VALIDERING AV IT-SYSTEMER

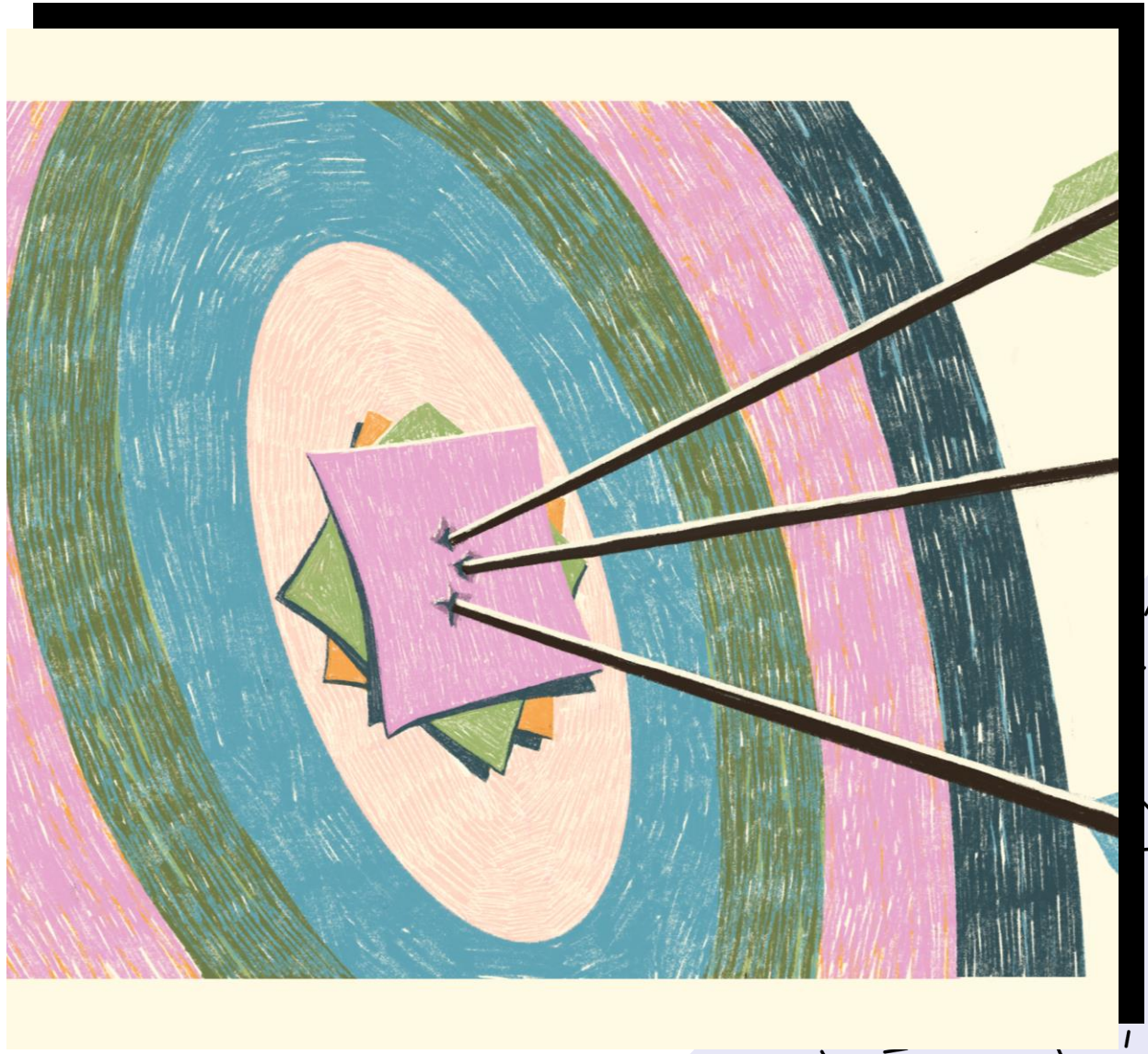
SAEED BEHDAD

TEKNISK BEDØMMER, IT

MÅLSETTING

Gi en forståelse av:

- Hva validering og verifisering av IT-systemer innebærer
- Hvorfor det er viktig i laboratoriemiljøer
- Kravene i ISO 17025 som gjelder for validering av informasjonssystemer



HVA ER VALIDERING OG VERIFISERING?

- **Validering:** Sikre at systemet oppfyller brukernes behov og forventninger.
- **Verifisering:** Teste systemet for å bekrefte at det fungerer riktig og uten feil.
- **Hvorfor dette er viktig:** For å beskytte dataene og sikre nøyaktige resultater i laboratorieprosesser.

HVORFOR ER VERIFISERING VIKTIG?

- Sikre pålitelighet og nøyaktighet av data
- Beskytte data mot feil og tap
- Øke tillit til resultater

ISO 17025 - KRAV I KAP. 7.11

Tilgang til nødvendig data og informasjon (7.11.1)

Validering av funksjonalitet i informasjonssystemer før bruk (7.11.2)

Beskytte systemer mot uautorisert tilgang og tap (7.11.3)

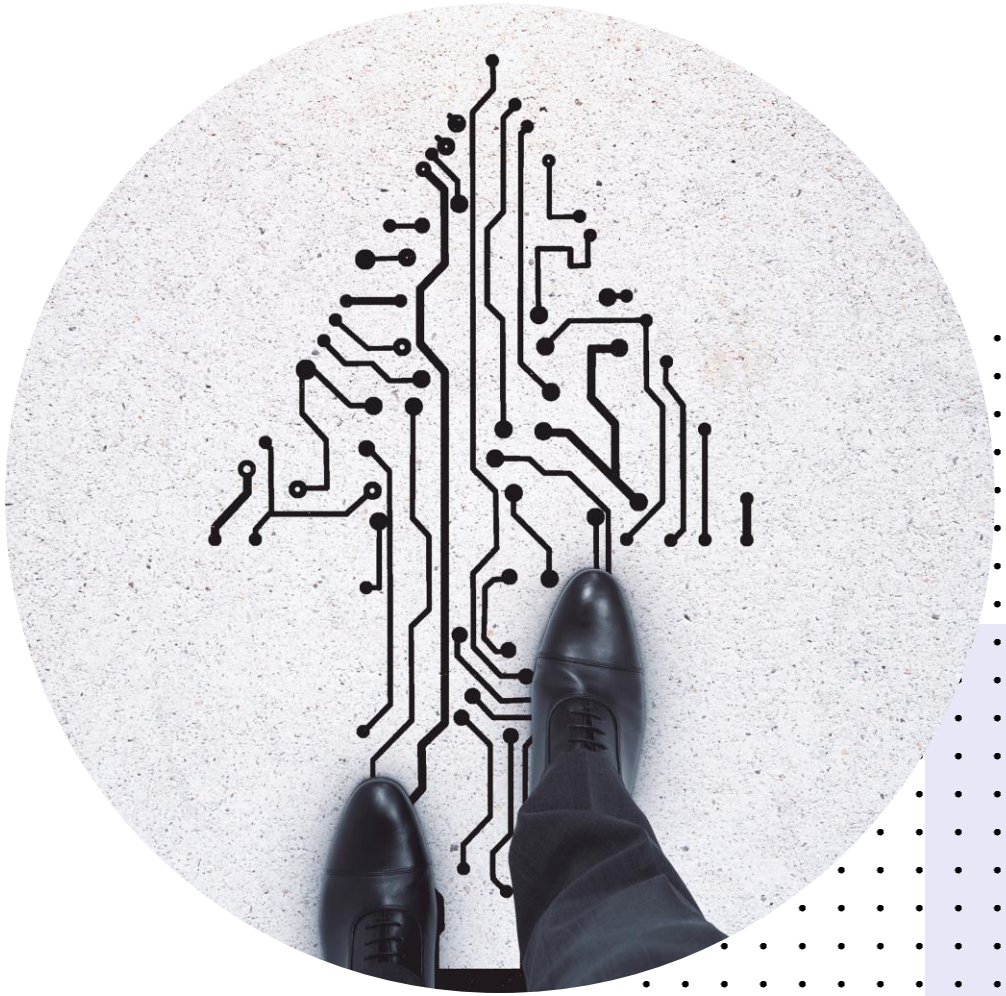
Sikre ekstern drift og vedlikehold oppfyller krav (7.11.4)

Tilgjengelighet av brukerveiledninger og dokumentasjon (7.11.5)

Kontrollere beregninger og dataoverføringer systematisk (7.11.6)

KRAV TIL VALIDERING FØR BRUK

- Planlegging av valideringsprosess og fastsettelse av testkriterier
- Kontroll av systemets funksjonalitet og pålitelighet
- Sikre at systemet fungerer som tiltenkt for alle nødvendige oppgaver
- Endelig godkjent rapport



ANSVARSFORDELING OG ROLLER

- Definer klare roller og ansvar i valideringsprosessen
  - IT-ansvarlig: teknisk testing og vedlikehold
  - Laboratorieansvarlig: verifikasjon av systemets funksjonalitet i henhold til arbeidsbehov
  - Dokumentasjonsansvarlig: sikring av korrekt og fullstendig dokumentasjon

HVA MÅ DOKUMENTERES

- Alle endringer, konfigurasjoner og eventuelle modifikasjoner av systemet
- Risikovurderinger, når relevant
- Testrapporter og rådata
- Formelt godkjent og signert valideringsrapport, og fullstendig dokumentasjon før implementering
- Informasjon om restrisiko og tiltak, når relavant
- Oppdaterte dokumenter (eks. prosedyrer og veiledninger)

RISIKOVURDERING AV IT-SYSTEMER

Når er det behov for risikovurdering eller ny risikovurdering?	
Systemoppdateringer og patching	•Ved større oppdateringer, endringer i programvareversjoner eller sikkerhetspatcher. •Risiko: Kan påvirke systemets funksjonalitet og kompatibilitet med eksisterende prosesser.
Endring i bruksområder eller funksjonalitet	•Når IT-systemet skal brukes til nye oppgaver eller får ny funksjonalitet. •Risiko: Nye bruksområder kan introdusere feil eller sårbarheter som ikke tidligere er vurdert.
Tilpasning eller modifikasjon av kommersielt programvare (OTS)	•Når det legges til spesialtilpasninger eller utvikles makroer/scripts i OTS-programvare (f.eks. Excel). •Risiko: Tilpasninger kan medføre uforutsette feilkilder og redusere dataintegritet.
Migrering av data eller integrasjon med andre Systemer	•Ved flytting av data til nye systemer eller integrasjon med eksterne databaser eller programvare. •Risiko: Økt risiko for datatap, feil i overføringen eller endringer i datakvalitet.
Endringer i brukerroller og tilgangsnivåer	•Når det gis tilgang til nye brukere eller når tilgangsnivåer endres. •Risiko: Økt sårbarhet for uautorisert tilgang og potensielle brudd på dataintegritet.
Endringer i IT-infrastruktur eller Driftsmiljø	•Ved endringer i fysisk eller virtuelt miljø som kan påvirke systemstabilitet (f.eks. serverflytting, endret nettverk). •Risiko: Endringer kan påvirke systemets ytelse, datatilgjengelighet og sikkerhet.

PS! Endring i formål med registreringer (jfr. GDPR og DPIA)

VALIDERING AV OFF-THE-SHELF SOFTWARE (OTS-PROGRAMVARE)

Hva menes med Off-the-Shelf (OTS) programvare?

Kommersielt tilgjengelig programvare ferdig utviklet for generelt bruk

Eksempler: Microsoft Excel, databaser, laboratorie-informasjonssystemer (LIMS)

Fordel: Tidseffektivt og ofte rimeligere enn spesialutviklede systemer

ISO 17025 - Hva sier standarden om OTS-programvare?

Kan betraktes som tilstrekkelig validert dersom den brukes innenfor sitt utformede bruksområde

Viktig å forstå programmets begrensninger og sikre at det er riktig konfigurert til formålet

FORDELER OG UTFORDRINGER MED OTS-PROGRAMVARE

Fordeler:

Ofte godt testet og standardisert

Brukervennlig og med kjent brukergrensesnitt

Support og oppdateringer fra leverandøren

Utfordringer:

Manglende fleksibilitet for spesifikke behov

Kan kreve ekstra kontroll for å møte laboratoriets krav

Risiko for inkompatibilitet ved integrasjon med andre systemer

NÅR TRENGER OTS-PROGRAMVARE EKSTRA VALIDERING

01

Hvis den brukes utenfor sitt opprinnelige bruksområde

02

Ved spesialtilpasninger eller tilleggsfunksjoner som påvirker ytelse og pålitelighet

Eksempel: Makroer eller script laget i Excel som endrer standard funksjonalitet

SJEKK AV BEREGNINGER OG DATAOVERFØRINGER

Hvorfor kontroll av beregninger er viktig?

- Sikrer at resultater er nøyaktige og pålitelige
- Forebygger feil som kan påvirke analyser og beslutninger

Metoder for Kontroll av Beregninger:

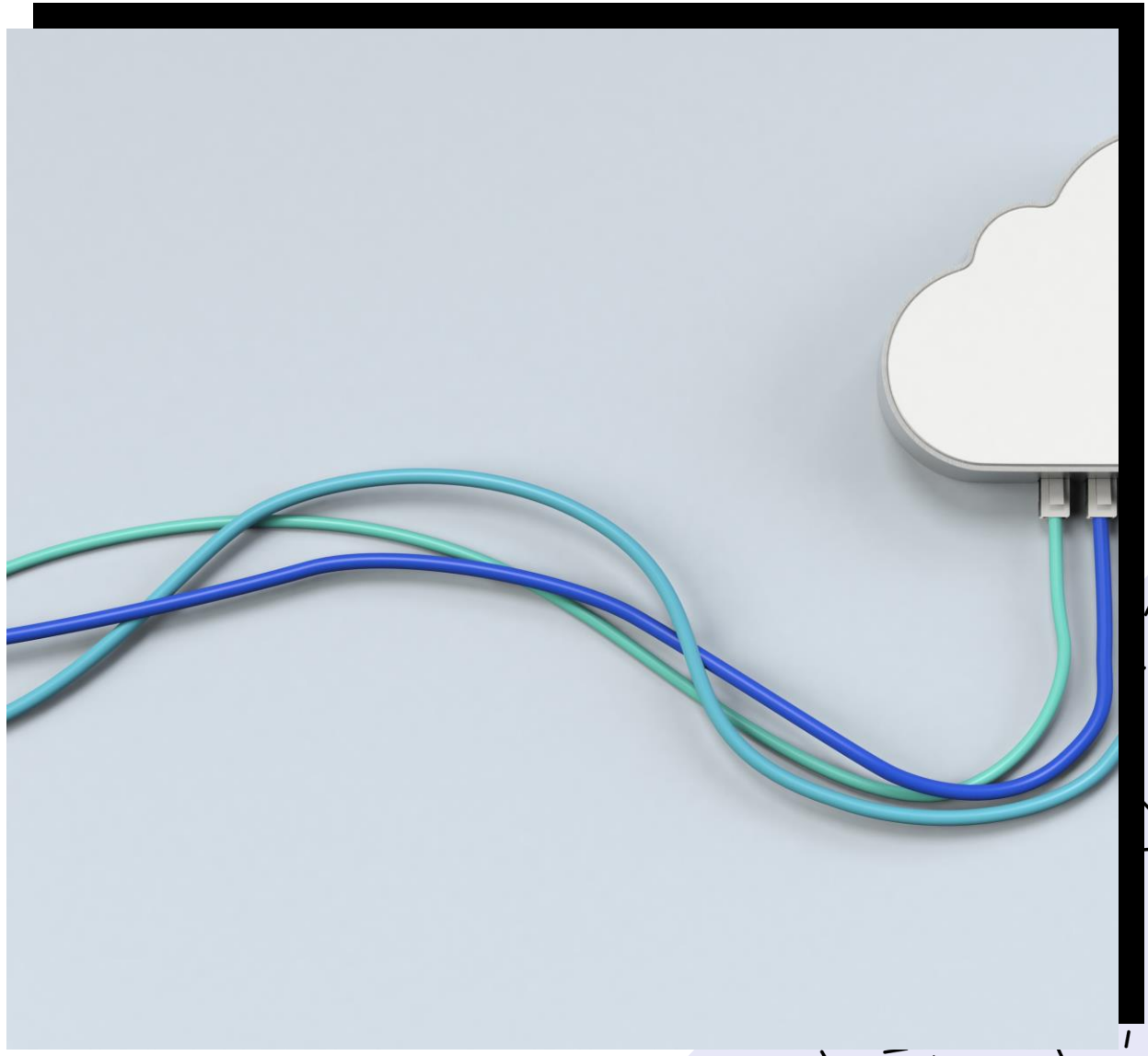
- **Automatiserte tester**: Eks.: Valideringsskript for gjentatte beregninger
- **Manuelle sjekker** Eks.: Sammenligning med tidligere kjente verdier

Kontroll av Dataoverføringer:

- **Dataintegritetskontroll**: Eks.: Sammenlikning av data fra registrering til «svarrapport» for å bekrefte dataintegritet
- **Loggføring av overføringer**: Dokumenter alle overføringer for sporbarhet

Dokumentasjon av Kontroller:

- **Sjekklister**: Eks.: Sjekkliste som inkluderer testtrinn og verifiseringsdato
- **Revisjonsspor**: Eks.: Sporbarhet tilbake til opprinnelig data og endringslogg



VALIDERING AV SIKKERHET OG INTEGRITET I INFORMASJONSSYSTEMER

Sikkerhetstiltak

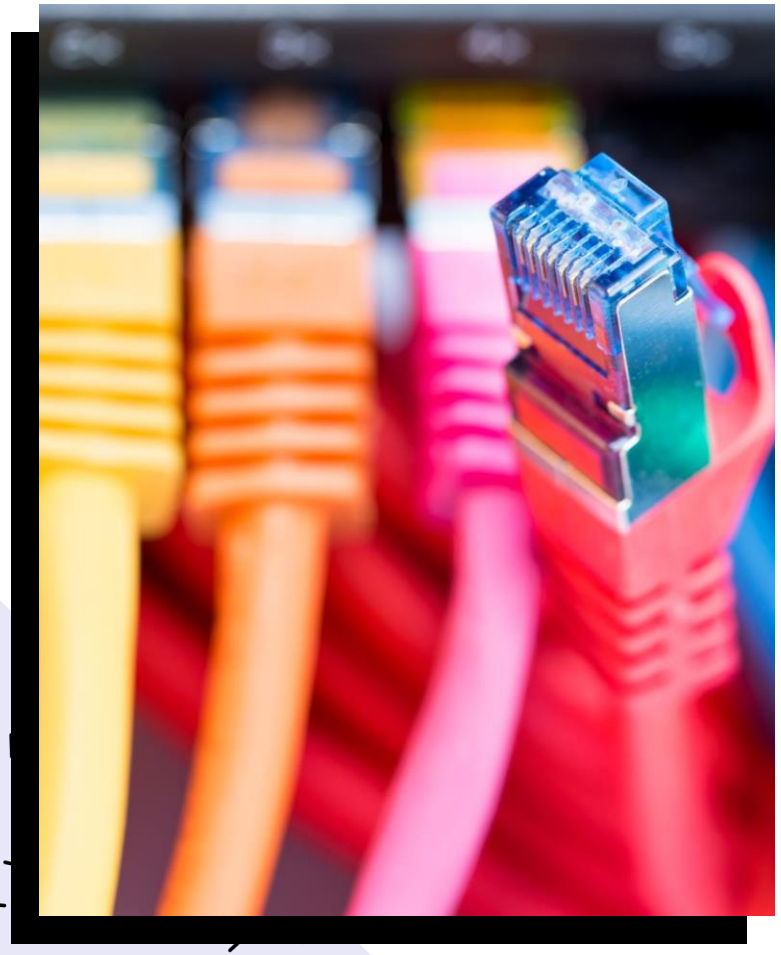
- **Tilgangskontroll**: Rollebasert tilgang, passordbeskyttelse, to-faktorautentisering
- **Loggføring**: Registrering av aktiviteter og endringer i systemet
- **Sikkerhetskopiering**: Regelmessige kopier, test av gjenoppretting

Dataintegritetstiltak

- **Kontroller**: Rutiner for å sikre data mot uautorisert endring, sjekkpunkter
- **Miljøsikring**: Systemet i miljø som beskytter mot fysiske skader

Testing og dokumentasjon

- **Sårbarhetstesting**: Identifisere sikkerhetshull (gjøres av ekstern kompetent part)
- **Funksjonstesting av grensesnitt**: Sikre korrekt dataoverføring
- **Dokumentasjon**: Loggfør tester, endringer og sikkerhetsoppdateringer



VALIDERING AV IT-SYSTEMER VED EKSTERN DRIFT OG VEDLIKEHOLD

Praktiske Steg for Validering:

1. Initial Validering av leverandørens systemer:
    1. Be om leverandørens valideringsdokumentasjon for IT-systemet som skal brukes.
    2. Sikre at dokumentasjonen viser at systemet oppfyller laboratoriets krav til nøyaktighet, sikkerhet og pålitelighet.
2. Risikovurdering før bruk:
    1. Utfør en risikovurdering for å identifisere sårbarheter, spesielt relatert til dataintegritet og tilgjengelighet.
    2. Valider at leverandøren har mekanismer for å håndtere potensielle risikoer (f.eks. sikkerhetsbrudd, driftsstans).
3. Verifisering av dataintegritet og tilgjengelighet:
    1. Gjennomfør tester for å bekrefte at data håndteres korrekt, uten tap eller endring.
    2. Valider at systemet sikrer kontinuerlig tilgang til data, også under uforutsette hendelser.
4. Periodisk validering og re-testing:
    1. Planlegg regelmessig re-testing av systemets ytelse og sikkerhet for å sikre fortsatt samsvar.
    2. Bruk stikkprøver for å validere at systemet fortsatt oppfyller standarder og kvalitetskrav.
5. Dokumentasjon og revisjon:
    1. Behold detaljert loggføring av all valideringer, testresultater og endringer som utføres av leverandøren.
    2. Dokumenter resultatene fra revisjoner og valideringstester som en del av laboratoriets kvalitetskontroll.

OPPDATERT BRUKERVEILEDNINGER OG DOKUMENTASJON

Hvorfor Dokumentasjon er viktig for validering?

- Sikrer at systemene brukes korrekt og effektivt
- Underbygger alle valideringsprosesser og tester
- Gir sporbarhet og oversikt ved revisjon eller feil

Nødvendig dokumentasjon

- **Brukermanualer**: Instrukser for riktig bruk og vedlikehold
- **Referansedata**: Spesifikasjoner for systemets funksjonalitet og testkriterier
- **Valideringsprosedyrer**: Steg-for-steg beskrivelser av tester og kontroller

Hvordan oppbevare og oppdatere dokumentasjonen:

- **Tilgjengelighet**
- **Endringslogg** (sporbarhet)
- **Periodisk gjennomgang**

EKSEMPLER PÅ VERIFISERINGSTILTAK I PRAKSIS

1. Funksjonalitetstesting av Systemet:

- Eksempel: Test av programvare for beregning av laboratorieresultater for å sikre nøyaktige resultater.
    - Utfør testkjøringer med kjente referansedata og sammenlign resultater for å validere programvarens nøyaktighet.

2. Kontroll av dataoverføringer:

- Eksempel: Verifisering av dataoverføring mellom laboratorie-informasjonssystemet (LIMS) og rapporteringssystemet.
    - Sjekk at alle data fra LIMS overføres korrekt uten tap eller endring ved å bruke egent kontrollmetoder som for eksempel datarevisjon (vertikal revisjon).

3. Endringskontroll ved oppdateringer:

- Eksempel: Testing etter en oppdatering i kommersiell programvare (f.eks. ny versjon av Excel brukt til databehandling).
    - Valider at endringen ikke påvirker eksisterende beregninger eller rapporter ved å sammenligne resultater før og etter oppdateringen.

4. Test av sikkerhetstiltak:

- Eksempel: Testing av tilgangskontroller i systemet for å sikre at kun autorisert personell har tilgang til sensitive data.
    - Utfør simuleringer av uautorisert tilgang for å bekrefte at sikkerhetstiltak som passord og tofaktorautentisering fungerer som forventet.

5. Sjekklister for manuelle prosesser:

- Eksempel: Bruk av sjekklister for manuell dataregistrering i tilfeller der systemet ikke er automatisert.
    - Verifiser registreringer ved å sammenligne med en kjent dataprøve, og loggfør sjekken for sporbarhet.

OPPSUMMERING

Viktige verifiseringstiltak:

- **Funksjonalitetstester**: Kontroller at systemene utfører oppgaver som forventet.
- **Sikkerhetskontroller**: Implementer tilgangsstyring, loggføring, og sikkerhetskopiering.
- **Dataoverføringskontroller**: Valider at dataoverføringer skjer uten feil eller tap.

Dokumentasjon og kontinuerlig overvåking:

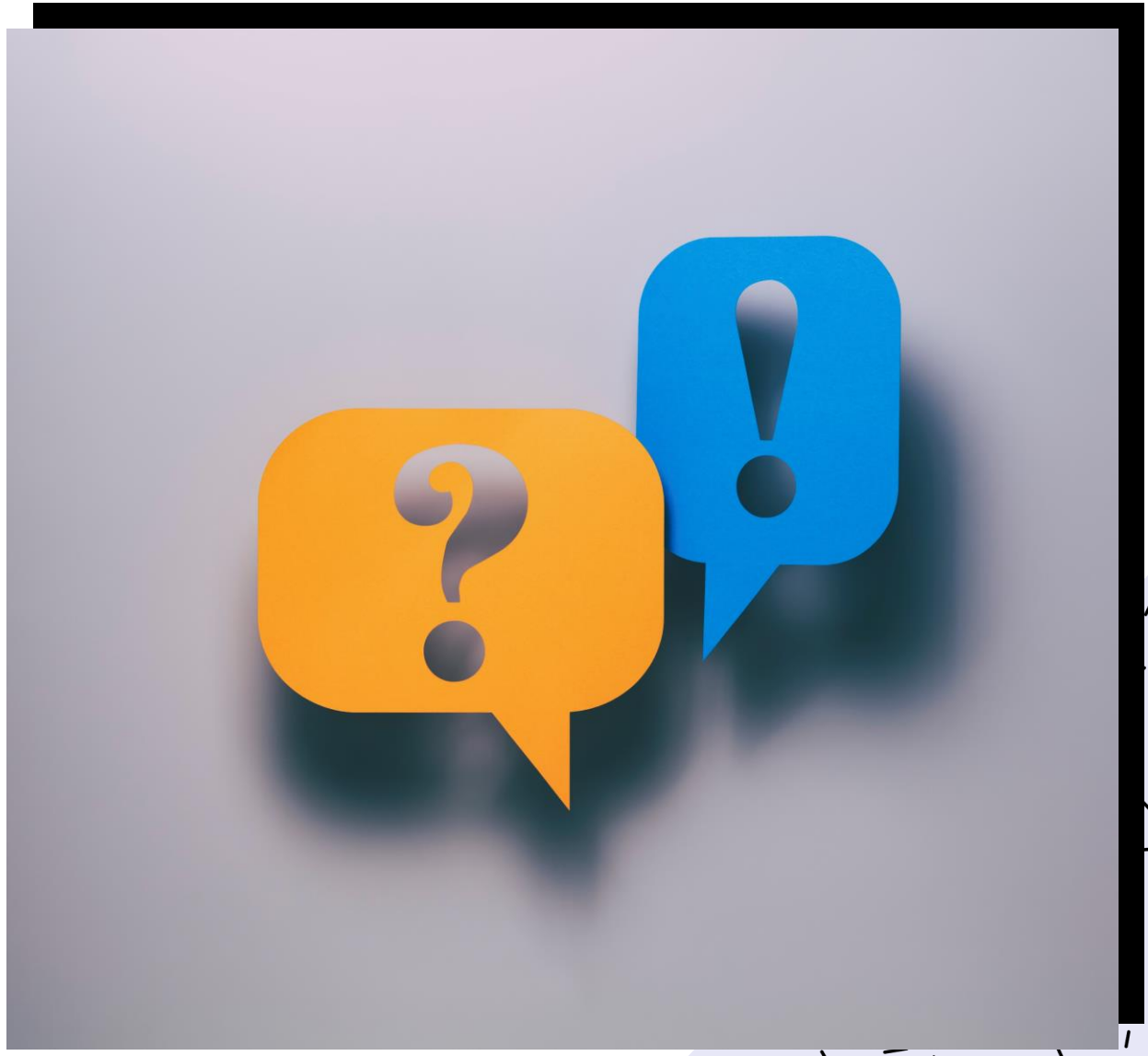
- **Dokumentasjon**: Hold oppdatert dokumentasjon av alle endringer, tester, og bruksprosedyrer.
- **Endringskontroll**: Bevar dokumentasjon og vurderinger for alle viktige aktiviteter og endringer.
- **Kontinuerlig overvåking**: Regelmessig gjennomgang og oppdatering for å sikre systemenes samsvar med kravene.

Hvorfor dette er viktig?

- **Dataintegritet**: Opprettholde nøyaktige og pålitelige laboratorieresultater
- **Samsvar**: Sikre at laboratoriets praksis er i tråd med ISO 17025 og andre regulatoriske krav
- **Risiko- og feilreduksjon**: Forebygge potensielle feil som kan skade omdømme eller resultater

SPØRSMÅL

- Praktiske utfordringer?
- Generelle problemstillinger i hverdagen?




TAKK FOR MEG