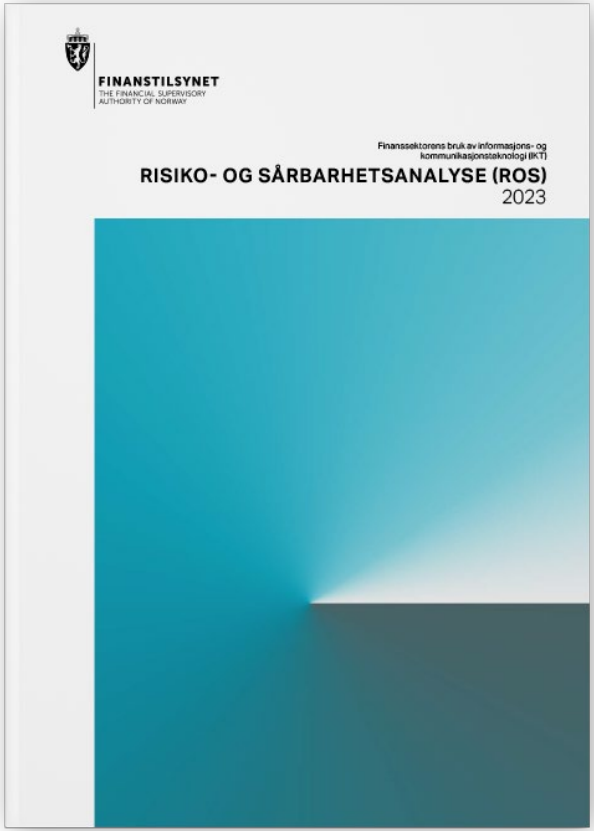
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2023

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Olav Johannessen, Seksjonssjef tilsyn IT og betalingstjenester, Pressebrief 9. mai 2023



- ✓ Viktigheten av robust finansiell infrastruktur
- ✓ Digitalt trusselbilde og kriminalitet
- ✓ Krigen i Ukraina – kritiske funksjoner
- ✓ IKT-hendelser og avdekkede sårbarheter
- ✓ Tilgjengelighet til tjenestene
- ✓ Svakheter og sårbarheter avdekket ved tilsyn
- ✓ Foretakenes vurderinger
- ✓ Utkontraktert IKT-virksomhet
- ✓ Tap ved svindel
- ✓ Misbruk av innloggingsinformasjon
- ✓ Samtaleroboter
- ✓ Digital robusthet
- ✓ Samarbeid innen sikkerhetsområdet
- ✓ Vurdering av risikobildet

Viktigheten av robust finansiell infrastruktur

Foto: Einar Aslaksen

- 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

- Trusselbildet i stadig endring
- Færre angrep på finansiell infrastruktur. Digital kriminalitet øker
- Organiserte kriminelle - fremmed etterretning
- Trusler
- Økt oppmerksomhet på
  - faren for systemiske cyberhendelser
  - viktigheten av digital robusthet og motstandsdyktighet
- Systemer for å avverge angrep stadig bedre

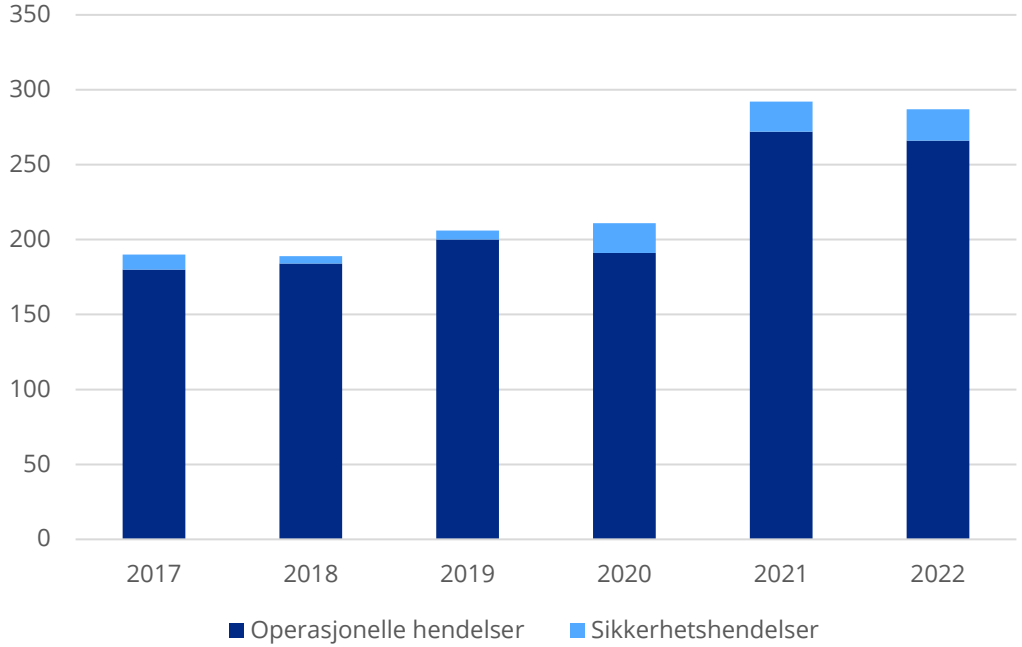
Foto: Colourbox

Krigen i Ukraina - Kritiske samfunnsfunksjoner

- 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
- Foretakene god kontroll på driftssituasjonen
- Iverksatt nødvendige tiltak
- Gode beredskapsplaner
- Særskilt oppfølging og ekstraordinære møter i BFI
- Aktuelle tema
  - Endringer i det geopolitiske landskapet
  - Det digitale trusselbildet
  - Besluttede sanksjoner

Ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2022

Foretakenes driftsstabilitet var tilfredsstillende og bedre enn tidligere år



Kilde: Finanstilsynet

IKT-hendelser og avdekkede sårbarheter i 2022

Alvorlige operasjonelle hendelser

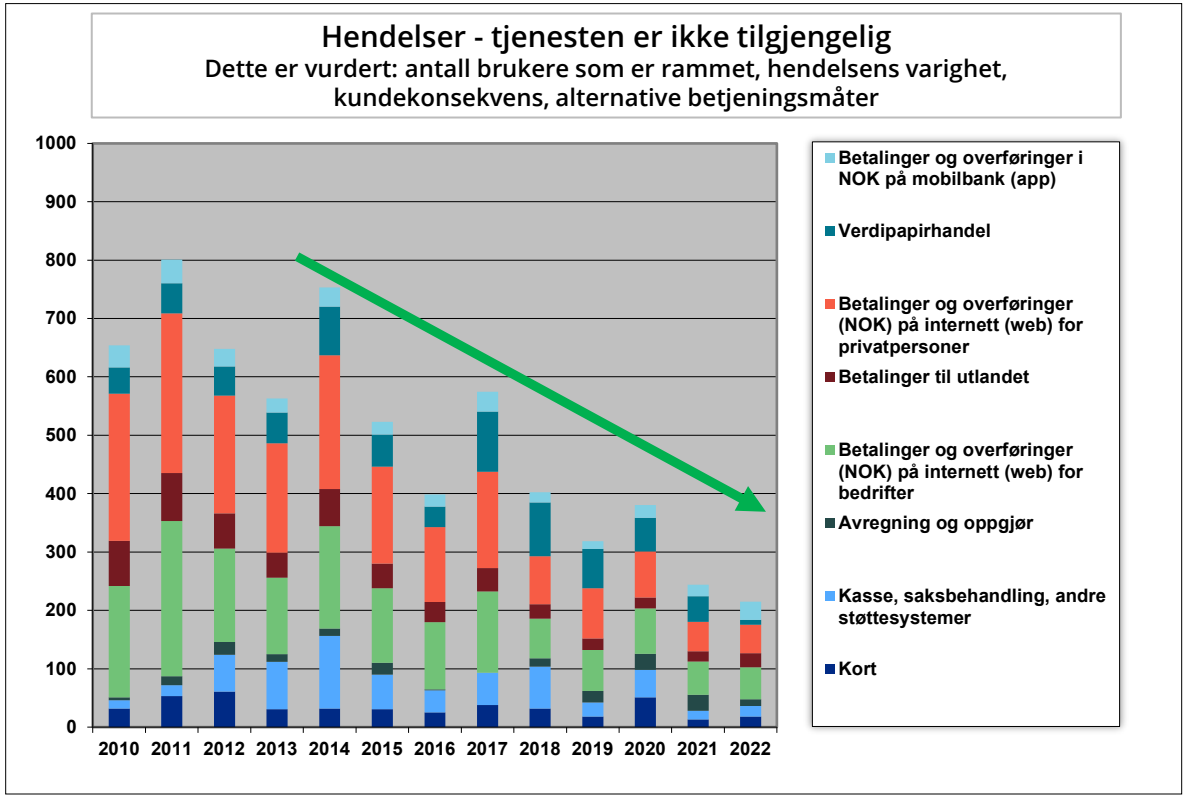
- Problemer med betaling med betalingskort i en rekke butikker 16. mai
- Uautorisert restart av verdipapiroppgjøret
- Feil medførte at aksjonærer ikke fikk deltatt på generalforsamling
- Feil i beregning av aksjeutbytte medførte for høyt utbetalt beløp
- Avvik knyttet til AML-systemer

Sikkerhetshendelser og sårbarheter

- Log4j
- Tjenestenektangrep
- Kompromittering av tofaktorautentisering
- Sikkerhetshendelser hos leverandør

- Hendelser knyttet til kontotilbyderes grensesnitt

IKT-hendelser – Tilgjengelighet til tjenestene



Kilde: Finanstilsynet

All time high!

Svakheter og sårbarheter avdekket ved tilsyn

- Arbeid med krisehåndterings- og beredskapsplaner
- Etterlevelse av gjeldende regelverk ved utkontraktering
- Oppfølging av leverandører, spesielt etterlevelse av krav til sikkerhet
- Involvering i leverandørens test av kriseløsninger
- IKT-kompetanse i andre forsvarslinje (etterlevelsesfunksjonen)
- Arbeid med datakvalitet
- Transaksjonsovervåking hvitvasking og terrorfinansiering
- Håndtering av sikkerhetsrelaterte kundeklager

Foretak og leverandørers vurdering av sentrale risiko- og sårbarhetsforhold knyttet til IKT-virksomheten

- Manglende oversikt kontroller i foretakets internkontroll
- Manglende kompetanse
- Mangler i sikkerhetsarbeidet
- Komplekse verdikjeder og knapphet på IKT-ressurser
- ID-tyverier
- Økt kompleksitet i systemporteføljen
- Høy utviklingstakt - risiko knyttet til endringshåndtering
- Mangler i beredskapsarbeidet
- Mangler i tilgangsstyring
- Mangler eller feil i data

Manglende tilgang på IKT-ressurser i kombinasjon med økt fare for angrep representerer etter Finanstilsynets vurdering en vesentlig risiko.

Utkontraktert IKT-virksomhet

Foto: Colourbox

- 240 meldinger om utkontraktering
- Økt bruk av skytjenester for både applikasjons- og infrastrukturtjenester
- Økning i antall plattformer å forholde seg til
- Ved utkontraktering
  - Vurdere risikoforhold
  - Sikre nødvendig kompetanse
  - Oppfølging inngå i foretakets system for risikostyring og internkontroll
- Utredelsesplaner (Exit-planer)

Enkelte avtaler oppfyller ikke IKT-forskriftens krav om rett til innsyn, revidering og tilsyn

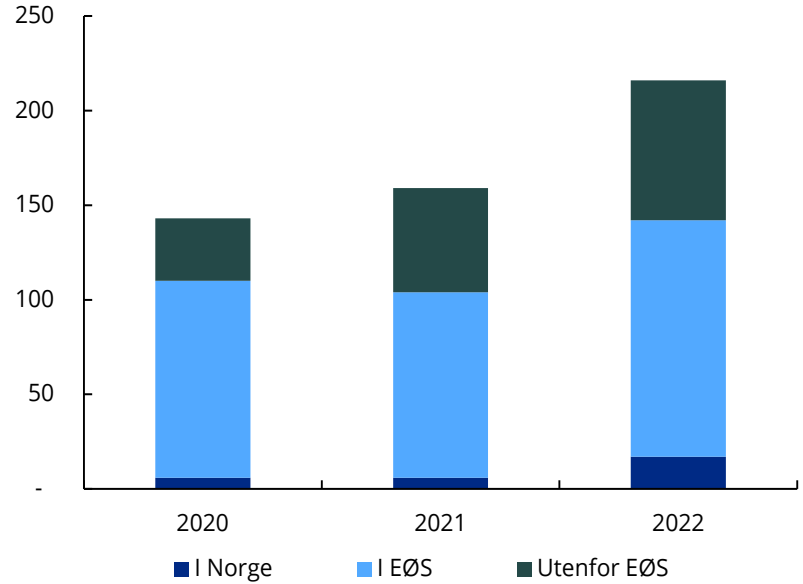
Tap ved svindel og angrep mot betalingstjenester

(beløp i mill. kroner)	2017	2018	2019	2020	2021	2022
TOTAL SVINDEL BETALINGSKORT	146,6	148,7	189,1	147,6	162,1	219,2
ANTALL KORT RAMMET AV MISBRUK (H1 2019)	68 162	65 024	34 999			
ANTALL TRANSAKSJONER MED MISBRUK (H2 2019)			110 580	205 000	147 000	156 402
TOTAL SVINDEL NETTBANKER (H1 2019)	7,6	28,4	3,6			
TOTAL SVINDEL KONTOBETALINGER (H2 2019)			301,0	355,5	346,5	394,9
SAMLEDE TAP				503,1	508,6	614,1

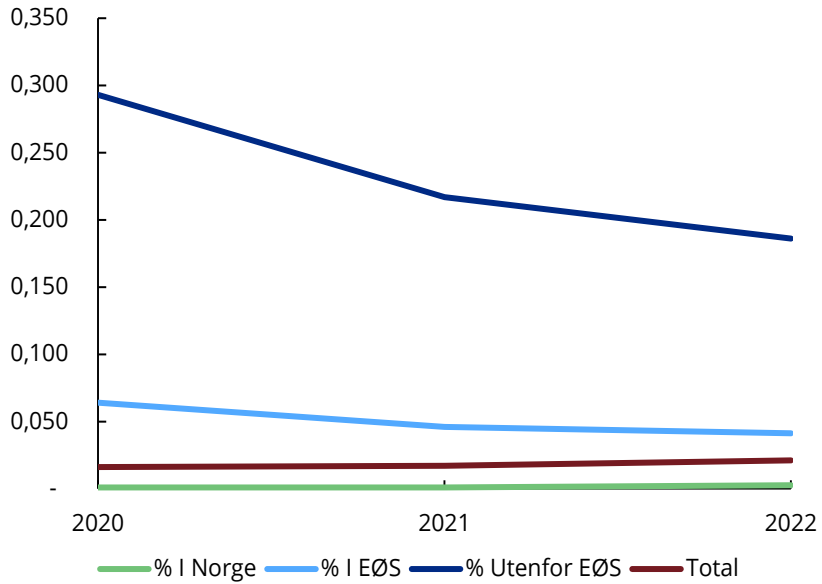
(tall i prosent)	2021	2022
SVINDEL BETALINGSKORT AV TOTAL TRANSAKSJONSVERDI	0,020	0,021
SVINDEL BETALINGKORT AV TOTALT ANTALL TRANSAKSJONER	0,006	0,006
SVINDEL KONTOBETALINGER AV TOTAL TRANSAKSJONSVERDI	0,00097	0,0009

Utviklingen i tap ved kortsvindelsvindel

Tap knyttet til kortbetalinger fordelt på geografi i mill. kroner



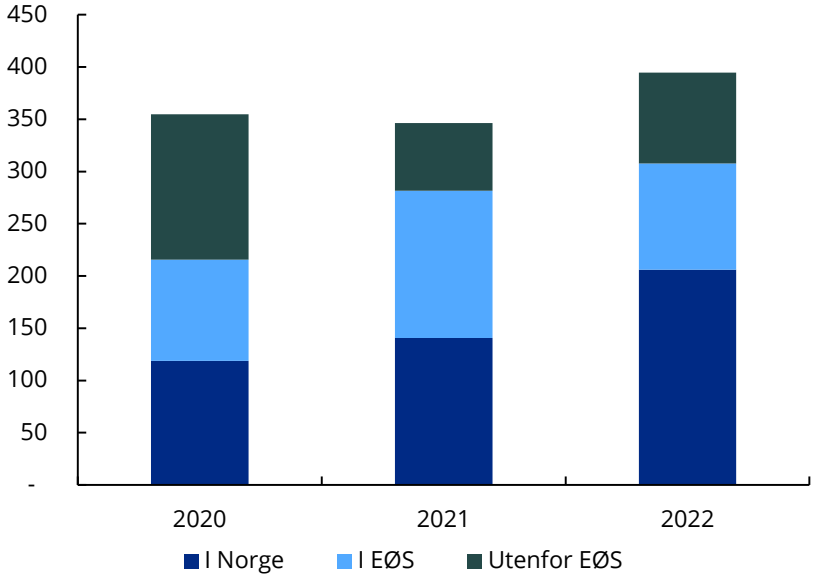
Tap i prosent av totale kortbetalinger fordelt på geografi



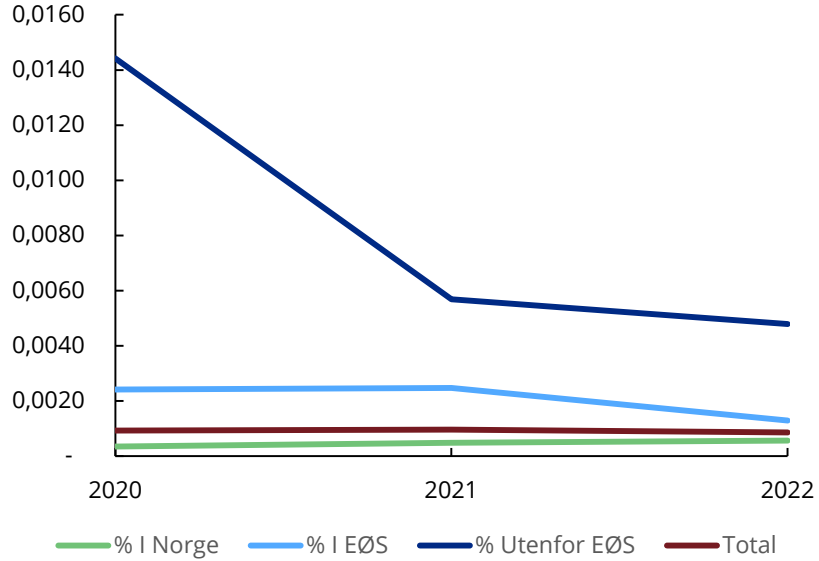
Kilde: Finanstilsynet

Utviklingen i tap ved svindel knyttet til kontooverføringer

Tap knyttet til kontooverføringer fordelt Fordelt på geografi i mill. kroner



Tap i prosent av totale kontooverføringer fordelt på geografi



Kilde: Finanstilsynet

Tap ved sosial manipulering

Sosial manipulering (beløp i mill. kroner)	2020	2021	2022
Svindleren manipulerer betaleren til en kortbetaling	9,2	16,6	21,5
Svindleren manipulerer betaleren til en kontooverføring	285,3	224,00	268,8
Totalt	294,5	240,6	290,3

Svindler utsteder betalingen (beløp i mill. kroner)	2021	2022
Svindel med betalingskort	145,2	202,1
– Hvorav svindel initiert gjennom fjernbetalingskanal (internetthandel)	136,0	180,6
– Hvorav svindel initiert via nærbetaling	9,2	21,5
Svindel med kontooverføringer	108,3	117,7

Misbruk av innloggingsinformasjon

Tyveri og misbruk av innloggingsinformasjon for finansielle tjenester

- BankID benyttes i stort omfang
- BankID-innloggingen ser forskjellig ut
- Krevende for brukerne å avgjøre om det er sikker nettsted
- Gir kriminelle bredt spekter av moduser i svindelvirksomheten

Misbruk av ansattes innloggingsinformasjon

- Tyveri av innloggingsdetaljer via en form for "man in the middel"-kriminalitet
- Elektronisk adgangsbevis, såkalt sesjonsobjekt
- Tilegner seg den ansattes rettigheter
- Kan benyttes til kriminelle handlinger

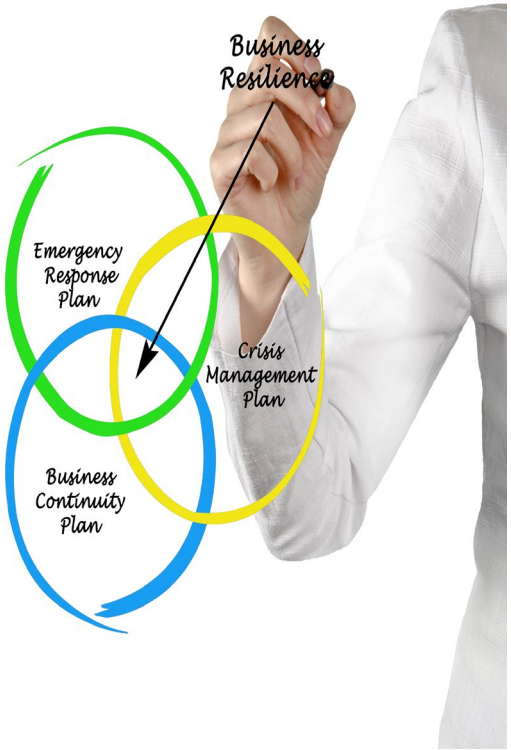
Foto: Colourbox

Samtaleroboter

- Integrert i vanlige arbeidsverktøy
- Ikke uten utfordringer eller risikoer
- Sensitiv personinformasjon
- Feilinformasjon eller misforstår spørsmål
- Svar man får, påvirkes av kildene til datasettene
- Bruk bør være basert på risikovurderinger

Foto: Colourbox

Digital robusthet



- Styrke arbeidet på IKT-området og bedre IKT-sikkerheten
- Tiltak i foretakene for å motvirke, avdekke, gjenopprette hendelser og håndtere konsekvenser
  - Regelmessige kartlegging av risiko og sårbarheter
  - Kartlegge verdier
  - Sikkerhetsoppdateringer
  - Fjerne passive og utdaterte systemer og komponenter
  - Kompetansetiltak
  - Overvåking og bruk av spesialisttjenester
  - Planer for gjenoppretting og håndtering av forretningsvirksomheten ved avbrudd
  - Scenariobaserte beredskapsøvelser og sikkerhetstesting (TLTP)
- Nasjonalt tiltak - TIBER-NO

Foto: Colourbox

Samarbeid innen sikkerhetsområdet

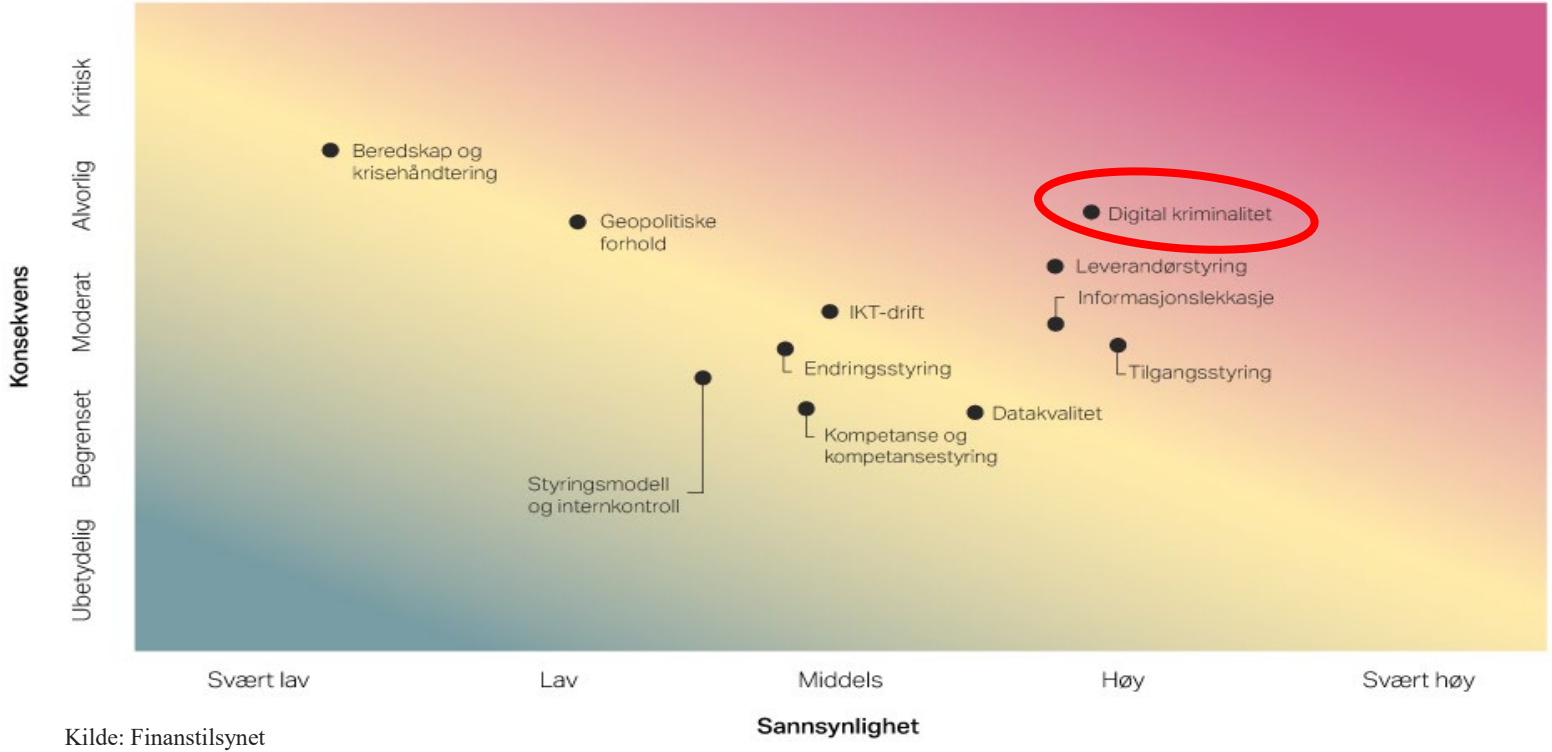
Foto: Colourbox

Samarbeid og informasjonsutveksling gir bedre risikoforståelse

- Nytt EU-regelverk for operasjonell digital robusthet (DORA)
- Rammeverk for koordinering ved systemiske cyberhendelser i EU/EØS (EU-SCICF)
- Nasjonal / Nordisk samhandling gjennom NFCERT
- Samhandling gjennom BFI og rollen som SRM
- Rammeverket TIBER-NO – Trusselbasert testing
- Veikart for cybersikkerhet i finansnæringen - Finans Norge

Finanstilsynets oppsummerende vurdering av risikobildet - Foretakene

Risiko knyttet til sårbarheter i foretakenes IKT-virksomhet



Kilde: Finanstilsynet

Den finansielle infrastrukturen er robust

+ Ingen IKT-hendelser i 2022 med konsekvenser for finansiell stabilitet
+ Tilfredsstillende driftsstabilitet
+ Tilgjengeligheten til tjenestene tilfredsstillende
+ Sentrale aktører kontroll på driftssituasjonen og iverksatte nødvendige tiltak raskt ifm. krigen i Ukraina
+ Beredskapen i betalingssystemet styrkes jevnlig
+ Arbeidet for å håndtere digital kriminalitet og operasjonell svikt

- Trusselbildet i stadig endring
- Digital kriminalitet mer kompleks, sammensatt og øker

Med bakgrunn i det digitale trusselbildet bør foretakene fortsatt styrke arbeidet på IKT-området for å opprettholde en robust finansiell infrastruktur ved å redusere sannsynligheten for operasjonelle hendelser, øke motstandsdyktigheten mot digital kriminalitet og bedre IKT-sikkerheten generelt.

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY