IT ADVISORY

IT-revisjon, Rev2403

Torkil Hindberg, Ansvarlig for IT-revisjon i KPMG
23.03.10

ADVISORY

Torkil Hindberg

- **Alder: 31 år**
- **Stilling: Senior Manager i IT Advisory i KPMG**
  - Ansvarlig for IT-revisjon
- **Utdanning:**
  - Siviløkonom
  - Mellomfag i Informatikk
- **Sertifisering:**
  - Certified Information Systems Auditor (CISA)

Agenda

- **IT-systemer og intern kontroll**
- **IT-revisjon**
  - Revisjon
  - Hva er IT-revisjon?
  - IT-revisjonsprosessen
- **Eksempel – salg**
- **Rammeverk og modeller for IT internkontroll og IT-revisjon**
- **Continuous monitoring**
- **Personvern**
  - Generelt om personvern
  - Spesielt om:
    - personalregister
    - Epost
    - Slettekrav

IT-systemer og intern kontroll

IT-systemer

IT-systemer er logikk!

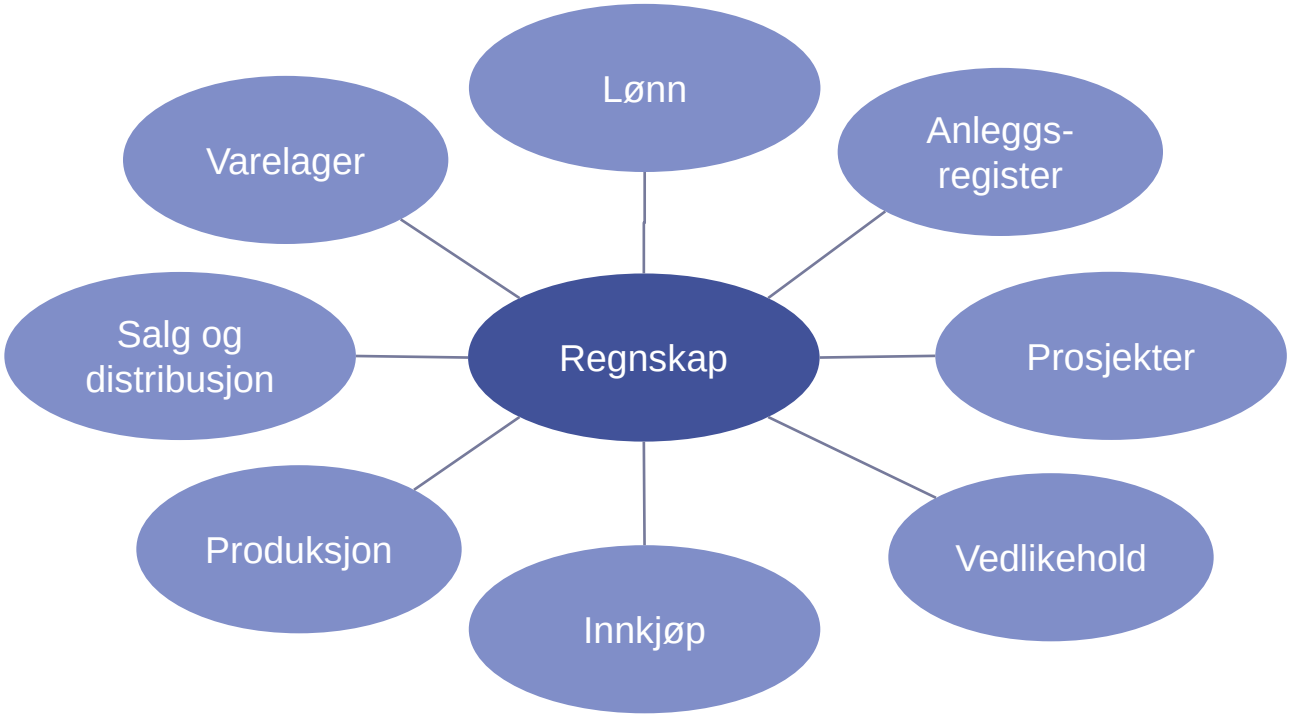
IT-baserte systemers natur

- Automatisk transaksjonsspor
- Ensartethet i behandlingen av transaksjoner
- Behov for sikring av variable data
- Sikker håndtering av behandlingsregler
- Sikring av faste data
- Arbeidsdelingsprinsipper implementert i systemet
- Sikring av grensesnitt

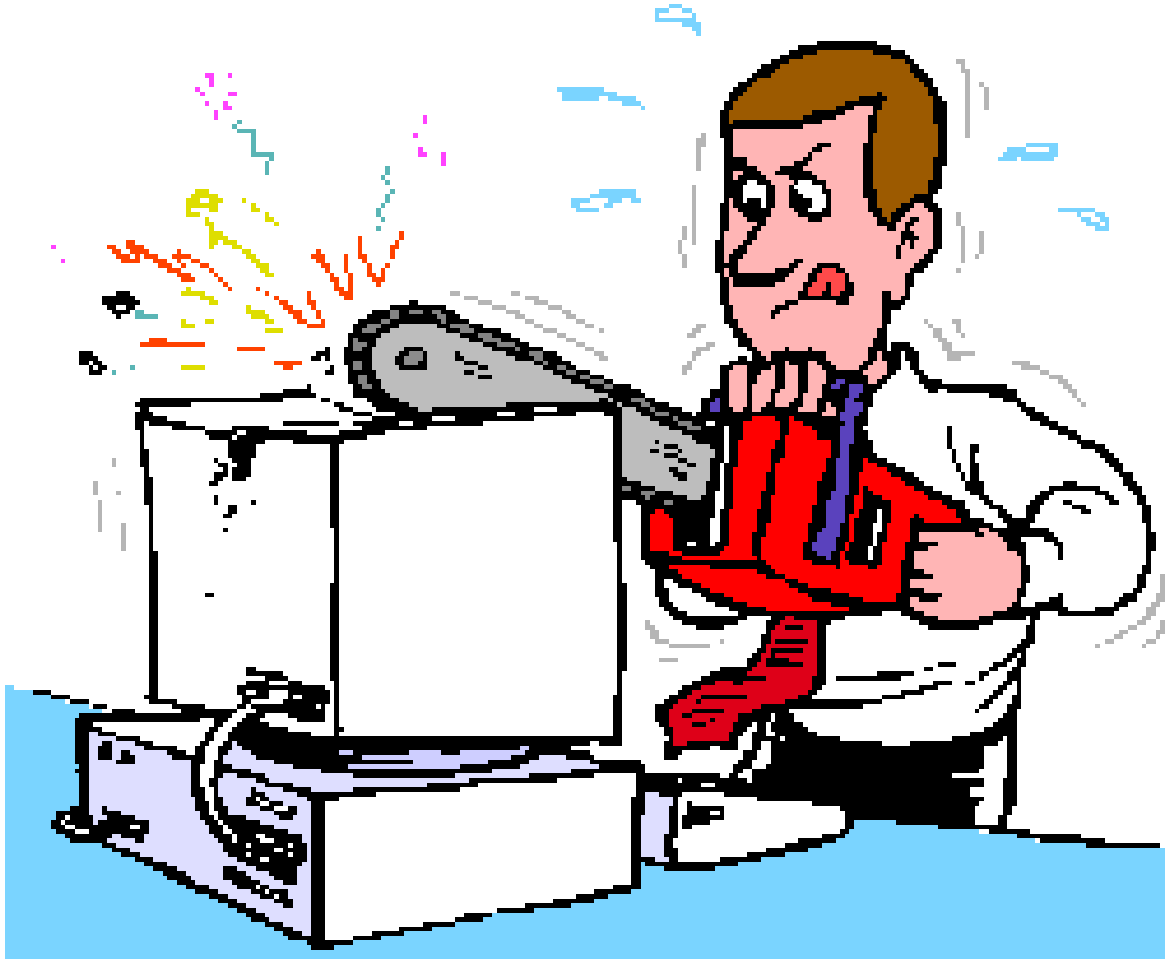
IT-baserte systemer

- **Enkle systemer med standard funksjonalitet**
  - Hovedbok
  - Kundereskontro
  - Leverandørreskontro
  - Rapporteringsmuligheter
- **ERP-systemer (Enterprise Resource Planning)**
  - Regnskapet er bare en liten del
  - Regnskapet får automatisk input fra flere forskjellige moduler som er integrert med regnskapet
- **Systemporteføljе satt sammen for å håndtere selskapets behov**

ERP-system



IT-revisjon



Hva er revisjon?

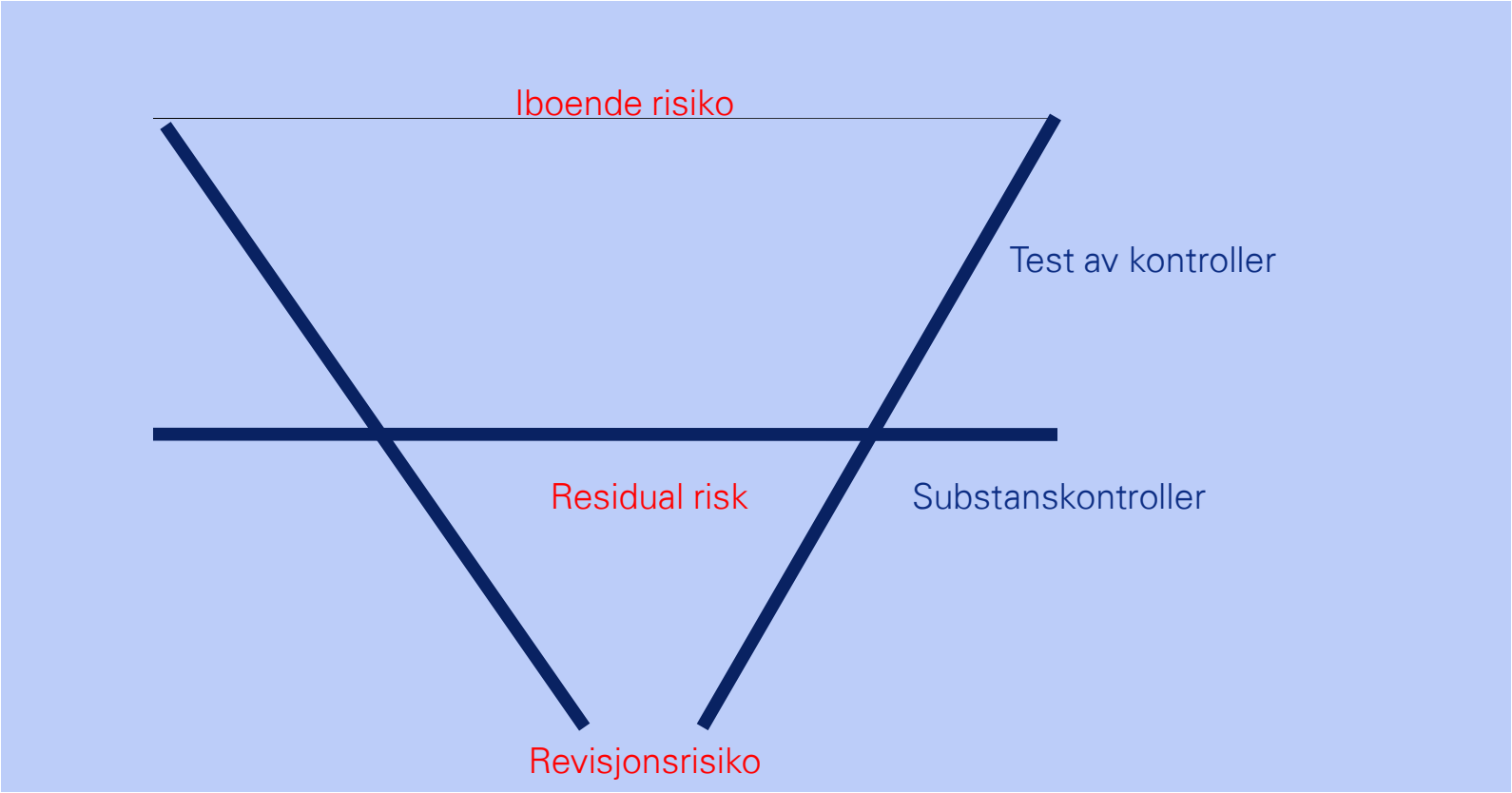
- **§ 5-1. Revisjonens innhold**
  - Revisor skal vurdere om årsregnskapet er utarbeidet og fastsatt i samsvar med lov og forskrifter, og om den revisjonspliktiges ledelse har oppfylt sin plikt til å sørge for ordentlig og oversiktlig registrering og dokumentasjon av regnskapsopplysninger i samsvar med lov og forskrifter. Revisor skal vurdere om opplysninger i årsberetningen om årsregnskapet, forutsetningen om fortsatt drift, og forslag til anvendelse av overskudd eller dekning av tap er i samsvar med lov og forskrifter, og om opplysningene er konsistent med årsregnskapet.
  - Revisor skal se etter at den revisjonspliktige har ordnet formuesforvaltningen på en betryggende måte og med forsvarlig kontroll.
  - Revisor skal gjennom revisjonen bidra til å forebygge og avdekke misligheter og feil.Revisorloven

Hva er revisjon?

- **Hensikten med revisjon er å gi brukerne en rimelig grad av sikkerhet for at årsregnskapet ikke inneholder vesentlige feil.**
- **”Forventningsgapet”**
- **Hvordan kan vi avgi en slik bekreftelse?**

Revisjonsrisiko

- ”Trakten”



IT-revisjon

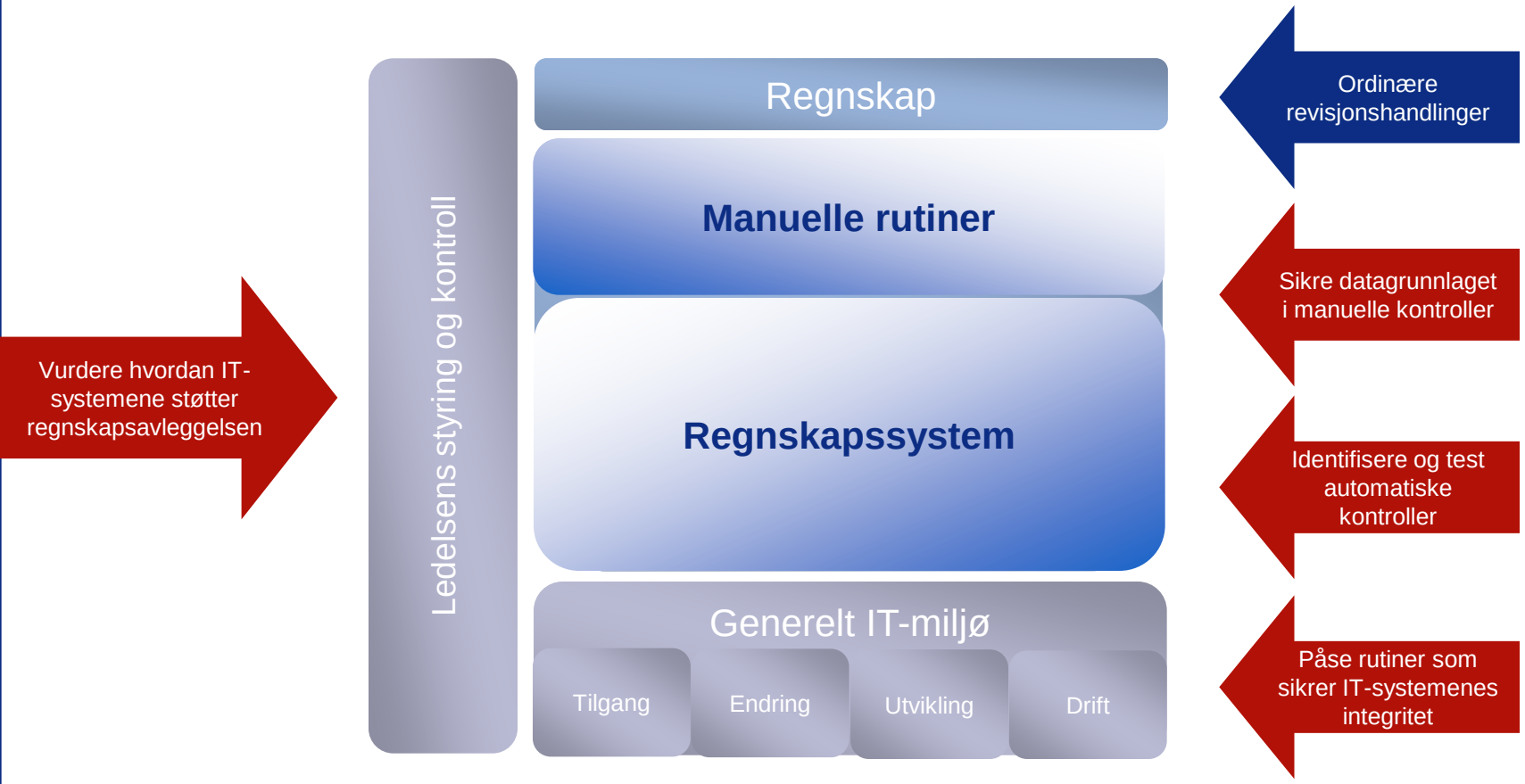
- **IT-revisjon som en del av finansiell revisjon er betegnelsen på metoder og revisjonshandlinger hvor man vurderer hvordan IT-systemene støtter opp under regnskapsavleggelsen.**

- **RS 315: Forståelse av foretaket og dets omgivelser og vurdering av risikoene for vesentlig feilinformasjon**
  - ”Revisor må opparbeide seg en forståelse av de delene av informasjonssystemet, herunder de tilknyttede forretningsprosessene, som er relevante for økonomisk rapportering…”

IT-revisjon

- **At foretaket anvender IT kan ha stor innvirkning på de metodene revisor benytter i sitt arbeid**
  - Påvirker iboende risiko og kontrollrisiko
  - Gir muligheter og begrensninger i forhold til tilgjengelige regnskapsopplysninger
- **Bedre effektivitet og kvalitet:**
  - Enkelt bekrefte rutinetransaksjoner ved å bygge på automatiske kontroller i IT-systemene
  - Anvendelse av dataanalyser som verktøy gir bedre effektivitet og kvalitet i substanskontrollene
- **Blir kompleksiteten for stor må ekspert involveres**

Integrert IT-revisjon - prosess

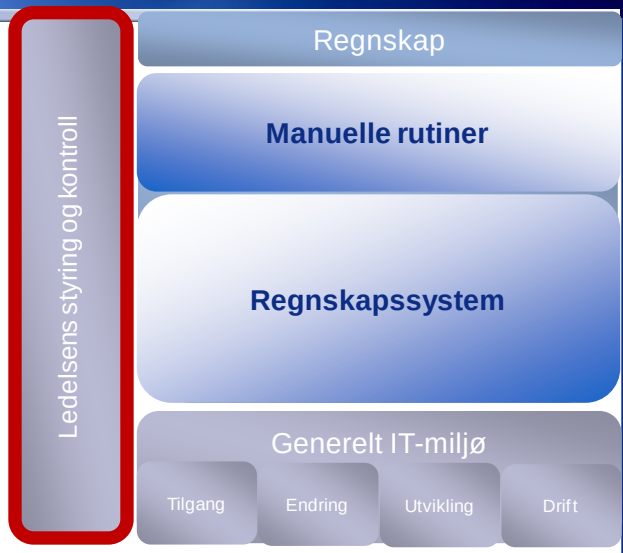


"IT- og finansiell revisor kompletterer hverandre og sikrer en målrettet og effektiv revisjon"

Forståelse av hvordan IT-systemene benyttes

- **Kartlegging av hvilke IT-systemer som benyttes og hvilke saldoposter de støtter?**
- **IT-systemenes art**
  - Standard
  - Tilpasset
  - Egenutviklet
- **Antallet systemer**
- **Homogen vs heterogen systemportefølje**
- **Integreringsgrad**
  - manuelle vs automatiske grensesnitt

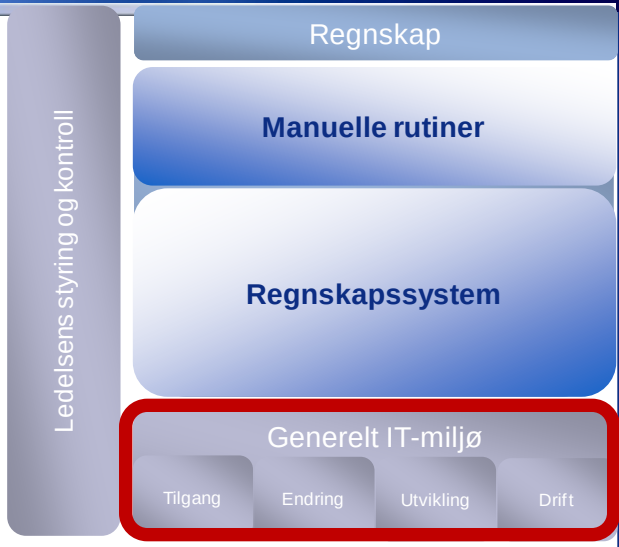
IT-relaterte kontroller på foretaksnivå



- **Målsetting:**
  - Påse at selskapets IT-systemer støtter opp under finansiell rapportering
- **Eksempler på kontroller**
  - IT-strategi som støtter forretnings-strategien
  - Avtaler med serviceorganisasjoner
  - Tilstrekkelig IT-kompetanse i bedriften
  - Policyer for sikkerhet, drift og endringer i IT-systemene
  - Organer for styring og kontroll av IT i selskapet

Generelle IT-kontroller (ITGC)

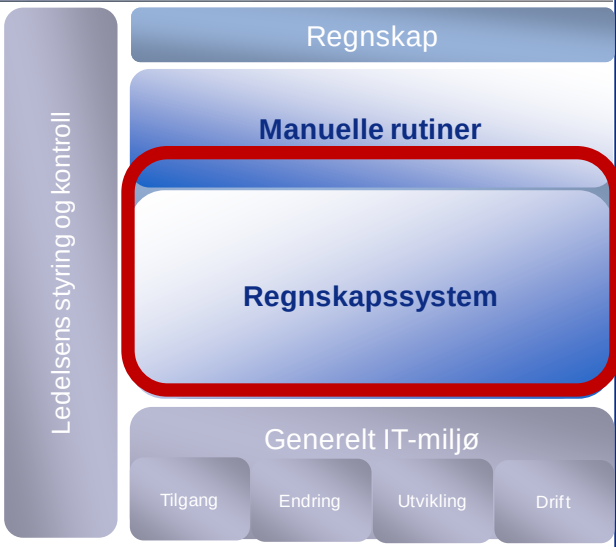
- **Målsetting**
  - Påse at selskapets IT-miljø sørger for integritet, konfidensialitet og tilgjengelighet i systemer og data
- **Kontrollkategorier**
  - Tilgang til systemer og data
  - Endringshåndtering
  - Utvikling og anskaffelse av IT-systemer
  - Drift av IT-systemer



Applikasjonskontroller

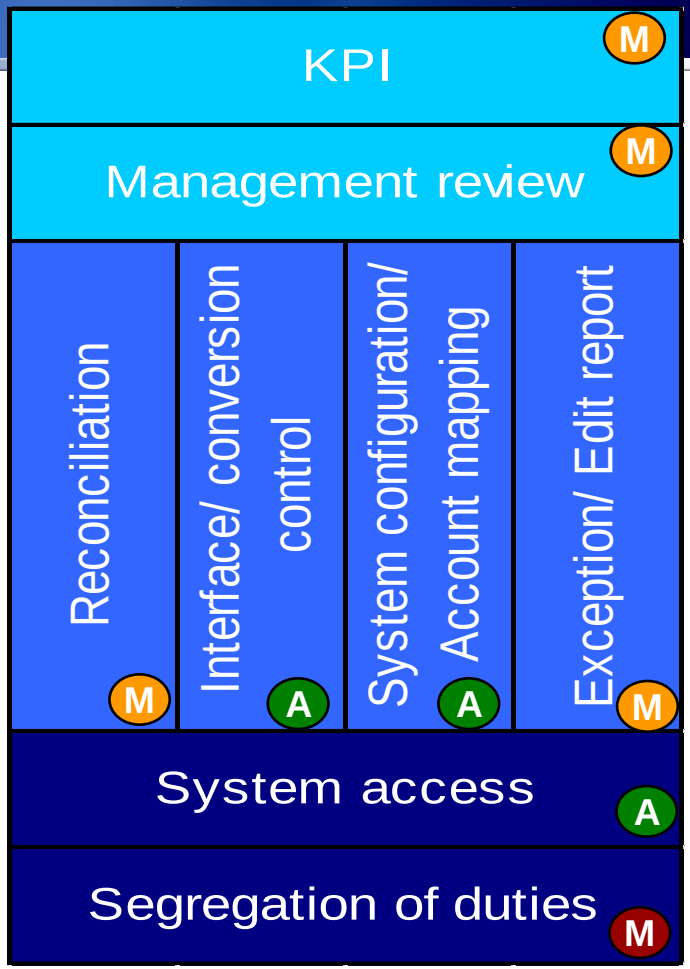
- **Kontroller på regnskapspåstands-nivå**

- **Typer kontroller:**
  - Automatiske
  - IT-avhengige
  - Manuelle



Kontrolltyper

- **De fleste kontroller har et IT-element (funksjonalitet)**
- **Som revisor må vi være sikker på at denne funksjonaliteten fungerer som den skal**

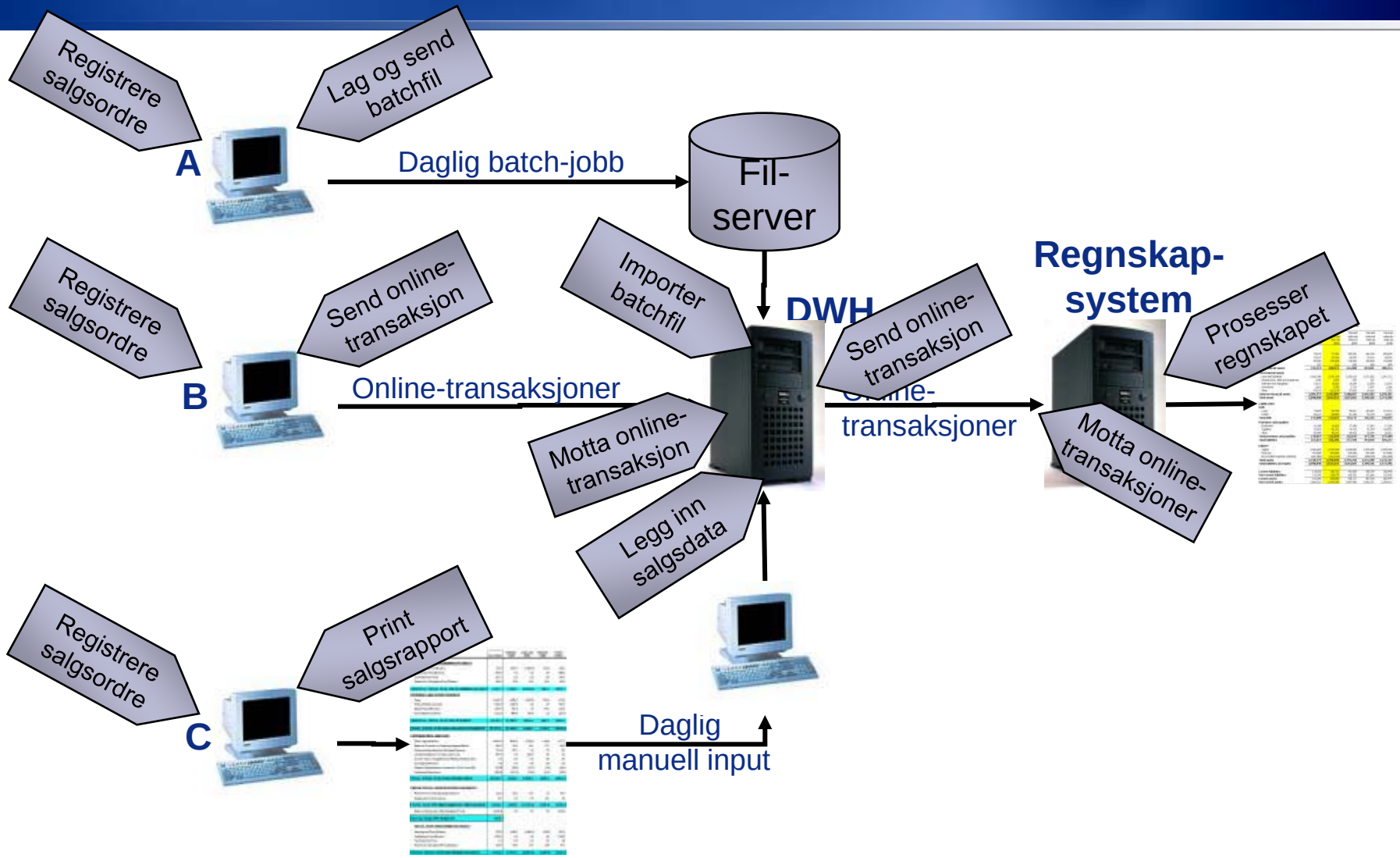


Substanskontroller (revisors egne handlinger)

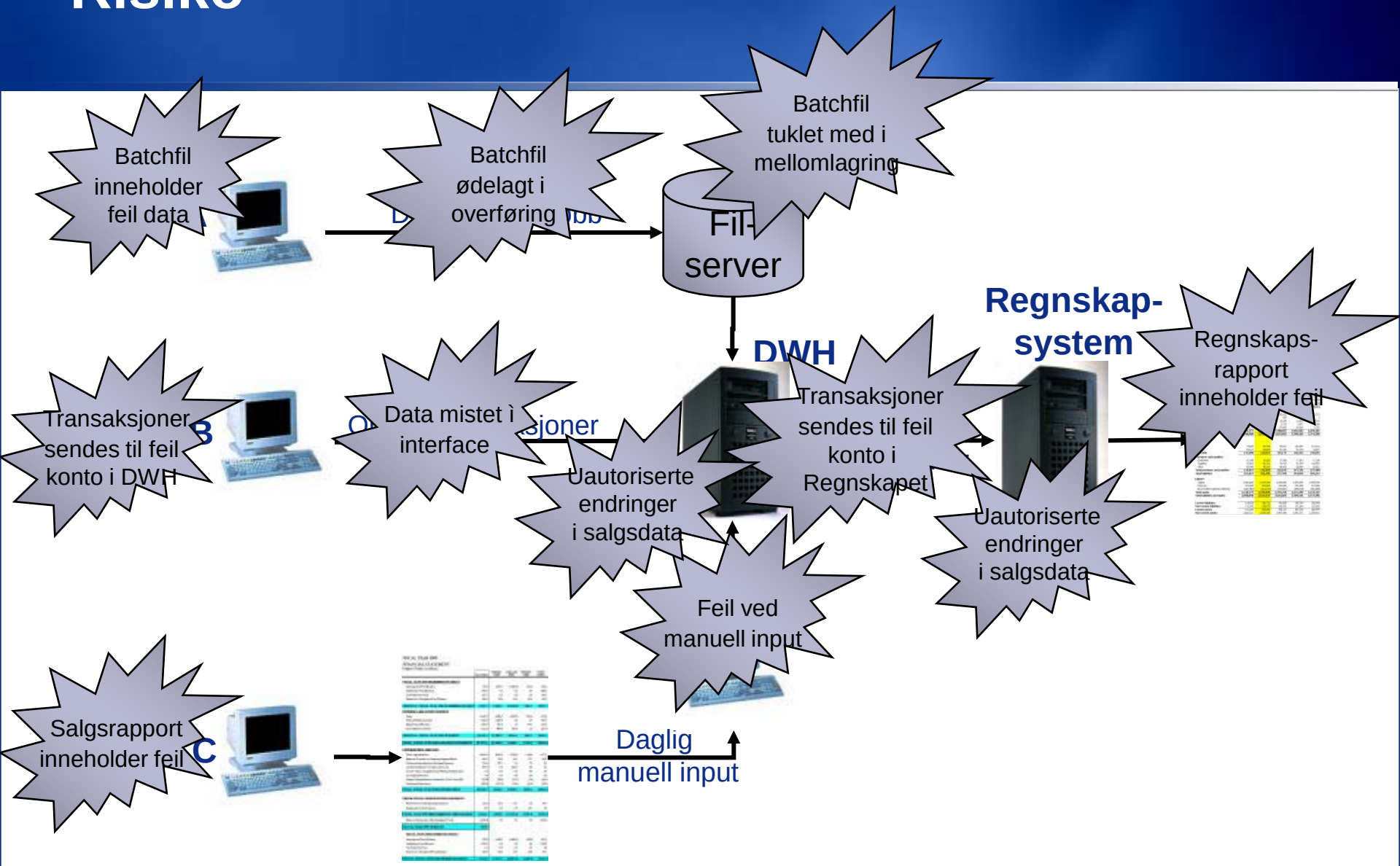
- **Substanskontroller er stort sett revisjonshandlinger rundt systemet**
- **Utfordringen med substanskontroller er store datamengder**
- **Substanskontroller utføres effektivt ved å benytte dataanalyseverktøy**
  - Gjøre et utvalg basert på statistiske metoder
  - Hente data fra flere kilder og sammenligne disse
  - Analysere om spesielle hendelser har inntruffet på hele populasjonen, for eksempel bokføring på helligdag

Eksempel - salg

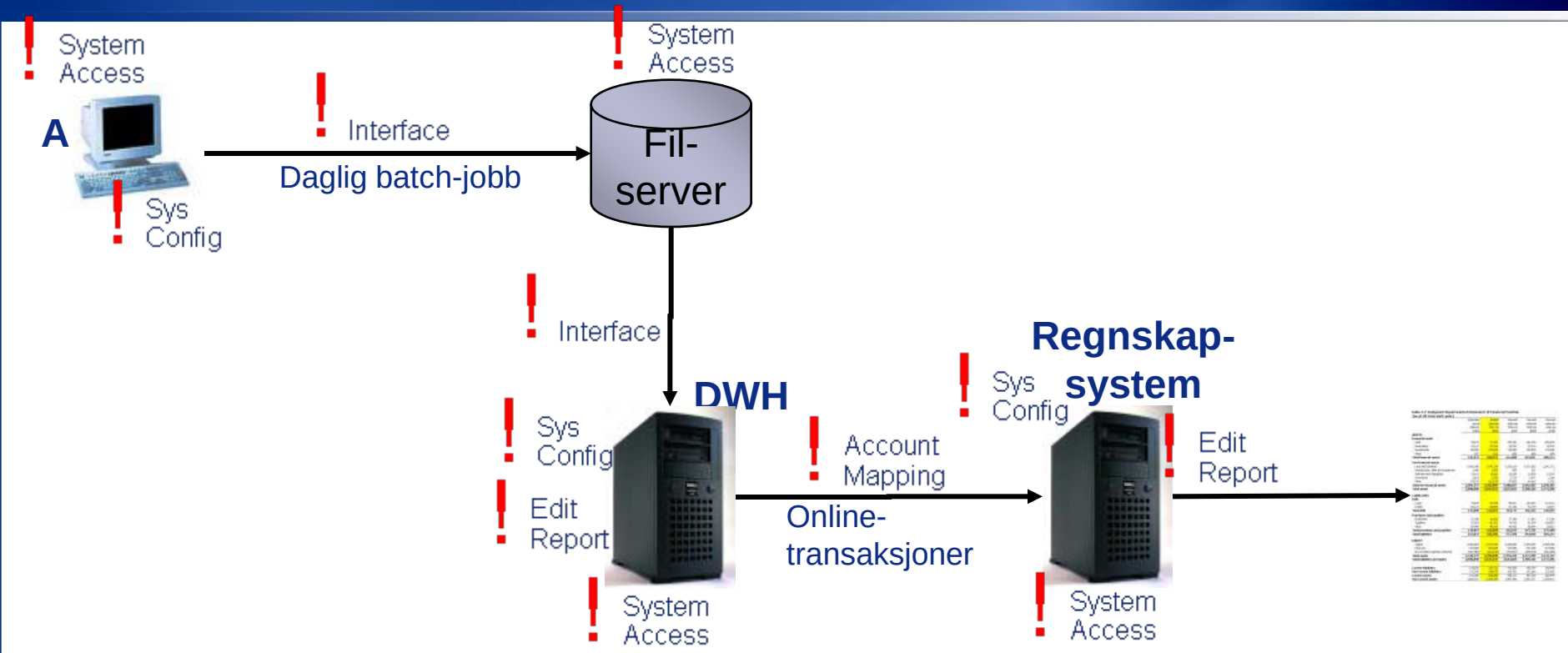
Accounting activities



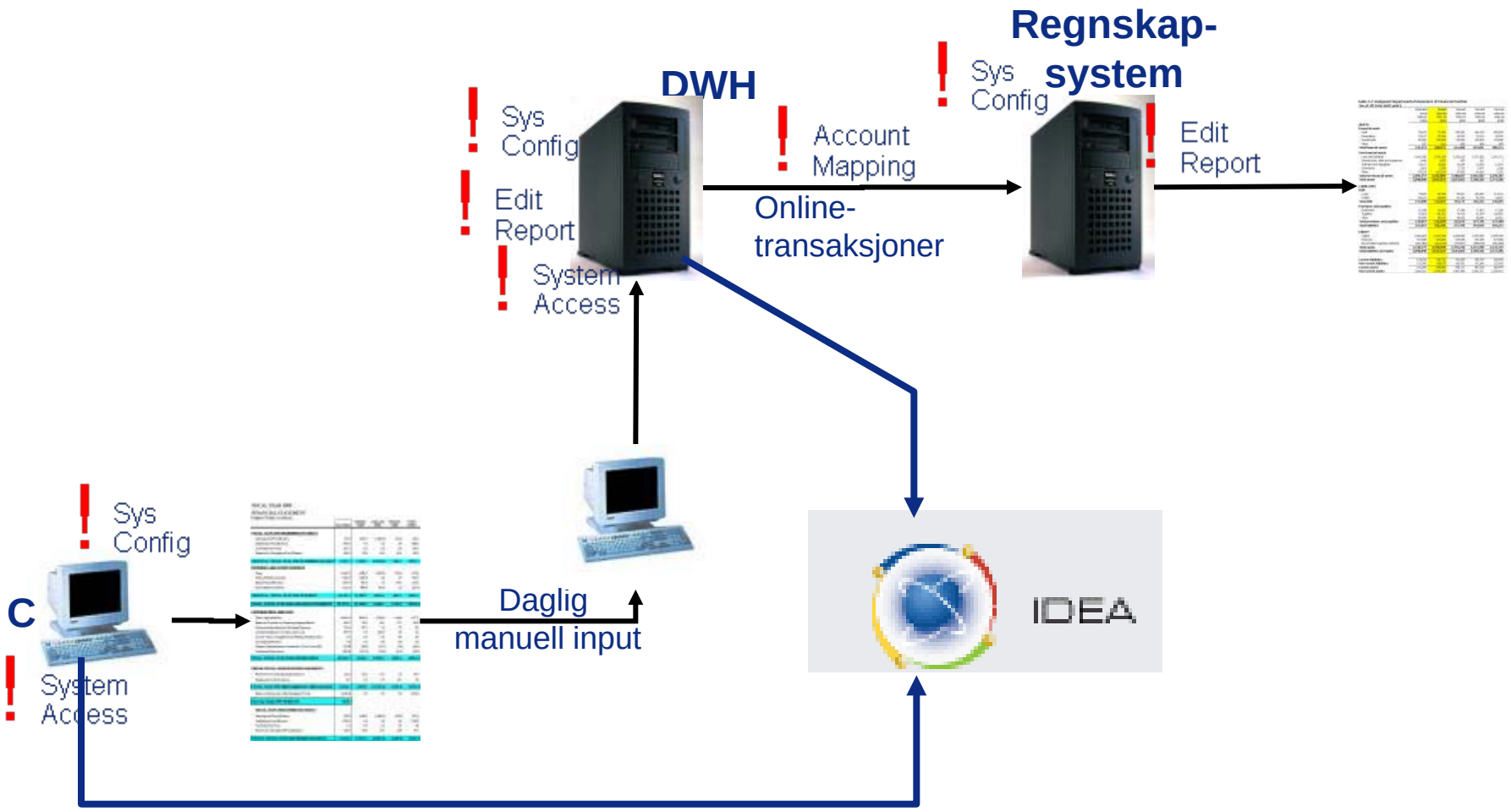
Risiko



Kontroller



Substanskontroller

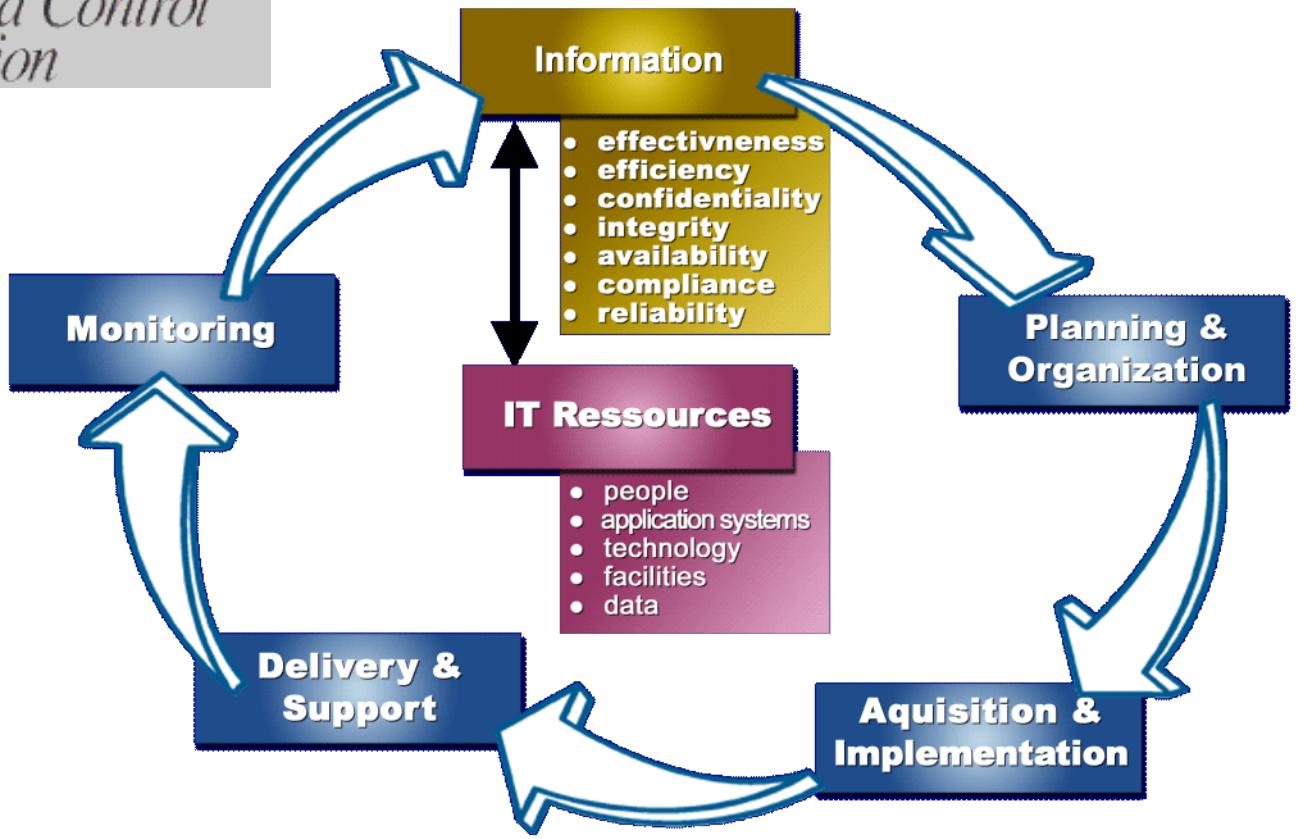


Rammeverk og modeller for IT internkontroll og IT-revisjon

Control Objectives for Information and related Technology (CobiT)

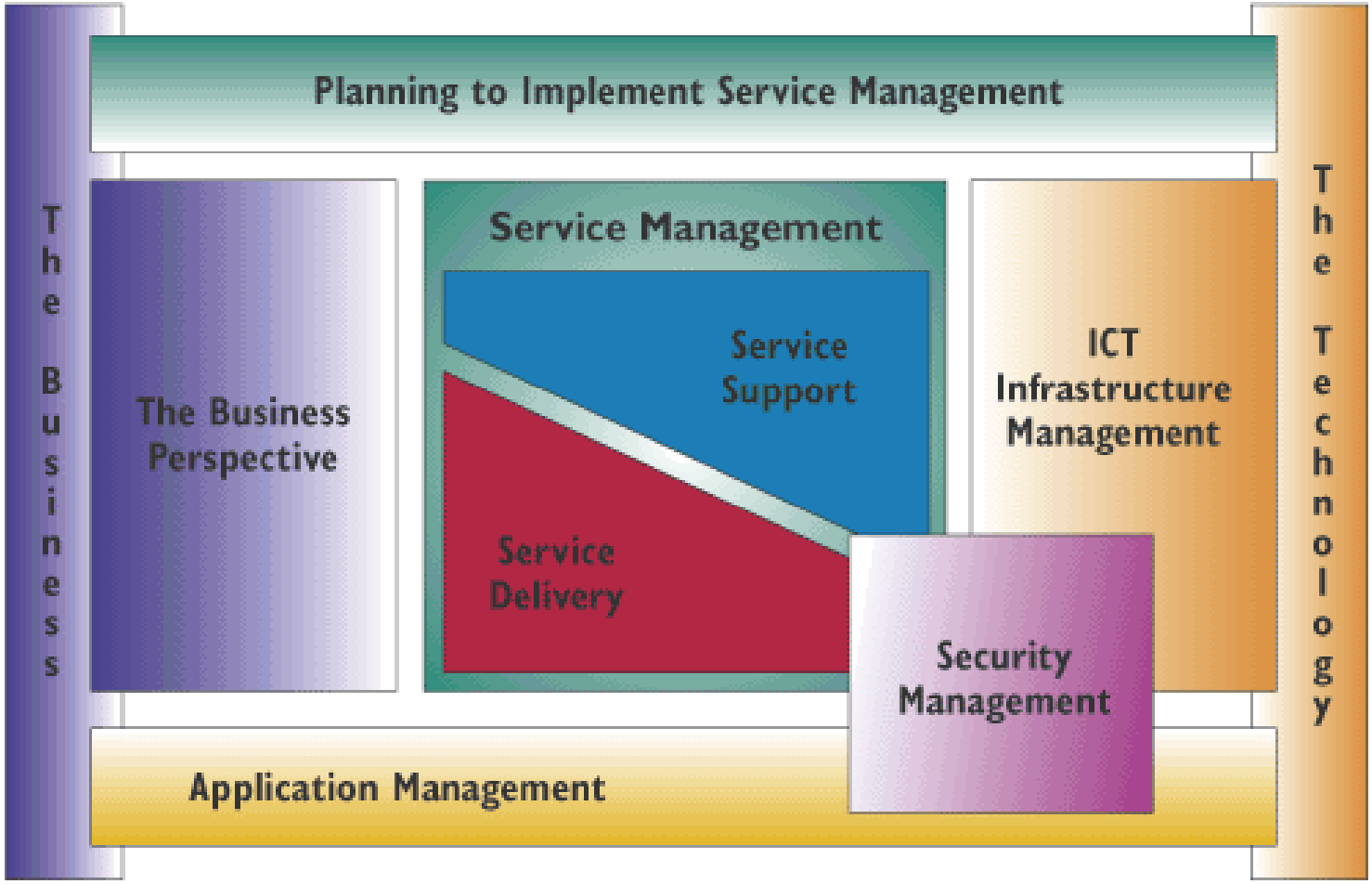
Information Systems Audit and Control Association

COBIT™
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

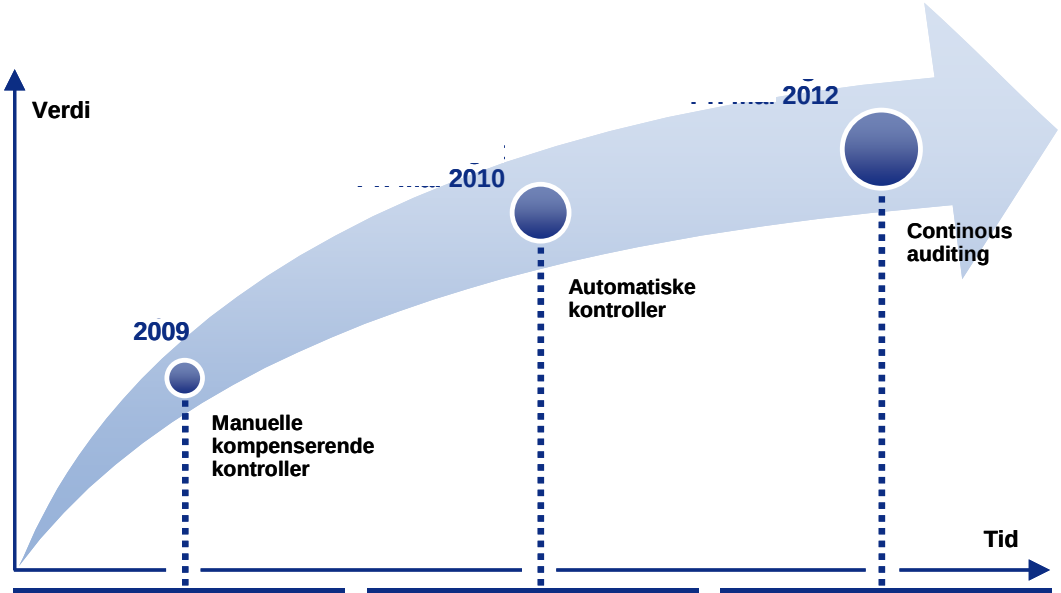


KPMG

Information Technology Infrastructure Library (ITIL)



AudIT Growth Model



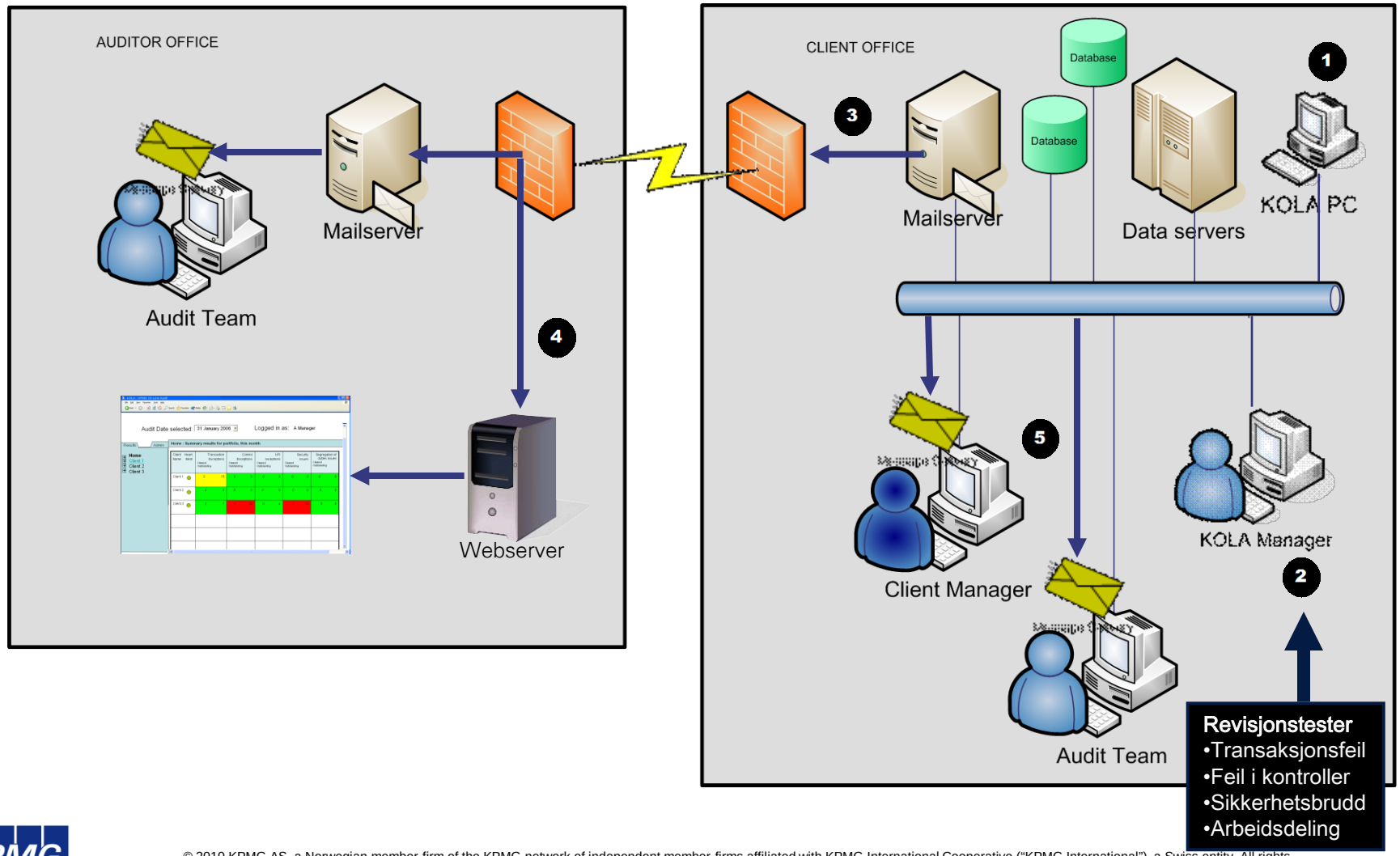
INNVIRKNING PÅ REVISJONEN	FORDELER FOR REVISJONEN	FORDELER FOR REVISJONEN
• Etterprøving av manuelle kontroller • Manuell og substantiv testing • Dupliserende og manuelle kontroller • Høyere kostnad forbundet med revisjonen	• Top-down tilnærming • Klarere fokus på nøkkelrisiko og svakheter • Mindre behov for testing • Mer kostnads- effektiv revisjon	• Mer effektiv revisjon gjennom mer automatisering og økt mulighet til å identifisere og rette feil, og mer tid til verdi-skapende analyse • Tidligere og raskere tilgang på informasjon og bedre datakvalitet for beslutning • Økt kontroll gjennom real-time overvåkning • Redusert kompleksitet og bedre styring • Maksimal kostnadseffektivitet

Continuous monitoring

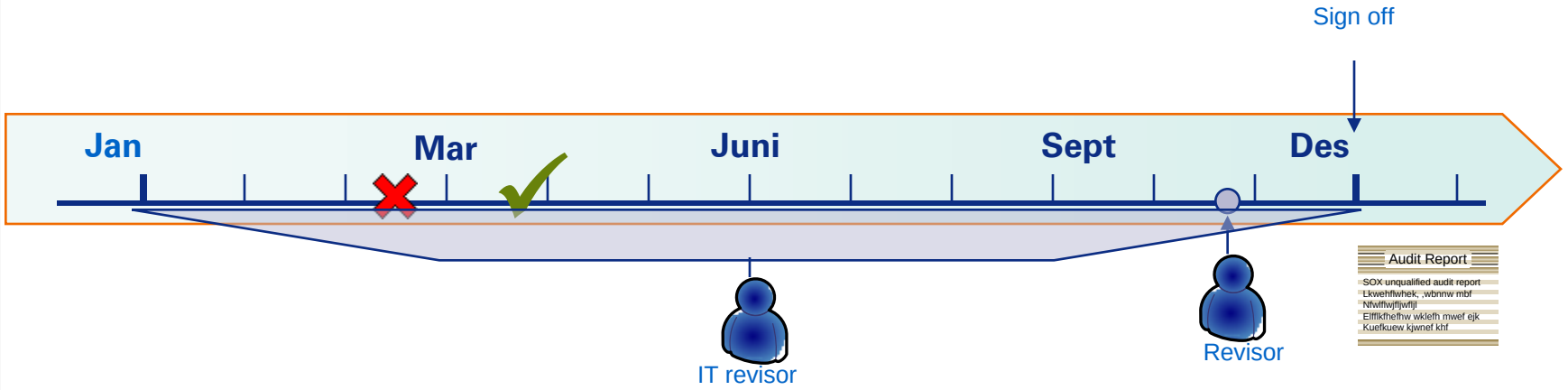
KPMG OnLine Audit (KOLA)

- **Kontinuerlig revisjon av internkontroll**
  - Ikke periodisk
- **Krever automatisering av kontroller og CA-verktøy**
- **Effektivisering av revisjonen (”regelverksmotor”) som**
  - Sikrer bevis på at prosesser går korrekt for seg
  - Får opp varsler om feil direkte
- **Selskapet får kontinuerlig tilbakemelding på om internkontrollen fungerer tilfredsstillende**

KOLA Audit model



KOLA påvirkning



- IT revisor reviderer kontroller kontinuerlig
- Kontrollen svikter/skrus av i februar og dette identifiseres straks
- Kontrolleier får beskjed og retter opp feilen
- Finansiell revisor vurderer kontrollen og konkluderer på at den er effektiv hele året
- Finansiell revisor kan bygge på kontrollen

Personvern

Personopplysningsloven

- **Gir rettigheter til enkeltmennesker**
  - Kontroll over opplysninger om en selv
- **Stiller krav til virksomheter**
  - Plikt til å sikre at enkeltmennesker har kontroll over opplysningene om seg selv
- **Folkeskikk satt i system**

Sentrale bestemmelser

- **§ 8. Vilkår for å behandle personopplysninger**
- **§ 9. Behandling av sensitive personopplysninger**
- **§ 11. Grunnkrav til behandling av personopplysninger**
- **§ 12. Bruk av fødselsnummer m.v**
- **§ 13. Informasjonssikkerhet,**
  - kapittel 2 i forskrift
- **§ 14. Internkontroll,**
  - kapittel 3 i forskrift

Viktige personvernprinsipper

Noen prinsipper står sentralt i oppbyggingen av personvernlovgivningen. Prinsippene bygger på et grunnleggende ideal om at den enkelte skal ha bestemmelsesrett over personopplysninger om seg selv.

SAKLIG BEGRUNNELSE
Behandling av personopplysninger skal være saklig begrunnet. Opplysningene skal samles inn til uttrykkelig angitte og legitime formål, og brukes i overensstemmelse med disse.

FRIVILLIG SAMTYKKE
Registrering av personopplysninger skal i størst mulig grad være basert på et frivillig, uttrykkelig og informert samtykke. Opplysninger i offentlige registre hvor registrering er pliktig, skal være lovhjemlet.

OPPLYSNINGSPLIKT FOR DEN BEHANDLINGSANSVARLIGE
Ved innhenting av personopplysninger har den enkelte uoppfordret rett til å få vite om det er frivillig eller obligatorisk å oppgi personopplysningene, hvilket formål opplysningene skal brukes til, og om de vil bli utlevert til andre.

RETT TIL INNSYN
Den behandlingsansvarlige skal bistå den registrerte med å gi innsyn i hvilke opplysninger som er lagret, hva de skal brukes til, og hvor de er hentet fra.

REGISTRERINGEN SKAL VÆRE RIKTIG
Opplysningene som registreres skal være korrekte og ajourførte.

FEILAKTIGE OPPLYSNINGER SKAL RETTES
Feilaktige personopplysninger skal endres, slettes eller sperres.

UNØDVENDIGE OPPLYSNINGER SKAL SLETTES
Overskuddsinformasjon og opplysninger som ikke lenger er nødvendige for formålet med registreringen, skal slettes.

INFORMASJONSSIKKERHET SKAL IVARETAS
Den behandlingsansvarlige skal sørge for tilfredsstillende informasjonssikkerhet. Det må kunne dokumenteres at rutiner og tiltak som sikrer personopplysningene blir etterlevd i praksis. I det offentlige må risikovurderingene også omfatte borgernes ulike forutsetninger for å ivareta egen informasjonssikkerhet.

STRENGERE REGLER VED FØLSOMME OPPLYSNINGER
Behandling av følsomme personopplysninger er underlagt særlig strenge regler.

RETTEN TIL Å VÆRE ANONYM
Borgeren har krav på å kunne ferdes anonymt. Når nye teknologiske løsninger tas i bruk, skal det legges til rette for at det fortsatt finnes muligheter til anonym ferdsel.

RETT TIL MANUELL VURDERING
Den registrerte har rett til å få en manuell vurdering av avgjørelser som fullt ut er basert på automatisk behandling av personopplysninger, dersom avgjørelsen er av vesentlig betydning for vedkommende.

Personvernrapporten 2009

Betraktninger om personvern

- **Nøkkelspørsmål**
  - Hva er personopplysninger?
  - Hvilke opplysninger behandler en virksomhet og hva vil det si å behandle?
    - Formål
    - Hjemmel
  - Hvem er ansvarlig for behandlingen av personopplysninger?
  - Hvordan behandles personopplysninger?
  - Hva betyr det at virksomheten skal oppnå tilfredsstillende informasjonssikkerhet?

Datatilsynet

- **Datatilsynets oppgave er å**
  - Føre tilsyn med Personopplysningsloven (og tilknyttet regelverk)
  - Ha en ombudsrolle samt rådgi i personvernspørsmål
- **Datatilsynet gjennomfører tilsyn basert på:**
  - ”Tilfeldig utvalg”
  - Saker som meldes inn (ansatte, kunder, media og lignende)
  - Tematilsyn
- **Varsel sendes med beskrivelse av hva, når, hvem osv**
  - Det er også vanlig å be om å få oversendt informasjon på forhånd
- **Det er viktig å svare presist på spørsmål og forstå terminiologi**
- **Er virksomheten uenig i Datatilsynets virkelighetsforståelse og/eller lovfortolkning, så kan de klage vedtaket inn til Personvernnemnda**

Personaladministrasjon

- **Virksomheten kan behandle opplysninger nødvendig for å ”administrere ansettelsesforholdet”**

- **Dette omfatter alle normale opplysninger**
  - Navn, adresse, fødselsnummer mv
  - Pårørende

- **Eksempel på hva som omfattes av personaladministrasjon kan være administrering av lønn, utvikling, opplæring, karriereplanlegging og behandling av disiplinærsaker.**

Personalregistre

§ 7-16. *Personalregistre mv.*

Arbeidsgivers behandling av ikke-sensitive personopplysninger om nåværende eller tidligere ansatte, personale, representanter, innleid arbeidskraft samt søkere til en stilling er unntatt meldeplikt etter personopplysningsloven § 31 første ledd.

Dersom det behandles sensitive personopplysninger, er behandlingen unntatt fra konsesjonsplikten etter personopplysningsloven § 33 første ledd, men underlagt meldeplikten etter § 31 første ledd. Unntak fra konsesjonsplikt gjelder under forutsetning av at:

a) den registrerte har samtykket i behandlingen eller behandlingen er fastsatt i lov,

b) opplysningene er knyttet til arbeidsforholdet, og

c) personopplysningene behandles som ledd i personaladministrasjonen.

Meldeplikt etter andre ledd gjelder likevel ikke behandling av

a) opplysninger om medlemskap i fagforeninger som nevnt i personopplysningsloven § 2 nr. 8 bokstav e,

b) nødvendige fraværsopplysninger og opplysninger som er registreringspliktige i henhold til lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven) § 5-1,

c) opplysninger som er nødvendige for å tilrettelegge arbeidssituasjonen på grunn av helseforhold.

Kilde: Lovdata

- **Dersom formålet med behandlingen for eksempel er overvåkning eller kontroll av ansatte, omfattes det ikke av unntaket.**
- **Bestemmelsen medfører at de aller fleste personellregistre er unntatt både konsesjons- og meldeplikt etter personopplysningsloven.**

Sensitive opplysninger

- **Sensitive personopplysninger: opplysninger om:**
  - a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
  - b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
  - c) helseforhold,
  - d) seksuelle forhold,
  - e) medlemskap i fagforeninger.
- **Det må foreligge hjemmel i lov eller samtykke fra den ansatte det skal lagres sensitive opplysninger om**
- **Personellregistre som bare inneholder ikke-sensitive opplysninger er unntatt meldeplikt.**

Sensitive opplysninger, forts

- **Under forutsetning av at det foreligger lovhjemmel eller samtykke kan følgende sensitive personopplysninger behandles uten både konsesjon og melding:**
  - Opplysninger om medlemskap i fagforening
  - Nødvendige fraværsopplysninger og opplysninger som skal registreres med hjemmel i arbeidsmiljølovens § 5-1
  - Opplysninger som er nødvendige for å tilrettelegge arbeidssituasjonen på grunn av helseforhold

Øvrige regler i personopplysningsloven

- **Behandlingen må følge de øvrige reglene i personopplysningsloven:**
  - Grunnlag i personopplysningslovens § 8. Vilkår for å behandle personopplysninger
  - Dersom personellregisteret skal inneholde sensitive opplysninger kreves det i tillegg at behandlingen oppfyller et av vilkårene i § 9. Behandling av sensitive personopplysninger
  - I tillegg må behandlingen oppfylle grunnkravene i § 11.

Eksempler på personopplysninger som en arbeidsgiver som hovedregel vil ha grunnlag for å behandle med utgangspunkt i §§ 8 a jf. 9 f:

1. navn
2. adresseopplysninger
3. statsborgerskap/bostedland
4. anropsnummer for teletjenester
5. fødselsnummer og annet nummer knyttet til person (rullenummer/arbeidstakernummer)
6. rubriseringsdata, (såsom kategori, type ansatt/representant, distrikt, type varer, kontonummer i regnskap, representantkategori, andre opplysninger til bruk i statistikk og annen bedriftsintern avregning)
7. kjønn
8. nærmeste pårørende
9. sivilstand
10. antall barn og barnas fødselsår og eventuell annen opplysning med betydning for rett til fravær ved barns sykdom, skolestart m.m.
11. stillingsbetegnelse
12. yrkesopplysninger som etter overenskomst eller tariffavtale som har betydning for lønns- og arbeidsvilkår
13. opplysninger om utdannelse og praksis
14. lønns- og provisjonsopplysninger
15. kontonummer
16. pensjonsopplysninger
17. trekk- og skatteopplysninger
18. ansettelses- og sluttdato (permisjoner e l)
19. sluttårsak
20. fraværsdato, type fravær og varighetMerk at eventuell diagnose ikke skal registreres.
21. firmabil e l
22. utlånte eiendeler
23. lån til ansatte eller garanti for lån
24. opplysning om den ansatte er mobiliseringsdisponert (ja/nei), evt militært løpenummer, grad, og rulleførende avdeling.

Kilde: Datatilsynet

Stor motstand mot epost-innsyn

Av Mats Lillesund (Computerworld) 24.04.2009 kl. 20:43 Kilde: VG NETT

Svært mange ansatte tar avstand fra at arbeidsgiver kan gå inn og sjekke eposten.

MOTSTAND: Jurist og seniorrådgiver Christine Ask Ottesen i Datatilsynet mener det er viktig at ansatte er klar over at arbeidsgiver eier eposten - og har i visse tilfeller rett til innsyn. (Foto: Mats Lillesund)

I mars trådte den nye epostforskriften i kraft. Den slår fast at arbeidsgiver kan gå inn og gjennomsøke epost og personlige lagringsområder. Det reagerer svært mange på

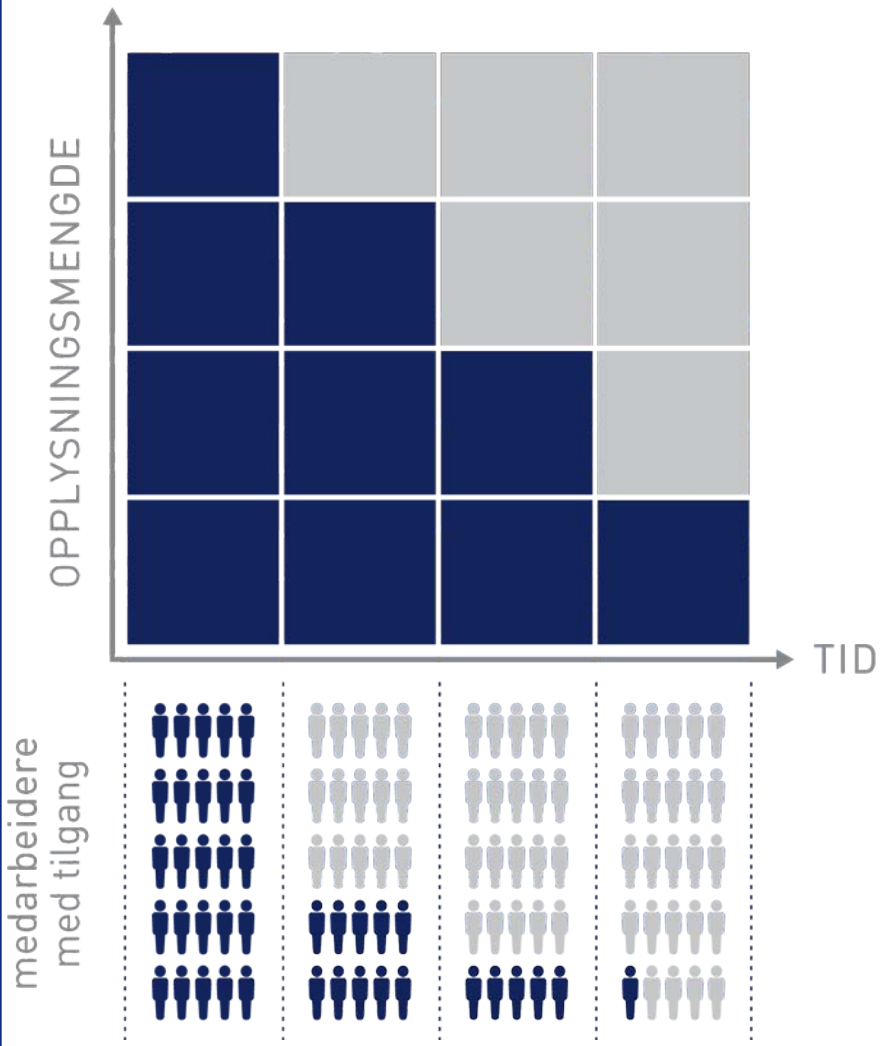
Innsyn i e-post

- **Det har vært mange mediaoppslag om dette tidligere**
  - Vinmonopolet, Bazar mfl
- **Det har også vært jobbet med eget tillegg om innsyn i e-post, men det strandet på spørsmålet om hvem som ”eier” e-posten**
- **Regelverket er nå klart**
  - Innsyn kan gjøres dersom virksomheten har ”grunn”
    - Dag-til-dag oppgaver
    - Mistanke om uetisk atferd
  - Informasjon om innsynet må gis den ansatte (ikke samtykke) og denne må gis mulighet til å bisitte/være representert
  - Viktig at alt er kommunisert på forhånd og at det dokumenteres

Lønnsslipper

- **Inneholder**
  - Fødselsnummer ref personopplysningsforskriftens § 10-2; elektronisk sending av fødselsnummer må sikres slik at det ikke er tilgjengelig for andre enn adressaten.
  - Kan inneholde særtrekk som forteller noe om en persons livssituasjon, straffbare forhold eller andre forhold med høye krav til konfidensialitet.
- **Tiltak:**
  - Kryptering:
    - Utsendelse av lønnslipper fra et eksternt regnskapsfirma til en virksomhets ansatte og/eller en spesifikk mottakeradresse.
    - Utsendelse av lønnsslipper til eksterne e-postadresser utenfor den behandlingsansvarliges informasjonssystem.
    - Virksomhetens e-post server står hos databehandler.
  - Ingen kryptering:
    - Utsendelse av lønnsslipper til lokale e-post adresser innenfor den behandlingsansvarliges informasjonssystem.
  - Portalbasert løsning med autentisering, hvor den ansatte kun får tilgang til lønnsslippen.

Lagringstrappen



Slettekravet:
§ 28. *Forbud mot å lagre unødvendige personopplysninger*

Presenter's contact details

Torkil Hindberg

KPMG

+47 406 39 835

torkil.hindberg@kpmg.no

www.kpmg.no