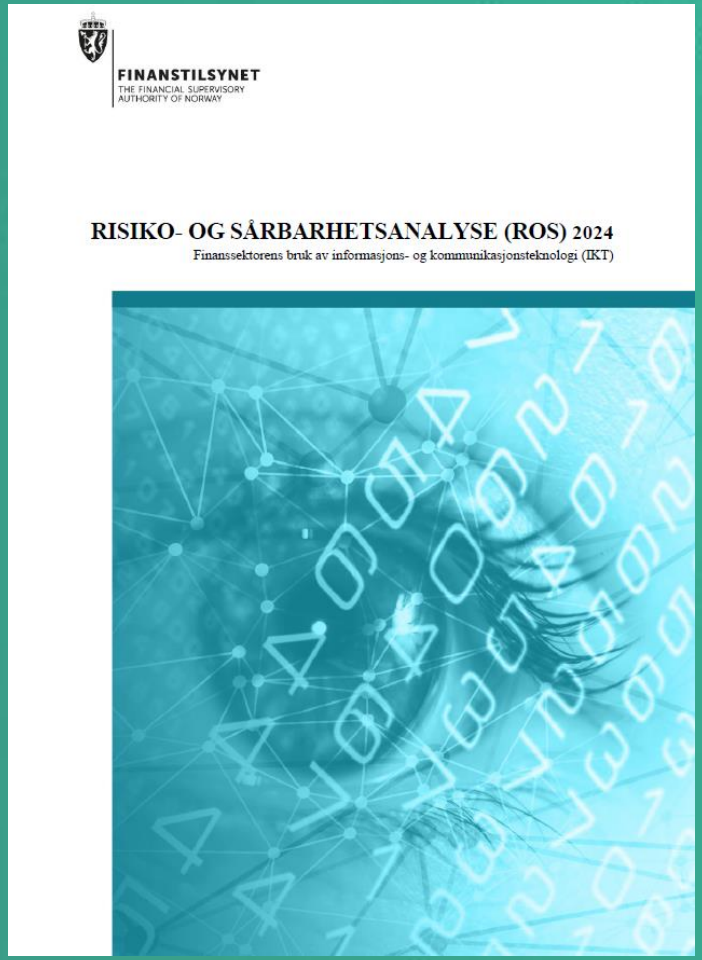
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2024

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Olav Johannessen, Seksjonssjef tilsyn IT og betalingstjenester, Pressebrief 7. mai 2024



- ✓ Digitalt trusselbilde og kriminalitet
- ✓ Viktigheten av robust finansiell infrastruktur
- ✓ Digital robusthet - tiltak
- ✓ Samarbeid innen sikkerhetsområdet
- ✓ IKT-hendelser og avdekkede sårbarheter
- ✓ Tilgjengelighet til tjenestene
- ✓ Mangler og sårbarheter avdekket ved tilsyn
- ✓ Utkontraktert IKT-virksomhet
- ✓ Foretakenes vurderinger av risikoområder
- ✓ Tap ved svindel
- ✓ Vurdering av risikobildet
- ✓ Oppsummering

Digital trusselbilde og kriminalitet

- Trusselbildet i endring – geopolitiske uro
- Trusselnivået høyt, men stabilt
- Færre angrep på finansiell infrastruktur – Digital kriminalitet øker
- Utvidet handlingsrom
- Uoversiktlige leverandørkjeder
- Trusler
- Økt oppmerksomhet på
  - faren for systemiske cyberhendelser
  - viktigheten av digital robusthet og motstandsdyktighet
- Systemer for å avverge angrep stadig bedre

Foto: Colourbox

Viktigheten av robust finansiell infrastruktur

- Finansiell stabilitet og velfungerende markeder
- Betalinger og transaksjoner i finansielle instrumenter
- Mange aktører og leverandører, sammensatt og kompleks
- Manglende robusthet
- Svikt kan gi samfunnsmessige konsekvenser
- Sensitiv informasjon

Foto: Einar Aslaksen

Digital robusthet – tiltak

Foto: Colourbox

- Ansvar for egne systemer, også ved utkontraktering
  - kartlegge egne risikoer, sårbarheter og verdier
  - iverksette forebyggende tiltak
  - håndtere angrep og følgeskader
  - bevisstgjøre ansatte
- Bruk av trusselvurderinger
- Tiltak for å motvirke angrep
- Sikkerhetstesting av egne systemer
- Gode beredskapsplaner og -øvelser
- Forsvar mot verdikjedeangrep
- Informasjons- og erfaringsdelingstjenester

Samarbeid innen sikkerhetsområdet

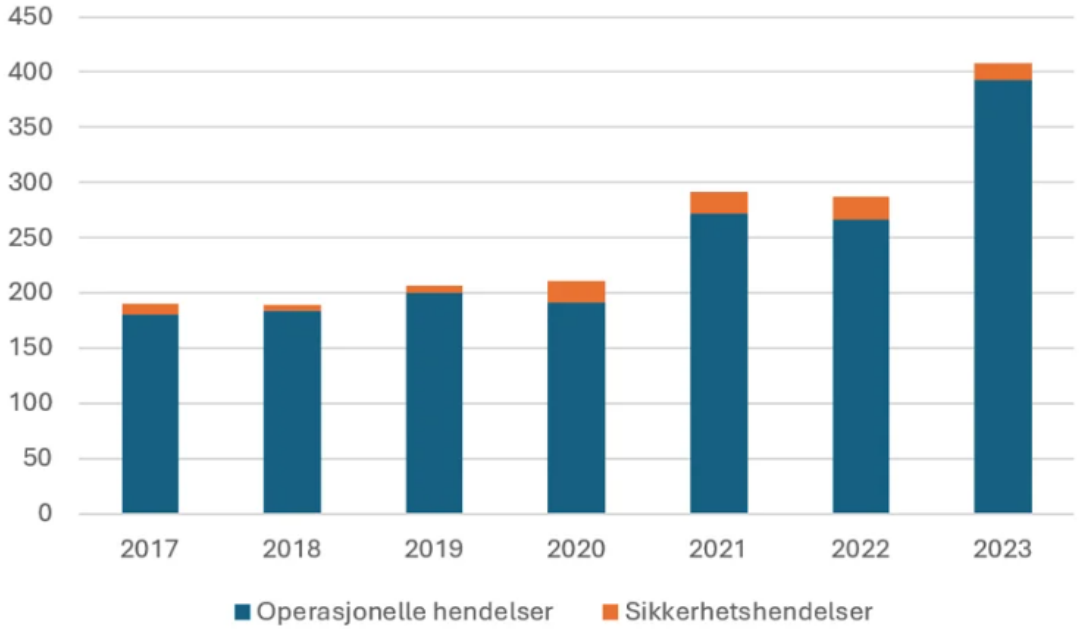
Risikoforståelsen og forsvarsevnen økes gjennom samarbeid og informasjonsutveksling

- Nytt EU-regelverk om digital operasjonell motstandsdyktighet (DORA)
- Rammeverk, koordinering systemiske cyberhendelser i EU/EØS (EU-SCICF)
- Samhandling BFI, rollen som SRM og nordiske/baltiske myndigheter
- Samhandling gjennom NFCERT – nasjonalt / nordisk
- Trusselbasert testing – TIBER-NO
- Etablering av rammeverk for vurdering av systemisk IKT-risiko
- Veikart for cybersikkerhet i finansnæringen – Finans Norge

Foto: Colourbox

Den finansielle infrastrukturen anses som robust
Ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2023

Driftsstabiliteten var tilfredsstillende og på nivå med de to foregående årene



Kilde: Finanstilsynet

IKT-hendelser og avdekkede sårbarheter i 2023

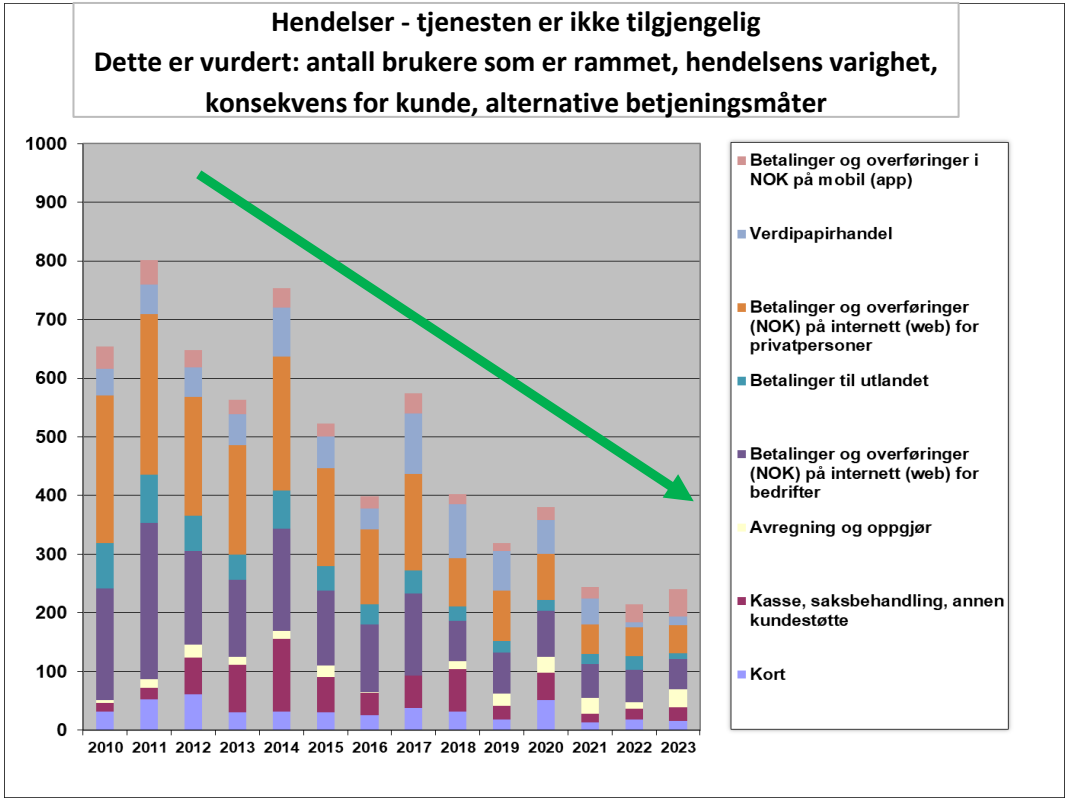
Alvorlige operasjonelle hendelser

- Feil på saldo grunnet dupliserte eller manglende transaksjoner
  - Korrekt saldo først gjenopprettet flere dager senere
  - Flest straksbetalinger, noe kortbetalinger
- Feil i løsninger etter planlagte endringer gjennomført av leverandør
- Avvik knyttet til AML-systemer

Sikkerhetshendelser og sårbarheter

- Sårbarheter i programvare utnyttet
- Tjenestenektangrep
- Kompromittering av e-post-kontoer
- Utnyttelse av sikkerhetshull

IKT-hendelser – Tilgjengelighet til tjenestene



Kilde: Finanstilsynet

Mangler og sårbarheter avdekket ved tilsyn

- Styring og kontroll med IKT-virksomheten
- Oppfølging av IKT-risiko i andre forsvarslinje
- Ressursbruk og fagkompetanse foretakets forsvarslinjer
- Leverandøroppfølgingen
- Kriseberedskapen
- Tilgangsstyring og oppfølging av logger
- Konfigurasjonsdatabasen (CMDB)

Utkontraktert IKT-virksomhet

- Betydelig del av IKT-risikoen
- Fortsatt økt bruk av skytjenester for både applikasjons- og infrastrukturtjenester
- Flere IKT-tjenesteleverandører, datasentre og plattformer
- Økt kompleksitet, mer sammensatt risikobilde, krevende oppfølging
- Store tjenesteleverandører kan bidra til å redusere risiko
- Konsentrasjonsrisiko
- Foretaket har ansvaret ved utkontraktering
- Observasjoner fra tilsynsvirksomheten
- Oppfølging av utkontraktert IKT-virksomhet

Foto: Colourbox

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

- Komplekse leverandørkjeder vanskeliggjør god leverandøroppfølging
- Aksept fra underleverandører strategier og retningslinjer
- Risiko knyttet til utkontraktering, særlig utenfor EØS
- Beholde kompetanse, nøkkelpersonrisiko
- Innsidetrussel
- Phishing og ransomware, svindel og ID-tyveri
- Cyberangrep, geopolitisk forhold
- Regulatoriske krav som medfører systemendringer
- Planer, prosesser og prosedyrer for kontinuitet og reetablering

Tap ved svindel og angrep mot betalingstjenester

- etter betalingstype

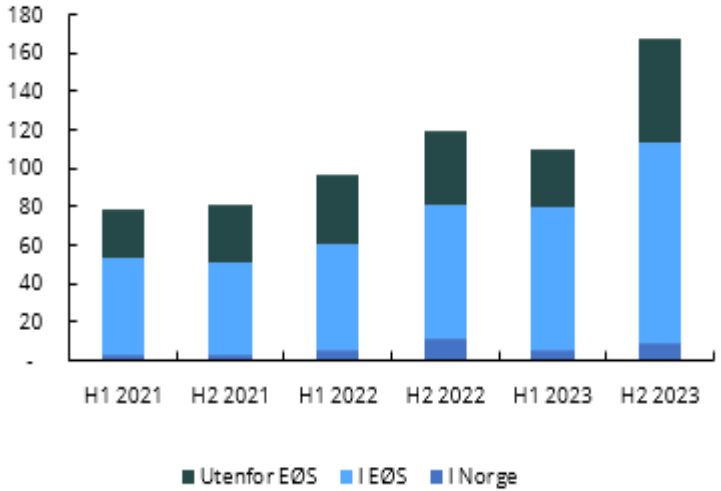
Beløp i mill. kroner	Svindeltransaksjoner - kontooverføringer (nettbank m.m.)	Svindeltransaksjoner med betalingskort rapportert av kortutsteder	Samlede tap
2023	647	281	928
2022	395	219	614
2021	347	162	508

(tall i prosent)	2022	2023
Svindel i prosent av total transaksjonsverdi	0,0013	0,0014

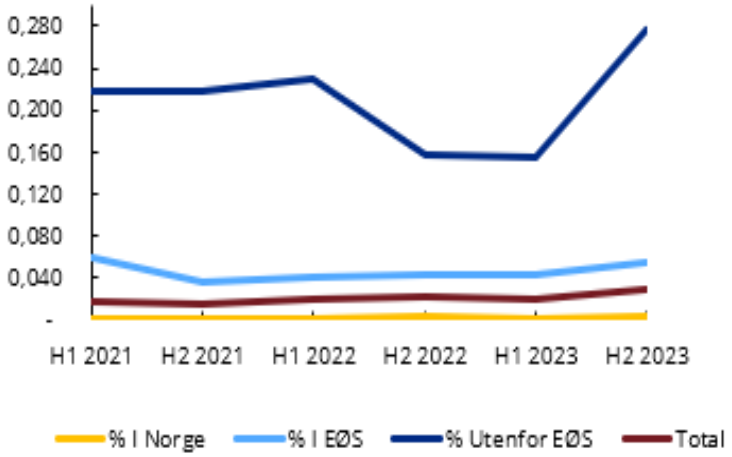
Kilde: Finanstilsynet

Utviklingen i tap ved kortsvindelsvindel

Tap knyttet til kortbetalinger fordelt på geografi i mill. kroner



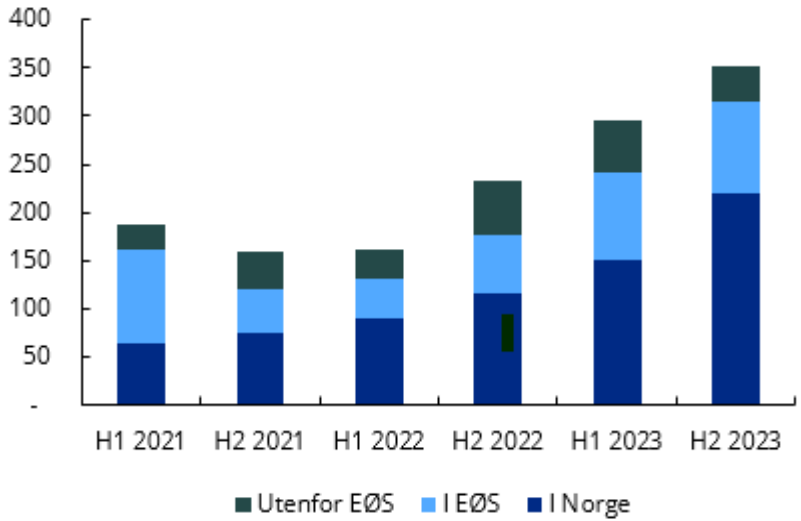
Tap i prosent av totale kortbetalinger fordelt på geografi



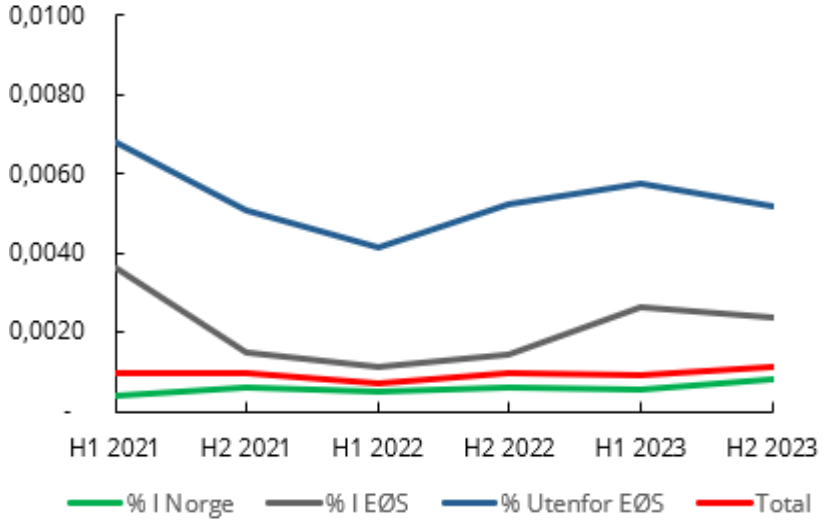
Kilde: Finanstilsynet

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 svindel og angrep mot betalingstjenester

- Hvem som har initiert svindelen

Svindleren manipulerer betaleren til å initiere en transaksjon - Sosial manipulering

Tabell 1

Sosial manipulering (beløp i mill. kroner)	2022	2023
Svindleren manipulerer betaleren til en kortbetaling	21,5	26,2
Svindleren manipulerer betaleren til en kontooverføring	268,8	442,2
Totalt	**290,3**	**468,4**

Kilde: Finanstilsynet

Svindleren initierer eller modifiserer betalingen

Tabell 2

Svindler initierer eller modifiserer betalingen (beløp i mill. kroner)	2022	2023
Betalingskort	197,7	252,8
Kontooverføringer	125,9	205,3
Totalt	**323,6**	**458,0**

Kilde: Finanstilsynet

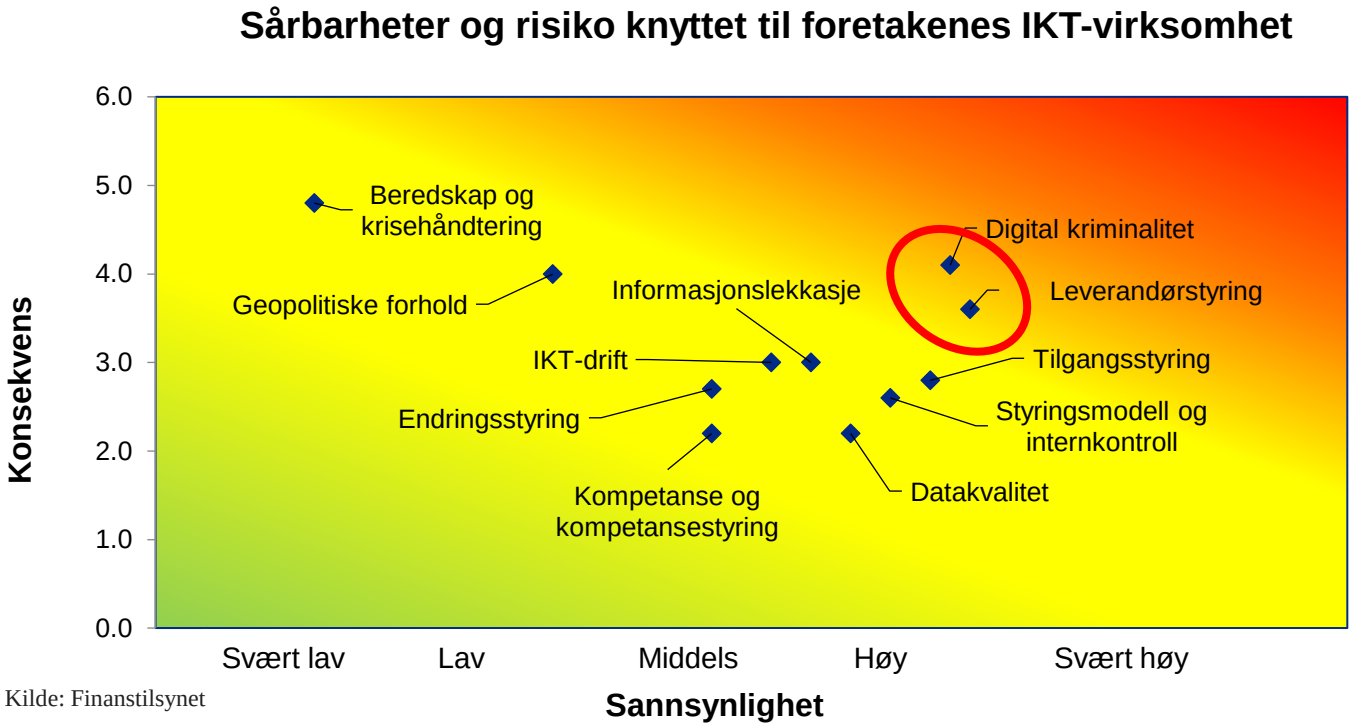
For 2023 kommer svindel ved kontantuttak på 2 mill. i tillegg

Stadig større andel av svindelforsøkene avverges

Betalingstype	Antall transaksjoner	Beløp
Betalingskort	1 082 792	1 303
Kontooverføringer	21 850	768
Totalt	**1 104 642**	**2 072**

Kilde: Finanstilsynet

Finanstilsynets oppsummerende vurdering av risikobildet - foretakene



Kilde: Finanstilsynet

Oppsummert
Den finansielle infrastrukturen anses robust

+ Ingen IKT-hendelser i 2023 med konsekvenser for finansiell stabilitet
+ Tilfredsstillende driftsstabilitet
+ Tilgjengeligheten til tjenestene var tilfredsstillende
+ Beredskapen i betalingssystemet styrkes jevnlig
+ Foretakene følger det digitale trusselbildet tett og iverksetter tiltak
+ Kontinuerlig arbeid 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 er det viktig at foretakene har gode trusselvurderinger, konsekvensanalyser og beredskapsplaner for sine systemer. De bør sikre at det gjennomføres sikkerhetstesting av foretakets systemer og at det etableres tilstrekkelige tiltak for å kunne håndtere angrep, herunder angrep mot sine leverandører.

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY