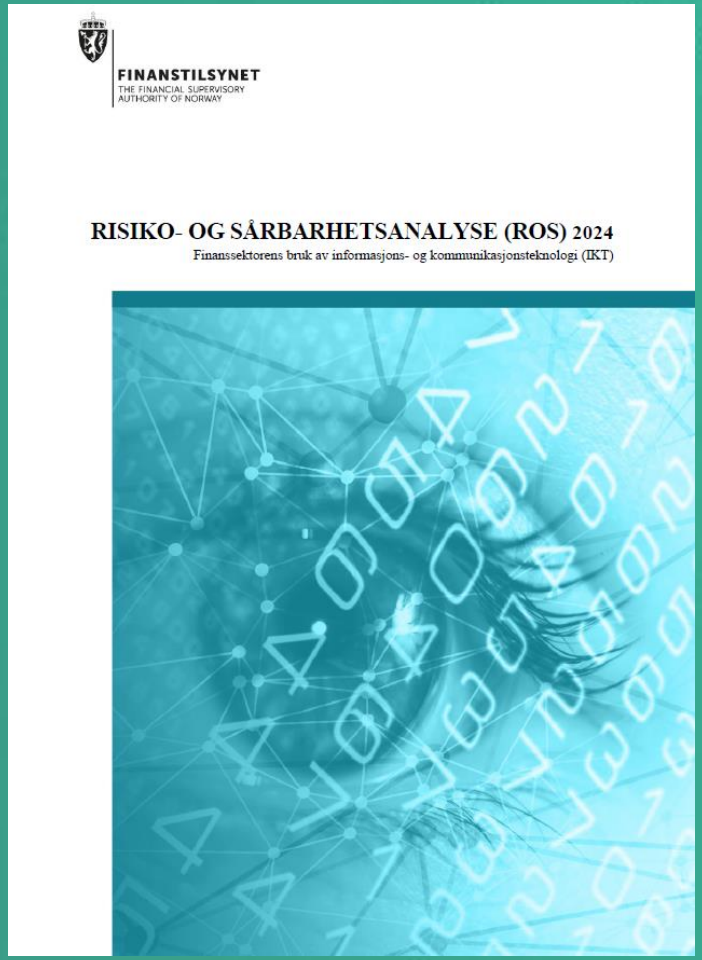
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2024

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Olav Johannessen, Seksjonssjef tilsyn IT og betalingstjenester, 5. juni 2024



- ✓ Digitalt trusselbilde og kriminalitet
- ✓ Digital robusthet - tiltak
- ✓ Samarbeid innen sikkerhetsområdet
- ✓ IKT-hendelser og avdekkede sårbarheter
- ✓ Tilgjengelighet til tjenestene
- ✓ Mangler og sårbarheter avdekket ved tilsyn
- ✓ Risiko utkontraktert IKT-virksomhet
- ✓ Foretakenes vurderinger av risikoområder
- ✓ Tap ved svindel
- ✓ Samlet vurdering av risikobildet
- ✓ Oppsummering

Digitale trusselbildet og kriminalitet

- Trusselbildet i endring – geopolitiske uro
- Trusselnivået høyt, men stabilt
- Færre angrep på finansiell infrastruktur – Digital kriminalitet øker
- Utvidet handlingsrom
- Uoversiktlige leverandørkjeder
- Trusler

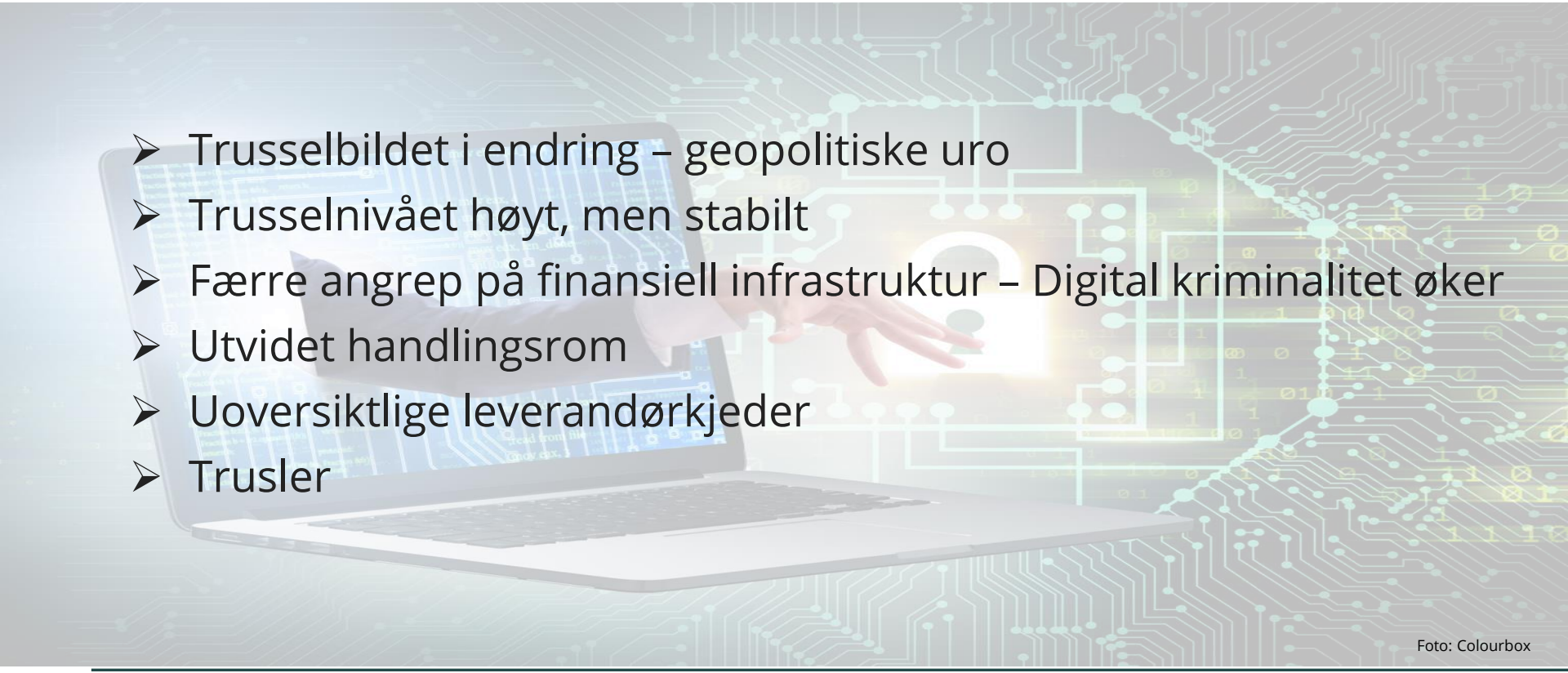
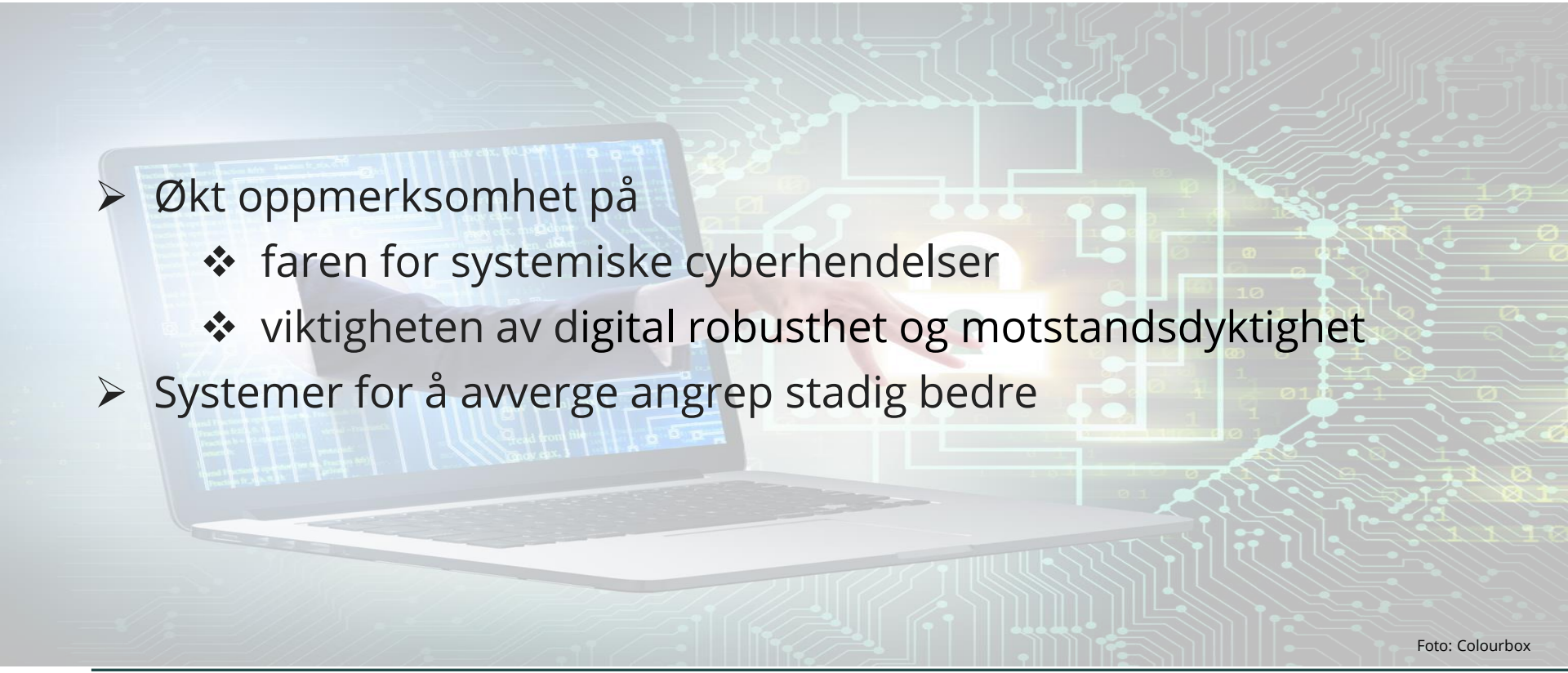


Foto: Colourbox

Digitale trusselbildet og kriminalitet



- Økt oppmerksomhet på
  - faren for systemiske cyberhendelser
  - viktigheten av digital robusthet og motstandsdyktighet
- Systemer for å avverge angrep stadig bedre

Foto: Colourbox

Digital robusthet – tiltak

- 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

Foto: Colourbox

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

Driftsstabiliteten var tilfredsstillende og på nivå med de to foregående årene - ingen kritiske hendelser i 2023

Alvorlige operasjonelle hendelser

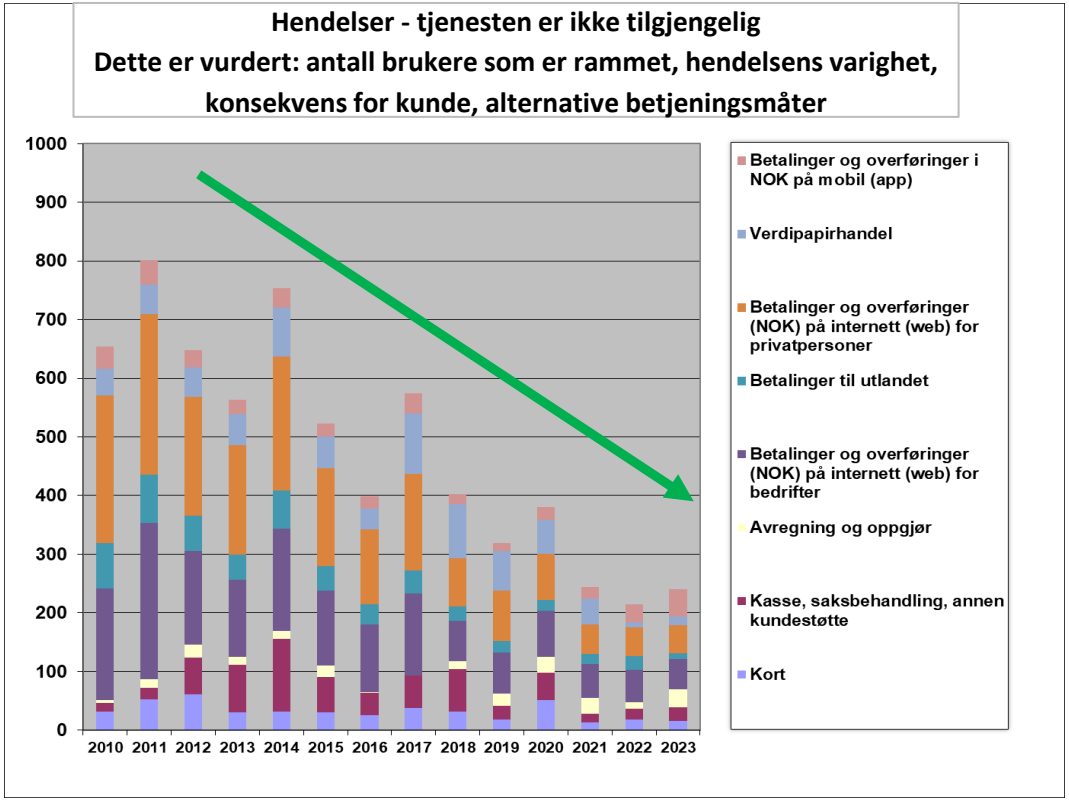
- Feil på saldo grunnet dupliserte eller manglende transaksjoner
  - Korrekt saldo først gjenopprettet flere dager senere
  - Flest straksbetalinger, noe kortbetalinger
- Feil i løsninger etter planlagte endringer gjennomført av leverandør
- Avvik knyttet til AML-systemer

Sikkerhetshendelser og sårbarheter

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

Kilde: Finanstilsynet

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)

Risiko knyttet til utkontraktert IKT-virksomhet

- Foretaket har ansvaret ved utkontraktering
- 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

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

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

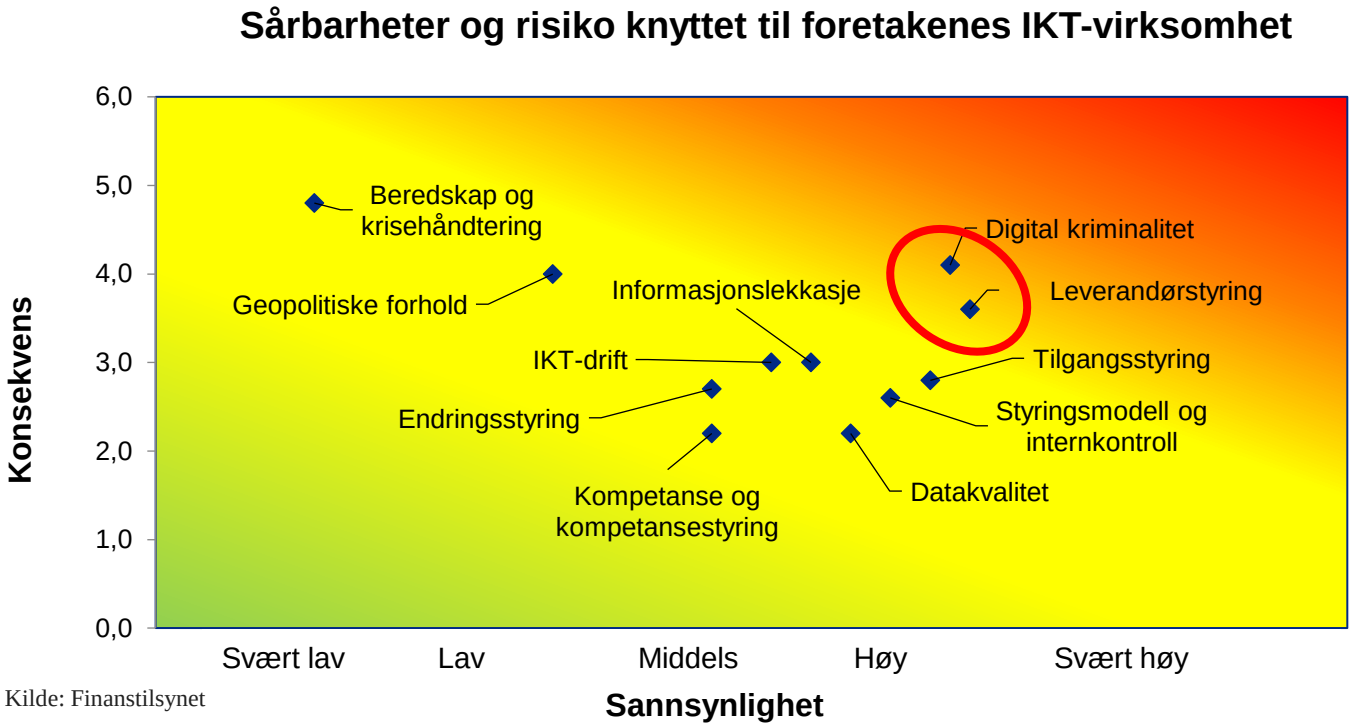
For 2023 kommer svindel ved kontantuttak på 2 mill. i tillegg

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

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
- Økt kompleksitet i IKT-driften


Digitale trusselbildet
Systemer
Sikkerhetstesting
Trusselvurderinger
Konsekvensanalyser
Beredskapsplaner
Håndtere angrep

DORA

- Gå gjennom kravene DORA stiller, hensyntatt proporsjonalitet og risikograd, der mange av kravene er absolutte
- Vurdere behov for oppdatering av rammeverk, prosesser, policyer, rutiner, registerføring mv.
- Ha særlig oppmerksomhet rettet mot områder som skal inngå i rammeverket for risikostyring.
- Involvere ledelse og styre
- Vurdere behov for å gjøre endringer i ledelses- og styrerapporteringen
- Vurdere behov for å styrke leverandøroppfølgingen, herunder styrket oppfølging av underleverandører
- Gå gjennom avtaler om IKT-tjenester, vurdere behov for oppdatering i samsvar med regelverket og lage en plan for dette
- Vurdere behov for kompetanse- og informasjonstiltak
- Forberede seg på og gjennomføre virksomhetsanalyser (Business Impact Analyses – BIA) og vurdere virksomhetens avhengighet av IKT-systemene
- Vurdere endringer i foretakets risikoappetitt knyttet til IKT-virksomheten, hensyntatt vurderinger fra virksomhetsanalysen
- Gå gjennom foretakets tre forsvarslinjer eller tilsvarende og vurdere behov for endringer, særlig med hensyn til oppfølging av leverandører og underleverandører, om tilstrekkelig uavhengighet er ivaretatt og om kompetansen er tilstrekkelig
- Løpende sette seg inn i nivå 2-regelverkene etter hvert som de fastsettes

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY