KREDITTILSYNET
The Financial Supervisory Authority of Norway

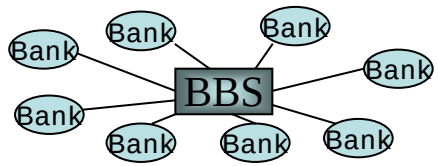
Sikkert som banken?
Hva IT-tilsyn er godt for

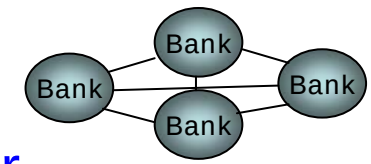
Annikken Seip
Seniorrådgiver IT-tilsynet
Abelia, 22. september 2005

Det jeg skal snakke om

- Kredittilsynet og IT-tilsyn
  - Hva vi fører tilsyn med, hensikt
  - Tilsynsmetoder,
  - Selvdeklarasjon vs. andre former for evaluering av sikkerhetstjenester
- Risikovurderinger
  - Hvor er finansinstitusjoner sårbare reint IT-messig?
- Nye betalingstjenester, betalingsinstrumenter og betalingssystemer,
  - Integrasjon med nye elektroniske tjenester, og
  - Manglende standarder.

Finansiell infrastruktur og bruk av informasjonsteknologi i Norge





- Samarbeid og standardisering, virker det fortsatt?
- Felles løsninger og samarbeid mellom bankene og operatørene; BBS/BankAxept, VPS og Oslo Børs
- Stor grad av standardisering mot kunder: minibanker, EFT/POS, kortbruk og girotjenester
- Offensiv bruk av nye distribusjonskanaler; Nettbank, hva med standardisering her? BankID, kan det gi svar?
- Nye tjenester og bruk av mobile enheter og bredbånd RFID-brikker.
- Nye samarbeids- og eierkonstellasjoner; nordiske banker
- Store endringer på leverandørsiden ?
- Standardisering; internasjonalt, europeisk og nasjonalt?

Regelverk

Omfattende lovverk som regulerer finansforetakene.

Almenaksjeloven

Lov om forretningsbanker / Lov om sparebanker

Lov om finansieringsvirksomhet

Personopplysningsloven/-forskriften

Hvitvaskingsloven/-forskriften

Lov om Betalingssystemer mv

Kredittilsynsloven

Verdipapirhandelsloven

Div forskrifter om representasjon i bankers styrende organer

Internkontrollforskriften

IKT-forskriften

Noen aktører/roller

- Foretakets egne styrende organer
- Intern revisjon
- Ekstern revisjon
- Ulike felles arenaer; FNH, Sparebankforeningen, BSK, ulike felles utvalg
- Finansdepartementet
- Kredittilsynet
- Norges Bank
- Datatilsynet
- BFI - Bankenes Beredskapsutvalg for den finansielle infrastruktur
- KIS - Koordineringsutvalget for informasjonssikkerhet
- Andre aktører innen informasjonssikkerhet, DSB og NSM

Kredittilsynet

- Kredittilsynsloven
  - Tilsynet skal se til at de institusjoner det har tilsyn med, virker på hensiktsmessig og betryggende måte i samsvar med lov og bestemmelser gitt i medhold av lov samt med den hensikt som ligger til grunn for institusjonens opprettelse, dens formål og vedtekter.
- IT-tilsynets virkemidler
  1. Regelverksutvikling/oppfølging
     - IKT-forskriften
     - Lov om Betalingssystemer mv,
       - Meldeplikten vedrørende systemer for betalingstjenester
  2. IT-tilsynsopplegget
     - Basert på IT-prosesser og internasjonal metodeverk CobiT (ISACA)
       Utviklet egenmelding med ca 180 kontrollspørsmål
     - Videreutvikle mot utvalgte tema; brannmur, virusbeskyttelse, katastrofe, og betalingssystemer (internett som infrastruktur)
  3. Risiko- og sårbarhetsanalyse
  4. Samarbeid/allianser, nasjonalt og internasjonalt

Planlegging og Organisering:

PO1 Definere IT-strategi
PO2 Definere informasjon og systemarkitektur
PO3 Bestemme teknologisk retning
PO4 Utforme IT-organisasjonen
PO5 Forvalte IT-investeringer
PO6 Formidle ledelsens mål og retning
PO7 Personalledelse
PO8 Sikre etterlevelse av eksterne krav
PO9 Risikovurdering
PO10 Prosjektstyring
PO11 Kvalitetsstyring

Anskaffelse og implementering:

AI1 Identifisere løsninger
AI2 Anskaffelse og vedlikehold av applikasjoner
AI3 Anskaffelse og vedlikehold av teknologisk infrastruktur
AI4 Utvikle og vedlikeholde prosedyrer
AI5 Installasjon og godkjenning av systemer
AI6 Endringsledelse og -håndtering

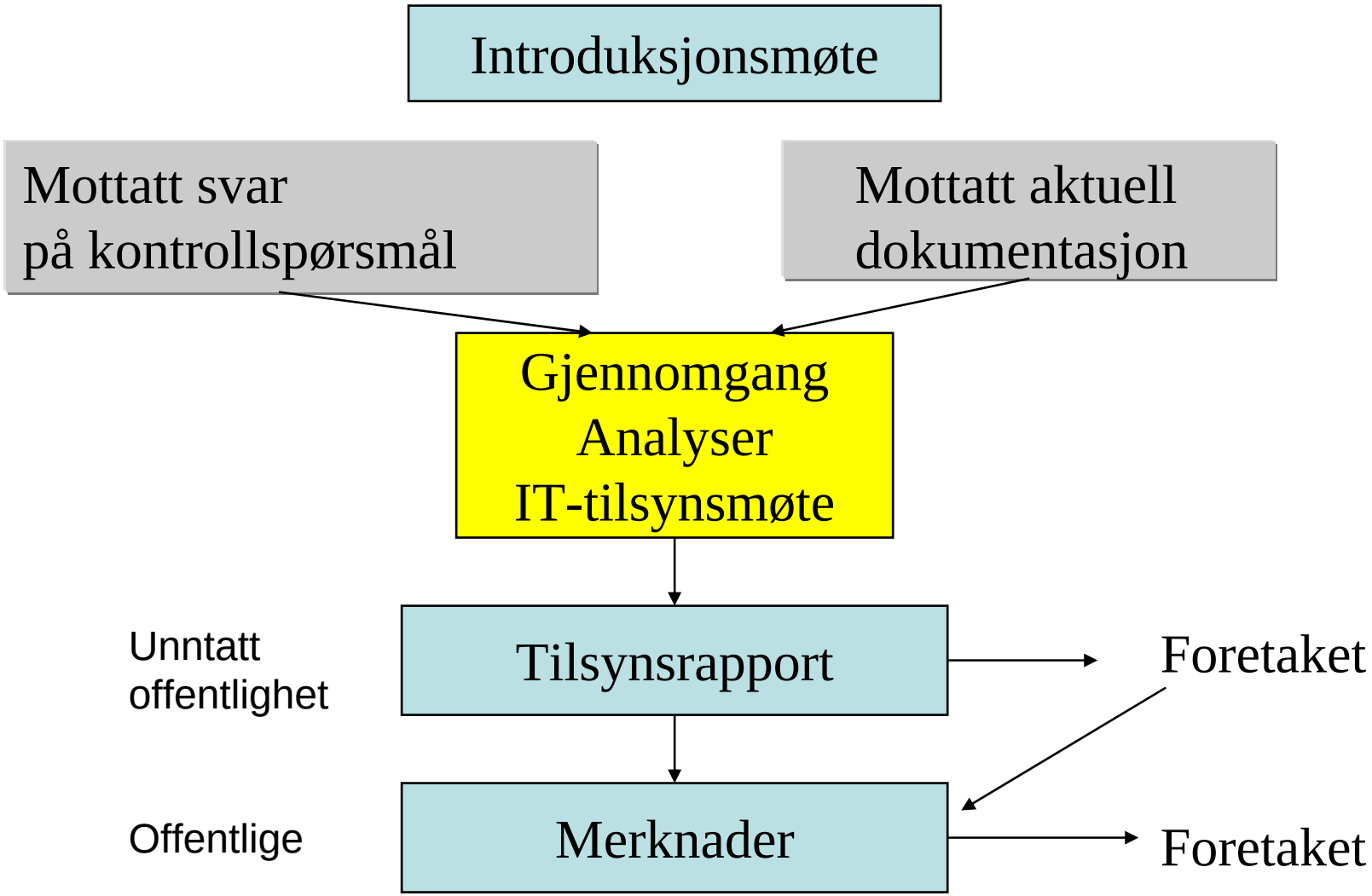
Leveranse og Støtte:

DS1 Definere og styre servicenivået
DS2 Styre tjenester fra eksterne IT-leverandører
DS3 Styring av ytelse og kapasitet
DS4 Sikre kontinuerlig service-/kriseplanlegging
DS5 Sikre systemsikkerhet
DS6 Identifisere og fordele kostnader
DS7 Brukeropplæring
DS8 Assistere og informere kunder
DS9 Konfigurasjonshåndtering
DS10 Håndtering av problemer og hendelser
DS11 Håndtering av data
DS12 Styring av fasiliteter
DS13 Styring av driften

Overvåkning:

M1 Overvåke prosessene
M2 Vurdere intern kontrollen
M3 Gjennomføring av uavhengig bekreftelse
M4 Sørge for uavhengig revisjon

IT-tilsyn


Introduksjonsmøte
Mottatt svar
på kontrollspørsmål
Mottatt aktuell
dokumentasjon
Gjennomgang
Analyser
IT-tilsynsmøte
Unntatt
offentlighet
Tilsynsrapport
Foretaket
Offentlige
Merknader
Foretaket

Utvidelse av IT-tilsynsopplegget

34 prosesser – 180 kontrollspørsmål

Katastrofebackup -26

VIRUS beskyttelse - 137

Betalingssystemer - 57

Nettbank - 46

Hvitvasking - 26

A) Testing	J	N
A 1 Er det gjennomført tilstrekkelige funksjonelle tester?		
A 2 Er det gjennomført fullverdig regresjonstest i produksjonslikt miljø?		
A 3 Er det gjennomført volum og ytelsestester?		
A 4 Er det gjennomført test av migrerings- rutiner fra test til produksjonstest-miljø?		
A 5 Er testene gjennomført på siste versjon av systemkomponenter iht.produksjonskonfigurasjonen?		
A 6 Er det gjennomført ende-til-ende test med alle relevante eksterne aktører?		
A 7 Er det gjennomført test av evt. konverteringsrutiner?		
A 8 Er det gjennomført test av driftsopplegg og driftsrutiner?		
A 9 Er alle avvikssituasjoner testet mht. varsling, recovery og restart?		

Brannmur - 24

System for IRB modellering

Meldeplikt betalingstjenester

aks@kredittilsynet.no

Tillit til systemer, produkter og organisasjoner

1. Stole på leverandørens forsikringer
2. Utføre egne tester
3. Få uttalelser fra en tredje part.

Selvdeklarasjon kan baseres på alle tre punktene.

Tredjeparten i punkt 3 kan være

- En bekjent, som bruker det samme systemet,
  eller
- Et uavhengig, tiltrodd, organ
  som er akkreditert til å utføre evalueringer og sertifiseringer

Selvdeklarasjon vs. sertifisering

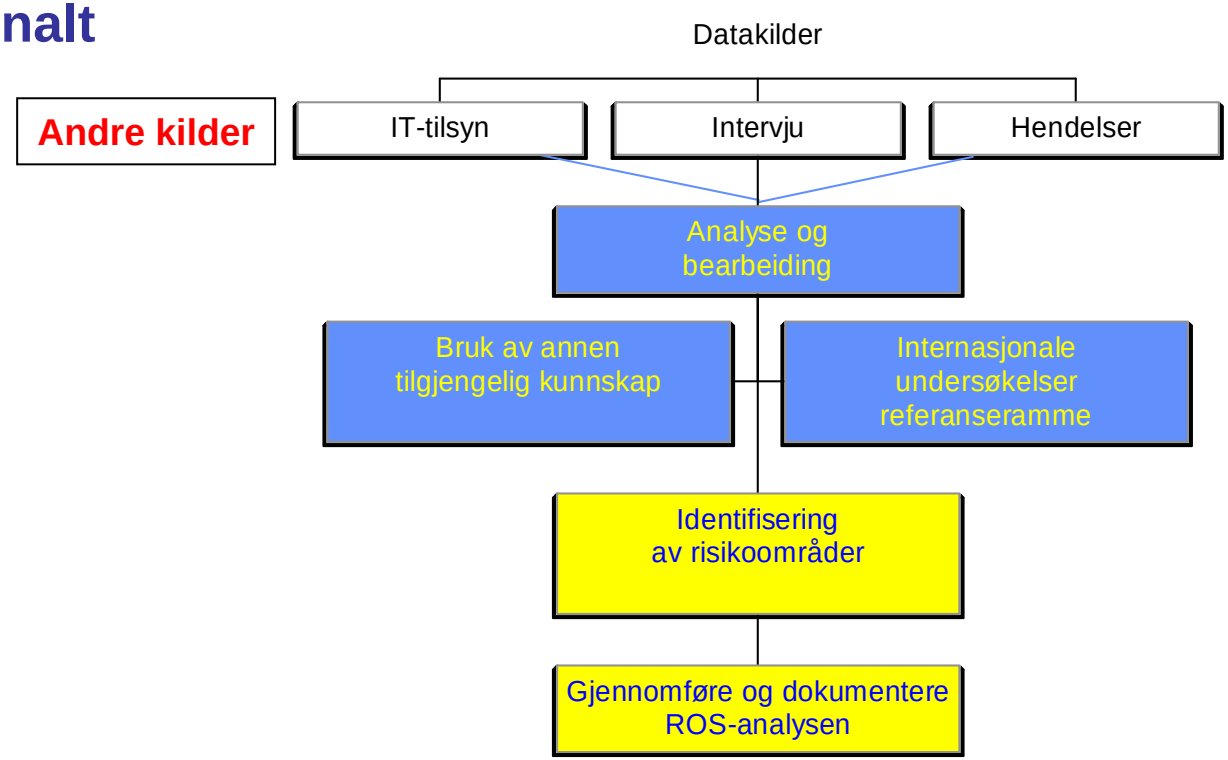
- Mer subjektivt
- Foretaket må tenke selv
  - Setter ned prosjekt
- Standard opplegg
- Ikke alle spørsmål passer
- Overordnete spørsmål
- Uklart formulert
- Misforstår
- Må kombineres med
  - annen dokumentasjon og
  - med intervju
- Dekker mer enn sikkerhet

- Mer objektivt
- Koster tid og penger
  - Det meste skal likevel gjøres
- Bare sikkerhet
- Internasjonalt anerkjent
  - Mai: 867 institusjoner i Japan er sertifisert etter IS 17799
  - Mange sertifisert etter CC

Risiko- og sårbarhetsanalyser

Kildegrunnlag:

1) **Gjennomførte IT-tilsyn i 2004**
2) **Strukturerte intervju med prioriterte foretak og personer**
3) **Registrerte hendelser, strukturerte og ustrukturerte**
4) **Informasjon fra samarbeidspartnere, nasjonalt og internasjonalt**



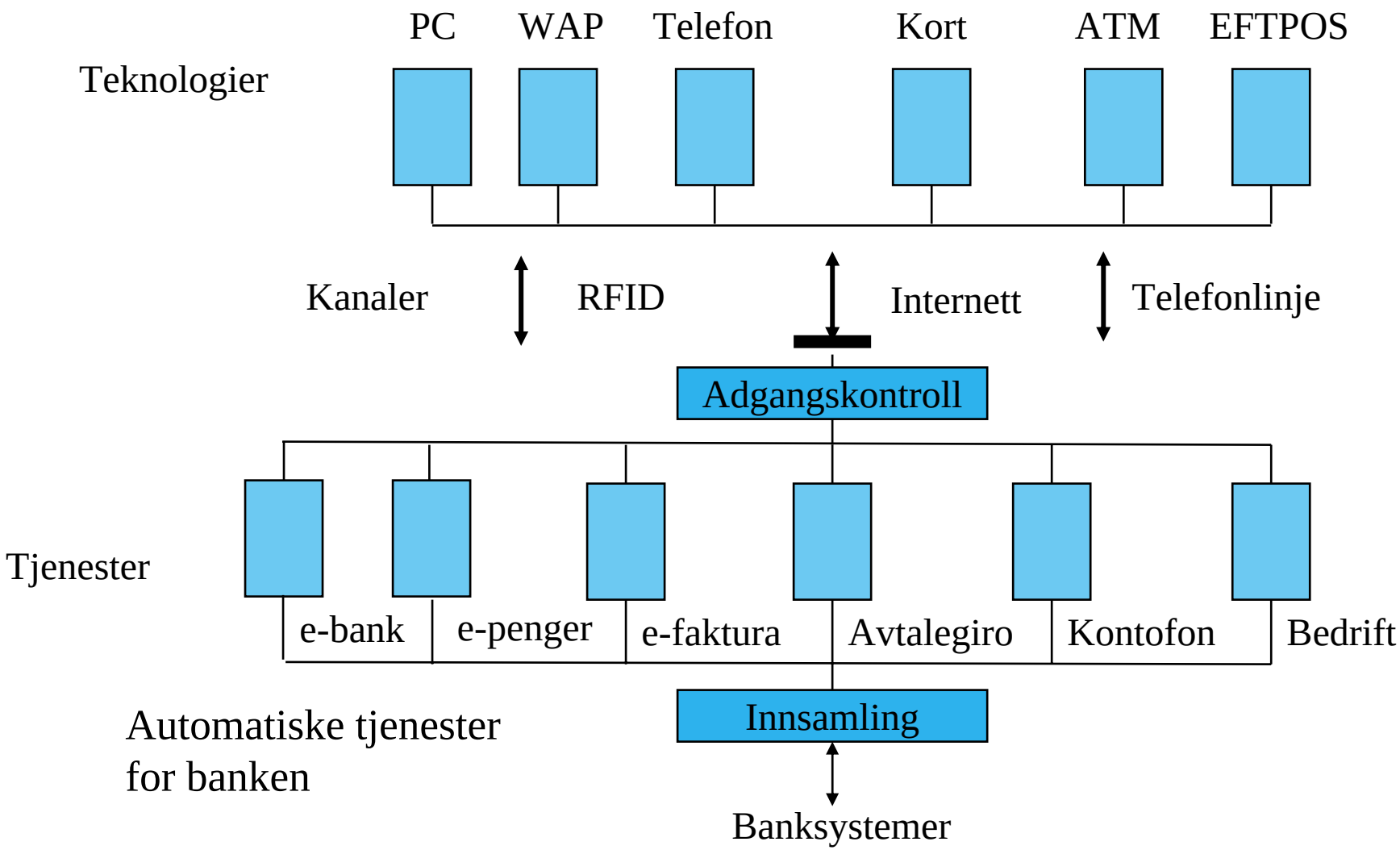
aks@kredittilsynet.no

4. Risiko- og sårbarhetsanalyse 2004

Resultater:

- ✓ Prosjektgjennomføring ved større IT-endringer
- ✓ Endringshåndtering og kontroll
- ✓ Virusbeskyttelse og brannmur
- ✓ Kontinuitets- og katastrofeløsninger
- ✓ Utkontraktering – flytting over landegrenser
- ✓ Bruk av Microsoft software og tilknytning til internett
- ✓ Leverandørkonsentrasjon, felles infrastruktur
- ✓ Ulike samarbeidskonstellasjoner og bruk av felles IT-løsninger
- ✓ Nettbankløsninger, autentisering og autorisasjon
- ✓ Gjennomføring av ROS-analyser
- ✓ Bruk av kredittkort i internetthandel

Elektroniske betalingstjenester



aks@kredittilsynet.no

Elektroniske betalingstjenester

- Elektroniske billetter i et lukket system
  - RFID
- Åpne betalingstjenester
- Vite at du handler
- Personvern
- Standarder
- Det offentliges deltakelse i standardarbeidet

Mobilhandelsmarkedet

Ferskt marked, mange konkurrenter

Teknologien kan brukes, men er fortsatt på vei

Teknologien er ikke helt den samme som for Internett,

- Restriksjoner på brukergrensesnitt, prosessorstørrelse, andre sikkerhetskonsepter, mange operatører

Andre verdikjeder, et ekstra lag mellom kunde og tjenesteyter

Kundenes oppførsel blir annerledes pga. andre muligheter