FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Betalingssystemer og IKT i finanssektoren
27. mai 2015

Risiko- og sårbarhetsanalyse (ROS) 2014
Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Olav Johannessen og Atle Dingsør

ROS-analysen 2014:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Innledning
2. Oppsummering
3. Finanstilsynets funn
4. Andre observasjoner
5. Utviklingstrekk, Aktuelle trender som kan påvirke risiko
6. Risikoområder
7. Finanstilsynets oppfølging
8. Ordliste

Hensikten med den årlige ROS-analysen er å speile risikobildet i finanssektorens bruk av IKT

ANSTILSYNET
ANCIAL SUPERVISORY
RITY OF NORWAY

- Skaffe oversikt
- Analysere
- Foreslå tiltak

Resultater fra tilsyn IT og betalingstjenester

Gjennomførte ROS-intervju og spørre-undersøkelser

Hendelses-håndtering

Data fra hendelsesdatabase

Betalingstjenester

Meldeplikt Betalings-tjenester

Annen relevant Informasjon

Beredskap
- BFI-sekretariatet
- Samarbeid andre myndigheter
- Infrastruktur betalings-systemer

Våre virkemidler
Regelverk, Innrapportering og Tilsyn

2. Oppsummering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Betalingstjenestene generelt er stabile og har hovedsakelig en god kvalitet, selv om det i 2014 var en økning i alvorlige hendelser som bidro til å redusere betalingssystemenes tilgjengelighet
- Økt kortsvindel med stjålet kortinformasjon
- Økte tap som skyldes at kundens innloggingsmekanisme er blitt stjålet og misbrukt
- Utviklingen i digital kriminalitet gjør forbrukerne mer sårbare
  - *Det er krevende for forbrukere å forholde seg til trusler og sårbarheter i finansielle tjenester*
- Den alvorligste trusselen er at inntrengere får tilgang til IKT-infrastruktur og applikasjoner gjennom målrettede angrep
- Omfattende endringer i finanssektorens IKT-virksomhet
  - *Endringene kan gi forbedringer, men de kan også skape nye sårbarheter.*

3. Finanstilsynets funn

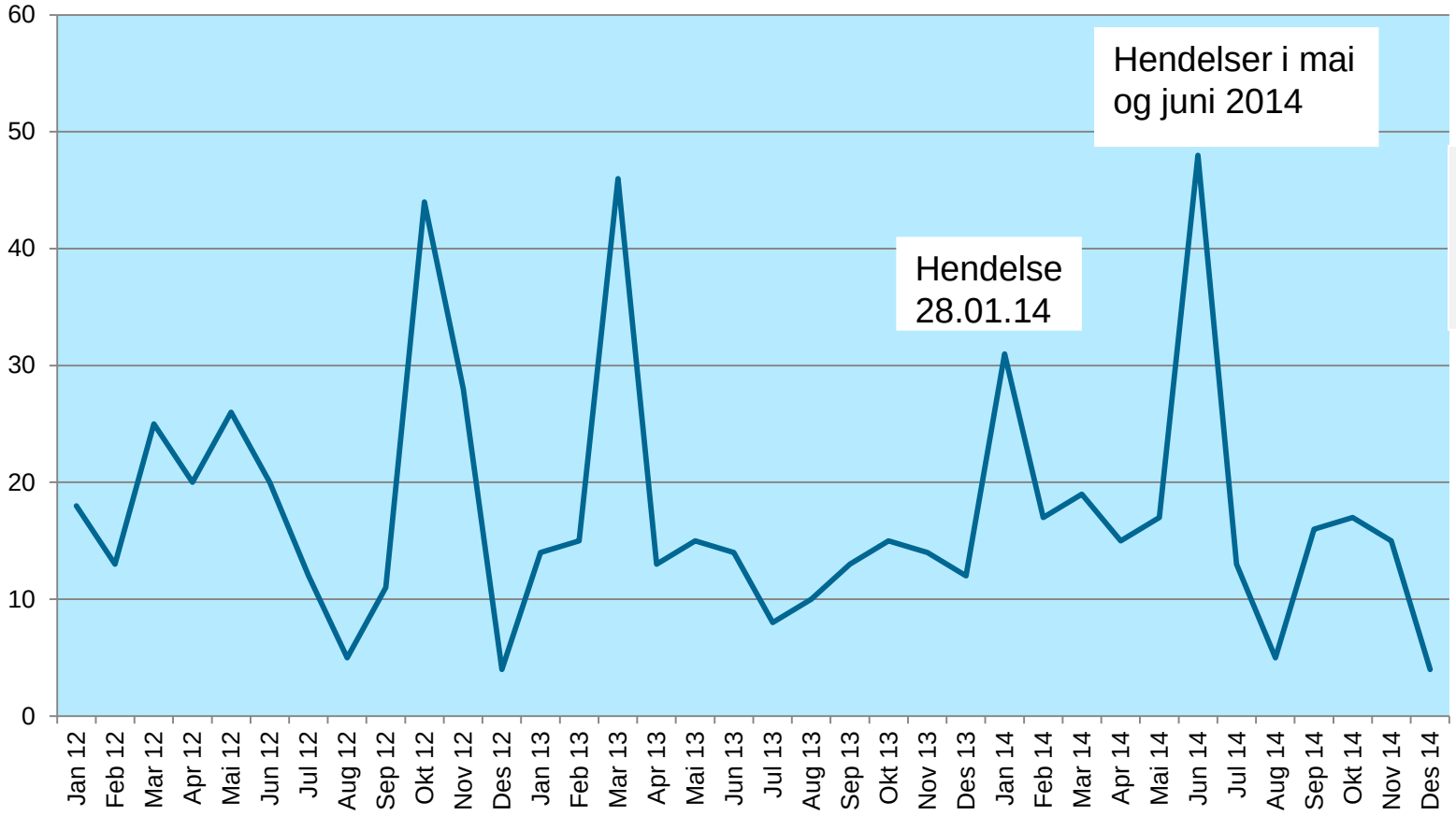
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Rapporterte hendelser 2014
2. Funn, observasjoner og vurderinger
   - Betalingssystemer og utvikling. Tapstall
   - Verdipapirområdet
   - Bank
   - Forsikring
   - Funn i andre foretak
3. Forbrukerområdet

Antall rapporterte hendelser i perioden 2012–2014

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Figur 2: Antall rapporterte hendelser i perioden 2012–2014



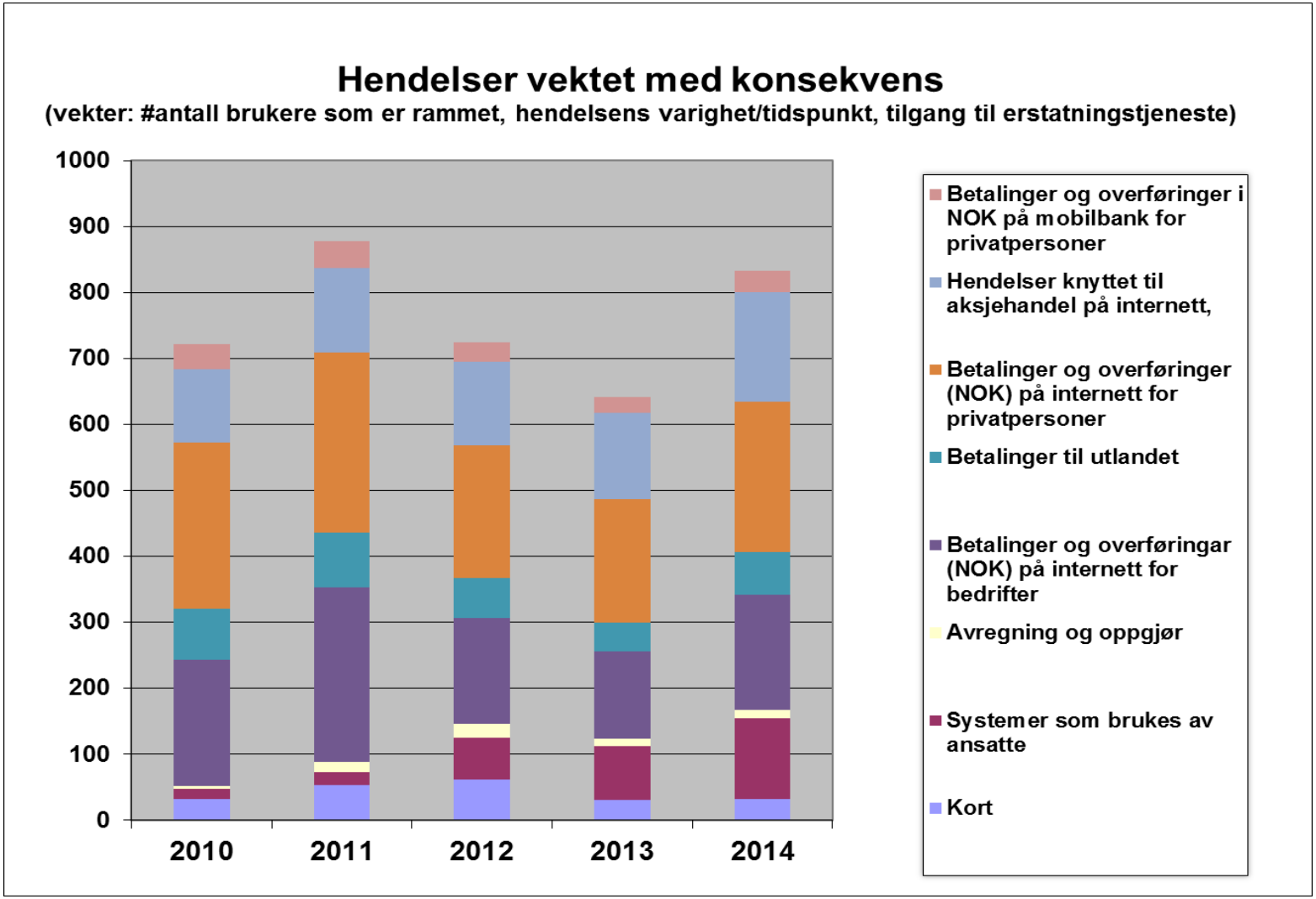
2011: 221 hendelser
2012: 216 hendelser
2013: 189 hendelser
2014: 217 hendelser

Kilde: Finanstilsynet

Hendelser vektet med konsekvens

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Figur 4: Hendelser vektet med konsekvens



Kilde: Finanstilsynet

Betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Flere alvorlige hendelser rammet betalingsformidlingen
2. Hendelser som oppstår i, eller treffer betalingsinfrastrukturen, rammer bredt og medfører raskt store konsekvenser
3. Endringer hyppig årsak til feil og avvik og det er derfor knyttet betydelig risiko knytte til dette
4. Robustheten i løsninger samsvarer i enkelte sammenhenger ikke med betalingsformidlingens sentrale rolle
5. Svakheter i driftsløsninger som skal sikre kontinuitet for betalingsformidlingen
6. Enkelte foretak har mangler i sine avtaler, bl.a. IKT-forskriftens regler om utkontraktering
7. Rask utvikling innen mobile betalingsløsninger, nasjonalt og internasjonalt
8. Finanstilsynet har gjort sårbarhetsvurderinger knyttet til mobilbaserte betalingsløsninger

Betalingstjenester - 2

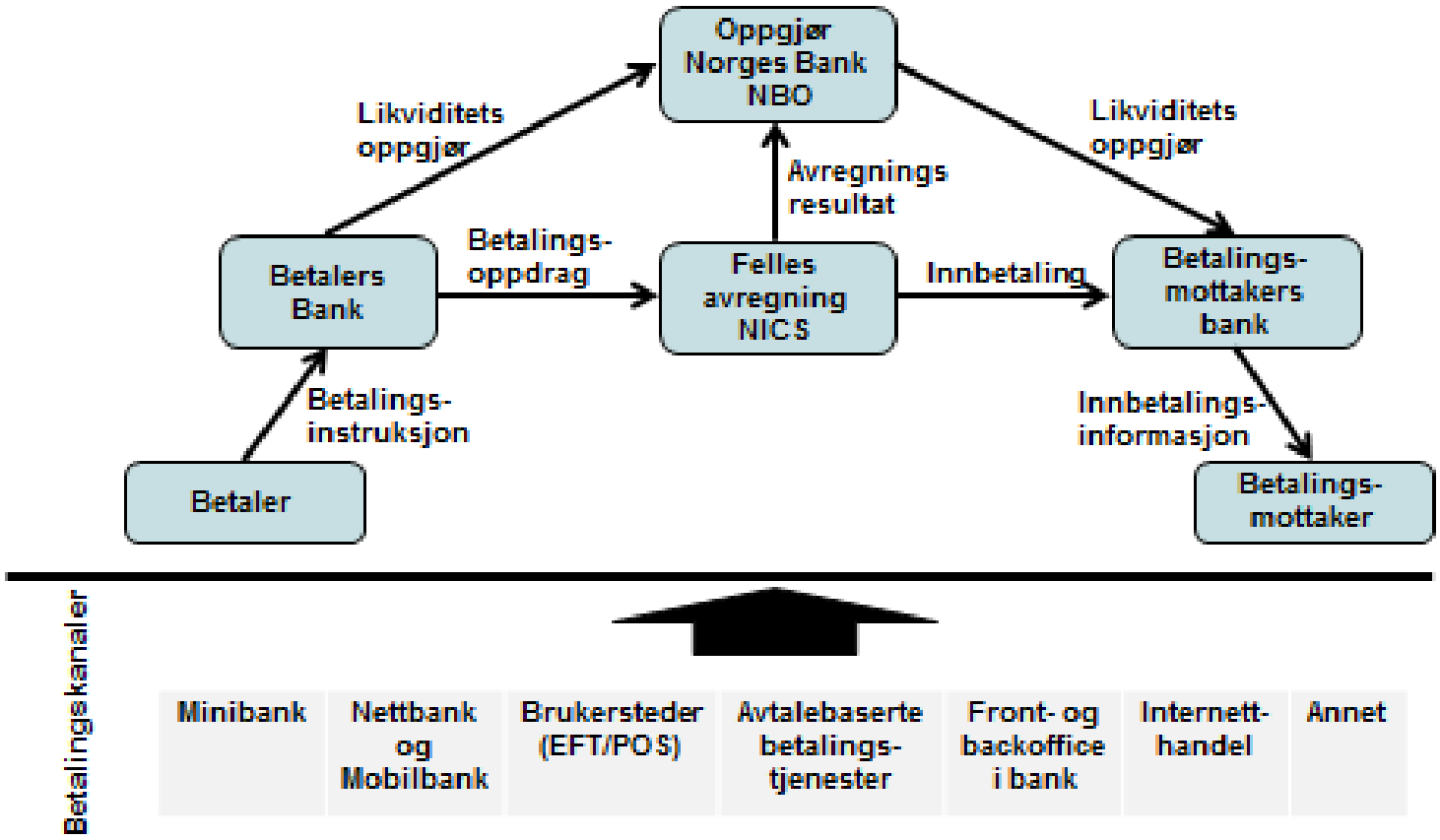
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

9. Fortsatt angrep som rammer betalingsformidlingen
   - *DDoS, phishing, trojanere, tyveri av kortinformasjon*
10. Ikke kjent med svindelforsøk via mobiltelefon i Norge
11. Finanstilsynets erfaring er at foretakene har god beredskap, at de har etablert godt forsvarsverk og at de iverksetter effektive tiltak som reduserer både skadeomfang og kunders tapsomfang

Transaksjonsflyten i det norske betalingssystemet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Forenklet bilde av transaksjonsflyten fra der betalingen oppstår, innsamling, avregning og oppgjør.



Stabil sentral betalings-infrastruktur

Flere hendelser hos foretakene som rammer betalings-tjenestene

Tap ved bruk av betalingskort
(tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 1: Tap ved bruk av betalingskort (tall i hele tusen kroner)

Svindeltype betalingskort	2011	2012	2013	2014
Misbruk av kortinformasjon, Card-Not-Present (CNP) (internetthandel m.m.)	24 190	35 701	51 954	**72 056**
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308	762	**524**
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869	51 534	**51 685**
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128	21 274	**21 266**
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544	9 570	**13 071**
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603	4 9 49	**5 510**
TOTALT	**125 718**	**135 153**	**140 043**	**164 113**

Kilde: Finanstilsynet

Antall betalingskort rammet av misbruk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 2: Antall betalingskort rammet av misbruk

Svindeltype betalingskort	2011	2012	2013	2014
Antall kort rammet av misbruk	16 784	20 332	22 531	38 541

Kilde: Finanstilsynet

Totaltapet på kortsvindel økte også i 2014. Det var også i 2014 en betydelig økning i svindel av typen «card-not-present» (CNP), mens det var en reduksjon i tapene knyttet til andre typer kortsvindel.

Tap ved bruk av nettbank
(tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 3: Tap ved bruk av nettbank (tall i hele tusen kroner)

Svindeltype nettbank	2011	2012	2013	2014
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064	1 327	552
Tapt/stålet sikkerhetsmekanisme	3 321	3 367	1 321	6 655
TOTALT	3 985	8 431	2 648	7 207

Kilde: Finanstilsynet

Verdipapirområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Høy stabilitet og god kvalitet kjennetegner verdipapirområdet
2. Betydelig endringsomfang på regelverksområdet (EU) vil påvirke infrastrukturen og innebærer endringsrisiko med behov for kvalitetssikring
3. Gamle såkalte legacy-systemer representerer en utfordring, og en fornyelse innebærer risiko under gjennomføringen
4. Bruk av skybaserte tjenester kan gi nye utfordringer ved at forretningsansvarlige i foretak går til «innkjøp» av IKT-tjenester uten å gå via egen IT-avdeling
5. Mangelfulle tilgangskontroller til sensitiv informasjon
6. Bruk av samme nettverksinfrastrukturer representerer en konsentrasjonsrisiko

Bank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Endringer på driftsleverandørsiden, både eierskifter og bytte av leverandører kan øke risikoen spesielt i endringsperioden
2. Reetablering av IKT-tjenester i en katastrofesituasjon vil kunne ta lenger tid enn antatt
3. Foretakene må sikre egen styring og kontroll av IKT-virksomheten, også ved utkontraktering
4. Manglende etterlevelse om krav til datasystemer og rapportering til Bankenes sikringsfond dersom foretaket blir satt under offentlig administrasjon
5. Mangelfull gjennomgang og kontroll av ansattes tilganger til systemer og applikasjoner
6. Utfordrende å styre og kontrollere klassifiseringsregler, spesielt mht. tilganger til graderte data og systemer

Forsikring

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Komplekse forsikringssystemer med sensitiv informasjon krever sikker og betryggende forvaltning og etablerte reserveløsninger
2. Få rapporterte hendelser tyder på god endringskontroll
3. De fleste hendelsene er knyttet til konfidensialitetsbrudd
4. Mangler i etterlevelse av forskriftenes krav ved utkontraktering
   - *Kan medføre mangelfull oversikt over, og kontroll med, IKT-virksomhet og IKT-risikoer*
5. Risikoanalyser ofte fragmenterte, mangelfulle og dekker ikke selskapets samlede IKT-virksomhet
6. Testing av kontinuitets- og katastrofeplaner synes å være et forbedringsområde
7. Sensitiv informasjon, kan være av interesse for inntrengere

Andre foretak

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Finanstilsynet gjør enkelte stedlige IT-tilsyn i inkassoselskaper og eiendomsmeglingsforetak. I tillegg må eiendomsmeglingsforetakene og inkassoselskapene svare på et forenklet egenevalueringsskjema med spørsmål om IT-virksomheten ved ordinære fagtilsyn.
- Finanstilsynet hadde i 2014 merknader til
  - Manglende beredskapsløsninger
  - Sikring av konfidensiell informasjon
  - Manglende rutiner for å håndtere sikkerhetshendelser
  - At foretaket peker på IT-leverandøren som ansvarlig for IT-prosessene.

Forbrukerområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Mangelfull ID-sjekk ved utlevering av BankID kan få store konsekvenser for forbrukeren som er rammet
   - *Gjaldt 15 av 150000 utleveringer i 2014*
2. Forbrukere kan bli svindlet ved netthandel mellom private parter dersom de ikke gjør bruk av handelssteders betalingstjenester
3. Forbruker må forsikre seg om at nettsteder har den nødvendige sikkerhet, som f.eks. kryptering (hengelås i adressefeltet)

4. Andre observasjoner

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Foretakenes vurdering av risiko
   - Intervjuer
   - Spørreundersøkelse
2. Risikoområder påpekt fra andre kilder
   - Intervju med sikkerhetsselskaper og internettjenesteleverandører
   - Rapporter fra internasjonale sikkerhetsorganisasjoner

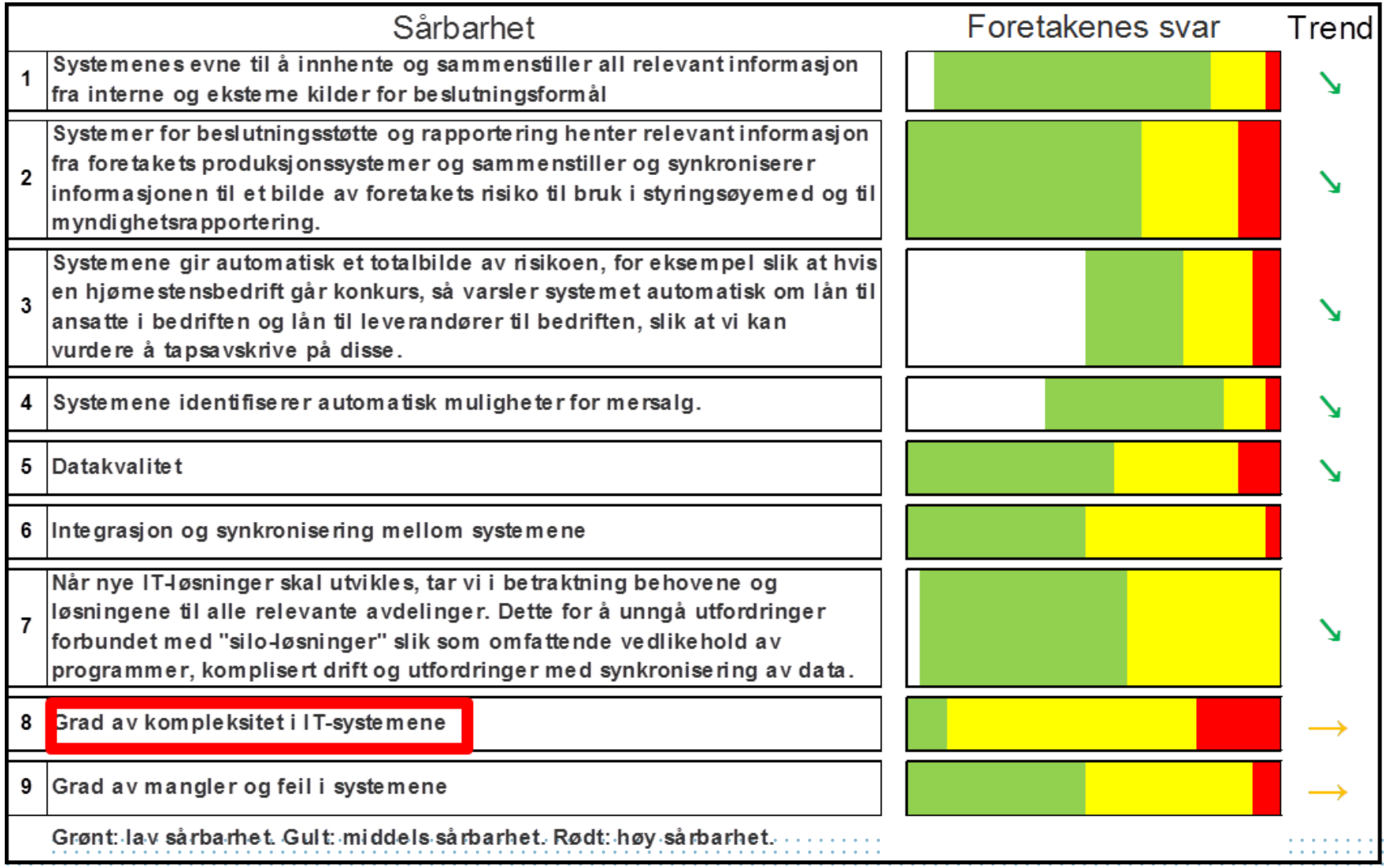
Intervjuer og spørreundersøkelser med foretakene

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. De mest fremtredende truslene synes å være at inntrengere får tilgang til IKT-infrastruktur og applikasjoner gjennom målrettede angrep.
2. Andre trusselområder som representerer betydelig risiko er:
   - økningen i IKT- og cyberkriminalitet
   - sikkerhetshull i programvare som kan utnyttes av kriminelle
   - den sterke avhengigheten til Internett
   - ansattes bruk av sosiale medier
   - informasjon som kommer på avveie
     - ✓ Utlevering av BankID kodebrikke, Personopplysninger
3. Kompleksitet i IKT-løsninger utgjør også en høy risiko for datakvalitet og stabil drift, og kan hindre nyutvikling.

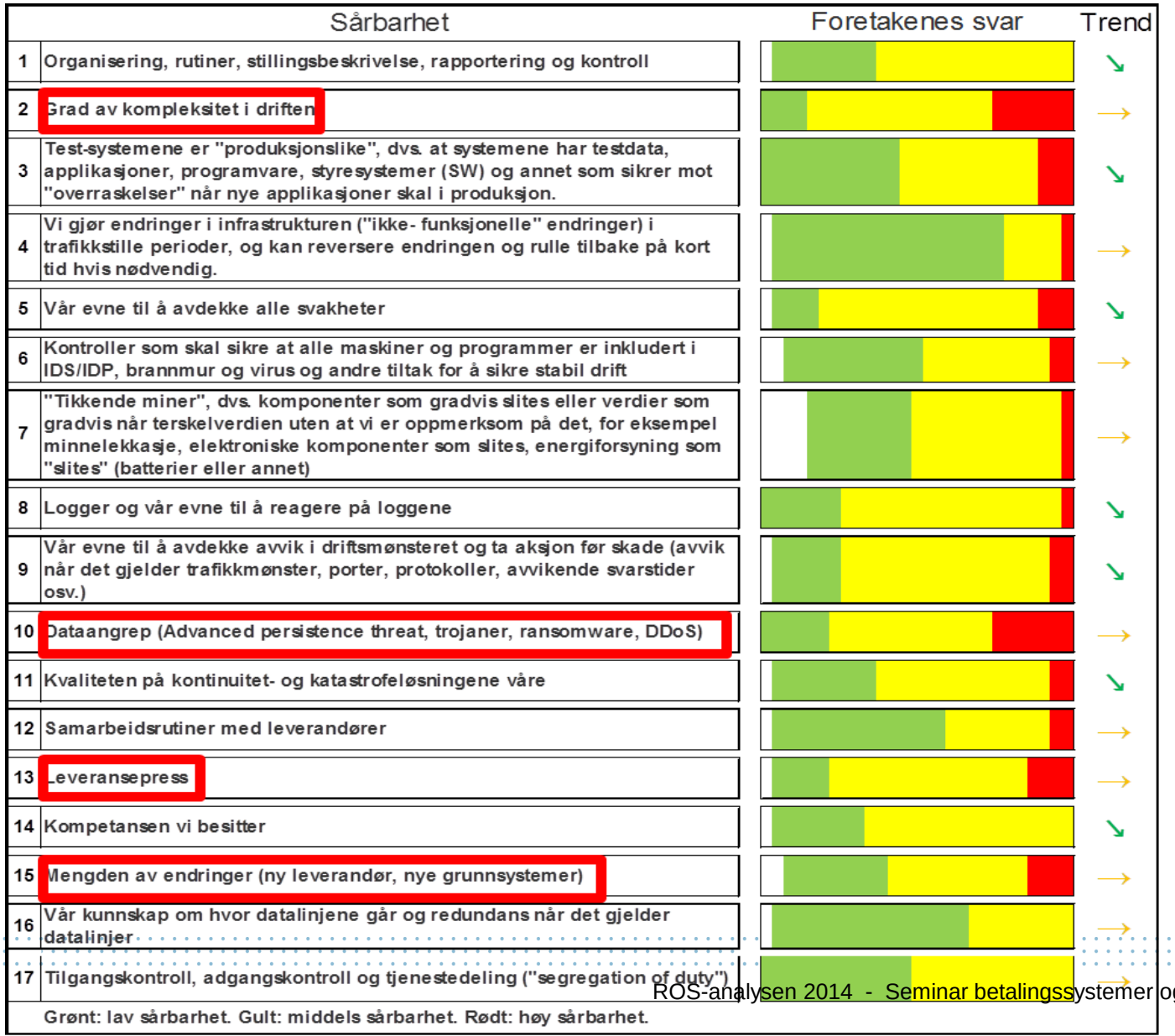
Støtte for strategiske beslutninger

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



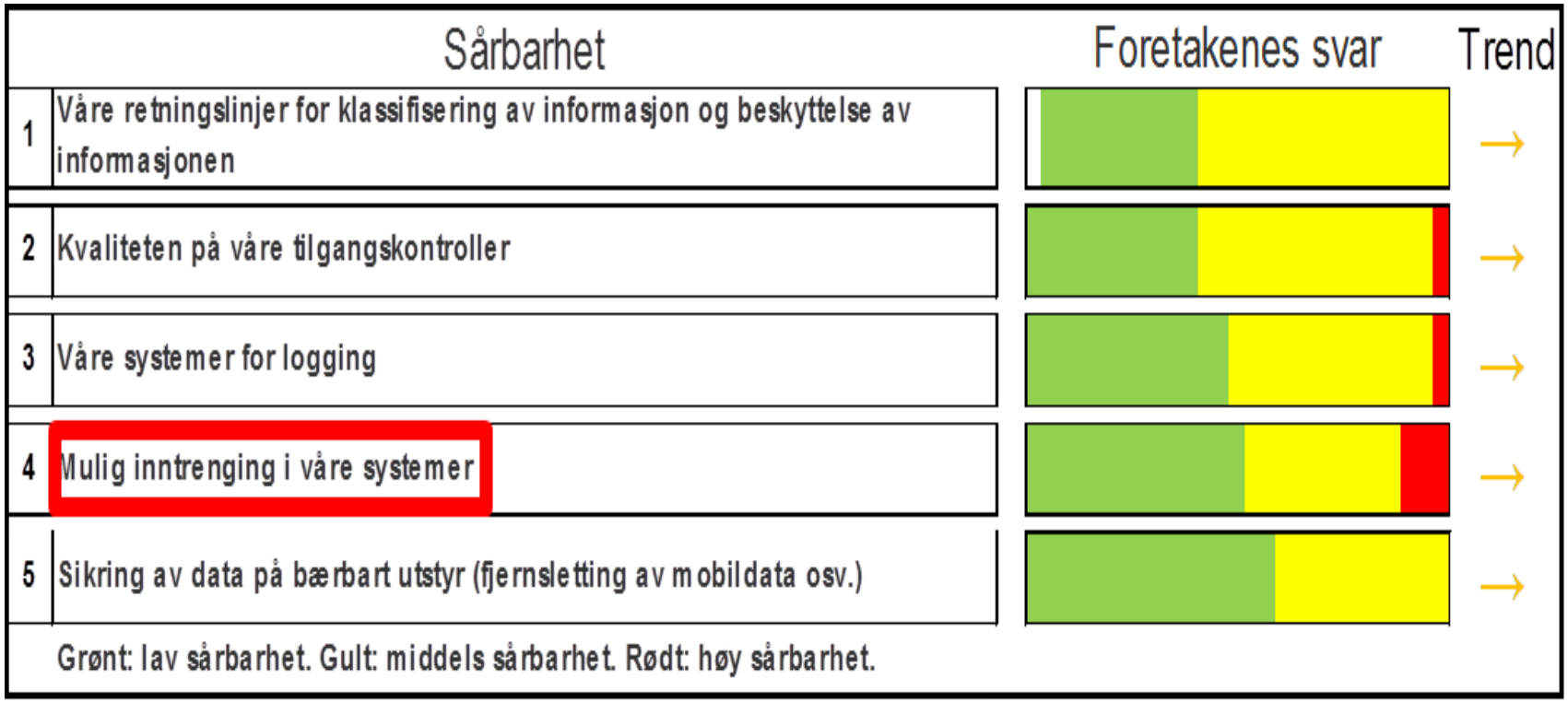
Avvik i driften

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



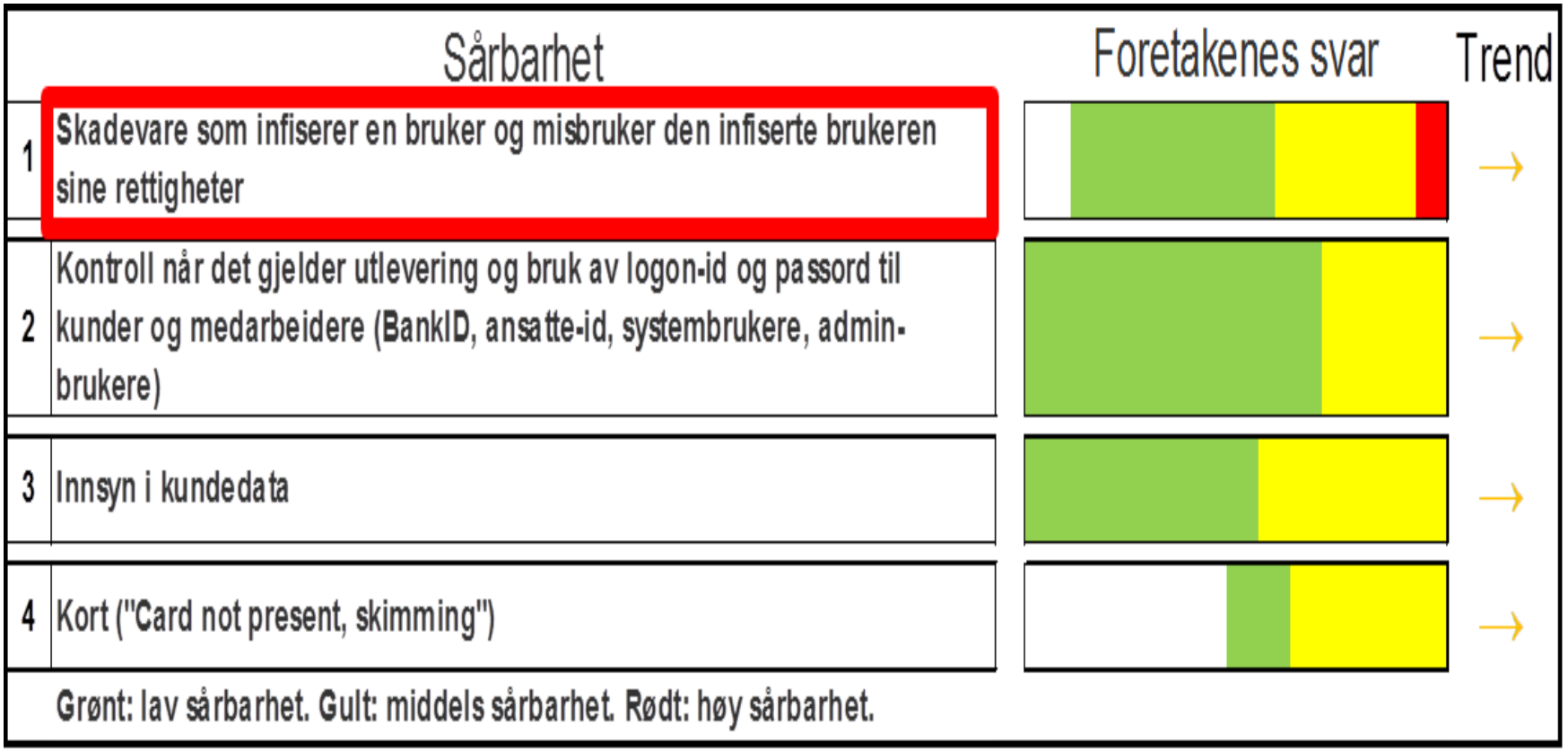
Data er ikke tilstrekkelig beskyttet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



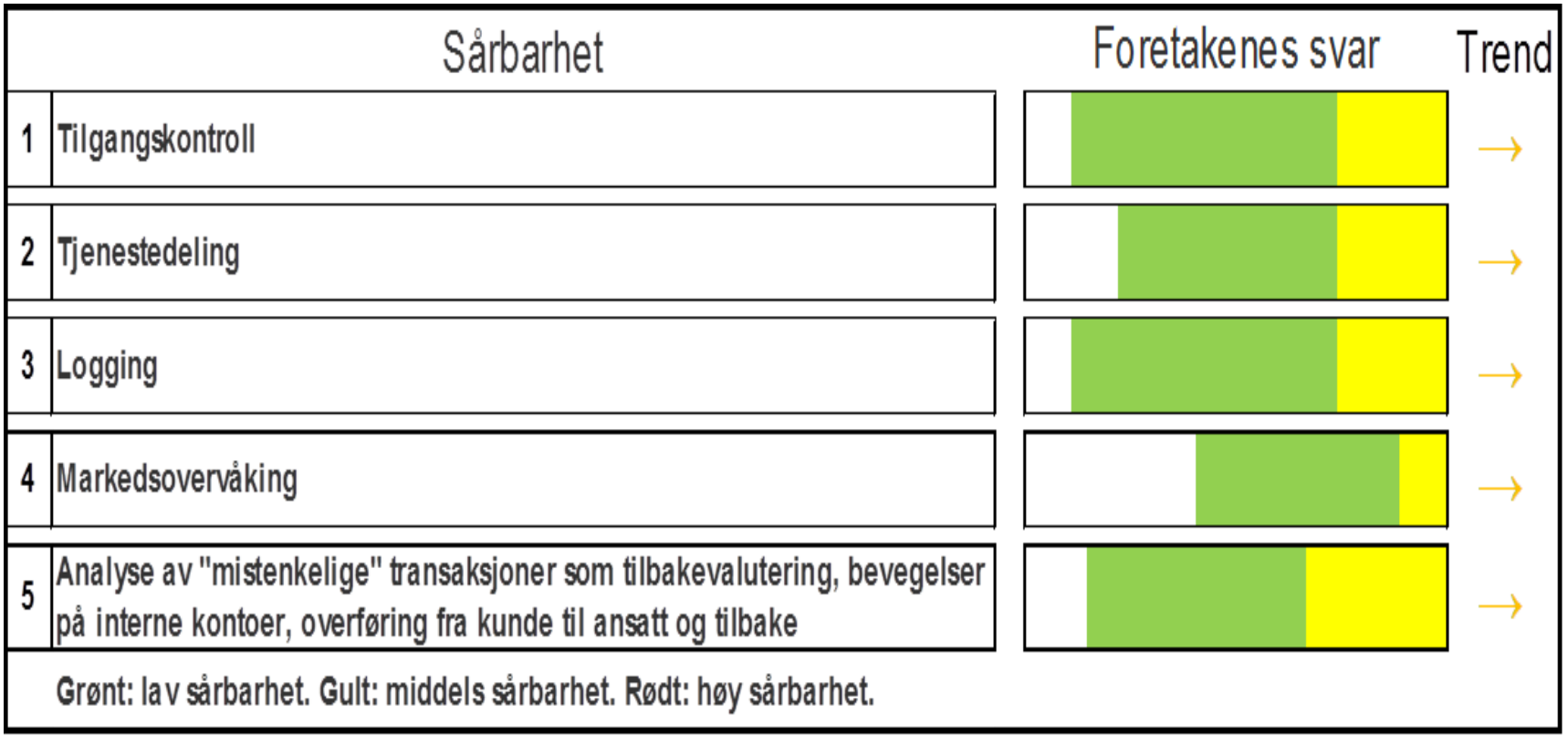
ID-tyveri

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



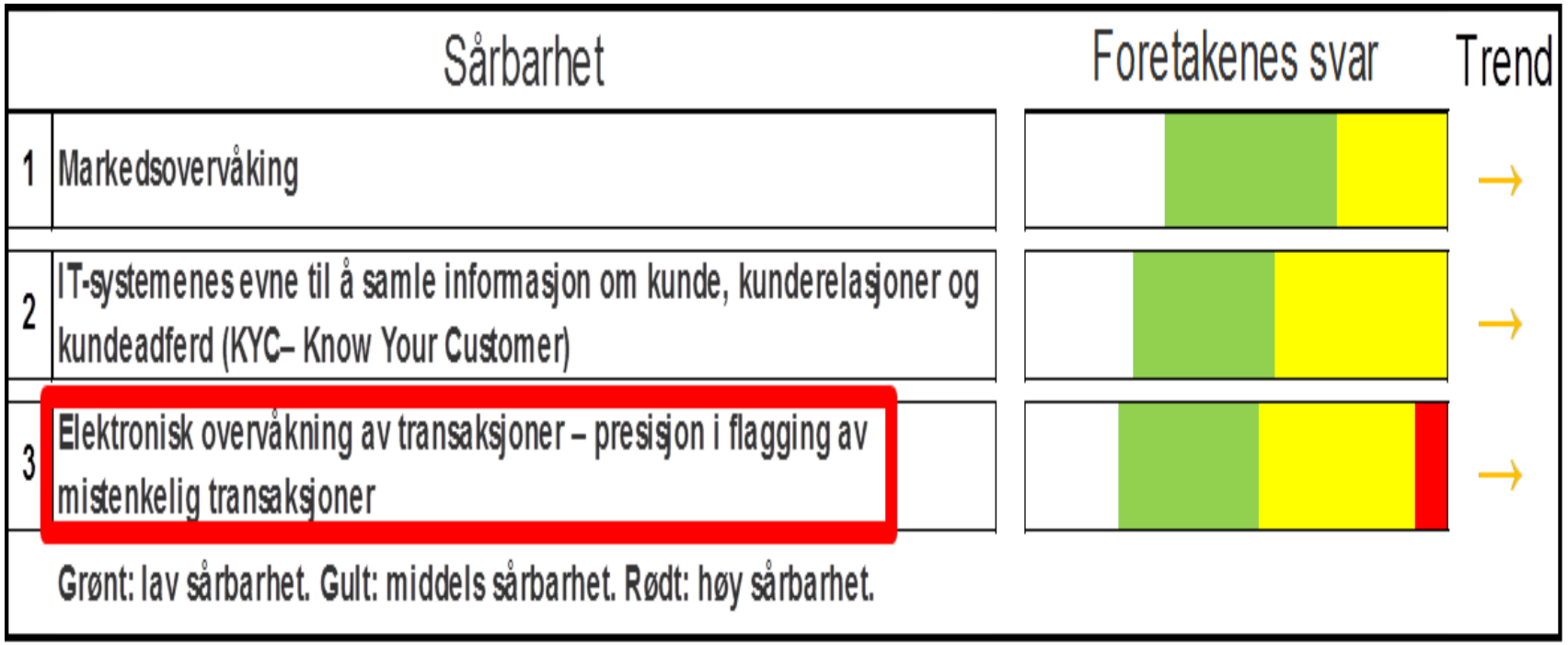
Misbruk av tilgang til datasystemene

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Hvitvasking

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Risikoområder påpekt fra andre kilder

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Norge et av de minst infiserte land når det gjelder PC-virus
- Foretakene bør sørge for at ISP-er tar en mer aktiv rolle i bekjempelse av DDoS og spam
- Advanced Persistent Threat (APT) - den største trusselen fra nettet
  - *Brukermedvirkning finnes i nesten 50 prosent av APT-inntrenginger*
- Foretakene må sikre at informasjon ikke kommer på avveie
- Sikkerhetsatferd viktig. 80–20-regelen kan benyttes i fordeling mellom menneskelige og teknologiske svakheter
- Datainnbrudd globalt økt i frekvens med 25 prosent siste året.
  - *Manglende sikkerhet i sluttbrukerleddet årsak til mer enn 50 prosent av innbruddene*
- Viktig å holde oppe forsvaret mot ondsinnede angrep fra nettet, feil kan medføre alvorlige konsekvenser både for foretaket og kundene.

Finanstilsynets oppsummering av IKT- og internettbasert kriminalitet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Trusselen fra cyberangrep øker ved at verktøyene som benyttes, blir mer sofistikerte og at metodene som benyttes, blir mer varierte
- Angrepene som gjøres, er målrettede og utføres ofte av organisasjoner som baserer forretningsdriften sin på kriminell virksomhet
- Denne typen organisasjoner har gjerne tilgang til ressurser med stor kunnskap innenfor IKT-området, nødvendig datakapasitet og god tilgang på finansiering av virksomheten

5. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Økende digital kriminalitet. Myndighetene vier dette større oppmerksomhet
2. Endringer i tjenesteleverandørmarkedet, organisering og eierskap og utkontrakteringslandskapet
3. Utviklingen i teknologi åpner for utvikling av mer effektive og brukervennlige tjenester. Høy endringstakt innenfor mobilbaserte betalingstjenester og utviklingen i sikkerhetsløsninger
4. Endringer i regelverk både
   - Nasjonalt
   - EU
5. Fellestiltak fra finansnæringen
6. Virtuelle valutaer

6. Finanstilsynets oppsummerende vurdering av risikobildet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Aktuelle risikoområder er vurdert ut fra kontrollmålene integritet, konfidensialitet, tilgjengelighet og at IT fungerer tilfredsstillende som støtte for forretningsdriften.

Kontrollmål	Vurderingstema (eksempler) Sårbarhet/kontrolltiltak	Risko	Trend
Integritet Informasjon og informasjonssystemer er korrekte, gyldige og fullstendige.	Datakvalitet Datamodeller Endringsbeskyttelse (hash) Tilgangskontroller	H	↗
Konfidensialitet Informasjon og informasjonssystemer er tilgjengelige bare for dem som skal ha tilgang.	Autorisasjon og Identitetskontroller Interne retningslinjer Kryptering (kvalitet) Logging	M	→
Tilgjengelighet Informasjon og informasjonssystemer er tilgjengelige innenfor de tilgjengelighetskravene som er satt.	Avhengighet av Internett Endringer i programmer og data Flytte driften Komplisert kjøreomgivelse Maskinvarefeil og Nettverksfeil Vedlikehold, opprydding og sanering	M	↗
Beslutningsstøtte: "IT fungerer tilfredsstillende som støtte for strategiske beslutninger, kundebehandling, saksbehandling og rapportering".	Avviksanalyse Konsekvensanalyse Tidlig varsling Totalt kundebilde "What if"-analyse	M	→

6. Finanstilsynets oppsummerende vurdering av risikobildet - 2

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

2. Risikoen knyttet til integritet er høy og økende, risikoen knyttet til konfidensialitet er middels og stabil, risikoen knyttet til tilgjengelighet er middels og økende og risikoen knyttet til at IT fungerer tilfredsstillende som støtte for forretningsdriften er middels og stabil.
3. Finansforetak var under angrep i 2014. Virkningen har vært dempet som følge av tiltak fra foretakene. Digitale angrep mot finanssektoren kan føre til at markedene og finansiell stabilitet kan bli truet.
4. Hyppigste feilårsak hos foretak er feil ifm endring i systemer og omgivelser, og de må fortsatt ha særlig oppmerksomhet rettet mot dette området.
5. Det er krevende for forbrukere å forholde seg til trusler og sårbarheter i finansielle tjenester på en kvalifisert måte, og finansnæringen har et stort ansvar for å bygge inn tilstrekkelig sikkerhet i løsningene.

7. Finanstilsynets oppfølging

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. IT-tilsyn og annen kontakt med foretakene
2. Arbeid med betalingssystemer
3. Oppfølging av hendelser
4. Beredskapsarbeid
5. Videreutvikling av tilsynsverktøy
6. Oppfølging av trusselbildet knyttet til digital kriminalitet

Takk for oppmerksomheten!

FINANSTILSYNET

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

www.finanstilsynet.no

Olav Johannessen & Atle Dingsør
Seksjonssjef seksjon for tilsyn med IT og betalingstjenester

E-post: ola@finanstilsynet.no & adi@finanstilsynet.no