Er data som forventet?
Kontroller i IT-systemer

Generelle kontroller
Applikasjonskontroller
Validering
Personopplysninger

Bokføringsloven

- Bokføringen styres av kravet til
  - (Kapitel 2) Regnskapsrapportering
  - (Kapitel 3) Spesifikasjonene
  - (Kap 4, 6 og 7) Dokumentasjon
- Bokføringen må være betryggende og metodisk (sikring og system)
- §4 grunnleggende bokføringsprinsipper
  - datakvalitet

Transaksjonsdata og faste opplysninger

- Transaksjoner
  - Minimumsdata (dato, dokhenv, konto, beløp)
  - Koder som er nødvendige for rapporter og spesifikasjoner
- Faste data
  - Koder som styrer bokføringen (dokumenteres)
  - Egenskaper ved (kan måtte dokumenteres)
    - Hensiktsmessige systemobjekter
      - Tabeller: KONTI, RESK, VARER,

Kvalitet

- Kost/nytte-modellen medfører
  - Utdatakvalitet påvirkes mest av inndatakvalitet
    - Øket betydning når sanntid og integrerte systemer
  - Internkontrollen definerer autoriserte transaksjoner med kjent forventning til kvalitetsfordeling
  - Test av kontroller foretrekkes fremfor direkte tester av rapporter og spesifikasjoner

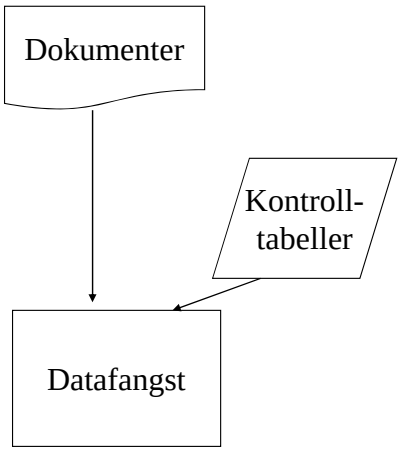
Generelle kontroller

- Gjelder hele IT-miljøet
- Kontroller med generell anvendelse på tvers av applikasjonene
- Kontrollkategorier
  - Operativsystem
  - Dataressurser
  - Arbeidsdeling og tilgangskontroll
  - Systemutvikling, anskaffelse og vedlikehold
  - Katastrofeplan og fysisk sikring
  - (Kontroller i Pcmiljø)

Applikasjonskontroller

- Applikasjon: En IT-anvendelse med brukerformål
- Nøyaktighet og integritet i applikasjonsdata
- Kontinuitet, fullstendighet og nøyaktighet

Datavalidering



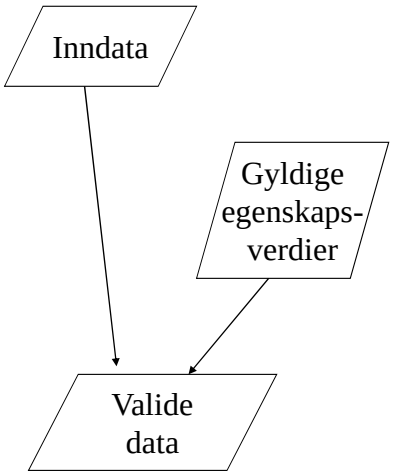
- Eksistenskontroll
- Formatkontroll
- Obligatorisk / valgfritt felt
- Sekvenskontroll
- Fulltekst verifikasjon av kode
- Kontrollsiffer m.v.
- Rimelighetskontroller

Redundans

- Overflødige data
  - kommer du i morgen? - kmr dui morgn?
  - Overflødig i forhold til tolkning / informasjon
- De overflødige data = redundante data brukes til kontroll
- Hva er overflødig her?

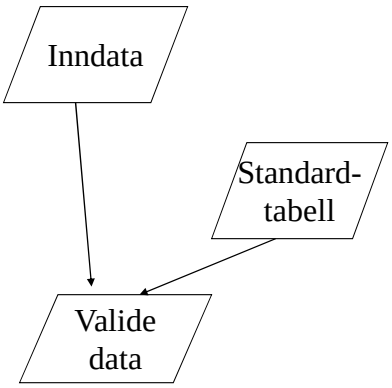
  2+3=5
- All kontroll forutsetter redundans

Eksistenskontroll



- En egenskapsverdi
  - f.eks. Kontokode 1500
- tillates ikke brukt hvis den ikke eksisterer i kontrolltabellen
  - f.eks i kontoplanen
- egenskapsverdien må opprettes først

Naturgitt eksistens



- Gyldige verdier definert i
  - skjemaet (data dictionnary)
  - programspråket
  - standardiserte tabeller i et standardbibliotek
- Hvordan ha tiltro disse standardverdiene?

Datatype

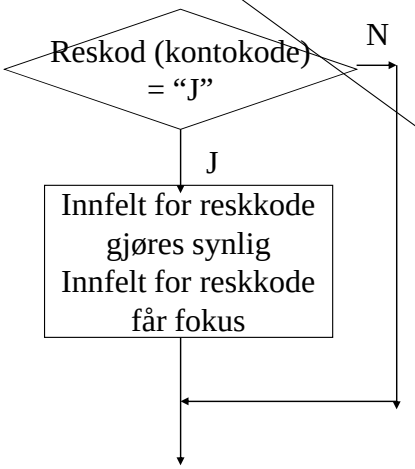
- Typedefinisjon i programmeringsspråket
- Typedefinisjon i skjemaet (data dictionnary)

- Heltall, flyttall, antall desimaler
- Numerisk, alfanumerisk
- Dato
- Mønster (tlfnr, mail-adresse, bankkonto)

Ekkokontroll

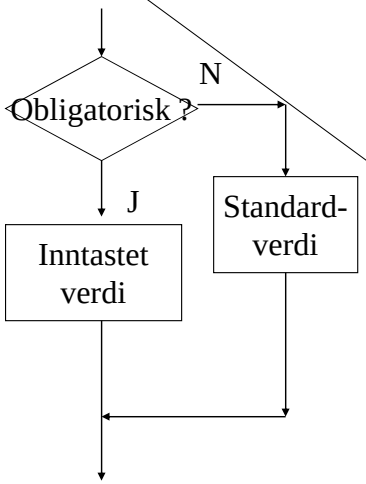
- Fulltekst verifikasjon av inntastet kode
  - Når reskontronr tastes vises kundens navn
  - Hvilken tabell brukes?
- En passiv kontroll for systemet
- En aktiv kontroll for brukeren
- Svak kontroll
  - Best som navigasjonshjelpemiddel

Sekvensavhengige felt



- Hvis kontokoden skal ha reskontro
  - felt for reskontrokode åpnes og får fokus
- ellers
  - feltet for reskontrokode er skjult
- Felter kan være
  - synlige / usynlige
  - åpne / sperret

Obligatorisk / valgfritt felt



- Skjemaet eller programmet forteller om feltet må fylles ut
- Standardverdi hvis ikke data registreres i feltet

(Hvilken standardverdi brukes for: Dato, ktonr, dokumentasjonsnr, resknr, mvakode, beløp, tekst, . .)

Kontrollsiffer

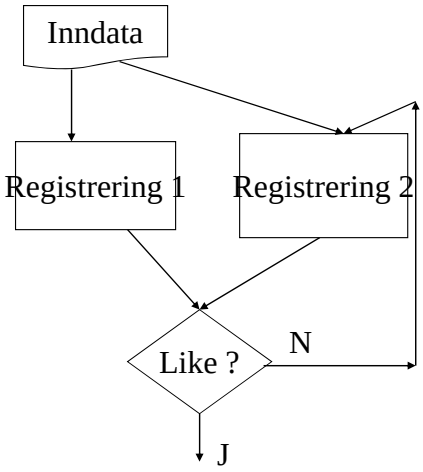
Etabler gyldige verdier

Kontroller om gyldig verdi

- S1, S2, . . ., Sn, Sk
- sk = $\sum$ v(i)*s(i) | m
- Vektene v og divisoren m avgjør hva slags feil som tas
  - omkast av to siffre
  - dobbeltslag
  - bortfall av enkeltsiffre
- antagelse om hyppighetsfordeling av feil

Søk i Google: kontrollsiffer

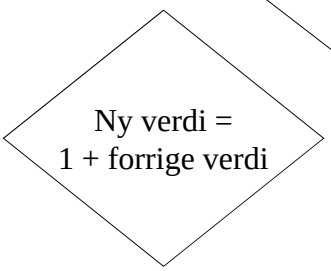
Dobbeltregistrering



- Skjelden kostnadseffektiv
- Bedre hvis
  - kun viktige felt
  - høy feilsannsynlighet
- Flerfelt polynomssum-kontroll
- Se utviklingen:
  - paritet, kontrollsiffer, polynomsum, (elektronisk signatur)

Sekvensnummererte poster

- Fullstendighetskontroll
- Kontroll eller inntastingseffektivisering ?



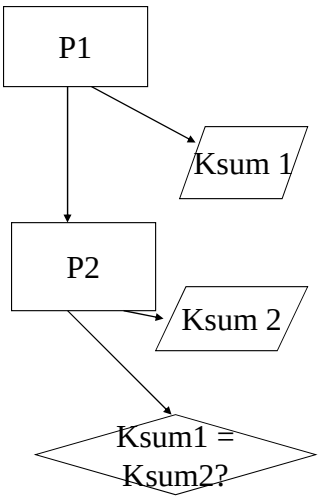
Rimelighetskontroller

- Forventningsverdi
- Akseptabelt intervall
- Oppdatering av grenser
  - manuelt
    - statisk: i program
    - dynamisk: i tabell
  - automatisk (gjennomsnittsverdi, grenser)
    - histogram
    - poissonfordeling

Hvor lagres valideringsparametrene

- I tabeller for faste data
  - KONTI
    - maxbeløp, forvbeløp, minbeløp
  - RESK
    - kredittgrense
  - VARER
    - forv_antall, Max_antall
- Egne valideringstabeller
  - kombinasjon RESK og VARER
- I databasens skjema (særlig hvis faste verdier)
- I dataprogrammene
  - statisk kontrollgrense

Kontrolltotaler



- Naturlige
  - dokumentsummer
  - bunkesummer
- Nonsenstotaler
  - summen har bare kontrollformål
- Summen må beregnes på to ulike steder i rutinen (programmet)

(*Google om: hash total*)

Nonsenstotaler

- Varenr Antall
- 2 10 12 Kontrollsum 1
- *(11 7 Kontrollvekter)*
- *22 + 70= 92 Kontrollsum 2*
- Hvilken sum kontrollerer best?

Avstemming

- Resultatet (summen, antallet) kan fremkomme på minst to måter
  - summering i tabell horisontalt og vertikalt
  - IB+trans=UB
  - ta vare på en bunkesum, kontroller siden
  - lagret sum (signatur) = beregnet sum (verifikasjon)
  - to ulike tidspunkter
  - to ulike steder

Validering vs etterkontroll

- Teknisk sett samme kontroller som ved etterkontroll ("revisjon")
  - ACL, IDEA, osv
- men kontrollen tas ved registrering

- Derfor er en etterkontroll med eksakt samme kontrollhandling som ved validering mindre effektiv
  - men, endrede parameterverdier mulig

Personopplysninger (Poppl §2)

- Personopplysningsloven
- Meldeplikt personopplysninger
  - Unntak: bl.a. mellomværende kunder og leverandører (POF§7-6 og 7-7, jf. §7-14)
- Konsesjonsplikt
  - sensitive opplysninger
    - Unntak: Personalregistre (POF§7-16)
      - Kundeopplysninger (POF §7-14)
- Nyttig
  - §13 Informasjonssikkerhet (POS kap 2)
  - §14 Internkontroll (POF kap 3)
- (Helseregisterloven)

Systemutvikling, koding, større systemer

Risiko ved utvikling, vedlikehold og drift

Klassisk systemutviklingsmodell

- SDLC: 5 faser
  - Problemformulering: kravsspesifikasjon
  - Logisk løsning: systemdokumentasjon
  - Fysisk realisering (programmering): programmer
  - Implementering ("eget systemutv-prosjekt"):
    - Opplæring
    - Tabeller for faste data
    - Tabeller for (tidligere) transaksjoner
  - Drift

Hvordan beskrive hendelser

- Tidspunkt
  - alternativer
- transaksjonstype
  - beslutningsregler, prosess
- plassering i kontrollsporet
  - før, etter, kilde
- gruppering v.hj.a. koder
  - kontokode
    - hvordan gruppere ?

Kodeplaner

- Almenne (kontorammer, eksterne benchmarks)
- Organisasjonsspesifikke
- Entydighet
  - hierarkiske
  - flerdimensjonale

Taksonomi

- Hva skal vi velge til å beskrive hendelsen, aktivet, osv ?
- Kan ses på som samme problem som ved bruk av faktoranalyse i statistikken
- Hvordan beskrive hendelsen
  - mest presis beskrivelse
  - færrest mulige varable

Eksempel: et varekjøp

- Hva er de viktigste egenskapene?
- Hva er formålet (-ene) med å beskrive varekjøpet?
- Hvor viktig er de ulike delene av beskrivelsen?

Ren informasjonsteori

- Betydningen av uavhengihet mellom registreringsbegrepene
  - full uavhengighet
  - fullt samsvar
  - mellomsituasjoner
- hvordan beskrive hvor godt vi sprer bruken av koder

Ulike verdier av hendelsene

- Teller hver transaksjon like mye ?
- Transaksjonens økonomiske verdi som vekt
  - (jfr. Monetary Unit sampling)
- Graden av overraskethet
  - først: de store trekkene, de vanligste grupperingene
  - så: det uventede, den skjeldne kombinasjonen

Varierende antall bilag

- Antallsfordeling trans pr kontokode:
- 3010 2000
- 3011 21
- 3020 8300
- 3021 2
- 3030 8
- 3040 0
- 3100 80

Kommentarer?

To registreringsbegreper

– Prosjekt	A	B	C	D
Konto				
6000	0	70	0	0
6100	92	0	0	0
6120	0	0	0	30
6150	0	0	87	0

- antall transaksjoner

- Endre rekkefølge rad, kolonne?
- Mønster ?

To registreringsbegreper

– Prosjekt	A	B	C	D	sum
• Konto					
• 6000	10	70	10	3	93
• 6100	92	20	0	0	112
• 6120	0	20	44	30	94
• 6150	0	0	87	0	87
• Sum	102	110	141	33	

- antall transaksjoner

Hvorfor omtale et større system - SAP

- Følelse for kompleksitet og omfang i et større system
- Egenskaper som skiller fra eldre / mindre systemer
- respekt for implementeringsjobben
- den kontinuerlige endringsprosessen
- noen sentrale termer

SAP R/3

- R/3
  - klient tjener
  - trelags modell
    - men kritisert for at middel-laget er for likt stormaskin-arkitektur
  - verdens største system for integrert styring
  - store implementeringsbudsjetter
  - hver modul har mer enn 1000 forretningsprosesser definert
  - mer enn 8000 tabeller styrer systemets oppførsel

Risiko

- Tabellstyrt system gjør at systemet kan brukes på mange måter
  - alternativer: kompilert, tolket, tabellstyrt
    - konsekvenser for endringskontrollen ?
- Men strukturelt lite fleksibelt
  - vanskelig å endre
- sentralistisk
  - bra for kontroll

Risiko

- Komplekst
  - lang læretid og høy lærekostnad
  - avhengig av konsulenter for implementering
- Krav til kompetanse i endringsledelse
- Bestemme korrekt organsisajon
  - Mange detaljerte beskrivelser og beslutninger må gjøres før implementering
- mulig konflikt med foretaksstrategi
  - bra hvis organisasjonsmodellen er hierarkisk
  - vanskelig hvis konserndøtre skal tillates unike driftsmodeller
  - hvis noe av logistikken er JIT og andre deler er beholdningsstyrt

Lag 1: Databasetjeneren

- Bruker standard databaser i markedet
  - Oracle, Informix m.fl
- Ren lagring, ingen forretningsprosesser her
  - generelt kan jo databaser lagre prosesser
  - vekt på tradisjonelle DBMS-oppgaver
    - tilgjengelighet, integritet, konfidensialitet
    - tilgangskontroll, samtidig bruk, låsing, tilbakerulling, sikkerhetskopier, oppdateringstjener, meldingstjener
- Skjemaet (I SAP kalt Data repository)
  - hvilke data er lagret
  - Hvilke egenskaper har entiteten
  - Hvilke attributter har hver egenskap
  - Sammenhenger

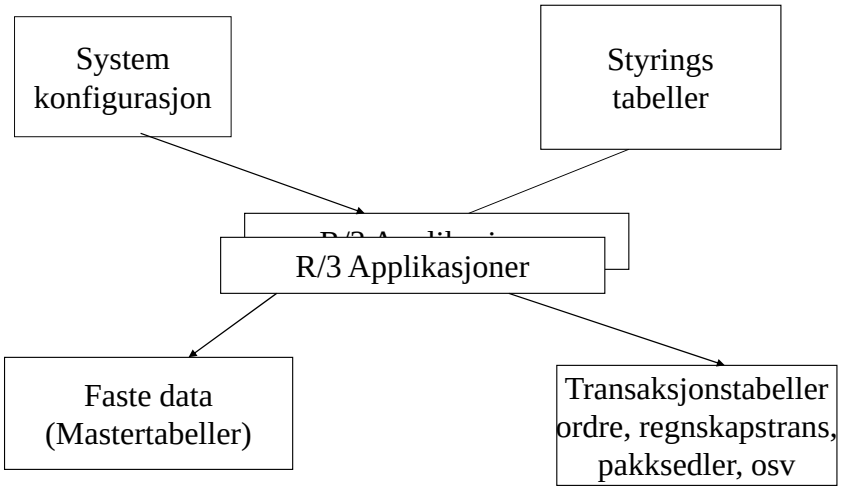
Lag 2:Applikasjonstjeneren

- I bunn: SAP kjerne og applikasjonstøtte
- Moduler
  - SAP-moduler og tredjepartsmoduler
  - BC: basis skjema
    - ABAP/4 Workbench, systemadminstrasjon
  - Business Workbench (Customizing, Bus's Navigator)
  - MM, SD, FI, osv moduler
  - skrevet i ABAP/4
  - kan kommunisere via API-er (et kommunikasjonsgrensesnitt – "tabellbeskrivelse" og definerte kommandoer)

Lag 3: SAP GUI (Presentasjonslaget)

- Kjører på klient-Pcen
- vindusknapper, vinduer, scrollbar
- brukers inndata
  - formatvalidering
- (Utnytter MS OLE
  - gir integrasjon til MS-Office)

Tabellstruktur



CTS Correction and Transportation System ("versjonsstyring")

- Flere forekomster (instances) av systemversjoner er mulig
- CTS oppdaterer følgende objekter
  - skjermbilder
  - hjelpetekster
  - programmer
- CTS oppgraderer ved overføring fra utviklingsforekomst til produksjonsforekomst av systemversjonen
- CTS lagrer data om systemendringer

Fokusskifte ved ERP-systemer

- Tradisjonelle satsvise kontroller reduseres
  - Irreversible konsekvenser i sanntid
  - Satsvise kontroller ikke lenger viktigst
  - Papirbasert kontrollspor svekkes / forsvinner
  - Tilgangsbehovene økes til å omfatte nye brukergrupper
  - Endring av faste data kan ha umiddelbare eller temporære virkninger for transaksjonsinnhold
- Og vi styrker istedet
  - Sanntids overvåking og måling
  - Mot ett kontrollpunkt istedenfor mange kp i hele rutinen
  - Noen få men automatiserte og strategiske kontroller erstatter mange delvis redundante sekvensielle kontroller

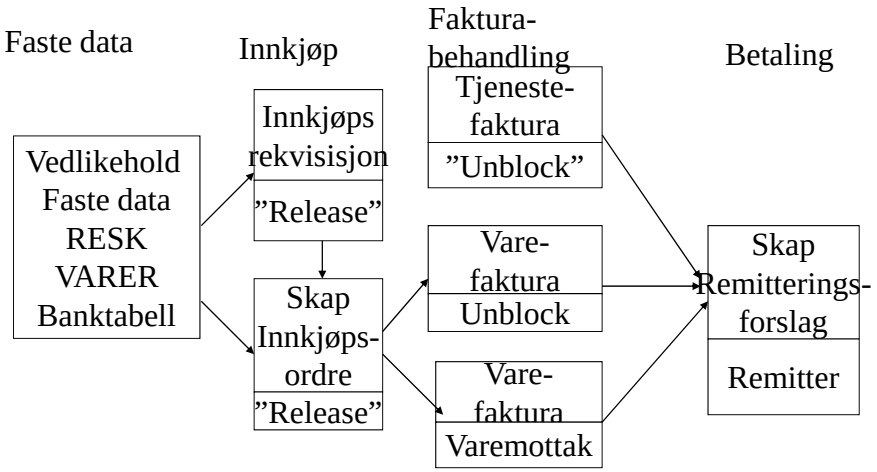
Revisjonsmodell pr forretnings-sykel

- Risikogrupper
  - Vedlikehold av faste data
  - Sentrale transaksjonsprosesser for området
  - Identifiser høyrisiko transaksjoner
  - Relevante autorisasjoner for disse
  - ”Single point of failure”
- Bevisinnsamling
  - Systemdokumentasjon
  - Hente tilgangsautorisasjon (transaksjonskode SE16) fra skjemaet (tabell USOBT_C)
  - Testing i testsystem med system trace
- Vurdering
  - Vurdere konsekvenser av svakhet

Hovedmodulene:regnskap

- FI Financial Accountning
  - likvider, “hovedbok”, kapitalinvestering
- CO Controlling
  - kostnader, planlegning, prosjekter, lønnsomhet, internordre, åpne poster, kostnadsfordeling
- AM Asset management
  - egne aktiva
  - leasede aktiva
  - tomter og bygninger

Blokkskjema: Fra innkjøp til remittering



Hovedmodulene: Personal

- Ledelse
- planlegge
- ansette / entledige
- lønn
- oppgavepliktige ytelser
- organisasjon
- arbeidsflyt (dokumentflyt)

Hovedmodulene: Produksjon og logistikk

- Materialplanlegning
  - struktur, varetabeller, hendelser, økonomi
- Vedlikehold
  - preventivt vedlikehold, reparasjoner, fremdrift, kostnader
- kvalitetsledelse
  - inspeksjon, bekreftelse, råvarer, VIA, FV, fremdrift
- produksjonsplanlegning og styring
  - ressurser, hendelser, sekvensering
- prosjektstyring

Hovedmodulene:
SD - Salg og distribusjon

- Prospect
- ordrebehandling (mottak, oppfølgning)
- distribusjon
- eksportkontroll
- transportledelse
- fakturering, rabatter

SAP Referansemodell
("standardeksempler for implementering")

- Formål: å forstå SAP
- hva må gjøres ved implementering
  - hva, hvem, organisering, informasjonsbehov
- EPC (Event Driven Process Chain)
  - beskriver programlogikken, erstatter programkart
  - hendelse
    - besvarer hvorfor noe skal gjøres
    - informasjon er underordnet/tilknyttet hendelser

Tre konstruksjonsprinsipper

- Hva skal gjøres ?
  - Sekvens, forutsetninger, kvalitet
- Hvem skal gjøre det ?
  - Effektivitet, sikkerhet,
- Hva slags data / informasjon trengs ?
  - Konkrete data
  - erfaring, intuisjon

Ulike modeller (av driften)

- Organisasjonsmodeller
  - organisasjonskart
- Oppgave- eller prosess-modeller
- Informasjons- eller data-modeller

Hendelsens attributter

- (1) navn, beskrivelse, konstruktør, startpunkt: intern, ekstern, systemuavhengig
- (2) Type: interaktiv, automatisk, manuell
- (3) Tid: fast, variabel, frekvens

MP-styring

- Varetabell
- Strukturtabell (Bill of Material)
- ressurser
- forkalkyle
- grovplan (bruttobehov)
- JIT (detaljplan, nettobehov, tider)
- etterkalkyle
- produksjonsordre, materialrekvisisjon

Litteratur

- Steinbart, Romney, Cushing: Accounting Information systems
  - Mange tilsvarende bøker med omtrent samme innhold og tittel
- IT Governance Institute (ISACA): Security, Audit and Control Features / SAP R/3; Rolling Meadows 2002 eller senere utgaver