FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2026

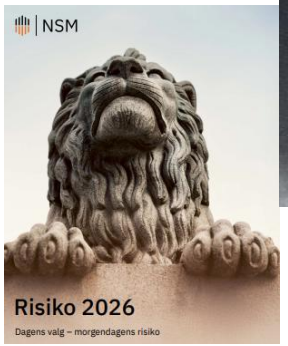
Knut Haugan, Avdelingsdirektør Risikoovervåking og makrotilsyn
Wenche Fagereng, Seksjonsleder IT og Betalingstjenester
10. juni 2026

Trusselbildet

- Den finansielle infrastrukturen i Norge vurderes samlet sett som robust og sikker

- Det digitale trusselnivået vurderes som høyt og i kontinuerlig utvikling
  - organiserte kriminelle og statlige aktører
  - komplekse leverandørkjeder og høy konsentrasjon
  - teknologisk utvikling
  - innsidere og sosial manipulasjon av ansatte

- Operasjonell teknologi, kvanteteknologi og skygge-IT



Avansert kunstig intelligens

- Frontier AI Models (FAIM)
  - Claude Mythos fra Anthropic
  - GPT 5.5-Cyber fra OpenAI
- KI benyttes i digitale angrep og til å avdekke sårbarheter
- Utfordrer etablerte sikkerhets- og sårbarhetsstyringsmodeller
- Konsentrasjonsrisiko og leverandøravhengighet

Beredskap i det finansielle systemet

- Beredskapen i finansnæringen er samlet sett er god, men behov for kontinuerlig utvikling

- DORA styrker digitale motstandskraften i finanssektoren
  - styring og kontroll av IKT-virksomheten
  - sikre kontinuitet i kritiske og viktige funksjoner
  - testing av motstandsdyktighet til egne systemer

    → 10 foretak er utpekt til trusselbasert penetrasjonstesting (TLPT)
  - planer og løsninger for å håndtere relevante scenarioer

- Styrket samarbeid, nasjonalt og europeisk

- Oppfølging av tiltak fra arbeidsgruppen for beredskap i betalingssystemet

Beredskap i det finansielle systemet

- Beredskapen i finansnæringen er samlet sett er god, men behov for kontinuerlig utvikling
- DORA styrker digitale motstandskraften i finanssektoren
  - styring og kontroll av IKT-virksomheten
  - sikre kontinuitet i kritiske og viktige funksjoner
  - testing av motstandsdyktighet til egne systemer

    → 10 foretak er utpekt til trusselbasert penetrasjonstesting (TLPT)
  - planer og løsninger for å håndtere relevante scenarioer
- Styrket samarbeid, nasjonalt og europeisk
- Oppfølging av tiltak fra arbeidsgruppen for beredskap i betalingssystemet

DORA scenarioer (ikke uttømmende):

- Cyberangrep
- Klimaendringer og naturkatastrofer
- Pandemier
- Fysiske angrep inkl. terrorangrep
- Innsidere og utro tjenere
- Kvaliteten på leveringen av en kritisk eller viktig funksjon forverres
- Svikt i kontorlokaler og datasentre
- Svikt i IKT-ressurser eller i ekom-infrastrukturen
- Manglende tilgjengelighet av ansatte og/eller medarbeidere med ansvar driftskontinuitet
- Politisk og sosial ustabilitet – også i jurisdiksjonen til tredjepartsleverandøren og datasenter
- Omfattende strømbrudd.

Finanstilsynets observasjoner

- **DORA**
  - Foretakenes arbeid med å innrette virksomheten etter DORA har gått fra en planleggings- og kartleggingsfase til implementering
  - Mange foretak har gjennomført gap-analyser og etablert styringsdokumenter
  - Det gjenstår arbeid med operativ implementering både internt i virksomheten og overfor tredjeparter

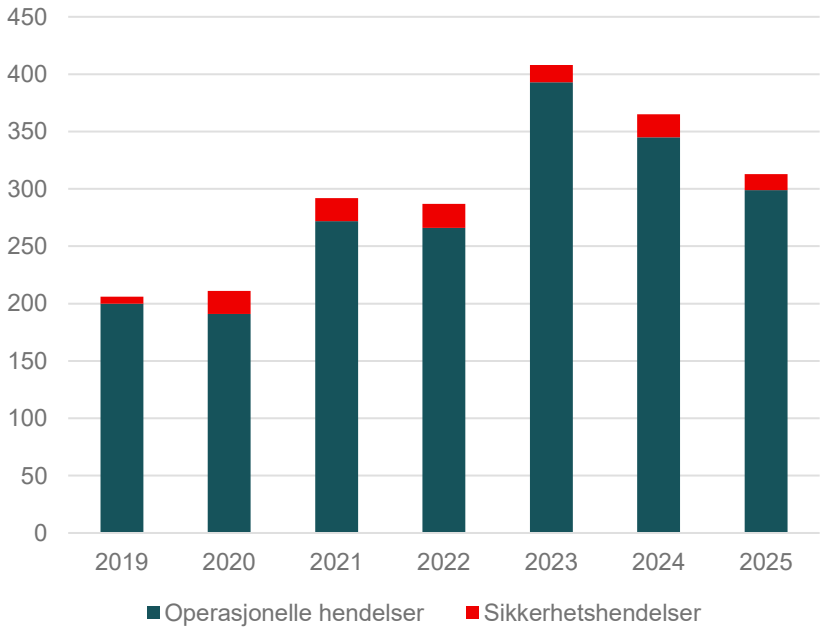
- **Beredskap og kontinuitet**
  - Foretakene har blitt bedre på konsekvensanalyser, og disse gir et bedre grunnlag for å identifisere kritiske tjenester og avhengigheter.
  - Testscenarioer og oppfølging av funn er ofte ikke gode nok

- **Leverandøroppfølging og endringshåndtering**
  - Fortsatt svakheter i kontroll av leverandørkjeder og underleverandører
  - Mange hendelser er knyttet til mangelfull endringshåndtering

Foretakenes egne observasjoner

- DORA driver mer strukturert styring, men også høyere kompleksitet
- Kompetansesituasjonen bedres, men kravene øker
- Leverandørkjeder og underleverandører er fortsatt krevende
- Geopolitikk øker risiko ved utenlandske leverandører
- Øvelser og beredskap er ikke tilstrekkelig helhetlige
- Skygge-IT/KI er et tydelig framvoksende risikoområde

Driftsstabilitet og tilgjengelighet var tilfredsstillende i 2025



- Antall rapporterte IKT-hendelser var noe lavere enn året før, og ingen hendelser hadde konsekvenser for den finansielle stabiliteten
- Samtidig viser hendelsesbildet at feil knyttet til brudd i dataintegritet, særlig i forbindelse med endringer og manuelle prosesser, kan få betydelige konsekvenser.
- DORA ble innført 1. juli 2025, og antallet rapporterte hendelser gikk noe ned i andre halvår

Flere hendelser med sektorovergripende konsekvenser

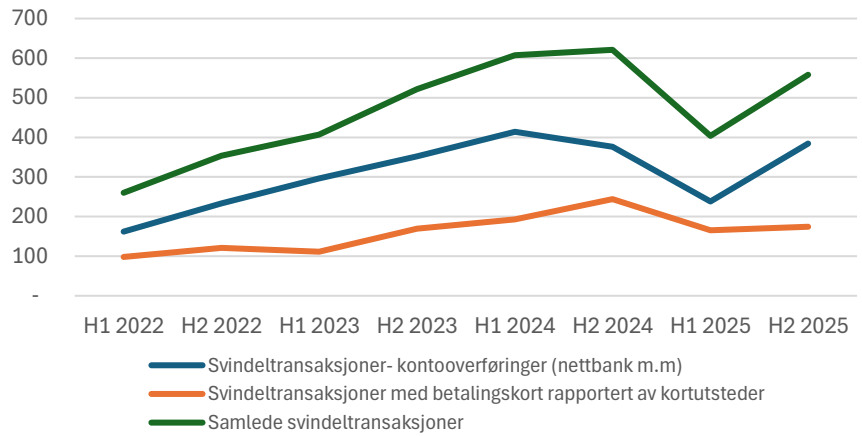
- Operasjonelle hendelser
  - Flere hendelser i skytjenesten Microsoft Azure som benyttes av mange foretak
  - Flere tilfeller av dupliserte transaksjoner/doble trekk som medførte feil på saldo
  - Noen hendelser knyttet til overvåking av hvitvasking og terrorfinansiering med konsekvenser som manglende transaksjonsovervåking og feil i sanksjonsscreeningen

- Sikkerhetshendelser
  - Kompromittering av IKT-leverandør med lekkasje av data til det mørke nettet
  - Flere tjenestenektangrep (Ddos)

Svindelen falt i 2025, men halvårsvariasjonene var større enn tidligere

- Svindelen falt markant i første halvår, men økte igjen i andre halvår
- Kontooverføringer utgjør den største delen av svindelen og driver utviklingen i totalbeløpet
- Kortsvindelen er mer stabil, med nedgang første halvår og svak økning andre halvår
- Svindelandelen av total transaksjonsverdi er noe lavere enn i 2024, men grunnet synkende totalverdi er andelen større enn i 2023 med tilsvarende samlet svindelbeløp
- Det ble forhindret svindel for til sammen 3,5 milliarder kroner i 2025

Periode	Konto-overføringer	Betalingskort	Samlet svindel	Andel av samlet verdi
2025	622	340	962	0,0018%
2024	790	437	1227	0,0020%
2023	648	281	929	0,0014%
2022	395	219	614	0,0013%



	**Beredskapen i finansnæringen er god, men må kontinuerlig utvikles for å møte nye trusler**
	**Det digitale trusselnivået er høyt og forsterkes av geopolitiske spenninger**
	**Leverandør- og verdikjederisiko er blant de mest kritiske sårbarhetene i finanssektoren**
	**Rask teknologisk utvikling gir både nye risikoer og sårbarheter og nye muligheter**

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY