FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2025

og

DORA

Olav Johannessen

Seksjonsleder, IT og betalingstjenester, 4. juni 2025

Risiko- og sårbarhetsanalyse (ROS) 2025

- ✓ Overordnet vurdering
- ✓ Driftsstabilitet
- ✓ IKT-hendelser og avdekkede sårbarheter
- ✓ Tilgjengelighet til tjenestene
- ✓ Trusselbildet
- ✓ Digital robusthet
- ✓ Beredskap
- ✓ Mangler og sårbarheter avdekket ved tilsyn
- ✓ Foretakenes vurderinger av risikoområder
- ✓ Tap ved svindel
- ✓ Vurdering av risikobildet
- ✓ Oppsummering

	Det digitale trusselbildet er høyt og påvirkes av geopolitiske endringer
	Den finansielle infrastrukturen i Norge er robust, sikker og effektiv
	God beredskap er avgjørende for å håndtere alvorlige hendelser
	Samlede tap ved svindel fortsetter å øke
	De mest sentrale sårbarhetene i finanssektoren er knyttet til foretakenes forsvarsverk mot digital kriminialitet, styringsmodell for IKT-virksomheten og mangelfull leverandørstyring

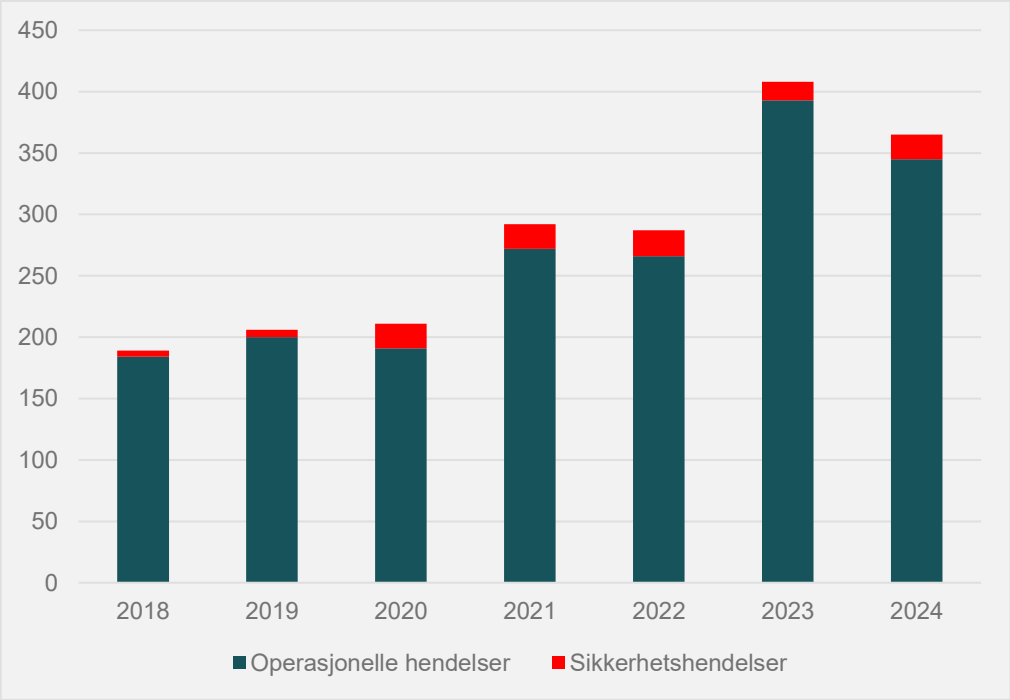
Driftsstabiliteten var tilfredsstillende og på nivå med de tre foregående årene - ingen kritiske hendelser i 2024

Alvorlige operasjonelle hendelser

- Feil på saldo grunnet dupliserte eller manglende transaksjoner
- Avvik knyttet til AML-systemer
- Feil i løsninger gjennomført av leverandør

Sikkerhetshendelser og sårbarheter

- Sårbarheter i programvare utnyttet
- Tjenestenektangrep
- Adversary-in-the-Middle angrep



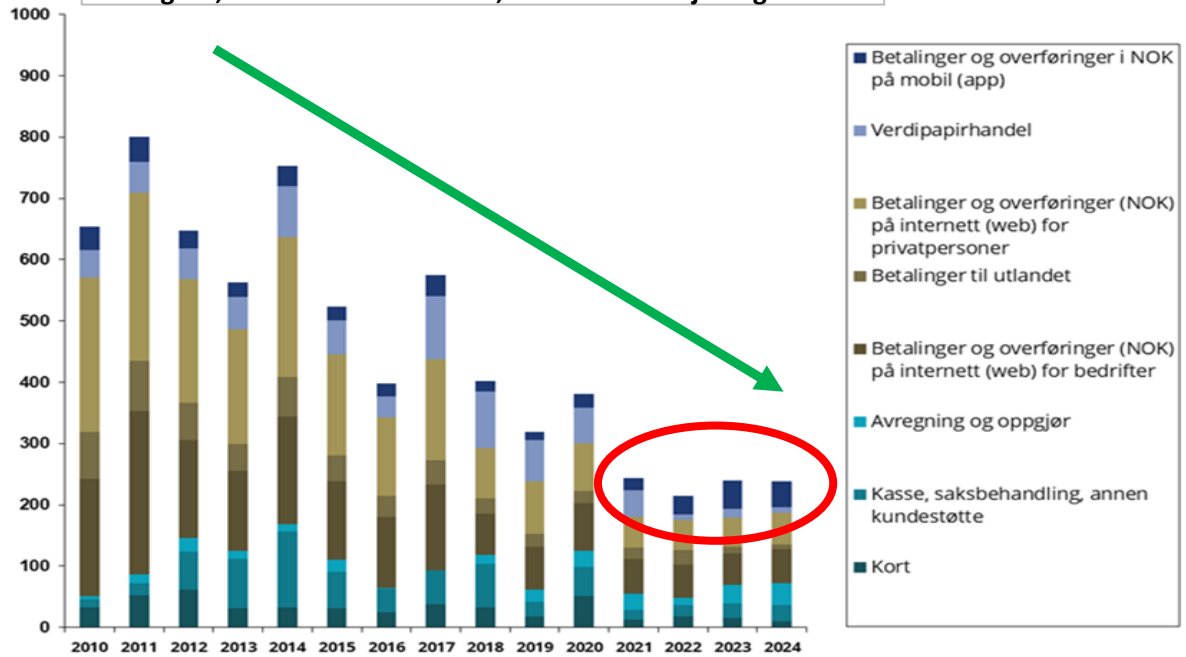
Doble trekk av eFaktura- og Avtalegiro-betalinger

- Oppsto 21. mai ifm. feil i driftskalender ved ekstra helligdager
- Feil saldo på kunders konti, både på avsender- og mottakersiden
- Flere dager før alle dupliserte transaksjoner var reversert
- Fulgt opp overfor bankene og andre relevante aktører
- Manglende kontroll/kvalitetssikring av driftskalendere
- Manglende risikovurdering av reverserings-/korrigeringsrutinen
- Korrigering av OCR/KID-transaksjoner utfordrende

Finanstilsynet forventer at alle aktørene i verdikjeden har tilstrekkelig oversikt og iverksetter tiltak for å hindre at en lignende hendelse med tilsvarende konsekvenser oppstår og for å styrke prosessen for korrigering/gjenoppretting. Det vil kreve samhandling på tvers av verdikjeden.

IKT-hendelser – Tilgjengelighet i tjenestene

Hendelser - tjenesten er ikke tilgjengelig
Dette er vurdert: antall brukere som er rammet, hendelsens varighet, konsekvens for kunde, alternative betjeningsmåter



Kilde: Finanstilsynet

Trusselbildet

Foto: Colourbox

- Trusselbildet i endring – geopolitisk uro påvirker
- Det digitale trusselnivået er høyt, endres kontinuerlig
- Færre angrep på finansiell infrastruktur
- Digital kriminalitet i form av svindel øker
- Systemer for å avverge angrep blir stadig bedre
- Utvidet handlingsrom
- Trusler
  - Uoversiktlige leverandørkjeder
  - Innsidetrussel
  - Svindel
  - Cyberangrep

Digital robusthet – Tiltak for å styrke motstandsdyktigheten

- Ansvaret til styret og ledelsen
- Forståelse av risikobildet
- Tiltak for å styrke forsvaret mot IKT-trusler

- Samarbeid og informasjonsutveksling

Foto: Colourbox

Beredskap

- Beredskapen er god
- Forutsetning for robust finansiell infrastruktur
- Må kontinuerlig utvikles
  - Det enkelte foretak og samarbeid i næringen
  - Samarbeid med myndighetene
- Trusselbildet krever tiltak som møter tidligere utenkelige scenarioer
- Konsekvensanalyser (BIA) til grunn for beredskapsplaner
- Gjenoppretting
- Øvelser basert på virkelighetsnære scenarioer
- Tiltak for å styrke beredskapen i betalingssystemet
- Kraftforsyning og elektronisk kommunikasjon
- Egenberedskap

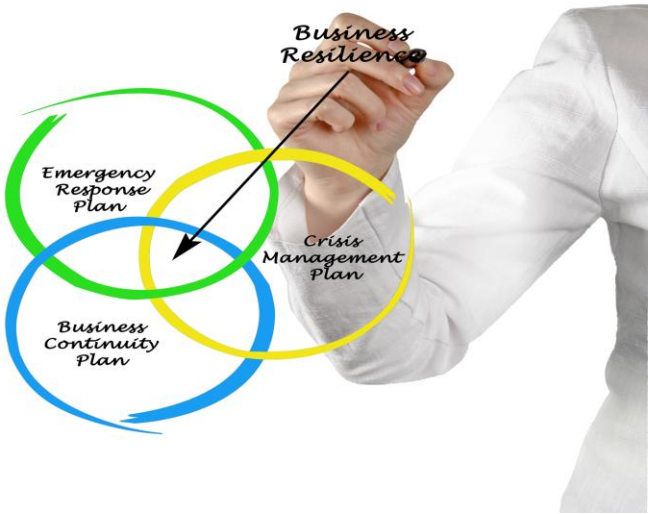


Foto: Colourbox

Mangler og sårbarheter avdekket ved tilsyn

- Utkontraktering av IKT-virksomhet
- Beredskap
- Rapportering av IKT-risiko og etterlevelse av styrende dokumenter
- IKT-drift

Finanstilsynet forventer at alle endringstyper inngår i foretakets prosesser for endringshåndtering, og at prosessene inkluderer en vurdering av behovet for å oppdatere beredskapsplaner

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

- Områder som framheves
  - Svindel
  - Cyberangrep og andre ondsinnede angrep
  - Geopolitiske endringer
  - Behov for endringer som følge av nye regelverk
  - Leverandørstyring, lengre og mer komplekse leverandørkjeder
  - Interne misligheter
  - Antihvitvasking og –terrorfinansiering
  - Virksomhetsstyring
  - Kompetanse og kompetansestyring
  - Beredskap og krisehåndtering

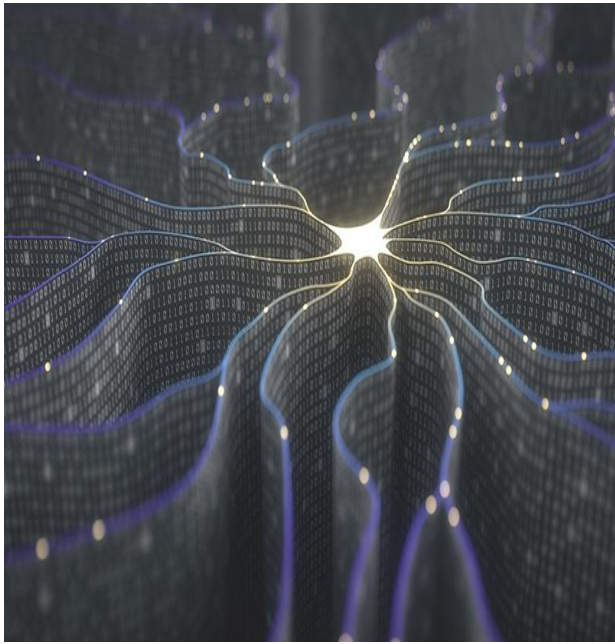
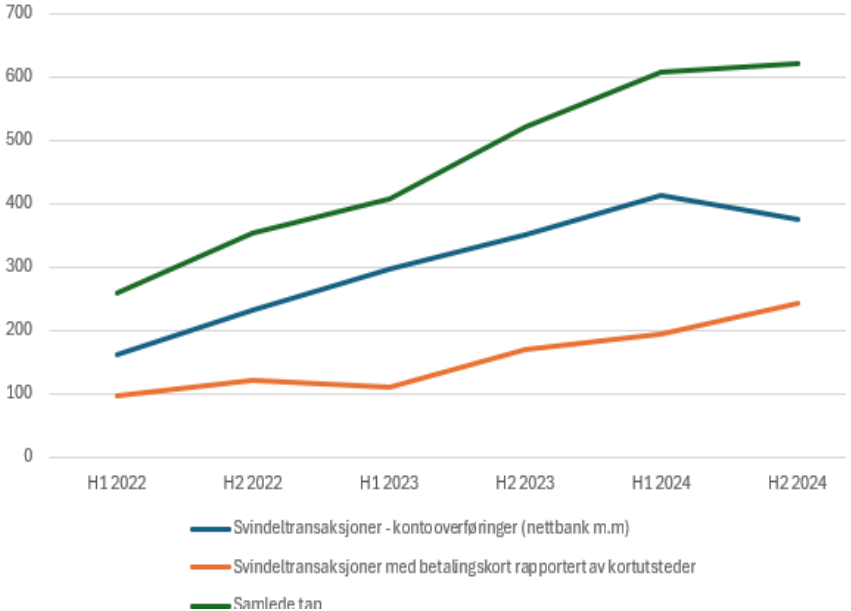


Foto: Colourbox

Tap ved svindel og angrep mot betalingstjenester

Etter betalingstype



Kilde: Finanstilsynet

År	Konto-overføringer	Betalings-kort	Samlede tap	Tap som andel
2024	790	437	1227	0,0020 %
2023	648	281	929	0,0014 %
2022	395	219	614	0,0013 %
2021	346	162	508	0,0014 %

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	2024
Svindleren manipulerer betaler til en kortbetaling	21,5	26,2	94,4
Svindleren manipulerer betaler til en kontooverføring	268,8	442,2	572,6
Totalt	290,3	468,4	667,0

Kilde: Finanstilsynet

Svindleren initierer eller modifiserer betalingen

Tabell 2

Svindleren initierer eller modifiserer betalingen (tall i mill. kroner)	2022	2023	2024
Betalingskort	197,7	252,8	335,1
Kontooverføringer	125,9	205,3	217,0
Totalt	323,6	458,1	552,1

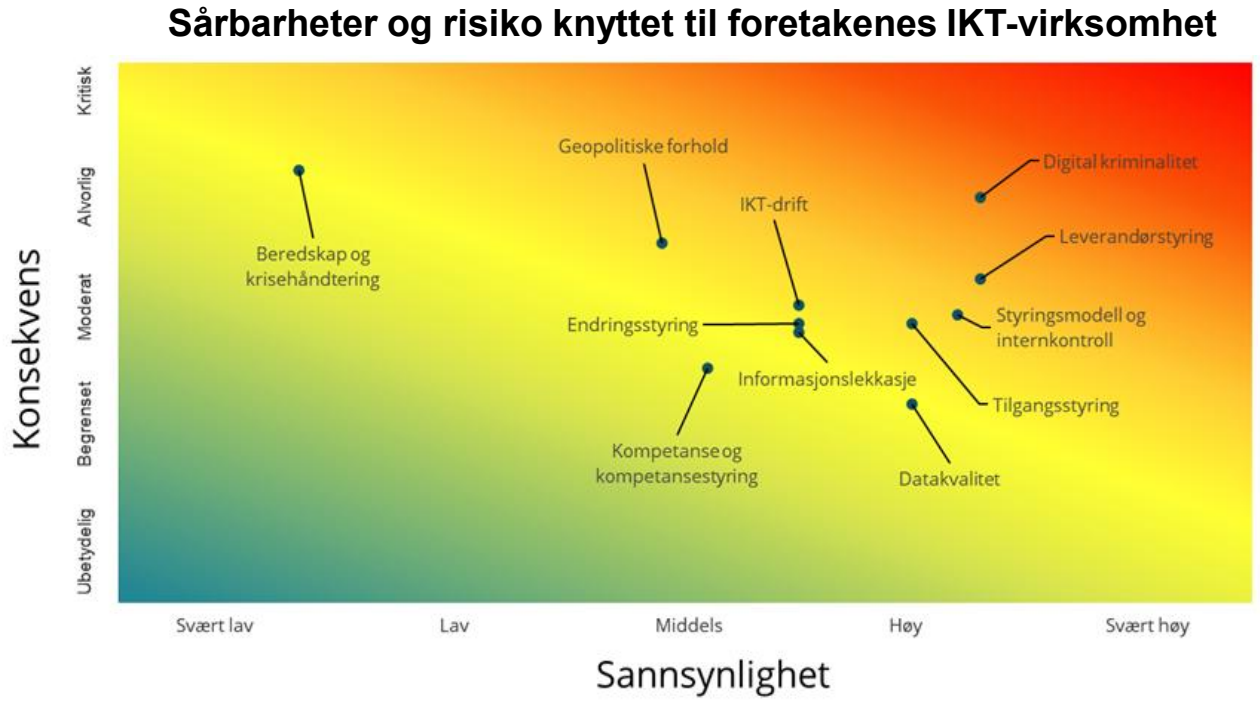
Kilde: Finanstilsynet

Stadig større andel av svindelforsøkene avverges

Betalingstype	Antall transaksjoner		Beløp i mill. kroner	
	2023	2024	2023	2024
Betalingskort	1 082 792	1 759 314	1 303	2 074
Kontooverføringer	21 850	19 273	768	891
Totalt	1 104 642	1 778 587	2 072	2 964

Kilde: Finanstilsynet

Finanstilsynets oppsummerende vurdering av risikobildet - foretakene



Kilde: Finanstilsynet

Viktig arbeid hos foretakene

Trusselvurderinger

Konsekvensanalyser

Beredskapsplaner

Testing

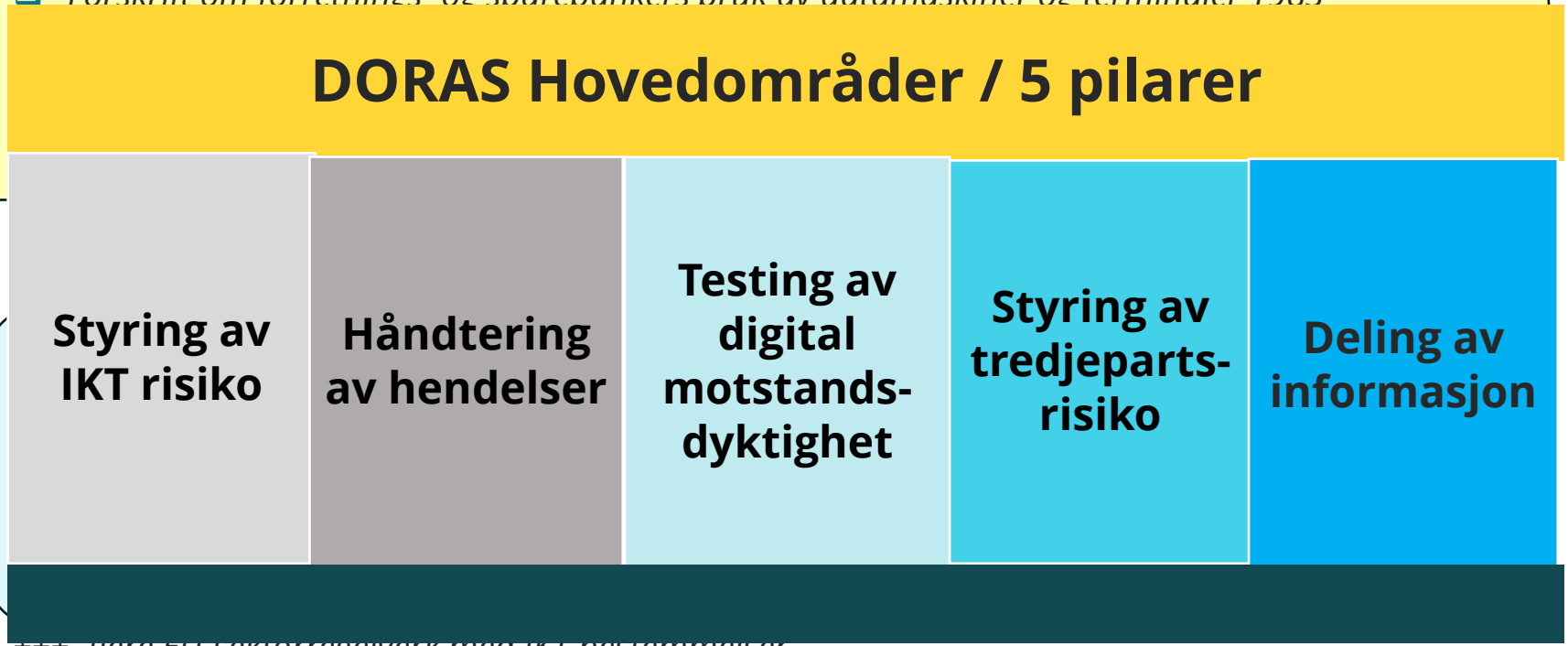
Tilstrekkelige tiltak

Lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

1. juli 2025

Fra forskrift om forretnings- og sparebankers bruk av datamaskiner og terminaler til DORA

- *Forskrift om forretnings- og sparebankers bruk av datamaskiner og terminaler 1983*



+++ *flere EU-sektorregelverk med IKT-bestemmelser*

DORA

- Sentrale aktiviteter
  - Styret og ledelsens ansvar
  - Virksomhetsanalyser
- Nivå 2 regelverk – forskrifter
- Fra IKT-utkontraktering til IKT-tjenesteavtaler
  - Avtalene i samsvar med DORA
  - Melding av kritiske eller viktige avtaler
  - Rapportering av register (RoI)
- Hendelsesrapportering
- Forenkling for grupper/allianser
- Informasjon, nettsider, Q&A, DORAQ&A@finanstilsynet.no for DORA-henvendelser, webinarer
- Tilsyn

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY