevante myndigheter herunder TCT i andre land.

Utkast til oppsummeringsrapport som beskriver den samlede testen med prosess, resultater og utbedringsplan skal deles med TCT-NO, slik at TCT-NO har mulighet til å kommentere før rapporten gjøres endelig. TCT-NO vil analysere resultatene av testingen, herunder identifiserte funn, trusler og sårbarheter. TCT-NO kan dele sine vurderinger og analyser – på et passende aggregert nivå – med andre foretak som deltar i TIBER-NO. Før TCT-NO kan dele slike vurderinger må det – for hver enkelt test – godkjennes av det testede foretaket.

Et av hovedmålene for TIBER-NO er å styrke den finansielle sektorens motstandsdyktighet mot cyberhendelser. TCT-NO vil derfor, i tilfeller der det er relevant, analysere resultatene av tester i andre jurisdiksjoner for å identifisere viktige funn og vanlige trusler og sårbarheter. TCT-NO vil dele disse med relevante interessenter til TIBER-NO. Slik deling må godkjennes av foretaket som testes.

TCT-NO har mulighet til å dele anonymiserte funn og læring fra TIBER-tester i Norge med «TIBER Knowledge Centre» (TKC). Det gjør det mulig for TKC å samle nøkkelfunn og danne seg et bilde av motstandskraften i den europeiske finanssektoren. All utveksling av informasjon mellom TCT-NO og TKC skal utføres på en sikker måte.

4.5 Samspill og kommunikasjonslinjer under testprosessen («Interactions during a TIBER-NO test»)

Alle parter involvert i en TIBER-NO-test har ansvar for at samarbeidet er godt og at det er en transparent tilnærming og effektiv gjennomføring. En forutsetning for en vellykket test er et nært og godt samarbeid mellom WTL og TCT-NO i alle faser av testen. Noen sentrale punkter for godt samspill er gjengitt nedenfor.

Ansvaret for den overordnede planleggingen og ledelsen av testen ligger hos det testede foretaket. WTL er ansvarlig for omfanget, scenariene og risikostyringen av testen, og for å sikre at testen er godkjent og validert av TCT-NO. WTL skal koordinere all testaktivitet, inkludert engasjement med tredjepartsleverandører. WTL skal sikre at leverandørenes prosjektplaner er en integrert del av foretakets samlede planlegging av testen. Omfanget av en TIBER-NO test skal godkjennes av foretakets styre eller toppledelse.

I avslutningsfasen er WTL ansvarlig for å involvere relevante aktører i foretaket (herunder ledelsen og «Blue Team») til felles gjennomgang og oppfølging. Hvis det har vært avvik i gjennomføringen av testen fra den opprinnelige planen, skal avvikene diskuteres med TCT-NO.

Selv om WTL er den primære kontakten for tredjepartsleverandørene til et foretak, bør TCT-NO også ha direkte kontakt med disse. Der viktige avgjørelser skal tas (f.eks. ved avvik fra avtalt omfang under testing) eller hvor interessekonflikter oppstår, skal både WTL og TCT-NO følge eskaleringsrutiner i egen organisasjon til sine respektive ledere.

Vedlegg 1 - forkortelser anvendt i denne veiledningen

BT	Blue Team, ledere og medarbeidere i foretaket som testes som ikke kjenner til testen.
DORA	Digital Operational Resilience Act for the financial sector
EBA	European Banking Authority
ECB	European Central Bank, den europeiske sentralbanken
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
GTL	Generisk trussellandskap, rapport om cybertrusler rettet mot finansiell sektor i Norge som brukes som grunnlag for planlegging av TIBER-tester
NFCERT	Nordic Financial CERT
RT	Red Team, team som gjennomfører inntrengingstesten
RTP	Red Team Provider, sikkerhetstestleverandør som gjennomfører inntrengingstesten
TCT-NO	TIBER-NO Cyber Team, gruppen som forvalter og foreslår eventuelle endringer i TIBER-NO og herunder støtter testing og har kontakt med ECB
TIBER	Threat Intelligence-Based Ethical Red-teaming, trusselbasert testing som gjøres ved hjelp av eksterne «røde» team/leverandører
TIBER-EU	Felles europeisk rammeverk for trusselbasert inntrengingstesting i regi av ECB
TIBER-NO	Det nasjonale TIBER-rammeverket i Norge
TKC	TIBER Knowledge Centre, forum for kunnskapsdeling mellom nasjonale TIBER myndigheter som drives av ECB
TTM	TIBER Test Manager, leder av en enkelt TIBER-test (inngår i TCT-NO)
TTIR	Targeted Threath Intelligence Report, trusselrapport som utarbeides i forkant av hver enkelt test
TIP	Threat Intelligence Provider, trusseletterretningsleverandør, dvs. leverandør av skreddersydd trusseletterretning for en spesifikk TIBER-test
TTP	Taktikk, teknikk og prosedyrer som benyttes av reelle trusselaktører
WT	White Team, gruppen som kjenner til og har ansvar for testingen hos foretaket som testes
WTL	White Team Lead, ansvarlig leder for White Team