FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Seminar 22. mai 2014

Risiko- og sårbarhetsanalyse (ROS) 2013
Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Seksjonssjef Frank Robert Berg

ROS-analysen 2013:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Innledning
2. Oppsummering
3. Utviklingstrekk
   - Aktuelle trender som kan påvirke risiko
4. Finanstilsynets funn og observasjoner
5. Risikoområder
6. Finanstilsynets oppfølging
7. Betalingssystemer og utvikling
8. Verdipapirområdet
9. Ordliste

Hensikten med ROS-analysen

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Samarbeid Finanstilsynet – Norges Bank

- Skaffe oss oversikt
- Analysere
- Foreslå tiltak

Leveranse

Årlig ROS-analyse
Risiko
Sikkerhet

- Resultater fra tilsyn – IT og betalingstjenester
- Gjennomførte ROS-intervju
- Hendelseshåndtering – Data fra hendelsesdatabase
- Betalingstjenester – Meldeplikt – Betalings-tjenester
- Annen relevant informasjon spørre-undersøkelser
- Beredskap
  - BFI-sekretariatet
  - Samarbeid andre myndigheter
  - Infrastruktur betalingssystemer

Våre virkemidler
Regelverk, innrapportering og tilsynsopplegg

3. Utviklingstrekk

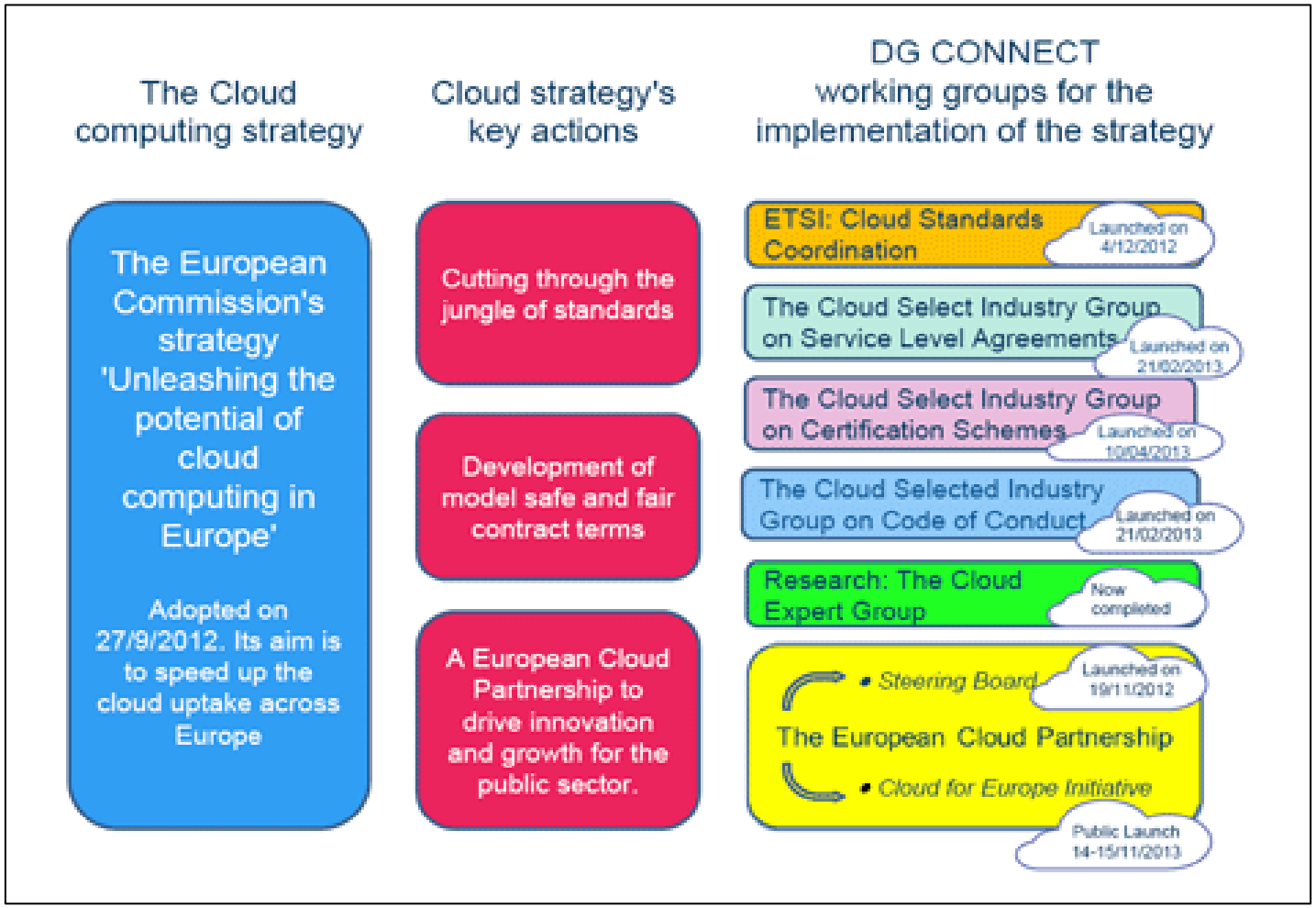
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Utviklingstrekk for skytjenester i EU
2. Samordning og endringer i EUs regelverk
3. Norske finansinstitusjoner og skytjenester
4. Organisering og eierskap
5. Endringer i sourcing-landskapet
6. Tekniske utviklingstrekk og risikoer/trusler
7. Virtuelle valutaer

3.1 Utviklingstrekk for skytjenester EU

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

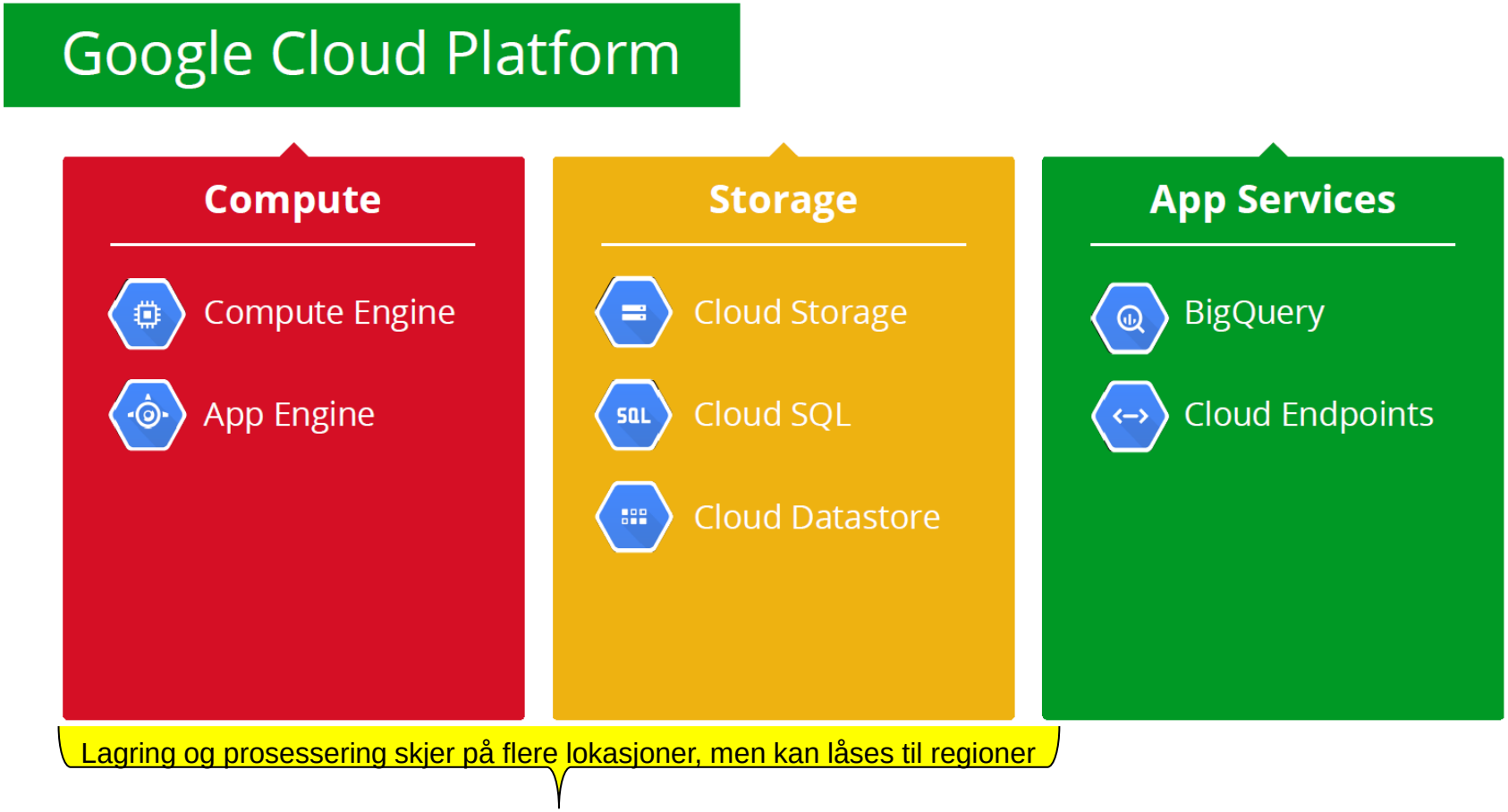
Figur 1:



Kilde: EU-kommisjonen

3.1 Eksempel på Google's strategi for Cloud computing

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Kilde: Google

3.2 Samordning og endring i EUs regelverk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Forordning om elektronisk ID
- Nytt betalingstjenestedirektiv – PSD2
- Forslag til reviderte «passporting guidelines» for betalingsforetak og e-pengeforetak
- Regulering av formidlingsgebyrer for kortbaserte betalinger – MIF-forordningen
- Direktiv for nettverk og informasjonssikkerhet (NIS-direktivet)
- Endringer i hvitvaskingsreglene

3.3 Norske finansinstitusjoner og skytjenester

3.4 Organisering og eierskap

3.5 Endringer i sourcing-landskapet

3.6 Fellestiltak fra finansnæringen

3.7 Tekniske utviklingstrekk og risikoer/trusler

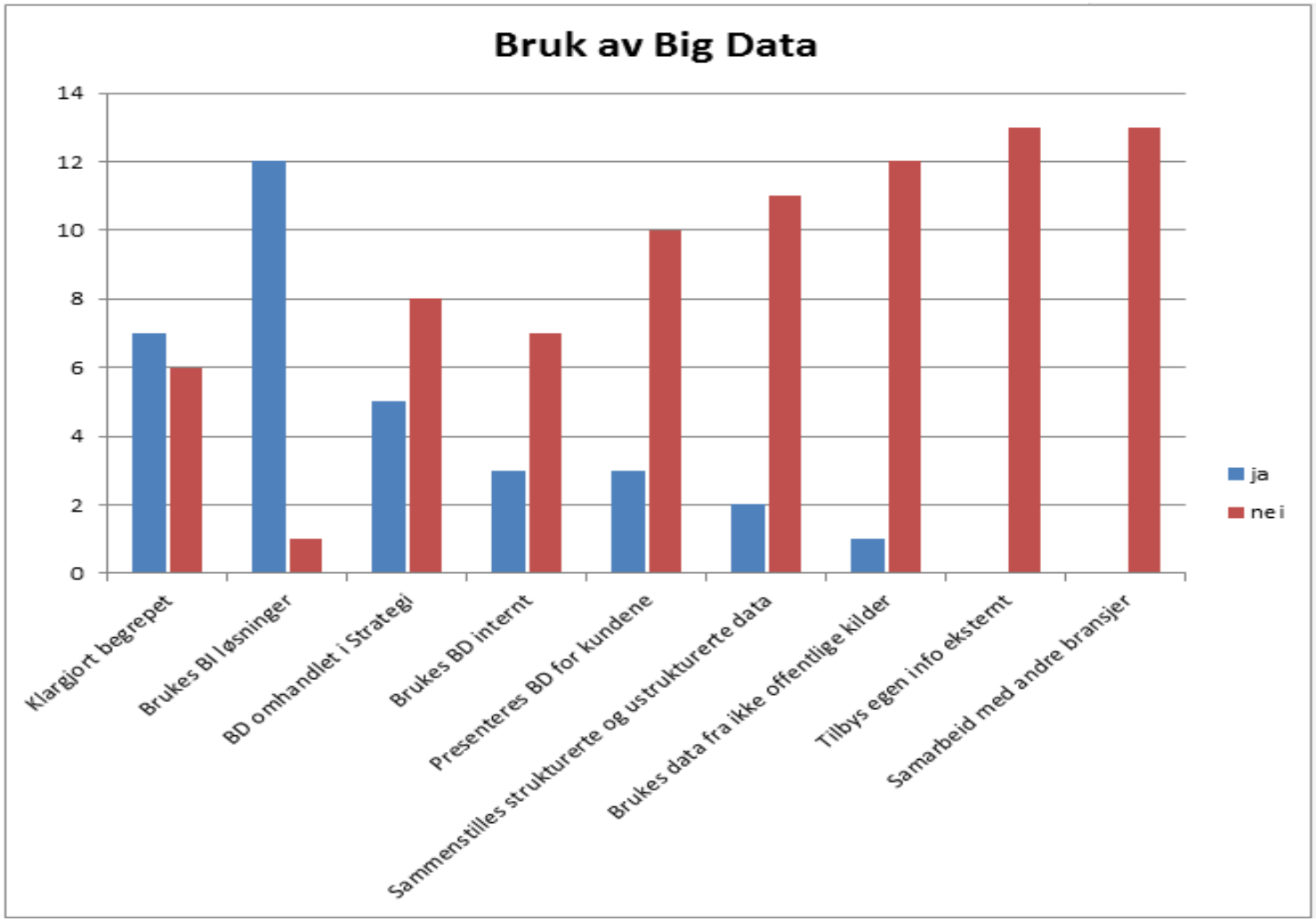
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Mobilbank
  - Stor økning i tjenestene
  - Mobiler med Android OS kan installere apper fra mange steder – risiko for piratversjoner
  - «Sandbox» - virtuell beholder (beskyttet område) som gir god sikkerhet hvis telefonen ikke er tuklet med.
- Ondsinnet programvare
  - Stor økning i phishing-forsøk
  - Bedre målretting i angrepene, og bedre språk

3.7.2 Big data (i norske banker)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Figur 2:



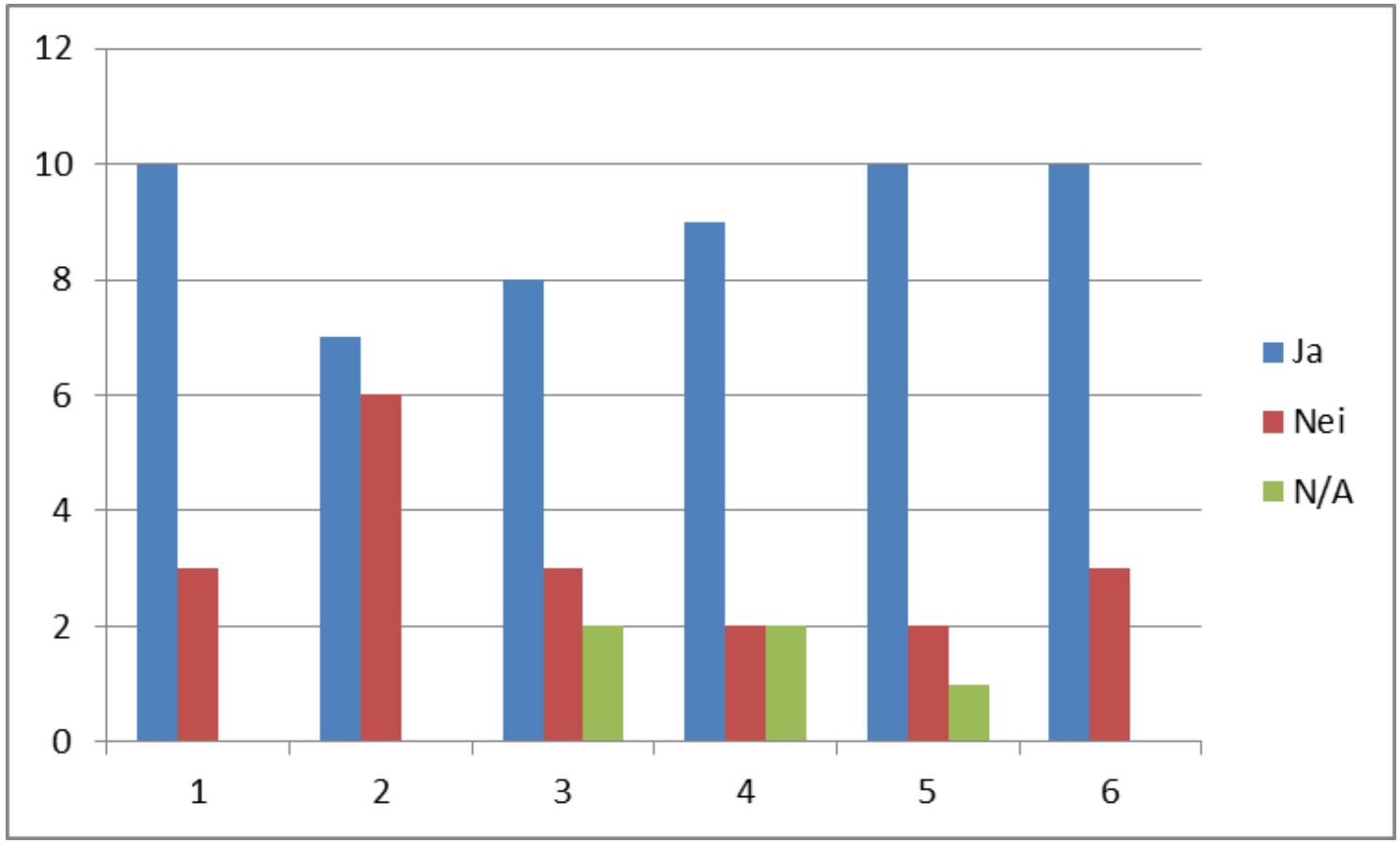
Kilde: Finanstilsynet

Spørreundersøkelse om skytjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Svarfordeling fra foretak om bruk/planer om bruk av skytjenester

Figur 3:



Kilde: Finanstilsynet

3.8 Utfordringer for forbrukerne

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Egne grenser for kunders egenandel ved misbruk som skyldes grov uaktsomhet kan ikke settes av det enkelte medlemsland.
- I Norge er det høy forbrukerbeskyttelse i gjeldende regelverk. Dette kan bli endret om forslag til samordnede regler for hele EØS-området blir vedtatt uendret.
- Betalingskort med RFID-chip kan åpne for en sårbarhet fordi kundene ikke kan nok om sikker bruk. Dersom hele lommeboka legges på kortleseren, kan kortleseren registrere alle de andre RFID-kortene i lommeboka. Ved bedrag vil ikke kortholder få melding om betalingstransaksjonen før konto kontrolleres.
- Kort med RFID-chip er klar for lesing, og funksjonen kan ikke skrus av. Det kan avlure PIN siden det ikke er begrensing i antall ganger kortet leses med feil PIN.

Utfordringer forts.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Noen konsekvenser for kundene kan bli:

- Økt bruk av kontaktløs betaling vil gjøre betalingsoversikten fra banken omfattende, og mange forbrukere vil aldri oppdage falske betalinger av små beløp.
- Når en forbruker oppdager en suspekt betaling, må de gjennom en relativt lang prosess for å få tilbake pengene samtidig som kunden ofte får lite informasjon som grunnlag for å kreve refusjon. Det kan også være tidsfrister og tungvinte rutiner ved klagebehandling.
- For å kunne vurdere bankutskriftene, må kunden ha noe å avstemme disse i forhold til, f.eks. kvitteringer.

3.9 Virtuelle valutaer (Bitcoin)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Finanstilsynet advarer mot virtuelle valutaer

- Du kan tape pengene dine på vekslingsplattformen.
- Pengene dine kan stjeles fra den digitale lommeboken din.
- Du er ikke beskyttet når du bruker Bitcoins som betalingsmiddel.
- Verdien av dine Bitcoins kan endres raskt, og kan til og med falle ned til null.

Finanstilsynet deltar i EBAs vurderinger av om virtuelle valutaer skal reguleres.

4. Finanstilsynets funn og observasjoner

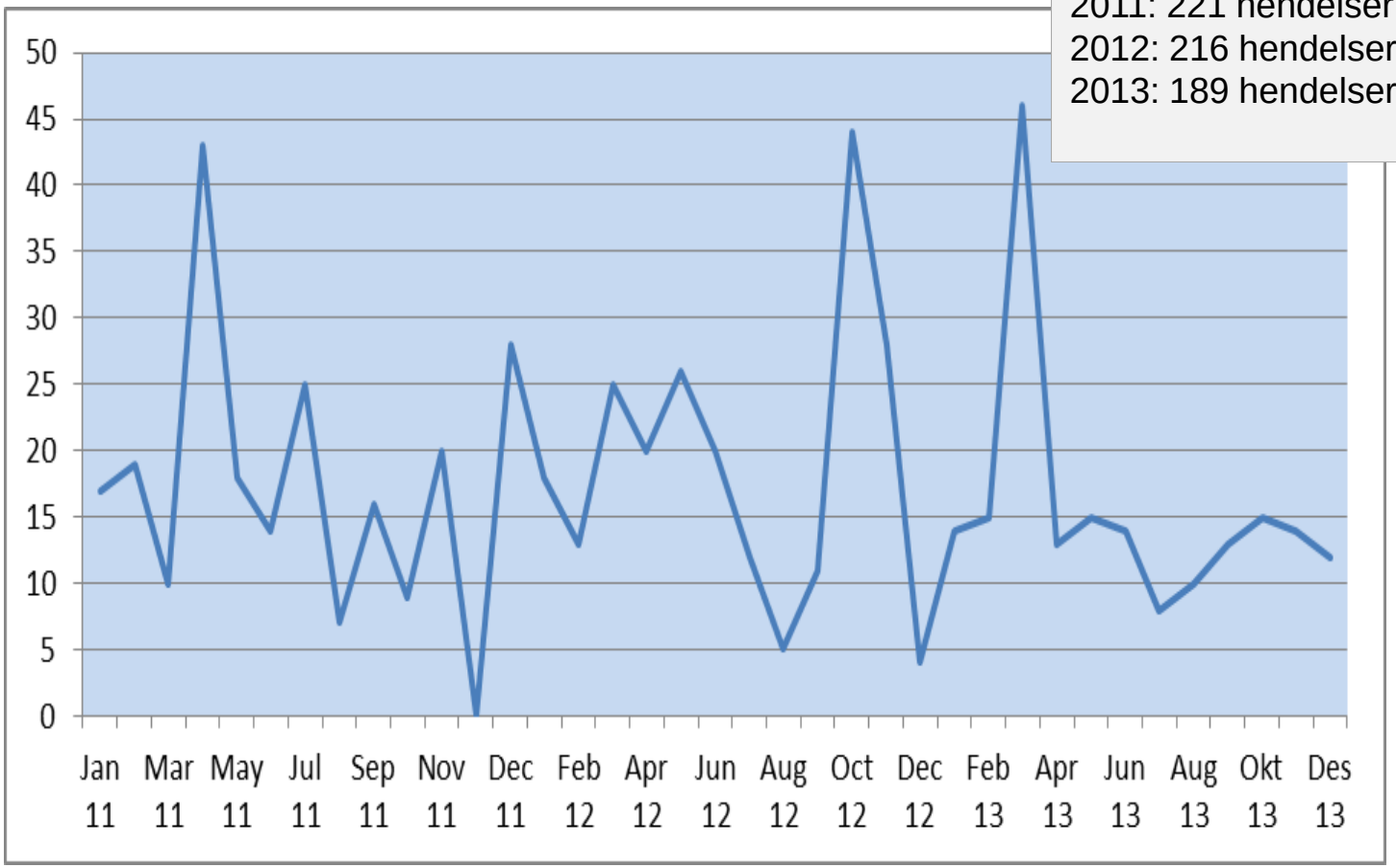
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Funn fra IT-tilsyn i 2013
2. Foretakets egne vurderinger
3. Rapporterte hendelser i 2013
4. Risikoområder identifisert fra andre kilder
   - Intervju med sikkerhetsselskaper
   - Rapporter fra internasjonale sikkerhetsorganisasjoner

Antall rapporterte hendelser i perioden 2011–2013

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

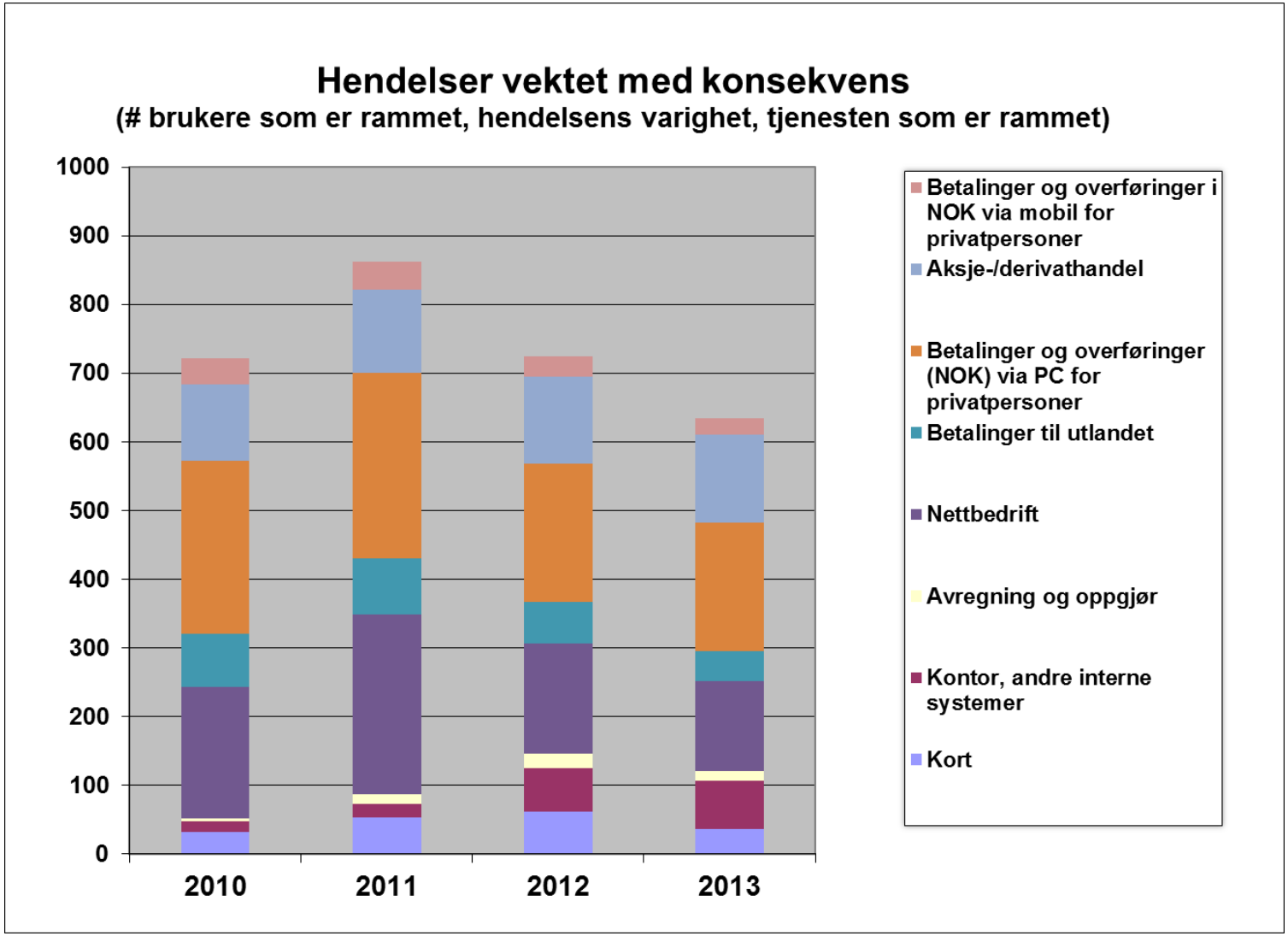
Figur 4:



Kilde: Finanstilsynet

Hendelser vektet med konsekvens

Figur 6:



Kilde: Finanstilsynet

5. Risikoområder 2013

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1	Omfattende endringer i IT-virksomheten →
2	Samhandling mellom flere aktører →
3	Mangelfulle risikovurderinger →
4	Angrep mot betalingstjenestene ~
5	Risiko fra eldre design og gamle komplekse systemer →

5. Risikoområder 2013

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Omfattende endringer i IT-virksomheten

- IT-driftssiden
- IT-forvaltning/vedlikehold
- Endringer i systemporteføljen
- Nye aktører for utvikling
- Endringer driftsleverandører

5. Risikoområder 2013 forts.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

2. Samhandling mellom flere aktører

- Nye aktører krever opplegg for samhandling og at flere blir involvert i kjeden.
- Dette kan gjelde både teknisk og i operasjonen og kan føre til uklare ansvarsforhold.
- Samlet kan dette øke sårbarheten i driften.

5. Risikoområder 2013 forts.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

3. Mangelfulle risikovurderinger

- Ta stilling til bruk av metodeverk og aktuelle standarder.
- Sikre at nødvendig kompetanse blir allokert.
- Ha en klar avgrensning (scope) av hva som skal risikovurderes.
- Etablere plan for gjennomføring.
- Klargjøre hvordan sikre nødvendig kvalitet.
- Mangelfulle eller risikoanalyser kan gi økt risiko.

5. Risikoområder 2013 forts.

Bruk av standarder for ROS-analyser

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

ISO 31000: 2009 Risikostyring Prinsipper og retningslinjer

ISO 31010: 2009 Risikostyring Metoder for risikovurdering

ISO/IEC 27005 provides guidelines for information security risk management

NIST Special Publication 800-30 Guide for Conducting Risk Assessments (USA)

COSO 2004 - Enterprise Risk Management - Integrated Framework

COBIT 5 framework, and Risk IT

NS 5814:2008 Norsk standard som favner vidt

5. Risikoområder 2013 forts.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

4. Angrep mot betalingstjenestene

- Angrep mot nettbanker
- Økt phishing-aktivitet
- Angrep mot minibanker
- Bruk av falsk informasjon i nettbutikker («card-not-present»)
- Angrep mot EFT-/POS-løsninger

Tiltakene i Norge har foreløpig bidratt til at tapene er på et akseptabelt nivå. Det skaper allikevel stor utrygghet for brukere av betalingstjenester som blir utsatt for angrep.

5. Risikoområder 2013 forts.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

5. Risiko fra eldre design gamle og komplekse systemer

- Mange sentrale løsninger er fra 1980- og -90-årene.
- Modernisering skjer i stor grad på utsiden.
- Teknologi og kompetanse kan bli vanskelig å opprettholde.
- Å vente for lenge kan representere en risiko – økt kompleks drift.
- Viktig med statusanalyser og klargjøring av problemstillinger.
- Flere banker og andre finansforetak har nå prosesser igangsatt for å skifte løsninger.

6. Finanstilsynets oppfølging

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. IT-tilsyn og annen kontakt med foretakene
2. Arbeid med betalingssystemer
3. Regelverksutvikling i Norge
4. Hendelsesrapportering
5. Beredskapsarbeid
6. Videreutvikling av tilsynsverktøy

7. Betalingssystemer og utvikling

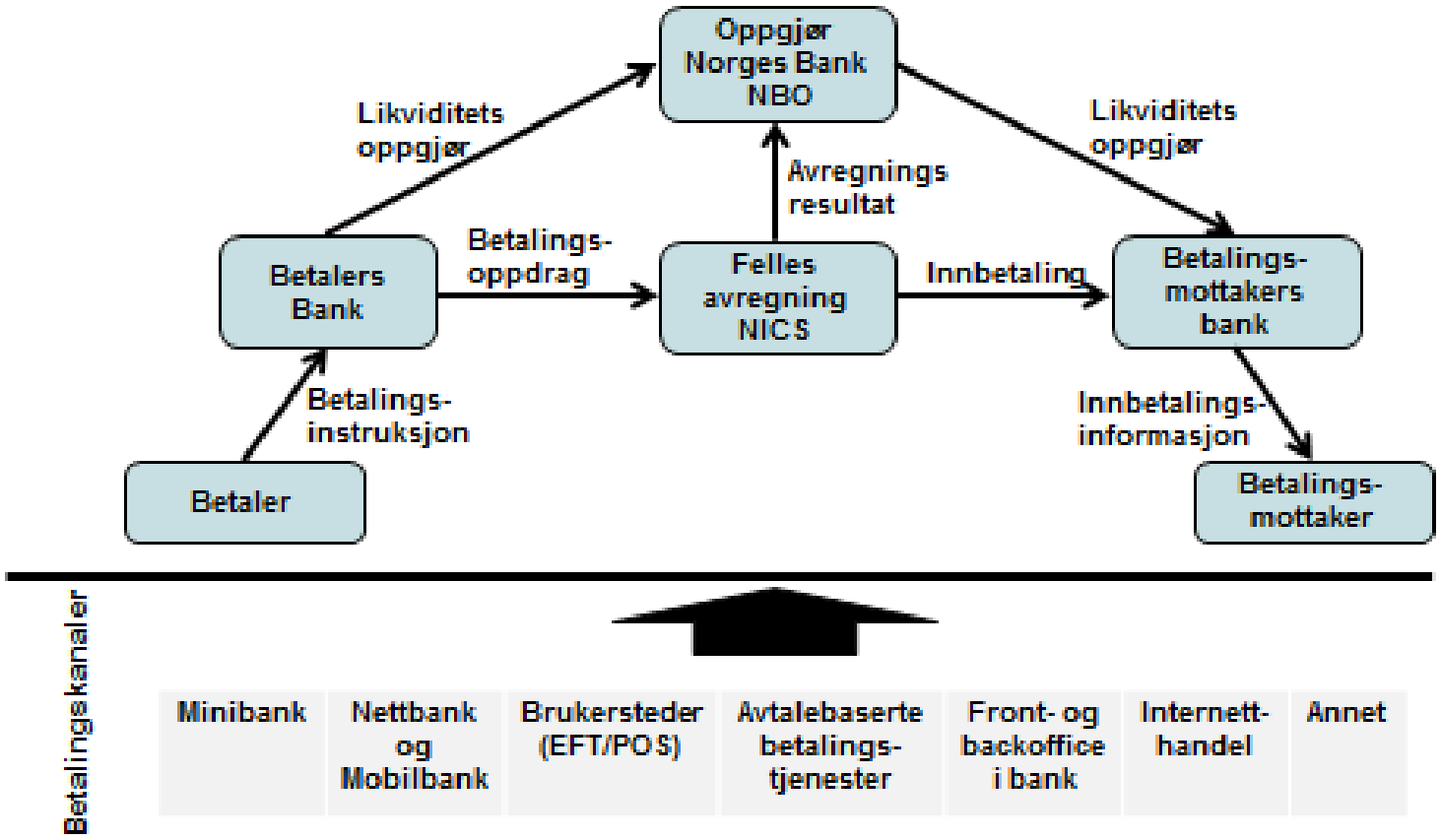
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Generelt om betalingssystemer
2. Risiko og sårbarhet i betalingssystemene
3. Styring og kontroll med betalingssystemene
4. Meldeplikten for betalingstjenester
5. Oversikt over årlige tap knyttet til betalingstjenester
6. Nettverk, mobil-vett og kort-vett
7. Regelverksutvikling i EU

Transaksjonsflyten i det norske betalingssystemet - Figur 7:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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



Stabilt

Flere hendelser

Tap ved bruk av betalingskort

(tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 1:

Svindeltype betalingskort	2011	2012	2013
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	24 190	35 701	51 954
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308	762
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869	51 534
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128	21 274
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544	9 570
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603	4 949
Totalt	125 718	135 153	140 043

Kilde: Finanstilsynet

Antall betalingskort rammet av misbruk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 2:

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

Totaltapet på kortsvindel økte noe i 2013. Det var en betydelig økning i svindel av typen «card-not-present» (CNP), mens det var en reduksjon i tapene knyttet til andre typer kortsvindel.

Kilde: Finanstilsynet

Tap ved bruk av nettbank

(tall i hele tusen kroner)

Tabell 3:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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

Kilde: Finanstilsynet

Phishing-angrep mot britiske banker

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Number of phishing websites targeted against UK banks and building societies by month 2005-2012

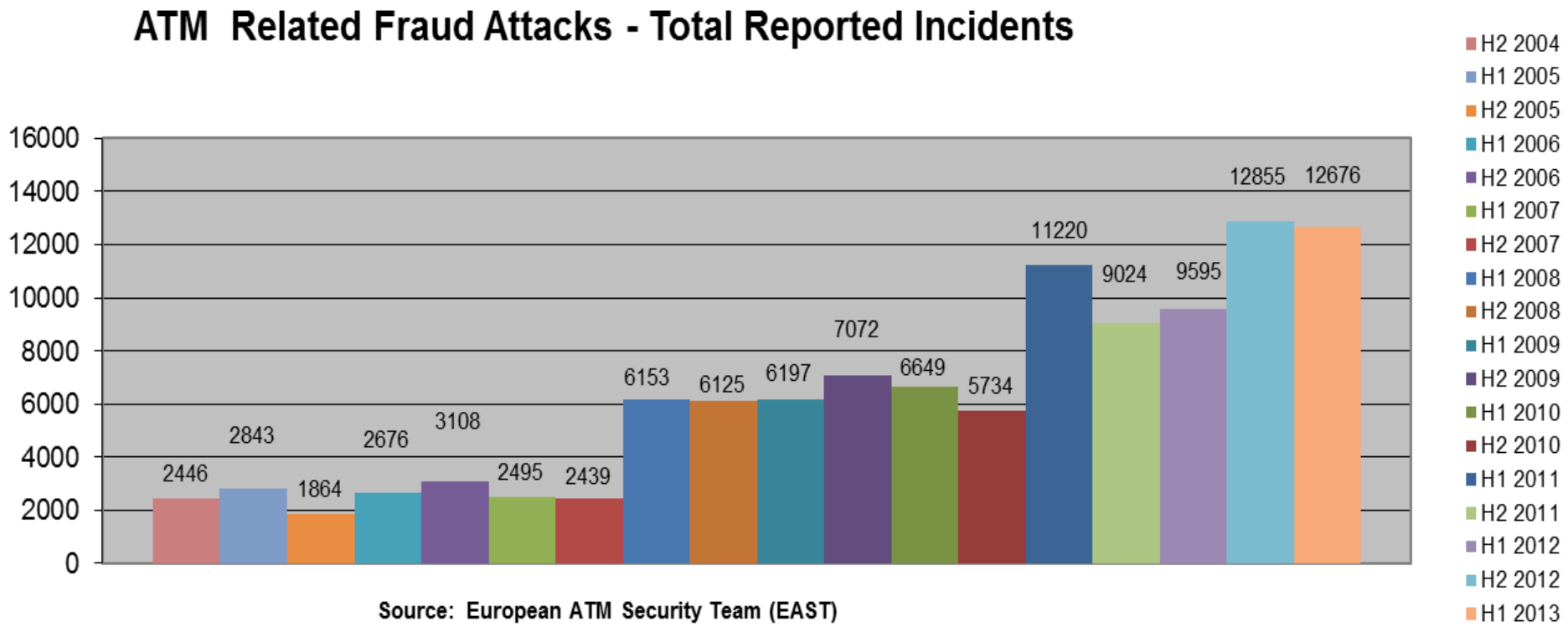
	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2012	18,252	6,629	14,362	20,669	24,578	26,818	39,767	41,734	27,869	30,036	3,523	2,404	**256,641**
2011	5,803	5,757	6,828	5,698	6,216	6,896	7,402	8,062	23,083	9,397	15,395	10,749	**111,286**
2010	2,654	3,135	4,810	4,335	5,406	5,277	5,873	5,861	5,689	6,977	4,552	7,304	**61,873**
2009	4,206	5,161	5,004	3,422	3,917	4,335	4,415	4,845	3,900	4,903	4,191	5,864	**51,161**
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	**43,991**
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	**25,797**
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	**14,156**
2005	18	29	27	54	72	122	153	160	190	267	255	353	**1,700**

Kilde: Financial Fraud Action UK

Minibankrelaterte svindelangrep innenfor EØS-området

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Figur 9:

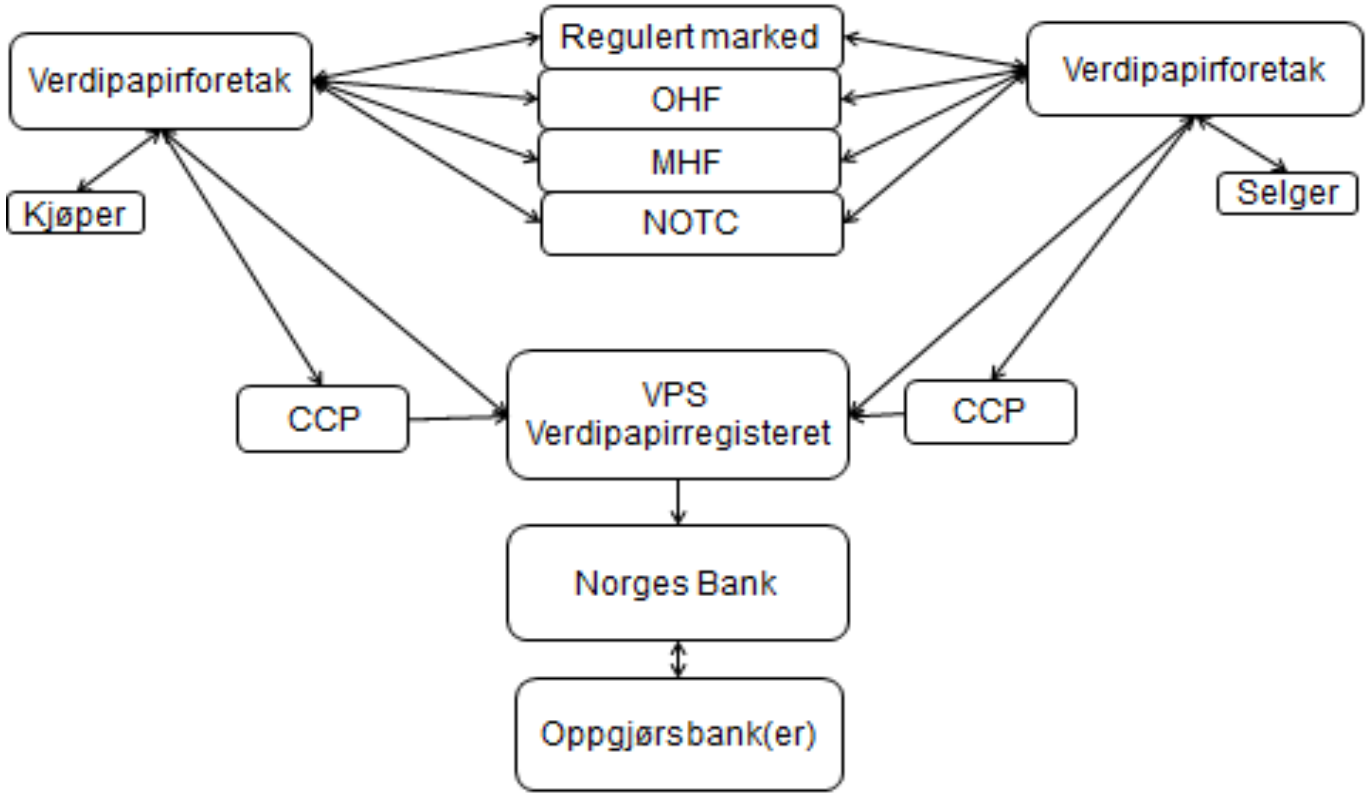


Kilde: EAST

Roller og sammenhenger i verdipapirsektoren

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

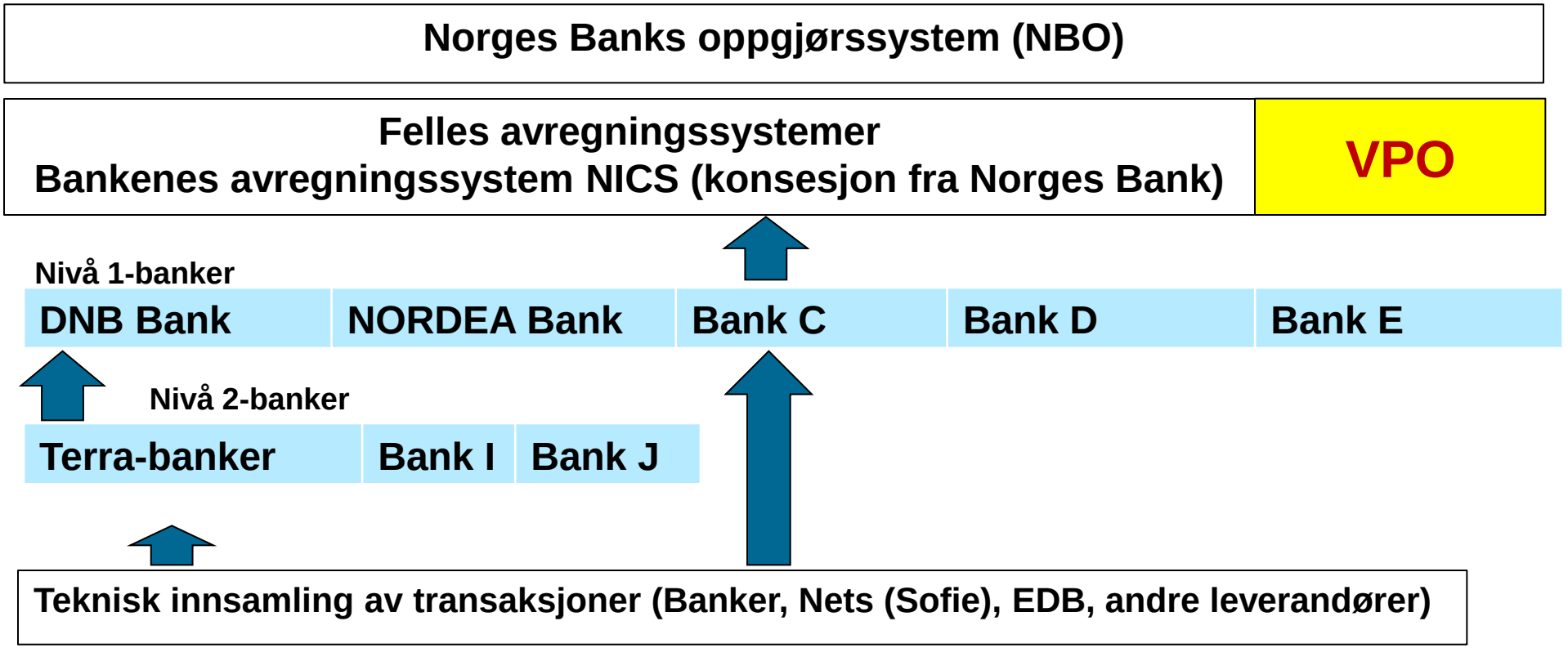
Figur 11:



Kilde: Finanstilsynet

Transaksjonsflyten fra der den oppstår, innsamling, avregning og oppgjør

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



8. Verdipapirområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Risiko for underinvestering ved redusert inntjening
2. Risikoer i forbindelse med algoritmehandel
3. Backoffice-systemer i verdipapirmarkedet
4. Utkontraktering av kjernesystemer
5. Konsentrasjonsrisiko på nettverksinfrastrukturen
6. Regelverksutvikling i EU
7. Verdipapirforetakenes håndtering av sensitive selskapsdata på IT-systemer
8. Risiko ved endringer av sentrale infrastrukturkomponenter for verdipapiromsetning

FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Takk for oppmerksomheten!

Frank Robert Berg

FINANSTILSYNET
Seksjon for tilsyn med IT og betalingstjenester

E-post: frb@finanstilsynet.no