

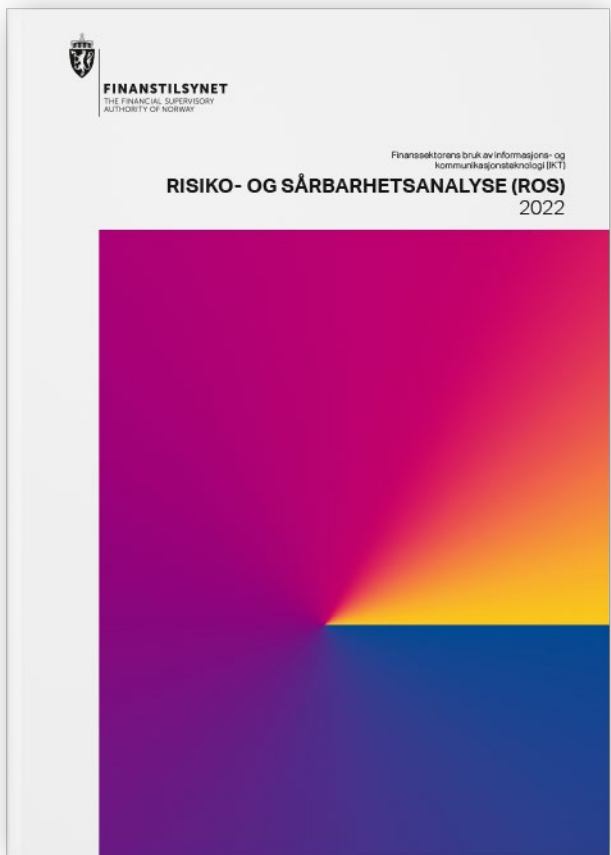


FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2022

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Olav Johannessen, Seksjonssjef tilsyn IT og betalingstjenester, Pressebrief 12. mai 2022



- ✓ **Hovedvurderinger**
- ✓ **Digital trusselbilde og kriminalitet**
- ✓ **Digital robusthet**
- ✓ **Samarbeid innen sikkerhetsområdet**
- ✓ **Koronapandemien og krigen i Ukraina**
- ✓ **IKT-hendelser**
- ✓ **Tap ved svindel**
- ✓ **Funn og observasjoner tilsynsvirksomheten**
- ✓ **Utkontraktering IKT-virksomhet**
- ✓ **Foretakenes vurderinger**
- ✓ **Risiko knyttet til digitale tjenester**
- ✓ **Vurdering av risikobildet**
- ✓ **Hovedfokus tilsynsvirksomheten 2022**
- ✓ **Oppsummerende vurderinger**

- Robust finansiell infrastruktur
- Trusselbildet i stadig endring
- Digital kriminalitet på samme nivå som i 2020
- Ingen IKT-hendelser i 2021 med konsekvenser for finansiell stabilitet
- Tilgjengeligheten til tjenestene bedre enn foregående år
- Tap ved svindel omtrent på nivå med 2020
- Avdekket sårbarheter som utgjør risiko
- Styrket beredskap i det elektroniske betalingssystemet



Foto: Einar Aslaksen

Viktigheten av robust finansiell infrastruktur



- Grunnleggende for finansiell stabilitet og velfungerende markeder
- Kompleks, sammensatt, mange aktører og leverandører
- Gjennomføring av betalinger og transaksjoner i finansielle instrumenter
- Svikt kan gi samfunnsmessige konsekvenser
- Manglende robusthet hos én enkelt aktør
- Sensitiv informasjon på avveie

Digital trusselbilde og kriminalitet



- Det digitale trusselbildet er i stadig endring
- Organiserte kriminelle - fremmed etterretning
- Omfanget av digital kriminalitet synes å være på nivå med 2020
- Avdekket alvorlige sårbarheter hos enkelte foretak
- Digital kriminalitet - ingen alvorlige hendelser så langt
- Systemer for overvåking, håndtering av hendelser og avverging av angrep
- Aktuelle trusler for Norge og norske interesser er
 - nettverksoperasjoner fra andre stater
 - bruken av løsepengevirus
 - angrep via digitale verdikjeder (leverandører / samhandlingspartnere)
 - angrep på sentrale tjenesteleverandører og datasentre
 - digital økonomisk vinningskriminalitet

Digital robusthet



Nasjonalt tiltak - TIBER-NO

- Rammeverket TIBER-NO, testing av cybersikkerhet i finanssektoren
- Motstandsdyktighet mot cyberangrep for kritiske funksjoner

Tiltak i foretakene for å motvirke, avdekke, gjenopprette hendelser og håndtere konsekvenser

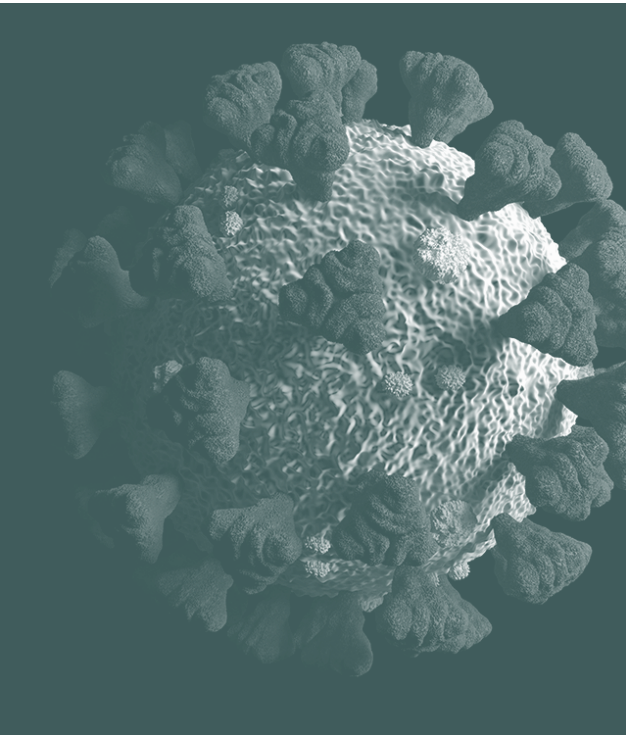
- Regelmessige risikovurderinger, kartlegge sårbarheter, iverksette tiltak
- Kartlegge verdier
- Sikkerhetsoppdateringer
- Fjerne passive og utdaterte systemer og komponenter
- Kompetansetiltak
- Overvåking og bruk av spesialisttjenester
- Planer for gjenoppretting av systemer og data, inkl tapte data
- Scenariobaserte beredskapsøvelser
- Planer for håndtering av forretningsvirksomheten ved avbrudd

Samarbeid innen sikkerhetsområdet

Samarbeid og informasjonsutveksling gir bedre risikoforståelse

- Samhandling gjennom NFCERT
- Samhandling gjennom BFI og rollen som SRM
- Rammeverket TIBER-NO
- Rammeverk for koordinering ved systemiske cyberhendelser i EU/EØS (EU-SCICF)
- Nytt EU-regelverk for operasjonell digital robusthet (DORA)

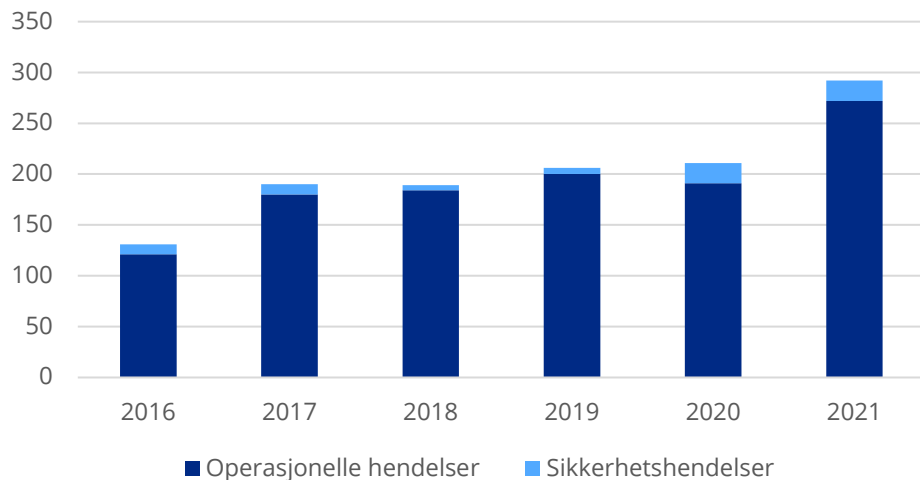
Koronapandemien og krigen i Ukraina



- Virksomheter som støtter viktige funksjoner
- Kritiske samfunnsfunksjoner, jf. DSB
 - Sikker formidling av kapital nasjonalt og til og fra utlandet
 - Gjennomføre betalinger og andre finansielle transaksjoner
 - Opprettholde tilgang til nødvendige betalingsmidler
- Særskilt oppfølging og ekstraordinære møter i BFI
- Gode beredskapsplaner
- Foretakene god kontroll på driftssituasjonen
- Iverksatt nødvendige tiltak
- Særskilte tema
 - Hjemmekontor
 - Endringer i det geopolitiske landskapet
 - Det digitale trusselbildet
 - Besluttede sanksjoner

Rapporterte hendelser

- Ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2021
- Høyere antall hendelser i 2021 enn i 2020, samt også tidligere år
 - antall sikkerhetshendelser på samme nivå som i 2020
 - antall operasjonelle hendelser vesentlig høyere i 2021 enn tidligere år
- Tilgjengeligheten til tjenestene anses imidlertid samlet sett bedre i 2021 enn tidligere år



	Operasjonelle hendelser rapportert	Sikkerhets hendelser rapportert
2016	121	10
2017	180	10
2018	184	5
2019	200	6
2020	191	20
2021	272	20

Kilde: Finanstilsynet

Hendelser og avdekkede sårbarheter i 2021



Alvorlige operasjonelle hendelser

- Driftshendelse i Danske Bank i oktober
- Kapasitetsproblemer ved bruk av BankID-appen og -kodebrikke fra slutten av november frem til jul
- Driftshendelse hos Verdipapirsentralen 1. februar
- Avvik knyttet til AML-systemer

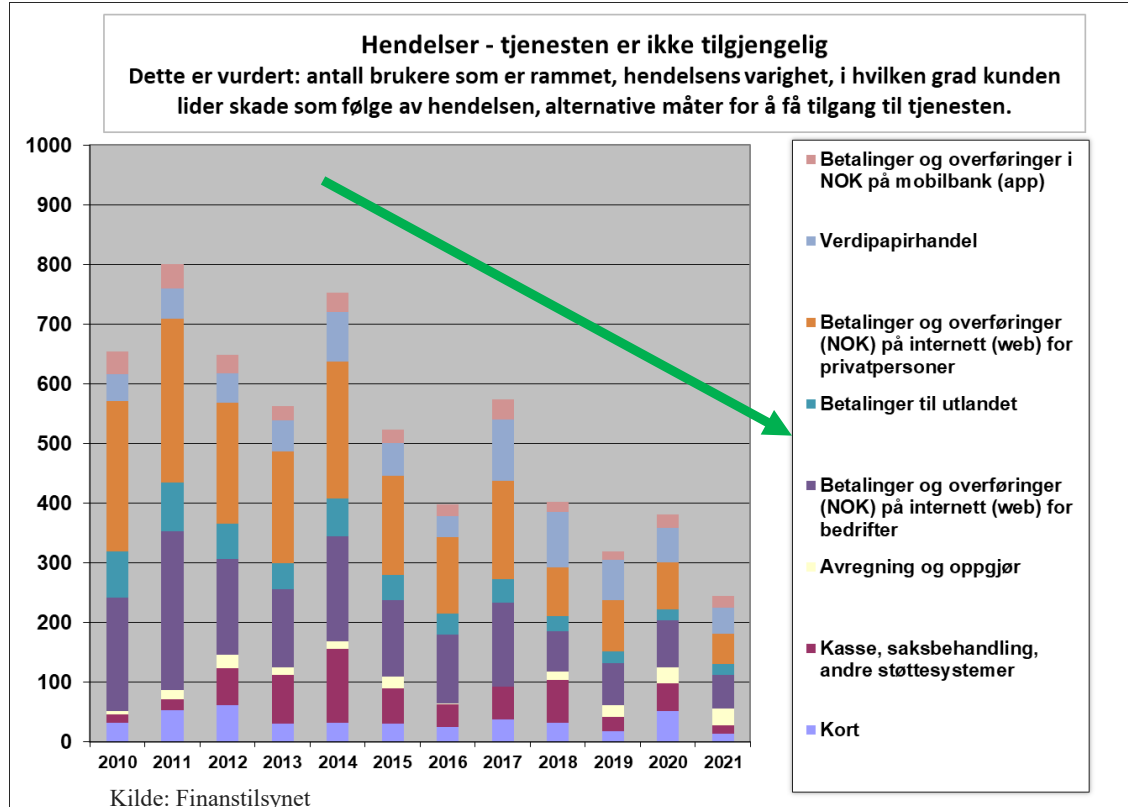


Sikkerhetshendelser og sårbarheter

- Log4j
- Virusangrep på e-post servere
- Ondsinnet kode i teksteditor
- DDoS
- Avdekkede sårbarheter
- Sikkerhetsbrudd, Ikke-tjenstlige oppslag

- Hendelser knyttet til kontotilbyderes grensesnitt

Hendelser – tilgjengelighet



All time high!

Tap ved svindel og angrep mot betalingstjenester

(tall i hele tusen)	2016	2017	2018	2019	2020	2021
TOTAL SVINDEL BETALINGSKORT	206 503	145 591	148 732	189 147	147 602	162 145
ANTALL KORT RAMMET AV MISSBRUK (H1 2019)	44 900	68 162	65 024	34 999		
ANTALL TRANSAKSJONEER MED MISSBRUK (H2 2019)				110 580	205 000	147 000
TOTAL SVINDEL NETTBANKER (H1 2019)	18 631	7 587	26 840	3 637		
TOTAL SVINDEL KONTOOVERFØRINGER (H2 2019)				301 000	355 000	346 000
TAP VED SOSIAL MANIPULERING (*)			298 000	500 000	295 000	240 600

*) SVINDEL
KORTBETALINGER
OG
KONTOBETALINGER
OMFATTER OGSÅ
TAP VED SOSIAL
MANIPULERING

(tall i prosent)	2020	2021
SVINDEL BETALINGSKORT AV TOTAL TRANSAKSJONSVERDI	0,016	0,020
SVINDEL BETALINGSKORT VED NETTHANDEL AV TOTAL TRANSAKSJONSVERDI	0,07	0,06
SVINDEL BETALINGSKORT AV TOTALT ANTALL TRANSAKSJONER	0,008	0,006
SVINDEL KONTOOVERFØRINGER AV TOTAL TRANSAKSJONSVERDI	0,00016	0,00097

Kilder: Finanstilsynet og Bits

Bankene forhindrer en stadig større andel av svindelforsøkene

Funn og observasjoner fra tilsynsvirksomheten

Svakheter og sårbarheter som utgjør risiko for at alvorlige hendelser kan inntreffe

Det er gjennom tilsynsvirksomheten blant annet pekt på

- Svakheter i foretaks arbeid med kontinuitets- og beredskapsplaner
- Mangler i dokumenteringen av IKT-infrastruktur
- Mangler knyttet til oppfølging av leverandører
 - Svakheter ved sikkerhetsarbeidet,
 - Kontroll med og oppfølging av tilganger
- Manglende retningslinjer for gjennomføring av sikkerhetstesting
- Ajourhold av dokumentasjon og nøkkelpersonrisiko
- Svakheter knyttet til testing og gjennomføring av IT-konvertering ved fusjoner

Det er også pekt på

- Bytte av driftsleverandør – håndtering av hendelser som rammer kritiske tjenester
- Mangler i dedikerte grensesnitt gir utfordringer for brukerne av disse

Nærmere omtale av utførte IKT-tilsyn finnes på Finanstilsynets nettsted

Utkontraktering av IKT-virksomhet

- "Alle" utkontrakterer
- Foretakets ansvar
- Over 170 meldinger om utkontraktering av IKT-virksomhet i 2021
 - Samarbeidende grupper
 - Konesjonsbehandling
- Flest meldinger knyttet til
 - Nets' salg av konto-til-konto-tjenester til Mastercard
 - Vipps' planlagte flytting av driften av BankID
- Felles betalingsinfrastruktur anses som IKT-utkontraktering
- Fortsatt økt bruk av skytjenester
- Flere plattformer, økt kompleksitet, mer sammensatt risikobilde
- Kvaliteten på arbeidet med utkontraktering synes fortsatt å øke
- Forankring av avtaler i egen ledelse bedre
- Nye foretak ikke like godt kjent med regelverket
- Nytt regelverk – Ny veiledning



Foretakenes vurdering av risiko

De mest fremtredende vurderingene:

- Økt trussel fra digital kriminalitet, flere angrepsflater, behov for tiltak
- Gode oversikter over virksomhetskritisk utstyr, programvare, forretningsfunksjoner, prosesser og informasjon, noe som er viktig for blant annet å ha kontroll med IKT- og sikkerhetsrisiko
- Tilstrekkelig innsikt i sikkerhetsarkitektur
- Rekruttering av informasjonssikkerhets-kompetanse og kompetanse for oppfølging av utkontraktert virksomhet
- Ny regulering som medfører behov for endringer i IKT-systemene
- Flerleverandørstrategi ved utkontraktering gir økt kompleksitet
- Egne ansatte med ansvar for kontinuitets- og kriseledelse og involvere forretningsområdene i BIA
- Oppfølging av tilgangsstyring for utkontrakterte IKT-tjenester, særlig ved utvidete tilgangsrettigheter
- Testsystemene samsvare med produksjonssystemene
- Klare skiller mellom første- og andrelinje i internkontrollen
- Konsekvensene av dårlig datakvalitet har blitt større
- Presisjonen knyttet til flagging av mistenkelige transaksjoner

Risiko knyttet til kundenes bruk av digitale tjenester

ID-løsninger

- "Slitasje" på ID-en
- Misbruk av ID-kjennetegn
- Sperre for kredittopplysninger

Betalingstjenester

- Sterk kundeautentisering
- Utfordringer anti-svindel analyse

Sikkerhet

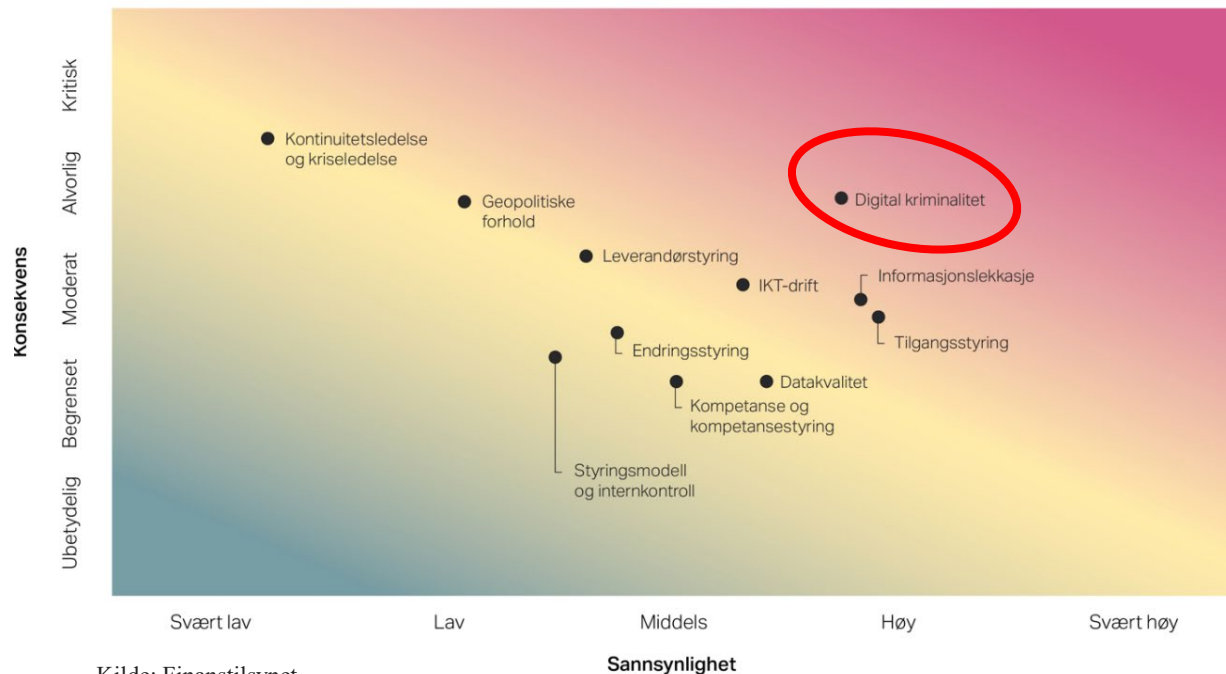
- Bruk av lenker

Prosjekt for å utarbeide og implementere tiltak for sikker bruk av digitale tjenester



Finanstilsynets oppsummerende vurdering av risikobildet - Foretakene

Risiko knyttet til sårbarheter i foretakenes IKT-virksomhet



Kilde: Finanstilsynet

De ulike risikoområdene er klassifisert etter sannsynlighet for at en uønsket hendelse oppstår og konsekvensene dersom hendelsen oppstår.

Hovedtema for tilsynsvirksomheten på IKT- og betalingstjenesteområdet fremover

- Styring og kontroll med IKT-virksomheten
- Organisering av IKT-/cyber-sikkerhetsarbeidet, sikkerheten knyttet til IKT-løsningene og at data ikke kommer uvedkommende i hende
- Trusselbildet knyttet til digital kriminalitet
- Beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet
- Oppfølging av IKT-hendelser og sårbarheter i IKT-løsningene
- Beredskapsarbeid og testing av kontinuitets- og kriseløsninger
- Styring, kontroll og oppfølging av utkontraktert IKT-virksomhet
- Større endringer i den finansielle infrastrukturen
- Betalingstjenester, herunder etterlevelse av PSD2
- Sikkerheten i betalingstjenestene og kunderettede løsninger
- IKT-løsninger for å avdekke hvitvasking og terrorfinansiering
- BFI vil følge opp beredskap og hendelser i den finansielle infrastrukturen

Oppsummering

- Den norske finansielle infrastrukturen er robust
- Tilgjengeligheten til tjenestene bedre en tidligere år
- Det digitale trusselbildet er økende og gis større oppmerksomhet
- Angreps-flatene har blitt flere og det er behov for ytterligere IKT-sikkerhetstiltak, kompetanseheving og økte IKT-sikkerhets ressurser
- Koronapandemien og krigen i Ukraina viste at de sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner og kan raskt iverksette nødvendige tiltak
- Samlede tap ved svindel på nivå med 2020, tap ved sosial manipulering lavere enn for 2020
- Svindel med sosial manipulering synes fortsatt å være en lukrativ metode for de kriminelle
- De fleste foretakene har inngått avtaler om utkontraktering av IKT-virksomhet. Økt bruk av skytjenester
- Kundenes bruk av digitale tjenester utsetter de for en rekke risikoer
- Det er gjennom tilsynsvirksomheten avdekket svakheter og sårbarheter som utgjør risiko
- Sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet anses som den mest sentrale risikoen knyttet til foretakenes bruk av IKT
- Foretakene bør fortsatt styrke arbeidet på IKT-området, både for å redusere sannsynligheten for avvik, håndtere avvik og for å forbedre IKT-sikkerheten
- Samarbeid og informasjonsutveksling innen sikkerhetsområdet gir bedre risikoforståelse



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY