Semicolon kokebok 2.0

Sjekkliste ved endring og etablering av informasjonsutveksling

Versjon : 2.0

Dato : 14. Mars 2014

Forfattere:

- Per Myrseth (DNV GL)
- Erlend Øverby (Karde AS)
- Terje Grimstad (Karde AS)
- Thom-Kåre Granli, Institutt for Privat rett, Juridisk fakultet, Universitetet i Oslo

Versjonshistorikk for dette dokumentet

Versjon & Dato	Kommentar og ansvarlig
1.0, Desember 2012	Basert på UDIs effektprogram og Semicolons erfaringer.
2.0, Mars 2014	Basert på innspill gjennom Semicolon case for DIFI i 2013 og andre Semicolon erfaringer.

Innholdsfortegnelse

1 Introduksjon

Hensikt med dette dokumentet er å gi mottaker og avsender i en informasjonsutveksling en sjekkliste for hva de bør avklare, utrede og beslutte når de innleder samarbeid om å etablere eller endre informasjonsutveksling.

Sjekklistene for avsender og mottaker som er beskrevet i dette dokumentet må sees i sammenheng med dokumentene:

- Veiledning i bruk av Semicolon kokebok
- Intensjonsavtale
- Utvekslingsavtale

Sjekklistene er ment å dekke sentrale spørsmål fra idestadiet frem til signert utvekslingsavtale. Utvekslingsavtalen med bilag beskriver bl.a. hvilken informasjon som skal utveksles for å oppnå hvilke mål. Etter signering av utvekslingsavtalen anbefaler vi at en starter detaljert design av nye arbeidsprosesser og design av ny IT-støtte for å realisere informasjonsutvekslingen.

Hindringer for informasjonsutvekslingen og elektronisk samhandling er:

- Organisatorisk og enkeltpersoners manglende vilje og evne til å samhandle
- Uavklarte og eller motstridende juridiske aspekter
- Budsjetter og ressurser, fraværende eller i utakt mellom etater.
- Ukjent eller lav datakvalitet
- Ukjent eller for høy risiko
- Uklart gevinstpotensial
- For lite innsalg av hvorfor informasjonsutvekslingen bør etableres.
- For liten vilje til å endre det faktum at borger/næringsdrivende for ofte er «brevdue» mellom offentlige etater.
- Fordeling av kostnader og uttak av gevinster mellom partene skaper ulik motivasjon for deltakelse.
- IKT-problemer, gjerne knyttet til eldre IT systemer eller mangel på et tidsvindu for å kunne gjennomføre koordinerte endringer hos flere parter.
- Termer og begreper som ikke lar seg samordne

Gjeldende arkitekturprinsipper for offentlig sektor er tjenesteorientering, interoperabilitet, tilgjengelighet, sikkerhet, åpenhet, fleksibilitet og skalerbarhet [19]. Semicolons sjekklister og avtaler vil hjelpe etater med å følge disse prinsippene.

Ansvaret for tilstrekkelig kvalitet på data som benyttes i saksbehandling, ligger hos bruker/mottaker. Avsender må beskrive og avgi data slik at mottaker har mulighet til å både vurdere om det er mulig

forstå dem og om de er egnet til bruk. Avsender har et ansvar for at avgitte data brukes i henhold til hjemler hos avsender.

En ferdig utfylt sjekkliste for både avsender og mottaker er anbefalte bilag til utvekslingsavtalen.

I tillegg til sjekklistene under, er det laget egne kapitler i dette dokumentet som beskriver viktige momenter, reiser spørsmål og gir litteraturhenvisninger som kan være relevant for etablering av informasjonsutvekslingen.

1.1 Vurdering av omfanget til sjekklisten

Kokeboken med sjekklister kan virke litt omfattende for noen informasjonsutvekslingsprosjekter. Vi vil derfor anbefale at prosjekter som benytter kokeboken gjør en analyse og vurdering av hvilke sjekklistepunkter som er relevante. Vi vil også anbefale at det vurderes hvilke sjekklistepunkter som bør dokumenteres og legges til intensjonsavtalen.

2 Sjekklister til intensjonsavtalen

2.1 Veiledning til kolonnene i sjekklistene:

Kolonnene i sjekklistene under har følgende betydning

- **Nr**: Er kun for identifikasjon og henvisning til spørsmålet.
- **Spørsmål**. Er basert på Semicolons arbeid med avtalene og sjekklistene. Motivasjon og forklaring til flere av spørsmålene er beskrevet i egne kapitler i dette dokumentet.
- **Ja/nei**. Avgrensning til ja eller nei som svaralternativer på spørsmålet er bevisst. Dette fordi ett nei bør fører til stopp eller utsettelse av prosjektet.
- **Dokument.** Her oppgis hvor spørsmålet er besvart, gjerne med henvisning til avtale-bilag, notat, rapport, forskrift etc.
- **Signatur & rolle**. Viser hvem som har ansvaret for at spørsmålet er tilstrekkelig utredet og at vedkommende har fullmakt og kompetanse til å besvare spørsmålet

Kolonner som kun finnes i sjekklisten for utvekslingsavtalen:

- **Kategori**. Viser hvilke av følgende kategorier det enkelte spørsmålet er knyttet til:
    - Informasjon: Fokuserer på informasjon med sin selvstendige verdi uavhengig av hvilket/hvilke IT-system som benyttes for å håndtere informasjonen. Beskrivelse av betydning og begrepsmodeller er koblet til dette laget.
    - Prosess: En etats interne prosess
    - Prosjekt: Det aktuelle prosjektet som bruker sjekklisten.
    - Jus: Knyttet til betydning av informasjon, hjemler for å innhente, benytte, avgi, samt krav til forvaltning og sikkerhet.
    - Risikostyring: gevinstanalysen, endringsstyring, kvalitetsledelse, risikoledelse mm.
- **Mottakersjekkliste.** Kommentar om punktet er gyldig kun for avsender eller både mottaker og avsender.

Følgende sjekkliste bør benyttes før en inngår intensjonsavtalen.

2.2 Intensjonsavtale: Sjekkliste for Mottaker

Nr	Spørsmål	Ja/nei	Dokument	Signatur & rolle
1	Har vi budsjett for gjennomføring av planleggingsfasen?			
2	Har vi beskrevet prosessen hvor data skal anvendes?			
3	Har vi beskrevet hvilke data vi trenger?			
4	Hvilke alternative kilder til data finnes, egen datafangst, hente fra andre, flette fra flere kilder etc.			
5	Har vi hjemmel til å spørre om data fra avsender? / Har vi hjemmel til å innhente data fra andre enn avsender.			
6	Har vi lov til å benytte data?			

2.3 Intensjonsavtale: Sjekkliste for Avsender

Nr	Spørsmål	Ja/nei/	Dokument	Signatur & rolle
1	Har vi aktuelle data?			
2	Er data underlagt utleverings restriksjoner?			
3	Er det hjemmel/lov til å avgi data til aktuelt formål?			
4	Kan data bli åpne data?			
5	Er det alternative kilder til sammenlignbare data?			
6	Har vi beskrevet prosessen for hvordan data blir opprettet og forvaltet?			
7	Har vi budsjett for gjennomføring av planleggingsfasen?			
8	Har mottaker egnede prosesser og sikkerhetsmekanismer for å kunne bruke og forvalte mottatte data?			

3 Sjekkliste til utvekslingsavtalen

3.1 Utvekslingsavtalen, sjekklister for Avsender

Denne sjekklisten for utvekslingsavtalen forutsetter at Avsendersjekklisten for intensjonsavtale er besvart.

Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker-sjekkliste
1. Er det alternative kilder til sammenlignbare data? Om flere kilder: • Basert på hvilke kriterier ble kilde valgt? • Er samme kilde best egnet gjennom hele året/livsløpet? • Er det de faktiske verdier fra datakilden som er interessant eller kan enkle ja/nei svar eller svar på over / under terskelverdier benyttes.		Bilag 1		Kopi
2. Er de valgte opplysningstypene for utveksling beskrevet slik at mottaker enkelt kan forstå dem. • Er informasjonsmodell, begrepsmodell med identifikatorer og utvekslingsmodell etablert for utvekslingen? Se kap 4.1 Beskrivelse av data. • Er opphavet og forvaltningsregimet til data beskrevet (provenance data) • Er kvalitetskrav til datakilden hensiktsmessig beskrevet?		Bilag 1 ,3		Snu sp.
3. Evner IT-systemene å hente ut de aktuelle data iht forventninger? • Kan avgiver systemene møte mottakers krav til SLA og risikoappetitt. • Er det beskrevet hvor i vårt system informasjon finnes og har systemet evne til å avgi de aktuelle data på en egnet måte for mottaker?		Bilag 1 ,3		Snu sp.
4. Er rettigheter, kilde og forvaltningskrav beskrevet på en hensiktsmessig måte for mottaker • Opphav til data klart? Se kap 4.2 Etablering og forvaltning, 4.3 aktiviteter & infobruk + [9] • Opphav til opplysningstyper? Er det gjort søk i SERES og evt. andre metadatakilder om noen har beskrevet relevant felles modell/deler av modell? • Hva/hvem en har data om (populasjon)? Se 4.1.1 Populasjon. • Tilhørende forvaltningsregime? Se kap 4,7 Datakvalitet • Sikkerhetskrav? Se kap 4.10 Sikkerhet		Bilag 1, 3		Snu sp.
5. Er juridiske krav og forutsetninger som avsender må forholde seg til i sin databehandling og utlevering kartlagt? • Er det rettslige grunnlaget for informasjonsbehovet beskrevet?		Bilag 1, 2		Snu sp.

Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker-sjekkliste
Se kap 4.3, virksomhetsmodell.				
6. Er det beskrevet en virksomhetsmodell som beskriver plassering av informasjonsutvekslingen? • Er kobling mellom arbeidsprosesser, informasjonsutveksling, IT-systemer og krav/jus beskrevet. • Er ansvar / eier for de prosesser som blir berørt av informasjonsutvekslingen klart Se også virksomhetsmodell kap 4.11 og Kap Jus 4.4.		Bilag 1, 2		Kopi
7. Håndtering ved endring i data som er utvekslet (klagebehandling mm). Det er en utfordring å vite hvilken tilstand en opplysning er i, og noen ganger må endringer i innhold eller tilstand til en opplysning ettersendes. • Er håndtering av endringer ved bl.a. klagebehandling i data beskrevet som aktiviteter mellom avsender og mottaker? • Er disse tilstander (ulike typer endringer) på data del av informasjonsmodell, begrepsmodell og utvekslingsmodell hos avsender? Håndtering ved feil i data. • Er håndtering av feilsituasjoner på data beskrevet som aktiviteter mellom avsender og mottaker? • Er disse tilstander (feil og ulike typer endringer) på data del av informasjonsmodell, begrepsmodell, prosessmodell og utvekslingsmodell hos avsender?		Bilag 1 Bilag 4 (SLA), 5		Snu sp.
8. Hvordan sikres tilstrekkelig datakvalitet • Hva kjennetegner gjeldende minimumsnivå for datakvalitet? Se kap 4.5 Transformasjoner, 4.7 Datakvalitet og 4.9 Endringer. • Er avsender og mottakers krav til datakvalitetsnivå beskrevet og harmonisert. Se 4.7 Datakvalitet og ISO 8000 [10]. • Hvordan måles og sikres forventet nivå av datakvalitet		Bilag 1		Kopi

9. Er virksomhetens kultur, modenhet, rutiner og kompetanse egnet for å etablere informasjonsutveksling.
Virksomhetene og evt. innleide virksomhetsutviklere, IT-ressurser mm, må spille hverandre gode for å få full uttelling av informasjonsutvekslingen.
• Har virksomheten hatt suksess med tilsvarende prosjekter
  o når det gjelder prosjektleveranser?
  o uttak av planlagte effekter?
• Har virksomheten egnede systemutviklingsmetoder, rutiner og verktøy?
		Bilag 1, 4		Kopi

Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker-sjekkliste
• Er IT arkitekturer og sikkerhetsarkitekturer egnet for ønsket informasjonsutveksling? • Har virksomheten prosjekteiere og prosjektledere som vil og kan håndtere prosjektet?				
10. Kan avsender forsikre seg om at mottaker forstår data korrekt? Er følgende beskrevet tilstrekkelig. • Avsenders tolkning av data? Se 4.1 Beskrivelse av data. • Mottakers tolkning av data? Se 4.1 Beskrivelse av data. • Transformering av dataformat, datastruktur og semantikk. Se 4.5 transformasjoner. Kan avsender forsikre seg om at mottaker får de opplysningene de rettslig sett har bruk for? Er følgende beskrevet tilstrekkelig. • Mottakers saksbehandling/ oppgaveløsning og virksomhetsmodell		Bilag 1 Bilag 1, 2		Kopi
11. Hvilke nye rutiner må etableres knyttet til utveksling av data? Eksempel på rutiner: • Sletterutiner internt • Håndtering av logger for datautveksling • Ettersending ved feil i data • Endringer som må håndteres knyttet til omgjøringsplikt hos mottaker • Varsling ved endringer i: forskrifter, tolkning av data/begrepsmodell, programvare og bruk av data, etc. • Er ansvar for risikostyring tydelig hos de involverte? Rutiner for håndtering ved feil på teknologi • Er håndtering av feilsituasjoner på teknologi beskrevet som aktiviteter mellom avsender og mottaker? • Er det tilrettelagt for test og driftsmessig overvåking av tekniske tjenester.		Bilag 1 Bilag 4 Bilag 5 Bilag 6 Bilag 4 (SLA)		kopi.
12. Er metodisk tilnærming og tidsplan for risikoanalyser avklart? Gjelder blant annet risikoanalyse av prosjektmål, effektmål og operasjonell risiko: • Design og etablering av datautvekslingen med tilhørende tiltak godkjent av relevant ansvarlig/ rolle? • Etablering av testmetode, testmiljø og testdata i et inter-etat testmiljø. • Er ansvar for etatsprosesser klart beskrevet og avklart.		Bilag 11: Mandat og prosjektplan		Kopi

Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker-sjekkliste
• Er ansvar for prosjektleveranser klart beskrevet og avklart. • Er ansvar for informasjonsutvekslingen beskrevet og avklart. • Endringer i informasjonsutvekslingen og konsekvenser på ulike nivå (teknisk, organisatorisk mm.) • Forhold hos involverte parter, inkl tredjeparter • Helheten av samhandlingen • Er ansvar for risikostyring tydelig hos de involverte Se kap 4.6 Risikoanalyser og risikostyring.		Bilag 6		
13. Er metodisk tilnærming og tidsplan for kvalitetsstyring avklart? • Er rutiner for kvalitetssikring etablert hos begge parter, eksempelvis ISO 9000 el. Eksempelvis: kvalitetssikring av: • Nye rutiner for saksbehandling, informasjonsforvaltning etc. • Ny teknologi og programvare, inkl. konfigurasjonsstyring av programvare • Nye grensesnitt internt og eksternt • Systemutviklingsrutiner, testing av programvare mm • Er ansvar for risikostyring tydelig hos de involverte • Etablering av sikkerhetsmekanismer Dette må sees opp mot avtalebilagene for bl.a. prosessbeskrivelse, begrepsmodeller og hjemmel/juridiske krav.		Bilag 11: Bilag 6		Kopi
14. Er metodisk tilnærming og tidsplan for gevinstrealisering avklart? • Hvordan er det planlagt å måle at gevinsten som lå til grunn for etablering av informasjonsutvekslingen, er oppnådd og hvem er ansvarlig?		Bilag 11		Kopi
15. Er innsalg og forankring av prosjektet samt etablering av budsjetter, mandat og fullmakter etc. etablert? • Gjelder for hver prosjektfase for etablering av informasjonsutvekslingen.		Bilag 11		Kopi
16. Er planlagte tidsvindu realistisk? • Utredningsaktiveter og risikoanalyser frem til avtaleinngåelse? • Utvikling av løsninger hos de enkelte, er det tilstrekkelig tilgang til ressurser for opplæring, systemutvikling, rutineutvikling etc. • Er det egnede tidsvindu hos alle involverte (også underleverandører og tredjeparter) som gjør det mulig å teste systemer, rutiner mm hos alle involverte.		Bilag 11		Kopi

Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker-sjekkliste
• Er endringer i saksbehandlingsrutiner og programvare mulig å gjennomføre på ønsket tid hos (i) avsender og (ii) mottaker, (iii) tredjeparter/ASP/Cloud tjenester og/eller offentlige felleskomponenter som Altinn, SERES mm.				
17. Hvordan håndteres endringer? Over tid endres måten vi jobber på, hvilke systemer som samvirker, hvor en mottar data fra etc. • Hvordan skal endringer som påvirker informasjonsutvekslingen håndteres? • Hvem har ansvar for å fange dem opp samt ta ansvar for at de blir håndtert? • Hvordan håndtere eventuelle økonomiske konsekvenser (som partene kan påføre hverandre)?		Bilag 5		Kopi
18. Må support, øvelser og avtaler koordineres? Vil innføring av informasjonsutveksling mellom etater føre til at øvelser, beredskap, supportavtaler, avtaler for tjenestenivå (SLA)/ oppetider m.m. må koordineres partene imellom?		Bilag 4		Kopi
19. Er rutiner for konfigurasjonsstyring av endringer som påvirker annen part beskrevet? • Er plan for innføring av konfigurasjonsstyring hensiktsmessig for å sikre informasjonsutvekslingen? • Er ansvar for godkjenning og gjennomføring av endringer plassert hensiktsmessig • Er nødvendige sw utviklingsmiljø, testmiljø og testdata og tilgjengelig for enkelt å håndtere feilretting og videreutvikling? • Er det etablert et forum/samhandlingsforum hvor partene møtes og diskuterer fremtid for samhandlingen. Konfigurasjonsstyring bør gjelde alle typer modeller, IT-systemer, operative rutiner for saksbehandling, informasjonsforvaltning, datakvalitet, data-transformasjoner og grensesnitt på alle nivåer.		Bilag 4, 5 Bilag 6 Bilag 10, Samledokument Bilag 10, Samledokument		Kopi
20. Er ansvar og innhold i tredjepartsroller og tjenester avklart tilstrekkelig? • Er det avhengigheter til andre parter, tredjeparter, driftsleverandører, forvaltere og driftsoperatører av felleskomponenter etc. Slikt må avklare og koordineres. • Er transformasjoner og protokollkonverteringer beskrevet og ansvar for vedlikehold og konfigurasjonsstyring av disse hensiktsmessig?		Bilag 5		Kopi
21. Har partene sikret seg tilgang til hverandres ressurser og tjenester • Gjelder personell, IT utstyr, kapasiteter, IT-systemer, sikkerhetsmekanismer, datakilder, økonomi • Tilgang til både egne og andres underleverandører (drift, nett, beredskap, felleskomponenter etc). Eksempelvis via Service Level Agreements for å nå krav til tilgjengelighet, kapasiteter, sikkerhetsmekanismer og protokoller osv.		Bilag 4, 11		Kopi

Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker-sjekkliste
Gjelder i de ulike prosjektfaser, initiering, utredning, utvikling, test og driftsituasjon.				

Spørsmålene i sjekklisten treffer ulike faser i et informasjonsutviklingsprosjekt, og noen treffer også forvaltningsfasen. Spørsmålene besvares i tidlig prosjektfase, mens effekten og risikoreduksjonen inntreffer på et senere stadium i prosjekt- og forvaltningsforløpet. Spørsmålene er rettet mot interoperabilitetslagene delt i tema som teknologi, informasjon og semantikk, arbeidsprosesser og støtteprosesser samt juridiske utfordringer. For å visualisere hvor sjekklisten treffer prosjektfaser har vi i figuren under grovt plassert de enkelte spørsmål inn i forhold til en matrise hvor aksene er henholdsvis prosjektfaser og interoperabilitetslag. Hensikten med denne øvelsen er å se hvor i matrisen vi har klart å bidra til bedring/risikoreduksjon versus hvor vi ikke har hatt fokus. Således vil også oversikten være til hjelp for lesere av dette dokumentet slik at det er tydeligere hvor vi ikke har fokusert.

Interoperabilietslaget for prosess og organisasjon vil være delt i virksomhetens hovedprosesser og støtteprosesser. Prosjektgjennomføring, systemutvikling og forvaltning vil være støtteprosesser. Gevinster vil vanligvis være knyttet til for eksempel saksbehandling som hovedprosesser.

3.2 Utvekslingsavtalen, sjekkliste for Mottaker

For hvert spørsmål i sjekklista er det kommentert om spørsmålet skal snus til å sette mottaker i sentrum eller om spørsmålsteksten kan kopiers som den står.

Mottakersjekklisten forutsetter at Mottaker-sjekklisten for intensjonsavtale er besvart.

4 Appendiks: Faglig supplement til sjekklistene

4.1 Beskrivelse av data/opplysningstype

Data bør beskrives i henhold til en 3-lags inndeling med modeller for følgende lag:

- **Begrepsmodell**, som beskriver/definerer hvordan data som utveksles skal tolkes.
    - Denne modellen lages gjerne i UML verktøy eller et ontologiverktøy.
    - Eksempel på metode og verktøy er SERES, evt verktøy som er evaluert i Semicolons notat «Survey on vocabulary and ontology tools» [29]
    - DIFI standard for begrepsbeskrivelser gjelder for dette nivået [6].
    - Opplysningstypene/begrepene som beskrives skal være uttrykt i denne modellen
- **Informasjonsmodell**, som beskriver den sammenhengen de utvekslede data skal tolkes i lyset av.
    - Denne modellen lages gjerne i UML-verktøy eller et ontologiverktøy.
    - Eksempel på metode og verktøy er SERES, evt se [29].
- **Utvekslingsmodell/meldingsmodell** som beskriver dataformatet som benyttes ved selve utvekslingen. Formatet må evne å koble alle verdier i en gitt utveksling til aktuelle begreper i en begrepsmodell.
    - Denne modellen lages gjerne som et XML Schema eventuelt som et UML klassediagram hvor XML Schema modell kan genereres basert på UML-modellen.
    - Eksempel på metode og verktøy er SERES.

Selv for små modeller vil en god editor som bistår med å holde de tre nivåene sammen være til stor nytte. Hver av disse modellene er i bevegelse ved endring av saksbehandlingspraksis, endring i lover og regler. Konfigurasjonsstyring er like viktig for disse modellene som for programkode. Mange prosjekter starter gjerne med å lage modellene i tekstbehandlingsverktøy eller regneark.

For å få med tidsdimensjonen ved informasjonsforvaltning og bruk, kan en stille spørsmål knyttet til endring, eksempelvis: Har det vært eller vil de bli endringer i:

1. hva data brukes til?
2. hvordan data tolkes?
3. hvilke lover og regler som gjelder ved utveksling, forvaltning og bruk av data.
4. hvordan data innhentes?
5. hvordan informasjon kobles til annen informasjon?
6. hvordan data oppbevares, struktureres, formatvalg etc?
7. datakvalitet eller måten en måler datakvalitet?

Gode begrepsmodeller skal kunne gi svar på bl.a følgende:

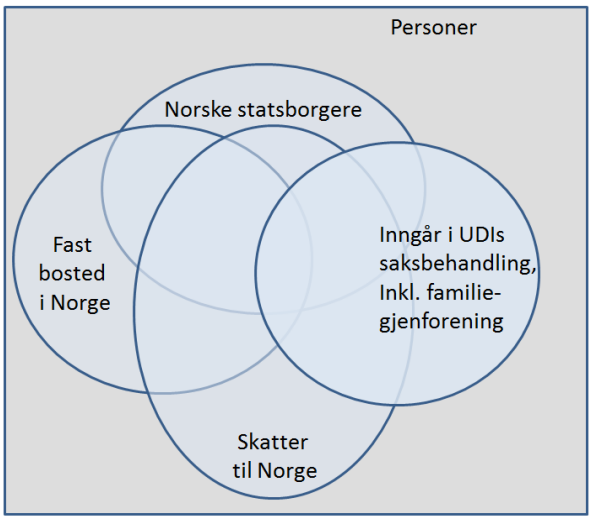
- Hvor kommer begrepene fra, eksempelvis lov, forskrift, praksis etc. Se også bilag 2 til utvekslingsavtalen, hjemmelsgrunnlag.
- Forhold til tilsvarende begrep hos de involverte parter samt juridisk kilde om det finnes. Vurdere om
    - begrepene er semantisk ekvivalente
    - begrepene er overlappende, Sub/Super type begreper, Synonyme begreper
    - hvordan transformasjoner av data mellom begreper kan gjøres
- Er avsender og mottaker modellene på samme nivå? Vanlig eksempel på ulikt nivå er hvis begreper hos avsender ikke er begreper hos mottaker, men verdier i en kodeliste i mottakers modell?

Supplerende litteratur kan være:

- Sjekkliste for testing av elektroniske meldinger mellom virksomheter [3]
- ISO 704 Terminologistandardisering [5]
- DIFI standard for begrepsbeskrivelser [6]
- SERES metoder for modellering og kvalitetssikring av modeller [7]
- Livssyklusprosess for utarbeidelse og forvaltning av begrepssystemer [22]
- Standard for begrepskoordinering[23]
- Kapittel om harmonisering av begreper, basert på Semicolon case for SKD 2013.

4.1.1 Populasjon og endringer i populasjoner

Som del av begrepsmodellen må det også beskrives egenskaper ved populasjonen eller mengden (hvilke personer/ bedrifter/husstander etc) en har data om. Eksempelvis har SKD oversikt over personer som har en skattemessig relasjon til den norske stat (det vil si en populasjon av personer), mens UDI trenger opplysninger om mange personer som ikke finnes i SKD sine systemer ei heller i folkeregisteret, det vil si UDI trenger informasjon om mange av de personer SKD har data om, men trenger også data om en rekke andre personer.



Figur 1, sammenheng og ulikhet i populasjoner av personer

Ven-diagrammet over søker å gjenspeile at populasjoner kan overlappe og at en person kan være med i flere populasjoner. Hvilke eller hvilke delmengder en person er med i vil også endres over tid.

Ved informasjonsutvekslingen er populasjon og endringer i populasjon vesentlig siden informasjons-utvekslingen etablerer en type distribuert informasjonssystem som er enklest å forvalte om det er mest mulig stabilt og konsistent over tid. Det hjelper lite å beskrive hvilke data du har i dag og sette opp informasjonsutvekslingen basert på et nåtids bilde, for så å oppleve at over tid så endres populasjonen hos deg eller dine partnere slik at forutsetninger for informasjonsutvekslingen ikke er til stede lengre. Denne utfordringen skal være ivaretatt om spørsmål «17. Hvordan håndteres endringer?» er godt besvart. Tilsvarende kan det bli utfordrende å finne ut hva som var tilstanden i summen av distribuerte informasjonskilder på et gitt tidspunkt.

4.2 Prosesser knyttet til etablering, forvaltning og utveksling av data

Prosesser hos avsender og mottaker bør beskrives slik at det er mulig å sette prosessmodellene sammen for å vise grensesnittet i informasjonsutvekslingen. Vanlig fremgangsmåte vil være først å beskrive aktiviteter og informasjonsutveksling hos avsender og mottaker slik det gjøres per i dag og deretter å beskrive hvordan en ønsker å gjøre det i fremtiden.

Funksjonelt eller logisk kan en forenkle med å utelate informasjonsflyt som involverer underleverandører, tredjeparter eller felleskomponenter for å forenkle. Ved design av teknisk løsning må disse aktørene og deres grensesnitt med i arkitektur og informasjonsflyt modellene.

Prosessdiagrammer som viser grensesnitt/dataflyt ut av en virksomhet må beskrive hva som gjøres før, under og etter utvekslingen. Hvor en starter å beskrive aktivitetene er et designvalg og må tilpasses det enkelte case og hvor saksbehandling og bruk av data starter. For å forstå diagrammene bør prosessdiagrammet beskrive kriterier for å starte det enkelte prosess-steg samt kriterier for at prosess-steget er ferdigstilt.

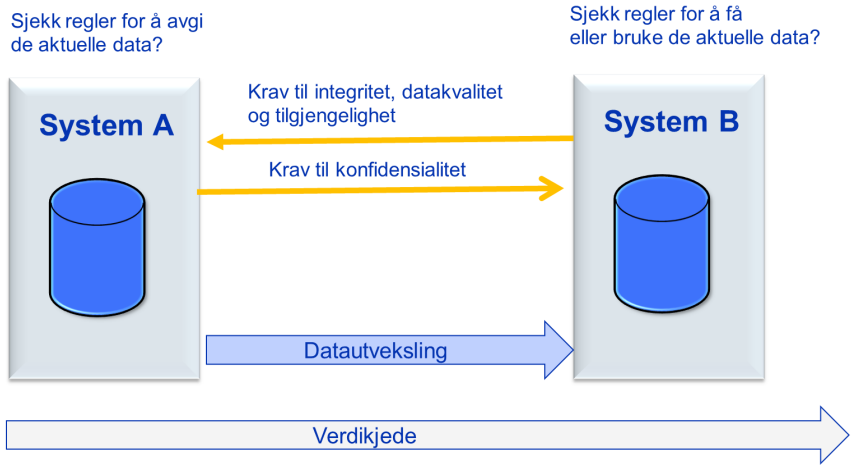
- Metodeforslag: En mulig metode og visualisering av informasjonsutvekslingen og samhandling er UML Swimlanes.
- Eksempel på verktøy: Swimlane diagramtype støttes i de aller fleste open source og kommersielle UML verktøy.

Avklaring om hva som skal inkluderes i prosessmodellen og hva som skal beskrives i prosa som tillegg er litt smak og behag, samt avhengig av hvor stor modell en ønsker å visualisere og forvalte.

Spørsmål som bør besvares ved etablering av informasjonsutvekslingen og samhandling som angår både prosess, livssyklus for data og informasjonsforvaltning er bl.a.:

1. Hvor i egen saksbehandlingsprosess produseres data?
2. Hvordan forvaltes data (informasjonsforvaltningsregime)?
3. Er data i en endelig tilstand, eller vil endring/klagebehandling etc. kunne føre til at endringer?
4. Ved endring i data, hva er prosessen og kriterier for om data skal ettersendes til dem som har gjort saksbehandling basert på gitte data?
    - Klagebehandling hos avsender, hvor klage tas til følge, skal oppdaterte data ettersende mottaker? Opplysningsplikt?
5. Hva er alternative data og tilstander?
6. Finnes historiske data, eller er det kun siste versjon som er aktuell?
    - Kan det være aktuelt å spørre etter data som var gyldige på tidspunkt x, eller ble data endret i løpet av periode a-b?

7. Hva er levetid til data som utleveres, hvor lenge etter utlevering anses de som gode nok for andres saksbehandling?
8. Hva er kriterier for sletting av data?
9. Skal data sendes til deponering hos Riksarkivet iht gjeldende arkivregler for offentlig sektor?
10. Ved lengre verdikjeder av datautveksling arves da plikter og begrensninger fra fler enn kun den som er avsender? Har avsender videresendt data han selv har mottatt og hvor det er knyttet betingelser/begrensninger til data? Se figur under, «Egenskaper ved informasjon arves i verdikjeder».
11. Hvilke rutiner er beskrevet som sikrer hensiktsmessig varsling av endringer som påvirker mottakers bruk av data? Eksempelvis oppdateringer i prosesser, lover, organisering, datakvalitet etc.

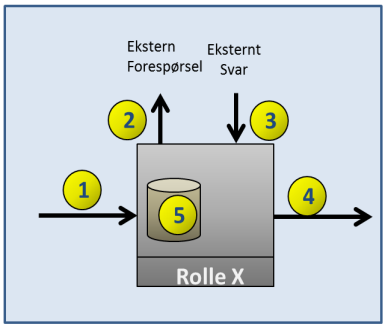


Figur 1, Egenskaper ved informasjon arves i verdikjeder

4.3 Kobling mellom aktiviteter og den informasjon som benyttes i aktiviteter

For hver aktivitet bør kobling til informasjon beskrives basert på følgende:

1. Input til aktiviteten fra annen intern aktivitet/hendelse eller tidstrigger.
2. Utveksling med ekstern aktør eller forespørsel om data fra ekstern aktør.
3. Mottak av data fra ekstern aktør, evt. mottak av forespørsel om data.
4. Output fra aktiviteten til intern tilstand/aktivitet.
5. Informasjon som er tilgjengelig for aktiviteten



Figur 3, Informasjon som bindeledd mellom aktiviteter

For hver av informasjonsflytpilene i figuren bør en sikre at en vet:

- kobling mellom aktiviteten og data, og videre til både informasjonsmodell og til begrepsmodell
- kobling mellom aktivitetsmodell med tilhørende dataflyt til jus
- hvilke datakvalitetskriterier som skal oppfylles og vurdering av om disse er tilstrekkelige for saksbehandling og for å oppfylle lover og krav
- hvilke sikkerhetsmessige aspekter som skal oppfylles og vurdering av om disse er tilstrekkelige for saksbehandling og for å oppfylle lovkrav
- hvordan feilhåndtering i saksbehandling, dataflyt, datakvalitet, teknisk system m.m. skal utføres.

4.4 Jus og hjemler for informasjonsutveksling

Følgende er sentrale betraktninger knyttet til jus, se også innholdet i utvekslingsavtalen som er en mer komplett opplisting av juridiske momenter.

Leseveiledning: Termene/ordene *begrep* og *opplysningstype* er benyttet med samme betydning i dette kapittelet.

Jus hos avgiver: Avgivers materielle regler definerer begrepene/opplysningstypene. Avgiver må derfor definere sine begreper grundig. Dersom dette er juridiske begreper, så vil definisjonen være en rettslig definisjon, og den vil være basert på kilder (rettskildefaktorer). Tolkningen kan og skal dokumenteres.

Disse definisjonene definerer opplysningstypene, og gir forståelsen av opplysningene/data/verdiene.

For at mottaker skal forstå verdiene av begrepene, er det nødvendig at avgiver forklarer den saksbehandlingen som leder til fastsettelsen av verdiene/opplysningene/dataene.

Jus hos mottaker er det rettslige grunnlag som inneholder vilkår for materielle avgjørelser som hører under mottakers personelle kompetanse/ansvarsområde. Vilkårene er i hovedsak formulert i lov og forskrift. Disse formulerte vilkårene er bare utgangspunktet for fastsettelsen av innholdet i vilkårene. Det er innholdet i vilkårene som definerer mottakers opplysningstyper, altså hvilke opplysningstyper som er relevante for mottaker. Innholdet i vilkårene må derfor fastsettes. Dette gjøres ved en prosess som kalles juridisk metode, og som er styrt av rettskildeprinsipper. Fastsettelsen av innholdet i vilkårene, og dermed hvilke opplysningstyper som er relevante kan enten gjøres generelt eller

konkret. Det mest hensiktsmessige er her at mottaker gjør dette konkret, som altså innebærer at mottaker tar standpunkt til om de opplysningene avgiver har er relevante under vilkårene. (Alternativt kan mottaker ta standpunkt til om enkelte elementer/kriterier i avgivers opplysningstyper er relevante.) Det er ikke særlig hensiktsmessig at mottaker tar generelt standpunkt til hvilke andre opplysningstyper som er relevante, abstrahert fra de konkrete opplysningstypene avgiver kan gi.

Resultatet må beskrives på en måte som er forståelig for de som skal lese dette, altså både jurister og teknologer? Dette er jurister hos mottaker og avgiver, og teknologer hos avgiver og mottaker. For at mottaker skal kunne ta standpunkt til om avgivers opplysningstyper er relevante, så forutsetter det at mottaker forstår avgivers opplysningstyper. Skinn enighet og skinn uenighet må oppklares, og det må verifiseres.

Dersom avgivers opplysninger umiddelbart er relevante for mottaker i henhold til dette, så kan utveksling skje uten videre.

Dersom det må gjøres noe med avgivers begreper/opplysninger, så kan de likevel utveksles, men kan ikke brukes hos mottaker uten tilpasninger/transformasjon.

Jus hos mottaker: Mottaker plikter å kvalitetssikre de opplysningstypene og opplysningene de får fra avgiver, og kan ikke benytte opplysningene i egen saksbehandling uten at de er tilstrekkelig sikre på at opplysningene er korrekte, og at de forstår opplysningenes innhold, jf forvaltningsloven § 17?

Dette medfører også at mottaker har en viss plikt å kontrollere avsenders organisasjon for opplysningsinnhenting/opplysningsfastsettelse. Dette gjelder særlig dersom beviskravene er forskjellige på avsendersiden og mottakersiden, og de opplysningene som utveksles er faktaopplysninger. Dersom avsenders opplysninger er opplysninger om innholdet i vedtak hos avsender, så må dette som utgangspunkt tolkes slik at opplysningene er tilstrekkelig gode. Spørsmålet om opplysningene er blitt forfeilet fra vedtak til oversendelse, er et annet spørsmål. Det er åpenbart at det ikke må skje, og at mottaker må kontrollere at avsenders system sikrer at dette ikke skjer. Hvordan dette skal sikres er ikke et rettslig spørsmål.

Jus som ramme: avgiver må forsikre seg om at de har rettslig anledning til å utlevere opplysningene til mottaker. Det beror på en tolkning og anvendelse av alle reglene om taushetsplikt hos avgiver og innhentingshjemmel hos mottaker.

Dersom avgiver bare kan utlevere opplysninger som er «nødvendige» i mottakers saksbehandling, (og slik vil innhentingshjemlene vanligvis måtte forstås enten det står uttrykkelig eller ikke), så innebærer det at mottaker må redegjøre for tolkningen av vilkårene i de materielle hjemlene (som altså må vise at avsenders opplysninger er relevante for mottakers saksbehandling) slik at avgiver kan se at opplysningene er «nødvendige».

Jus hos mottaker: I relasjon til personopplysningslovens behandlingsansvar, så blir mottaker behandlingsansvarlig for opplysningene ved overlevering, og dette betyr antakelig at avsender ikke har noe rettslig plikt til å kontrollere hvordan mottaker benytter opplysningene. Unntak kan nok tenkes for enkelte typer opplysninger og i relasjon til enkelte persongrupper.

Relevante spørsmål kan være:

1. Har vi hjemmel for å be om data fra annen etat?
2. Er det krav til levetid for data?
3. Hvordan skal sletting håndteres?
4. Fletting / kobling av registre, er det problematisk?
5. Er det krav til oppdatering, omgjøringsplikt mm.
6. Hva er krav til integritet?
7. Hva er krav til konfidensialitet?
8. Hva er krav til sporbarhet?
    - Hvor kommer data fra, har din avsender også mottatt data fra en annen avsender/borger/næringsdrivende?
9. Hvem/hvilke rolle har og har hatt innsyn til data? (tilgang og aksessrettigheter)
10. Hvem planlegger å benytte de aktuelle data videre og til hva?

Vanlige lover og regler som kan gjelde for informasjonsoppbevaring, utveksling, åpenhet, sletting, kobling av informasjon er:

1. Personopplysningsloven
2. Offentlighetsloven
3. Arkivloven
4. Regnskap og revisjonslovgivning
5. Sikkerhetsinstrukser

4.5 Transformasjoner

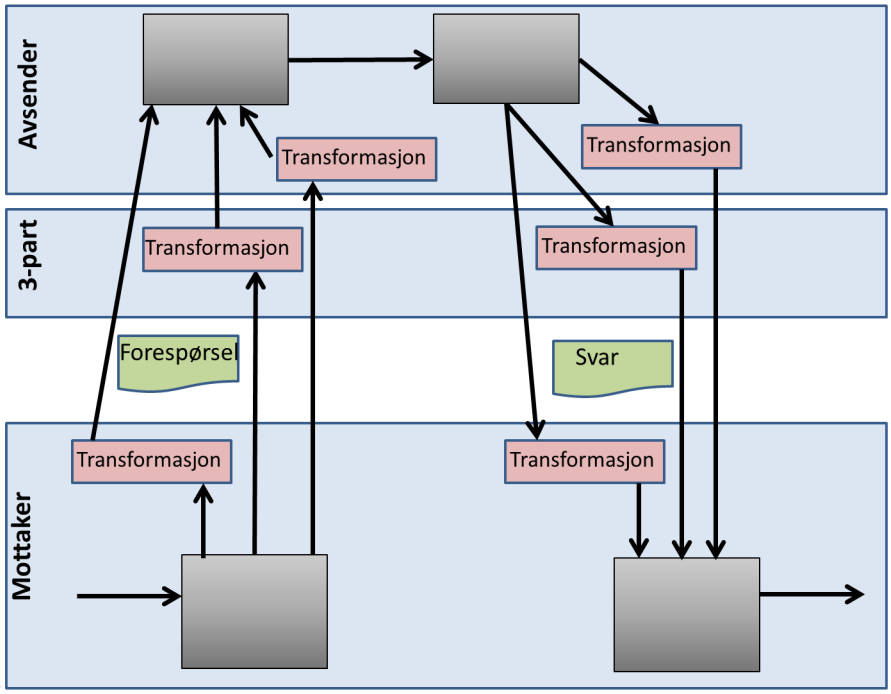
Når en sender en forespørsel om data til annen etat og får svar i henhold til forespørsel skjer det en rekke transformasjoner. Eksempler på transformasjoner er:

- Bæreprotokoll, selve utvekslingsmekanismen på et lavere teknisk nivå.
- Sikkerhetsmekanismer hvor kombinasjoner mellom kanalsikkerhet, meldingssikkerhet og skallsikkerhet/sikre soner og applikasjon med autentisering og autorisasjonsstyring benyttes.
- Formatkonvertering, mellom formater som for eksempel: eksportformat for database, XML, CSV, EDIFACT, RDF, proprietære format osv.
- Modellkonvertering, transformerer data i et gitt format til å være i overensstemmelse med en annen informasjonsmodell enn kilde.
    - Attributt-tilpasninger. Eksempelvis, om et avsender system skiller på fornavn, mellomnavn og etternavn, vil data kunne konverteres presist til en modell for fornavn + etternavn hvor mellomnavn er siste del av fornavnet. Motsatt vei går ikke, dermed er dette en transformasjon med tap i presisjon, dvs. hva som er mellomnavn blir vanskelig å finne ut i data som er i henhold til modellen hos mottaker.
- Begrepskonvertering, er mulig i en del tilfeller der sammenhenger mellom begreper er tydelig beskrevet.
    - Eksempel: avsender kan ha mer presise begreper enn mottaker. Det åpner for muligheten til at alle data som er i henhold til avsenders begrep også vil være innenfor definisjonen av mottakers begrep. Konkretisert: Om avsenders begrep for personinntekt per år (iht et gitt regelverk) er mer presist enn mottakers tilsvarende personinntekt per år begrep, vil mottaker trolig kunne benytte data som er i henhold til avsenders begrepsmodell. Motsatt trenger ikke være tilfelle, det må utredes om er mulig.

- Eksempel på endring av benevnelse/type: en kan for mange formål omforme opplysninger som er oppgitt per år til et gjennomsnitt per mnd. Om en da spør på inntekt for juni 2012 må mottaker vite at svaret er et gjennomsnitt og ikke faktisk verdi.

- Populasjonstilpasninger. Informasjonsutvekslingen utfordrer offentlig sektor i retning av å se på seg selv som forvalter av et stort distribuert informasjonssystem. Ulike offentlige registre og saksbehandlingssystemer vil ha data om ulike deler av befolkningen, bilparken, næringslivet etc. Det må derfor avklares hva fravær av data om et objekt i et system egentlig betyr og hva som skal gjøres om et spørsmål ikke returnerer et svar.

Som figuren under viser to hovedtidspunkt for transformasjon, det er ved spørring og ved svar.



Figur 4, Transformasjoner av data, vanlige alternativer

Den som spør kan lage en forespørsel basert på sin informasjons- og begrepsmodell og transformere spørringen til modeller hos den som skal avgi informasjon. Alternativt kan tredjepart eller avsender gjøre transformasjon av spørringen. Når svaret på forespørselen lages kan avsender transformere til mottakers modell, evt. tredjepart eller mottaker kan selv gjøre transformasjonen.

I praksis blir det ofte transformasjoner både ved spørring og ved svarhåndtering. Disse transformasjonene er kritiske for at utvekslingen skal fungere i henhold til hensikt.

I forbindelse med transformasjon endres gjerne data fra eksakte verdier som konkret diagnose til et svar som er godt nok for den som spør. Eksempelvis kan svaret være «sykemeldt». I noen tilfeller håndteres de faktiske verdiene og terskelsvar på ulike måter sikkerhetsmessig siden de kan ha ulik krav til konfidensialitet.

Det er sentralt at mottaker har tilstrekkelig forståelse for saksbehandlingen bak dataene (hvordan verdiene har fremkommet) både internt hos avsender, men også hva som skjer med data i transformasjonene.

4.6 Risikostyring, kvalitetssystemer og gevinstrealisering

Det er sentralt at deltakerne ser forskjell på et informasjonsutvekslingsprosjekt mellom etater / virksomheter og et etatsinternt IT-prosjekt.

> Et bilde kan være forskjellen på en enkelt fotballspiller som har individuelle ferdigheter versus fotball-lagets kollektive ferdigheter. Treneren skal hjelpe både på det individuelle og det kollektive plan. Tilsvarende må prosjekter for informasjonsutveksling ha en trener og risikostyring, kvalitetssikring og gevinstrealisering må fokusere på både individuelt nivå og kollektivt nivå. Suksessen er et resultat av lagets kollektive prestasjoner.

Tre tilnærminger til måloppnåelse er (1) risikostyring, (2) helhetlig kvalitetssystem og (3) gevinstrealisering. Disse tre bør ved informasjonsutvekslingen sees i sammenheng og avsender og mottaker har gjerne ulike tradisjoner for hvilken tilnærming de legger mest vekt på i prosjektgjennomføring og i organisasjons-forbedringsprogrammer. Fokus må endres fra å være etatsinternt til å fokusere på kollektive mål. Etatene skal sikre gevinster basert på informasjonsutvekslingen og de må spille hverandre god. Kulturmessig vil fokus på kollektiv måloppnåelse by på endring og utfordringer. Vi anbefaler å se de tre hovedspørsmålene under samlet for å sikre at hovedmål, leveranser og gevinster skal være godt egnet og kunne realiseres.

12	Risikostyring	Er metodisk tilnærming og tidsplan for risikoanalyser avklart?
13	Risikostyring	Er metodisk tilnærming og tidsplan for kvalitetsstyring avklart?
14	Risikostyring	Er metodisk tilnærming og tidsplan for gevinstrealisering avklart?

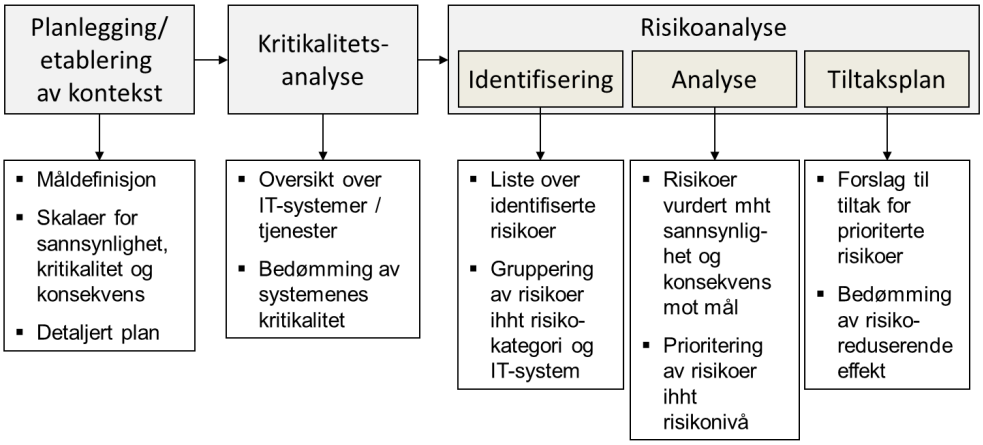
Flere av elementene som er sentrale i gevinstrealisering er også sentrale i de andre måtene å strukturere "prosjekter" på. Vi anbefaler at etatene ser disse tre (12-14) som supplerende, men også overlappende. Utfordringen for etatene blir å kombinere de ulike tilnærmingene. Sjekklista utfordrer etatene til å ta stilling til hvordan de tre tilnærmingene er tenkt benyttet. Ved å bruke risikotilnærming for gevinstrealisering, dvs at en gevinst som kanskje ikke oppnås er en risiko, da kan en benytte risikometoder med tiltak også for å sikre gevinstrealisering. Se mer om gevinstrealisering i kapittel gevinstrealisering, 4.8.

DIFIs maler og arbeid med risikostyring fokuserer primært på informasjonssikkerhet, men i beskrivelse av motivasjon viser DIFI overordnet forståelse for hva potensialet ved god risikostyring kan bety for virksomheter. DIFIs formuleringer i veilederen [21] er som følger:

> *Kunnskap om risiko- og mulighetsbildet*
>
> *God informasjonssikkerhet forutsetter kunnskap om risiko- og mulighetsbildet. For å kunne prioritere riktig og begrunne sine valg, eventuelt manglende valg, av sikkerhetstiltak, må virksomheten først ha oversikt over egne oppgaver og verdier, hvilke regler som gjelder og hvilken trussel og risiko de står overfor. Sikkerhetstiltak kan avverge og forebygge trusler, men også gjøre løsninger mulig som ikke ellers ville vært gjennomførbare.*

Semicolons undersøkelser om risikoanalyser i IKT prosjekter viser at det er et stort forbedringspotensiale både i utnyttelse og utbredelse [26].

I Semicolons tilnærming vil en i analysefasen se på informasjonsutvekslingen som et distribuert informasjonssystem og samhandlingen mellom organisasjoner som et verdinettverk eller en verdi kjede. Risiko som hindrer god endring og gevinstrealisering er primærfokus ved Semicolons risikotilnærming. To viktige deler må på plass for å oppnå god risikostyring, det er et risiko rammeverk og en risikoprosess. Risikorammeverk setter den enkelte risikoanalyse og tiltak inn i en større sammenheng. Vanlig prosess for risikoanalyser er illustrert i figuren under.



Figur 5, Vanlige aktiviteter i en risikoanalyse.

Risiko rammeverk, valg av avgrensninger for analysen er avgjørende for hva en vil kunne finne av risiko og foreslå av tiltak. Det vil ved prosjekter for elektronisk informasjonsutveksling være relevant å gjøre risikoanalyser på: prosjektet, selve leveransen fra prosjektet, bruk av leveransene fra prosjektet, drift av ny løsning, hindringer for gevinstrealisering og forvaltning.

Valg av fokus i en risikoanalyse avgjør i stor grad hvilke risikoer som blir identifisert. Under planlegging av et prosjekt skal en definere hvordan en ønsker å måle risiko. Under er det listet ulike utgangspunkt for IT risiko analyser og hva en ofte velger av risikomål.

- **Interne prosjekter (internt i en virksomhet) ,** risikomål:
  - tid, kost og kvalitet for prosjektleveransen
  - Samt integritet, tilgjengelighet og konfidensialitet ved leveransen/ ved drift
- **Informasjonsutvekslingsprosjekter,** risikomål:
  - tid, kost og kvalitet for prosjektleveranser hos flere virksomheter.
  - samt integritet, tilgjengelighet og konfidensialitet ved drift

Punktene over viser at det vanligvis er de samme risikomålene for interne prosjekter som det er for informasjonsutvekslingsprosjekter. Forskjellen er kontekst og avgrensning på analysen. Velger en å se risikomål ut fra rolle kan det fremstilles som følger:

- **Prosjekteier/bestiller**, risikomål:
  - Forretningsmessige mål/ gevinster, tid, kost, kvalitet, omdømme
- **Daglig leder**, risikomål:
  - Forretningsmessige mål, kost, omdømme, være i overensstemmelse med regler/ compliance, sikre lisens for å drive virksomheten.

En del virksomheter opererer på lisenser for å utføre virksomheten (finansielle lisenser som bank, lege) og tap av lisens vil sette deg ut av business.

- **IT-sjefen i de enkelte virksomheter:**

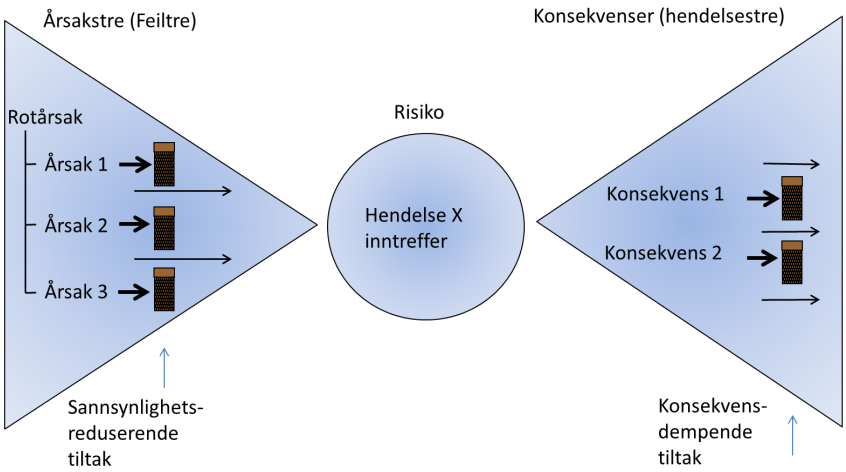
  Risikomål**:**

  - Tilgjengelighet, konfidensialitet og integritet
  - Compliancekrav mot IKT-standarder, grensesnitt og egen referansearkitektur etc.
  - Levetidsrisiko på utstyr, hardware, software, lisenser, utviklings og testmiljø etc
  - Økonomi
  - Omdømme
  - Leveringsevne på endringer, innovasjonsevne

- Tema som typisk gir utfordringer for IT sjefen er:
  - Teknisk gjeld og integrasjonsgjeld
  - Informasjonsforvaltning inklusive datakvalitetsgjeld og manglende masterdataforvaltning
  - Porteføljestyring av prosjekter og deres leveranser
  - Security i virksomhetens infrastruktur og i grensesnittet til dem en utveksler informasjon med.
  - Kvalitet og etterlevelse av rammeverk, metoder, prosesser og støtteverktøy for IKT governance/styring, drift, utvikling, innovasjon
  - Kvalitet og oppfølging av risikometodeverk både for prosjekter og operasjonell IT risiko.
  - Kvalitet på IKT arkitekturer og lojalitet til å være compliant med valgte standarder
  - Arkitektur og kvalitet på testrammeverk og testmiljø
  - Verktøystøtte for systemutvikling og test prosessene
  - Kompetansebehov
  - Konfigurasjonsstyringsutfordringer

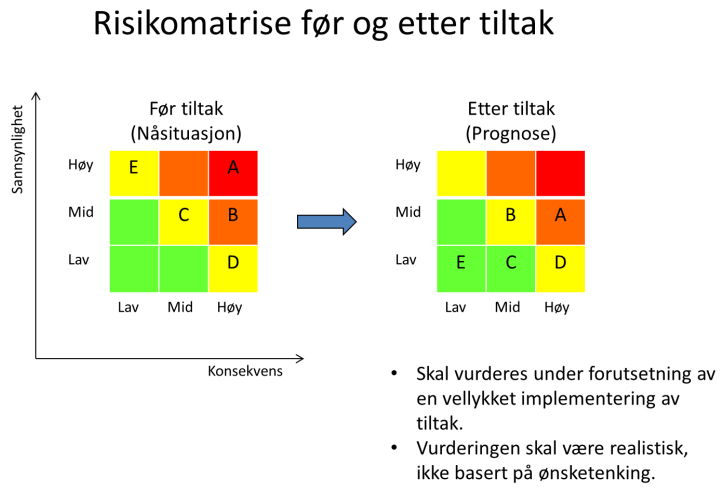
Se appendiks om «Teknisk gjeld og integrasjonsgjeld» for ytteligere beskrivelser av IKT og gjeldsutfordringer.

Når risikoer er identifisert og sannsynlighet og konsekvens vurdert gjennomføres identifisering og systematisering av tiltak. Hensikten med tiltakene er å redusere risiko og vanligvis vil tiltak føre til enten redusert sannsynlighet eller redusert konsekvens. Figuren under viser forskjellen på tiltak som har til hensikt å redusere sannsynligheten for at en risiko inntreffer, versus tiltak som har til hensikt å redusere konsekvens ved at en risiko har inntruffet.



Figur 6, sløyfe, BowTie figur for tiltak

Ved bruk av sjekklistene bør mengden risiko i et prosjekt (tid, kost, kvalitet) og i prosjektleveransene (tilgjengelighet, integritet, konfidensialitet) allerede være godt redusert, men ved gjennomføring av en risikoanalyse vil en få klarlagt restrisikoen avsender og mottaker er eksponert for. Enkelte risikoer vil kun gjelde avsender eller mottaker, og derfor bør de involverte kjøre selvstendige risikoanalyser. Det kan oppstå situasjoner hvor en risiko hos avsender kan være positivt for mottaker, dette er typisk tilfelle når endring i samhandling fører til at risiko flytter seg fra en part til en annen.



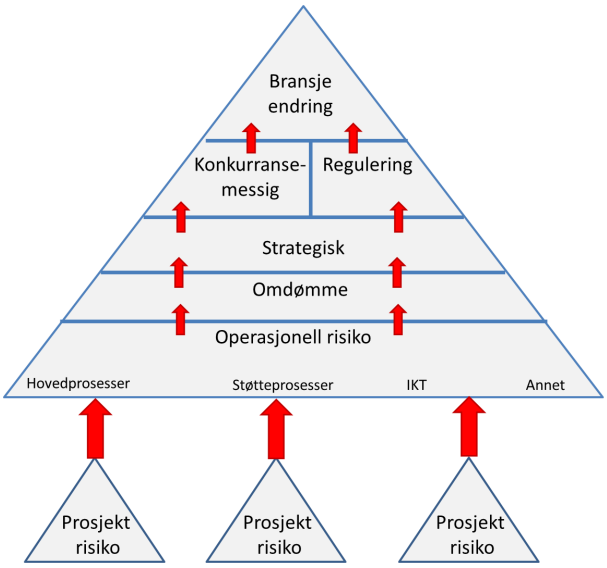
Figur 7, Risikonivå før og etter vellykket tiltak

De enkelte risikoer og tiltak plasseres hos en ansvarlig rolle evt. person.

Når risikoanalysen er ferdig går man over en fase med risikostyring. Da gjelder rutiner for å fange opp risiko som oppstår ved ulike typer endringer og hendelser. Ansvarlig for risikostyringen må sørge for at risikobildet oppdateres med jevne mellomrom.

Noen risikoer er av en slik karakter at selv om de oppstår i et prosjekt så er de så kritiske at de påvirker prosjekteier og gjerne også gjeldene organisasjon. Risikoaggregering er et utfordrende fagområde og hvor det er kontekstavhengig hvilke risikoer som skal løftes til høyere nivå. Figuren

under viser et eksempel på å visualisere risiko i en risikopyramide som kan brukes for å vise hvilken vei ulike risikoer kan ta oppover i virksomheten.



Figuren er ment å illustrere hvordan en risiko knyttet til et prosjekt eller daglig drift kan flyte oppover og bli en styresak eller trigge nye reguleringer for et helt marked evt. endre måten en industri tenker og bygger sine løsninger.

Når en virksomhet gjennomfører et sett av risikoanalyser trengs det et rammeverk, dvs

- et etablert metodeverk for gjennomføring av risikoanalyser og kursing
- IKT støtte
    - for å systematisere risikoer i den enkelte analyse
    - se utviklingen over tid for et prosjekt, produkt, operasjonelt område el.
    - se sammenhenger mellom risikoanalyser
    - aggregering av risikoer i for eksempel en pyramide tilnærming.
- Planer for hva virksomheten skal gjennomføre risikoanalyser på
- Hvordan interne versus eksterne ressurser skal benyttes til å kjøre risikoanalyser

Supplerende litteratur kan være:

- ISO 31000 Risk management – principles and guidelines
- Use the risk pyramid to assess risk in five minutes [27].
- Risikovurdering - en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. DIFI [20]
- Risikoanalyse, KITH [21]
- Unveiling Barriers and Enablers of Risk Management in Interoperability Efforts. [26]
- Utredning av standarder for risikostyring av informasjonssikkerhet i offentlig forvaltning. DIFI 1. Feb 2012.

4.7 Kvalitet på data

Kjent og tilstrekkelig datakvalitet er en viktig forutsetning for videre bruk av informasjon og sikre gevinster ved informasjonsutveksling. Dette er spesielt viktig ved automatisering av

informasjonsbehandlingen og saksbehandlingsbeslutninger basert på utvekslet informasjon. Ved samhandling er det sentralt for partene å erkjenne at det som er tilstrekkelig datakvalitet for et bruksområde ikke trenger å være tilstrekkelig for andre. Måling og forbedring av datakvalitet er et kontinuerlig arbeid som krever metoder, ressurser, verktøy og styring. Det er per i dag godt etablerte standarder for datakvalitet som er velegnet for et mangfold av bruksscenarier.

Lav datakvalitet er i seg selv en show-stopper for å kunne dra nytte av informasjonsutveksling. Uten tilstrekkelig kvalitet på data som mottas kan data heller ikke benyttes til saksbehandling. For å unngå show-stopper situasjoner er det viktig at alle prosesser knyttet til datakvalitet er godt beskrevet, at alle input-data er kvalitetssikret og at det finnes en beskrivelse av hvilket kvalitetsnivå og kvalitetsregime disse dataene har fulgt.

Supplerende spørsmål rundt datakvalitet kan være:

1. Er data av en kvalitet som gjør at organisasjonen kan avgi dem uten avtaleklausuler om mulige feil og mangler?
2. Er prosesser for å sikre datakvalitet beskrevet? Eksempler på prosesser kan være:
    a. Sikring av datakvalitet ved mottak/innhenting?
    b. Sikring av datakvalitet ved fletting av datakilder
    c. «Vasking» av data mot for eksempel andre kilder?
    d. Periodiske analyser for å sjekke status og utviklingstrender for datakvalitet.
    e. Kontrollere data mot andre kilder for å identifisere evt avvik/forskjeller. Gjøres dette kun på utvalg av data eller for alle data som mottas, benyttes?
3. Er kvalitetsindikatorer og kvalitetsnivåer definert?
4. Er analyser av datakvalitet gjort på de data som skal utveksles?
5. Bør avsender stille krav til datakvalitet i datakilder hos mottaker før avsenders data benyttes hos mottaker?
6. Hvordan påvirker transformasjoner datakvalitet?
7. Har avsender og mottaker konkrete krav til datakvalitetsnivå beskrevet i for eksempel i henhold til ISO 8000?
8. Hvor lav datakvalitet kan avsender utlevere uten å varsle mottaker?
9. Hvordan er datakvalitetsprosess og datakvalitetskrav hos avsender og mottaker harmonisert?
10. Utveksles tilstrekkelig med livsløpsinformasjon sammen med de data som utveksles (Provenance informasjon)? Sagt på annen måte, utveksles data sammen med beskrivelse av opphav og livssyklusstatus, eller vet mottaker på annen måte hva som er opphav og livssyklusstatus på data? [9]

Målbare datakvalitetskrav som er koblet til både datakvalitetsprosesser og selve data bør med i utvekslingsavtalen eller relevante bilag.

Ved informasjonsutveksling oppstår den situasjon at virksomheter blir avhengig av hverandres informasjon og dermed også prisgitt hverandres datakvalitet. En måte å systematisere denne utfordringen på er å ta utgangspunkt i datakvalitet/integritet og tilgjengelighet. Mange fagområder utvider scope for å få større nedslagsfelt for sine tema. Slik er det også med datakvalitetsfaget versus IKT risiko hvor risiko-termen *integritet* også vil omfatte datakvalitet.

Under er en liste med ti rot-kildeproblemer til datakvalitet som alle vil være til stede i mer eller mindre grad ved informasjonsutveksling. Ti rot-kilder til datakvalitetsproblemer er i følge Journey to Data Quality [16 s80]:

1. *Multiple Data Sources.*

- *Multiple sources of the same information produce different values for this information. This can include values that were accurate at a given point in time.*

2. *Subjective Judgement in data production*
   - *Information production using subjective judgment can result in the production of biased information.*
3. *Limited computing resources*
   - *Lack of sufficient computing resources limits accessibility to relevant information.*
4. *Security/accessibility trade off:*
   - *Easy access to information may conflict with requirements for security, privacy, and confidentiality.*
5. *Coded data across disciplines:*
   - *Coded data from different functions and disciplines is difficult to decipher and understand. Also codes may conflict.*
6. *Complex data representations:*
   - *Algorithms are not available for automated content analysis across instances of text and image information. Non-numeric information can be difficult to index in a way that permits location of relevant information.*
7. *Volume of data.*
   - *Large volumes of stored information make it difficult to access needed information in a reasonable time.*
8. *Input rules too restrictive or bypassed.*
   - *Input rules that are too restrictive may impose unnecessary controls on data input and lose data that has important meaning. Data entry clerks may skip entering data into a field (missing information) or arbitrarily change a value to conform to rules and pass an edit check (erroneous information)*
9. *Changing data needs.*
   - *As information consumers' tasks and the organization environment (such as new market, new legal requirements, new trends) change, the information that is relevant and useful changes.*
10. *Distributed heterogeneous systems.*
    - Distributed heterogeneous systems without proper integration mechanisms lead to inconsistent definitions, formats, rules, and values. The original meaning of data may be lost or distorted as data flows and is retrieved from a different system, time, place data consumer, for same or different purpose.

Supplerende litteratur kan være:

- ISO 8000 Data Quality [10]
- Journey to Data Quality [16]
- Data Quality. [17]

4.8 Gevinstrealisering

Bevisst holdning til gevinstrealisering øker sjansene for at potensiell nytte (gevinst) identifiseres tidlig og at identifisert nytte faktisk realiseres. Gevinstrealisering handler kort fortalt om tre ting:

- Etablere gode (og omforente) mål

    - målene konkretiseres på et slikt nivå at det er klart beskrevet hvilken nytte (gevinst) som forventes og i hvilket omfang.
- Etablere (gevinstrealiserings)plan med tiltak for å håndtere risiko og nå målene
    - dette overlapper med tidligere beskrevne tiltak for å redusere risiko, men kan også gå utover en vanlig risiko-tilnærming der en fokuserer på å unngå nedsiden/tap. Risikostyring kan benyttes for å styrke mulighetene. Planen skal også inneholde informasjon om hvordan målinger skal gjennomføres og dermed legge godt grunnlag for målinger (underveis og når gevinstene forventes realisert). På samme måte som med risiko anses det som viktig å etablere ansvar for ulike tiltak og når de enkelte gevinstene forventes realisert.
- Oppfølging, måling og evaluering
    - gevinstrealiseringsplanen danner grunnlag for oppfølging av tiltak og planlagte gevinster. Endringsledelse er sentralt i oppfølgingen. Målinger gjennomføres som spesifisert i gevinstrealiseringsplanen. Det er regnet som god praksis å evaluere måloppnåelse og vurdere grunnlag for eventuelle nye muligheter som har oppstått som følge av arbeidet som er gjort.

Det er viktig at punkt 1 og 2 adresseres tidlig i et prosjekt siden disse legger grunnlag for oppfølging og endelig realisering av gevinster. Dette kapittelet henger sammen med kapittel 4.11 om Virksomhetsmodell.

4.9 Håndtering av endring av opplysninger, klagebehandling og omgjøring

Ved bruk av informasjon fra avsender og hvor informasjonen kan endres etter at den er benyttet i mottakers saksbehandling, må det avklares hva som skal gjøres om data hos avsender/kilden endres. Hovedutfordringen er klagebehandling kombinert med omgjøringsplikt.

Punkter som kan være relevant å avklare i denne sammenheng kan være:

- Push eller pullmodell av data og påbegynte klager.
    - Skal avsender logge hvem de har oversendt data om og ettersende innen kjente frister?
    - Skal mottaker sende forespørsel til avsender om oversikt over relevante data som er endret hos avgiver?
- Er det behov for å harmonisere klagefrister?
    - Eksempel, en borger har fått avslag hos UDI på oppholdstillatelse/familiegjenforening med begrunnelse i lav inntekt. Borgeren har en klage gående hos SKD for fastsettelse av inntekt i forbindelse med ligning. Borgeren får medhold og ny verdi for inntekt fører til at søker kommer over en terskelverdi hos UDI for å få oppholdstillatelser. UDI vedtak skal egentlig endres, men klagefrist hos UDI kan være utgått før SKD har ferdigbehandlet klagen. Sett fra borgers ståsted er dette en veldig uheldig situasjon.

Skal trigger for å informere annen etat om endring være at:

- Borger har sendt klage?
- Konklusjon på klage foreligger og klagen førte til endring?

- Avsender skal uansett sende info når de endrer informasjon som har vært utvekslet for å inngå i ande etaters saksbehandling.

4.10 Sikkerhet

Etablering av ulike typer sikkerhetsmekanismer er en forutsetning for etablering av elektronisk samhandling. Tilfredsstillende sikkerhetsmekanismer og rutiner må være tatt i bruk for å tilfredsstille lovkrav i forbindelse med:

1. Mottak av data
2. Forvaltning og sletting av data
3. Avgivelse av data
4. Anonymisering av data
5. Rapportering og statistikk
6. Testmiljøer for informasjonsutvekslingen, inklusive evt tredjeparter.
7. Ved omorganisering eller endring av ansvar og arbeidsoppgaver

For hvert av punktene over vil vanlige tema innen datasikkerhet være:

- Konfidensialitet: Å sikre at informasjon bare er tilgjengelig for de som skal ha tilgang.
- Integritet: Å sikre at informasjon er korrekt og fullstendig.
- Tilgjengelig: Å sikre at informasjon er tilgjengelig innenfor de krav som er satt.
- Sporbarhet og ikke-benekting (Engelsk: Non repudiation): Beskriver metoder som skal dokumentere at en handling (på informasjon) virkelig har vært gjort av en konkret definert person/system.
- Autentisering: å autentisere en person kan bety å kontrollere vedkommendes identitet/elektroniske ID eventuelt ID til et system som representerer en person eller rolle.

Se gjerne:

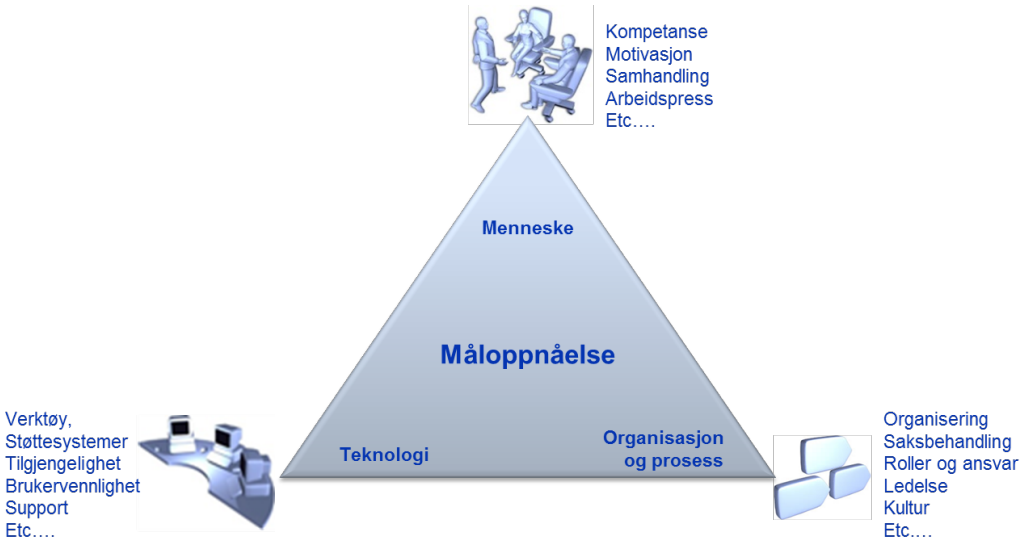
- ISO/IEC 27010 — Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.

4.11 Virksomhetsmodell

Med en virksomhets målbilde, eller et større prosjekts målbilde, menes en beskrivelse av en fremtidig tilstand. Perspektiver som bruker/kunde, økonomi, interne prosesser og organisasjonen/teknologi beskrives. Målbildet bør knyttes opp til virksomhetens visjon og uttrykke et ambisjonsnivå med endring fra dagens situasjon til en definert framtid. IKT-målbildet skal være tett koblet til målbildet til virksomheten.

En strategi er definert som en beskrivelse av veien til målet. Den kan gjerne deles opp i delstrategier og eventuelt knyttes opp til strategiske temaer. Det er vanlig at virksomheter i sine strategier sier noe om hvordan virksomhetsmodellen bør være på et tidspunkt i fremtiden og strategien skal konkretisere de endringer i virksomhetsarkitekturen som bidrar til å nå virksomhetens målbilde. Etablering av informasjonsutveksling er i denne sammenheng en endring i virksomhetsmodell og vil kunne bidrar til å nå strategiske mål.

En virksomhetsmodell skal gi oversikt og sammenhenger mellom prosesser, IKT og mennesker (MTO). IKT kan igjen brytes ned i informasjonsressurser, IT–systemer og IT-infrastruktur.

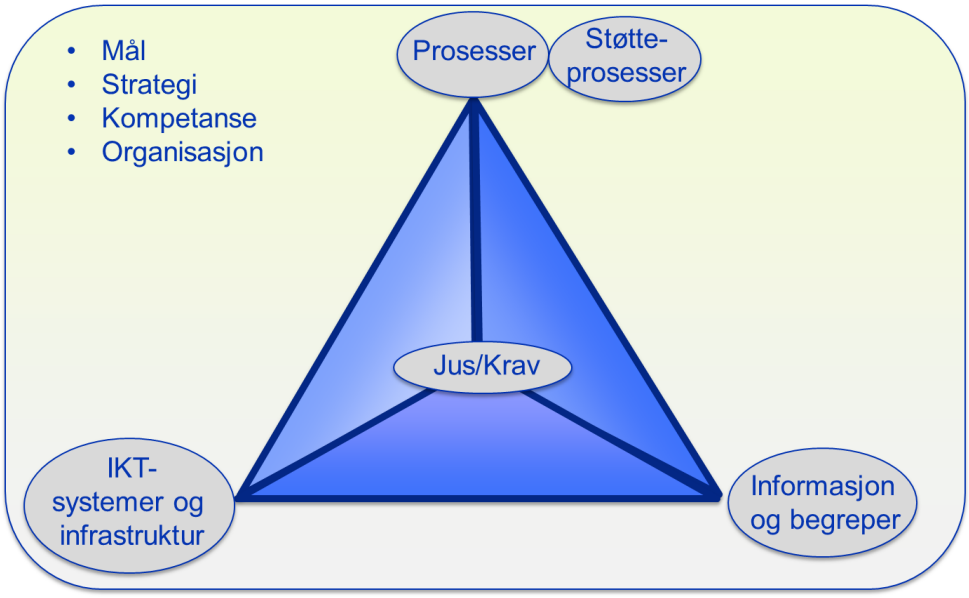


Figur 8, overordnet generell virksomhetsmodell

En virksomhetsmodell trenger styring. Og med styring her forstår vi:

- At det konkretiseres hva virksomheten forventer av virksomhetsmodell, IKT avdelingens rolle og tjenester, samt hvordan IKT prosesser og tjenester blir målt. (governance/ kravstiller)
- Prosessene internt i en IKT avdelingen skal sikre at IT understøtter både virksomhetens mål og hovedprosesser på en god måte. (management, gjøre jobben)
- Målinger, for å se at forventningene til virksomhetsmodell og IKT avdelingen blir oppnådd. (respons til governance)

Det finnes mange tilnærminger for virksomhetsmodeller og figuren under fokuserer på de delene av virksomhetsmodellen som er tettest knyttet til informasjon som ressurs og informasjonsforvaltning. Informasjonsforvaltning vil i en organisasjon være en støtteprosess.



Figur 9, Virksomhetsmodell med fokus på informasjonsforvaltning

I en offentlig virksomhet vil prosesser for systemutvikling, informasjonsforvaltning, konfigurasjonsstyring, risikoanalyser etc være støtteprosesser. For et programvareselskap vil systemutvikling være en hovedprosess. Figuren over søker å fokusere på skillet mellom it systemene og informasjon som ressurs. Det er en økende modenhet for å fokusere på informasjon som noe selvstendig og med egen verdi siden informasjonen overlever systemer i levetid og informasjonen utveksles mellom systemer og er stafettpinnen som får prosesser til å trigges.

4.12 Budsjett og planlegging

Dette anses som vanlig prosjektutfordring, men budsjettene må harmoniseres og periodiseres slik at alle aktører kommer i mål med leveranser som hjelper hverandre frem til et felles mål om informasjonsutveksling. Denne prosessen kan typisk ta 2-3 år om satsningsforslag til departementer blir del av budsjettplanleggingen.

4.13 Metoder og modenhetsmålinger ved etablering og forvaltning av informasjonsutveksling

To virksomheter som skal etablere informasjonsutveksling bør være kjent med hverandres modenhetsnivå innen systemutvikling, virksomhetsmodeller og prosessforbedring. En novise organisasjon vil ha store utfordringer med å følge en moden, og novisen vil også kunne tilføre den modne aktøren adskillig risiko.

For mer informasjon og sammenlikning av noen av metodene under se appendix «Eksempel på metoder for etablering av elektronisk samhandling» i dokumentet «Etablering av modell for elektronisk informasjonsutveksling» levert DIFI som Semicolon leveranse, våren 2014.

Dette kapittelet lister noen relevante standarder og initiativ. En del av teksten er hentet fra wikipedia eller organisasjonen/standarden egne hoved-websider. Listen er på ingen måter komplett, men vi tror den kan være til nytte for å vise mangfoldet og hjelpe med å skaffe oversikt i noen av metode-alternativ-diskusjonene som foregår i virksomheter. Valg av metode er styrende for hva en velger å fokusere på og kan føre til at sentrale gevinster og risikoer ikke blir oppdaget og håndtert på en god måte. Listen starter med internasjonale og avslutter med norske initiativer.

ISO/IEC 12207 Systems and software engineering

ISO/IEC 12207 Systems and software engineering — Software life cycle processes is an international standard for software lifecycle processes. It aims to be the standard that defines all the tasks required for developing and maintaining software.

Software life cycle processes is an international standard for software lifecycle processes. It aims to be the standard that defines all the tasks required for developing and maintaining software.

ISO/IEC 15504 Information technology — Process assessment

also known as SPICE (Software Process Improvement and Capability Determination), is a set of technical standards documents for the computer software development process and related business management functions. ISO/IEC 15504 initially was derived from process lifecycle standard ISO/IEC 12207 and from maturity models like Bootstrap, Trillium and the CMM.

ISO/IEC 27010

ISO/IEC 27010 — Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.

ISO/IEC 14662:2010 open edi

Specifies the framework for co-ordinating the integration of existing International Standards and the development of future International Standards for the inter-working of Open-edi Parties via Open-edi and provides a reference for those International Standards.

TOGAF

The Open Group Architecture Framework (TOGAF®) er et rammeverk for virksomhetsarkitektur som benyttes for design, planlegging, implementering og forvaltning av en virksomhets informasjonsarkitektur.

For samhandlingsformål kan en løfte scope for metoden til å omhandle mer enn en virksomhet og det antas at metoden også da vil være nyttig for flere virksomheter som skal samhandle. Metoden er nært knyttet til kjente programvareutviklingstrender og UML-tradisjonen for programvareutvikling.

http://en.wikipedia.org/wiki/The_Open_Group_Architecture_Framework

Lean software development

Lean software development (LSD) is a translation of lean manufacturing and lean IT principles and practices to the software development domain. Lean philosophy regards everything not adding value to the customer as waste. Such waste may include:

- unnecessary code and functionality
- delay in the software development process
- unclear requirements
- insufficient testing (leading to avoidable process repetition)
- bureaucracy
- slow internal communication

Six Sigma for software development

Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization

Agile software development

Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen tight iterations throughout the development cycle.

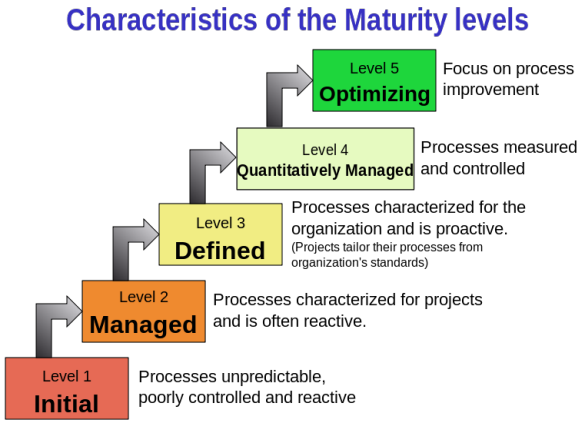
Waterfall/fossefall software development

The waterfall model is a sequential design process, often used in software development processes, in which progress is seen as flowing steadily downwards (like a waterfall) through the phases of Conception, Initiation, Analysis, Design, Construction, Testing, Production/Implementation, and Maintenance.

The waterfall development model originates in the manufacturing and construction industries; highly structured physical environments in which after-the-fact changes are prohibitively costly, if not impossible. Since no formal software development methodologies existed at the time, this hardware-oriented model was simply adapted for software development.

Capability Maturity Model Integration (CMMI)

Et eksempel på initiativ med utbredelse i USA er Capability Maturity Model Integration (CMMI [25]). Dette er en metode med profiler for systemutvikling, tjenesteforvaltning og innkjøp, Metoden har vist suksess innen programvareutviklingsmiljøer. CMMI sin oppdeling av nivåer er vist i figuren under.



TickITplus

Er en metode med utbredelse i UK og Sverige [28].

> *It is intended to offer a flexible, multi-level approach to IT quality and certification assessment and can be applied at whatever level is deemed appropriate to the quality and process maturity of the organization and the needs of its customers. If multiple IT standards need to be addressed, these can be covered under one certification arrangement.*

TickIT provides a certification process as does Capability Maturity Model Integration (CMMI) and Six Sigma. Like ISO 15504 and ISO 12207, TickIt is focused on the software development and engineering processes.

ITIL, IT service management

The Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published in a series of five core volumes, each of which covers an ITSM lifecycle stage. ITIL underpins ISO/IEC 20000 (previously BS15000), the International

Service Management Standard for IT service management, although differences between the two frameworks do exist. [Wikipedia]

UMM

UMM er utviklet og forvaltet av UN/CEFACT og har røtter tilbake til EDIFACT, open-edi og ebXML initiativer.

Det er en metode for å kartlegge mulighetsrom, modellere og beskrive hvordan elektronisk samhandling mellom organisasjoner kan og bør utføres. Metoden anvendes for å systematisere og beskrive forretningsmessige krav til ikt og beskrive samhandlingsscearier. Output fra metoden er teknologiuavhengige beskrivelser over:

- Informasjonsmodeller, hvilke informasjon som flyter mellom hvilke parter
- Betydningen av informasjon og kodelister.
- Use case modeller og prosessmodeller, Hva de enkelte partene kan og skal gjøre når de sender eller mottar informasjon.

De enkelte partnere som inngår i samhandlingen kan benytte disse beskrivelsene til å bygge sine interne IKT løsninger og etablere nødvendige avtaler.

Niem

NIEM er et USA-basert community med et sett av verktøy og metoder for å øke gjenbruk av informasjon og øke samhandling mellom offentlig organisasjoner og mot næringslivet.

Helsedirektoratet, Elin-metoden

ELIN-prosjektets mandat har vært å gjennomføre standardiserte utviklingsprosjekter for å understøtte nødvendig helsefaglig kommunikasjon for praktiserende leger via deres elektroniske pasientjournalsystemer.

Generell/ overordnet metodikk som ligger bak eResept er såkalt ELIN-metode [47].

Altinn, metode for å etablere tjenester

Altinn har metodeprofiler for følgende tjenester [13]:

- Innsendingstjeneste
- Meldingstjeneste
- Formidlingstjeneste
- Innsynstjeneste
- Samhandlingstjeneste
- Lenketjeneste

Metodeprofil som er mest relevant for etat til etat informasjonsutveksling er samhandlingstjenesten. Denne vil trolig bygge på de andre metodeprofilene, men er for tiden under utarbeidelse.

SSB, Statistisk Sentralbyrå

Erfaringene fra mange års arbeid med datainnhenting fra registre har resultert i systematisk fokus på datakvalitet som del av informasjonsutvekslingen inn til SSB.

Et viktig steg i kvalitetsregimet er inngåelse av avtaler med etatene som SSB mottar data fra, kalt «Avtale om utlevering av data til SSB og samarbeid om kvalitet i administrative data». For hver avtale er det utarbeidet bilag om hvilke data som skal utleveres samt når og hvordan dette skal skje. Videre et Bilag med kontaktinformasjon bl.a. for hvert register samt et Bilag med oversikt over de kvalitetsrapportene som SSB skal lage (en rapport for hvert register).

Prosjektveiviseren, DIFI

Prosjektveiviseren er Difis anbefalte prosjektmodell for gjennomføring av digitaliseringsprosjekter i offentlige virksomheter.

Prosjektmodellen

- er rettet mot prosjektledere og prosjekteiere, og har som formål å bidra til flere vellykkede prosjekter
- er et sett med faser som prosjekter skal gjennom med angitte beslutningspunkter
- dekker hele prosessen fra prosjektets konsept til overlevering og avslutning, samt realisering av gevinster
- kan benyttes i alle typer prosjekter
- er en tilpasning av PRINCE2® til IKT prosjekter i offentlige virksomheter i Norge. Dette innebærer blant annet at gjeldende felles offentlige føringer er tatt inn i rammeverket

Det er laget en egen profil som kalles «Prosjektveiviseren for e-handel».

4.14 Prosess for avklaring av komplekse begreper

DIFI har utviklet en standard for begrepsbeskrivelse (http://www.difi.no/artikkel/2012/05/standard-for-begrepsbeskrivelser) den prosess som beskrives her er utfyllende i forhold til denne standarden, og egner seg for begreper som krever en formell prosess for å avdekke hvilket verdirom de har.

I arbeidet med begrepsharmonisering kan det i noen tilfeller være vanskelig å komme frem til et harmonisert begrep. Den prosess som er beskrevet i dette kapittelet beskriver en fremgangsmåte som bør følges ved begreper som det kan være vanskelig å harmonisere eller koordinere gjennom enklere prosesser, hvor det med enklere prosesser menes serier med møter hvor innholdet og definisjonen til et begrep diskuteres.

Den metode som er beskrevet her er en formell fremgangsmåte basert på velkjente prinsipper for avklaring av gyldighetsområdet til begreper.

Metoden tar for gitt at det allerede er gjennomført enklere harmoniseringsforsøk og at begrepene som skal harmoniseres er kjente. Slike metoder kan for eksempel være DIFI sin ”Standard for begrepskoordinering.”

I dette dokumentet har vi brukt som gjennomgående eksempel at det er to forskjellige etater som har behov for å få koordinert sine begreper, men behovet for koordinering kan også gjelde innen en organisasjon, denne prosess vil ha samme gyldighet innen en organisasjon.

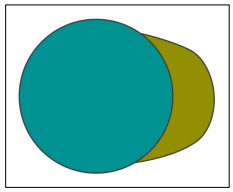
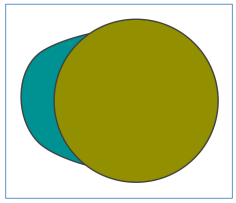
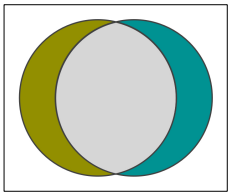
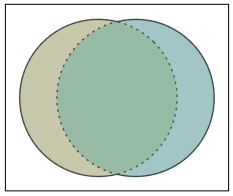
Selv om man er eller blir ening om betydningen av begreper er det ikke dermed sagt at avgiver har den ønskede populasjon, datakvalitet, hjemmel, IT støtte osv til at informasjonsutvekslingen kan etableres.

4.14.1 Koordinering av regler

Den fremgangsmåte etat2 må benytte for å klarlegge sammenhengen mellom regelen til etat1 og etat2 er en prosess som omfatter[1]:

A. -tolkning av eget lovgrunnlag med sikte på å klarlegge hvilke faktiske tilfeller som faller innenfor regelen,
B. -beskrivelse av resultatet av denne tolkningsprosessen,
C. -sammenlikningen med de faktiske tilfeller angitt av etat1 i regelen til etat1,
D. -angivelse av i hvilken utstrekning reglene er sammenfallende;

Resultatene av denne koordineringen kan beskrives som fem alternativer:

A	alle faktiske tilfeller i etat1 er forskjellige fra faktiske tilfeller til etat2. Begrepene er forskjellige og det er ikke behov for noen koordinering.	
B	alle faktiske tilfeller i etat2's regel faller inn under referansen til etat1's regel, men ikke alle tilfeller som omfattes av etat1's regel faller inn under referansen til etat2's regel (etat1's regel har en mer omfattende referanse (denotasjonen omfatter flere tilfeller) enn etat2's regel).	
C	(motsatt av B): ikke alle faktiske tilfeller i etat2's regel faller inn under referansen til etat1's regel, men alle tilfeller som omfattes av etat1's regel faller inn under referansen til etat2's regel (etat2's regel har en mer omfattende referanse/denotasjonen omfatter flere tilfeller enn etat1's regel).	
D	(kombinasjon av B og C): Reglene til etat2 og etat1 har delvis overlappende referanse, men slik at noen tilfeller som faller inn under etat1's regel faller utenfor etat2's regel, og motsatt.	
E	Fullstendig koordinert regel; alle faktiske tilfeller som omfattes av etat2's regel, og bare disse omfattes av etat1's regel. (Med andre ord; uttrykkene som angir vilkårene for to rettsvirkninger har samme meningsinnhold, og er dermed «samme begrep»).	

I tilfellet med fullstendig koordinering er det mulig for etat2 å forstå verdiene, og de angitte verdiene[2] er relevante for etat2. Dette gir grunnlag for informasjonsutveksling (av rådata) fra etat1 til etat2, eventuelt fra en fellesforvaltning til etat1 og etat2[3]. Slik informasjonsutveksling vil isolert sett

[1] For ordens skyld: Dette arbeidet kan skje fortløpende, og det er ikke nødvendig å analysere den ene etatens begreper først.
[2] Eksisterende referanse hos arbeidsgiver.
[3] Under EDAG er det Etatenes Fellesforvaltning (EFF) som samler inn dataene fra arbeidsgiver, og NAV, SKD og SSB henter dataene fra EFF.

være en effektivisering som isolert sett gir rasjonaliseringsgevinster. Informasjonsutveksling forutsetter at øvrige juridiske krav er oppfylt.

I tilfellene B/C og D er reglene ikke koordinert. Dette kan håndteres på tre alternative måter:

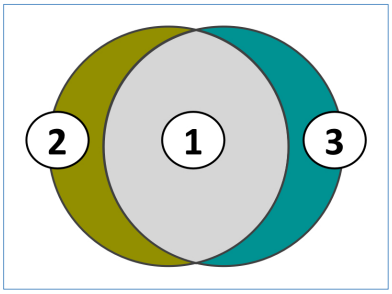
- Harmonisering av begrepene, se punkt 9 nedenfor
- Resignere, og akseptere at begrepene ikke er eller kan gjøres likere, tilfelle A.
- Konstruksjon av nye begreper, se punkt 2:

4.14.2 Konstruksjon av nye begreper

Dette fremstilles her som to forskjellige alternativer, men flere kombinasjoner er mulige:

1. Transformering til nytt begrep. Uttrykket «transformering» innebærer at vi konstruerer ett nytt begrep som omfatter **minste felles multiplum**, altså ett begrep som omfatter alle de faktiske forholdene/kriteriene.[4]
2. Konstruksjon av nytt begrep som bare omfatter de kriterier som omfattes av begge de opprinnelige begrepene. Siden de opprinnelige begrepene ikke var ett sammenfallende begrep, vil det av denne prosessen bli en **rest**, som er de kriterier/faktiske forhold som bare ble omfattet av det ene eller det andre begrepet. Hvordan skal denne «rest» håndteres? Denne rest kan transformeres til nytt begrep, eller behandles som flere begreper, osv.[5]

Et transformert begrep er dårlig egnet for **informasjonsutveksling** eller i felles **informasjonsrapporteringssystemer** (som EDAG), for opplysningene som innhentes i henhold til et slikt begrep vil per definisjon være for upresist enten for den ene eller for begge etater (avhengig av om de opprinnelige begrepene hadde hver sine kriterier som ikke ble omfattet av det ander begrepet). I EDAG er 'overtid' et eksempel på et slikt transformert begrep: Det omfatter både bare tillegget og hele overtidsbetalingen. Begrepet er imidlertid tilstrekkelig presist for Skatteetaten som beskatter overtidsbetalingen, men det er litt for upresist for SSB. Ytterligere et eksempel er 'bonus', som omfatter bonus som utbetales både basert på egeninnsats og basert på bedriftens resultat.



I figuren så er 1 det transformerte begrepet hvor de faktiske tilfellene er overlappende, og det vi har harmonisert. For å ivareta etatenes behov må det utvikles nye begreper for å dekke forskjellene i 2 og 3.

4.14.3 Vurdering av harmoniseringsbehov og harmonisering av regler

I tilfellene B/C og D er reglene ikke koordinert, og dersom konstruksjon av nye begreper ikke er fruktbart, så oppstår spørsmålet om reglene bør harmoniseres. Dette er neste stadium i prosessen og

[4] Dette innebærer en lite presis definisjon, og slik transformering vil særlig være aktuelt i situasjoner hvor det ikke er nødvendig med et mer presist begrep. (Skatteetatens bonus-begrep er et eksempel på dette)
[5] Dette er typiske tilfeller hvor overføring til manuell behandling er særlig aktuelt.

innebærer at etaten(e) må vurdere om det foreligger noe harmoniseringsbehov. Denne vurderingen er en konsekvensanalyse.

Harmonisering av tilfellene B/C kan lede til større grad av sammenfall (men fortsatt B/C), eller fullstendig sammenfall (tilfelle E). Resultatet av en harmonisering av tilfellet D kan være harmonisering til større sammenfall, men fortsatt et D-tilfelle, harmonisering til et B/C-tilfelle eller harmonisering til et fullstendig koordinert/harmonisert E-tilfelle.

Resultatet av harmoniseringen og de vurderinger som ligger til grunn for harmoniseringen må presenteres og dokumenteres i henhold til virksomhetens dokumentasjonskrav.

5 Referanser

1. ISO/IEC 27010 — Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.
    - http://www.iso27001security.com/html/27010.html
2. Sjekkliste for informasjonssikkerhet i kraftforsyningen
    - http://www.nve.no/Global/Sikkerhet%20og%20tilsyn/Kraftforsyningsberedskap/Sjekkliste%20for%20informasjonssikkerhet%20i%20kraftforsyningen.pdf
3. Sjekkliste for testing av elektroniske meldinger mellom virksomheter, September 2010. Nasjonalt meldingsløft. Helsedirektoratet.
    - http://www.helsedirektoratet.no/publikasjoner/sjekkliste-for-testing-av-elektroniske-meldinger-mellom-virksomheter/Sider/default.aspx
4. NIEM user guide, se primært side 58-68
    - http://reference.niem.gov/niem/guidance/user-guide/vol1/
5. ISO 704, Terminology work -- Principles and methods/ NS-ISO 704 – terminologistandardisering på norsk
    - http://www.sprakrad.no/nb-NO/Toppmeny/Publikasjoner/Spraaknytt/Spraknytt-12011/NS-ISO-704/
6. DIFI standard for begrepsbeskrivelser
    - http://www.standard.difi.no/filearchive/2012-02-02-mal-begrepsbeskrivelser-0-9.pdf
7. Konseptskisse SERES, Brønnøysundregistrene, juni 2008.
    - http://www.brreg.no/samordning/semantikk/SERES_konseptskisse_v1_0.pdf
8. NIEM quality assurance strategy and plan. 20. Mai 2008.
    - http://reference.niem.gov/niem/guidance/quality-assurance-strategy-and-plan/1.0/quality-assurance-strategy-and-plan-1.0.pdf
9. Provenance interchange working group charter
    - http://www.w3.org/2011/01/prov-wg-charter.html
10. ISO 8000 Data Quality
    - http://en.wikipedia.org/wiki/ISO_8000
11. Issues and guidance for opening governmental judicial research data. Anneke Zuiderwijk et al. EGOV 2012.
12. Semicolon: Veiledning i bruk av kokeboken. Thom-Kåre Granli (Institutt for Privat rett, UIO), Terje Grimstad (Karde), Per Myrseth (DNVKEMA) og Erlend Øverby (Karde).

13. Altinn nett. For planlegging, utvikling og forvaltning av tjenester i Altinn https://altinnett.brreg.no/
14. Intensjonsavtale om elektronisk utveksling av opplysninger. Semicolon, Thom-Kåre Granli
15. Avtale om elektronisk utveksling av opplysninger, med bilag. Semicolon, Thom-Kåre Granli.
16. Journey to Data Quality. Yang W. Lee, Leo L. Pipino, Richard Y. Wang, James D. Funk. The IT press, 2006.
17. Data Quality. Consepts, Methodologies and Techniques. Carlo Batini and Monica Scannapieco. Springer 2006.
18. Arkitekturprinsipper Difi versjon 1.0 Side 1 av 8 03.04.2009
19. Overordnede IKT-arkitekturprinsipper for offentlig sector. DIFI, 3. April 2009. http://www.difi.no/filearchive/ikt-arkitekturprinsipper_bhnq1.pdf
20. Risikovurdering - en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. DIFI, januar 2010. http://www.difi.no/filearchive/rapport-veiledning-til-rammverket-versjon-0-1.pdf
21. Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon. KITH Rapport 13/2000. http://www.kith.no/upload/995/R13-00Risikoanalyse-v1.pdf
22. Livssyklusprosess for utarbeidelse og forvaltning av begrepssystemer. Semicolon, Februar 2011, Versjon 1.0. Vibeke Dalberg, DNV; Per Myrseth, DNV; Jim Yang, KITH. http://www.semicolon.no/Rapport_prosess_begrepssystem_Final.pdf
23. Standard for begrepskoordinering. DIFI. Versjon/dato: 0.8 / 2012-10-21
24. Capability Maturity Model, http://www.sei.cmu.edu/process/index.cfm Carnegie Mellon University
25. Capability Maturity Model Integration, http://cmmiinstitute.com/ Carnegie Mellon University.
26. Unveiling Barriers and Enablers of Risk Management in Interoperability Efforts. HICSS-47. By Pernille Monstad Røberg, Leif Skiftenes Flak and Per Myrseth.
27. Use the risk pyramid to assess risk in five minutes. Gartner research. 2 may 2011. Originally used in Royal Bank of Canada annual report for 2004.
28. TickITplus. http://www.tickitplus.org/
29. Survey on vocabulary and ontology tools. Including a methodology for comparing tools. By Per Myrseth, DNVKEMA; Jim J. Yang, Norwegian Directorate of Health; Erlend Øverby, Karde.

6 Appendiks: Teknisk gjeld og integrasjonsgjeld

Hva er teknisk gjeld

Definisjon: Begrepet "Teknisk gjeld" henviser til eventuelle konsekvenser ved mangler og svakheter i programkode, SW-arkitektur, IT-plattform eller systemutvikling. I systemer som endres vil mangler og svakheter øke om ikke mottiltak iverksettes. Så lenge manglene ikke utbedres representerer de en gjeld som igjen medfører renter i form av økt kompleksitet, merarbeid og økt risiko.

Definisjonen over er inspirert av Wikipedia Technical Debt[6], Software Entropy[7] og Managing Technical Debt [2].

Integrasjonsgjeld (delmengde av teknisk gjeld) gjelder grensesnitt mellom systemer og data som utveksles mellom systemer. Tilsvarende kan en også argumentere for at manglende dokumentasjon både teknisk, drift og brukerdokumentasjon er en form for gjeld som er med på å øke kostnader ved bruk, drift og vedlikehold.

Begrepet er brukt for å illustrere at det gjenstår arbeid med programkode, SW-arkitektur, grensesnitt og/eller IT-plattform for å komme opp på ønsket kvalitetsnivå. Så lenge dette arbeidet er ugjort representerer gjelden en risiko og prisen for å få utført arbeidet er en utsatt kostnad i form av at merarbeid og risiko påløper. Med kvalitetsnivå menes her at programkode, SW-arkitektur, grensesnitt og/eller IT-plattform oppfyller: (i) funksjonelle krav, (ii) ikke-funksjonelle krav og (iii) krav gitt av systemutviklingsmetoder, standarder og god praksis.

Teknisk gjeld oppstår typisk når:

- Tid er viktigere enn kvalitet i utvikling/ endring av et system
- Pris er viktigere en kvalitet i utvikling/ endring av et system
- Det ikke foreligger tilstrekkelig gode rutiner for systemutvikling og kvalitetssikring av programkode
- Det er manglende evne eller vilje til å sikre kvalitet

Eksempler på bidrag til den tekniske gjeld er:

- Kode som bare er gjort midlertidig uten komplett testing av alle eventualiteter
- Alle "TODO" statement i koden som er utsatt, eksempelvis dokumentasjon, effektivisering av kode, mm.
- Kode som ikke er dokumentert.
- Programkode som "svelger" feil uten å gjøre noe med disse.
- Utsettelse eller manglende oppgradering av programvare, programvaremiljø og IT-plattform.
- Mangelfullt testdesign og testdekning.
- Mangelfull kravspesifisering og mangelfullt design
- Overlapp og kompatibilitetsutfordringer mellom "denne kodebiten" og annen kode. Eksempelvis deler av koden er kopiert og brukes flere steder.
- Upresis/feil tolkning av data i systemet dvs. bruk av data og programmert logikk. Gjelder når brukere, jus/regler og tilgrensende systemer endrer sin bruk og tolkning av data. Også organisasjonsendringer er en kjent utfordring for ulike IT-systemer.
- Koden ferdigstilles og tas i bruk før en har avklart om den oppfyller funksjonelle og ikke-funksjonelle krav.
- Alle de ting som er blitt utsatt fordi prosjektet må levere på tid / kost og ikke oppnår tilstrekkelig kvalitet.

[6] http://en.wikipedia.org/wiki/Technical_debt
[7] http://en.wikipedia.org/wiki/Software_entropy

En vanlig virksomhet har en blanding av (i) egenutviklet programvare, (ii) hyllevare med større tilpasninger, (iii) hyllevare med kun konfigurering for virksomhetens bruk og (iv) integrasjoner mellom systemene. Hvert av systemene i disse kategoriene har sine livsløp og systemene vil bli faset ut og grensesnitt endret. Normalsituasjonen er at store deler av informasjonen i systemene skal leve videre i nye systemer. Virksomhetens evne til å påvirke oppbygging og håndtering av teknisk gjeld vil for disse være forskjellig, men summen av gjeld vil uansett være virksomhetens ansvar å ha et bevisst forhold til.

IKT relatert gjeld kan sees i samanheng med:

- Informasjonsforvaltnings-gjeld, som omfatter gjeld innen begrepsforvaltning, datakvalitet, masterdataforvaltning mm.
- Andre interoperabilitetsutfordringene som organisatorisk og juridisk gjeld.

I en del situasjoner ønsker en å ta opp økonomisk gjeld for å oppnå virksomhetens mål. Slik vil det også være med teknisk gjeld og programvareutvikling. Ved bruk av smidige metoder og pilotering kommer en raskt ut i markedet med sin løsning og får rask feedback fra brukere. Ønsker en å fokusere på tid og er inneforstått med at en tar opp teknisk gjeld, kan dette være en god suksessformel. Om pris er hovedfokus, kan en redusere kost på første versjon ved å ta opp teknisk gjeld. Det som vil være avgjørende er om en vet hvor stor teknisk gjeld en har til en hver tid, hvor den tekniske gjelden befinner seg i systemet, og at en har en plan for hvordan hele eller deler av gjelden skal nedbetales. Det er ikke uvanlig at større organisasjoner klager over at 70-90 % av IT budsjettet går til vedlikehold av eksisterende programkode og IT-plattform. For mange er nok store deler av disse 70-90 % nedbetaling av teknisk gjeld.

Levetid for et større IT-system er ofte i intervallet 5-10 år. I et livssyklusperspektiv er det fristende å øke gjelden (for å kutte kostnader) mot slutten av levetiden. Dette fordi systemet skal termineres og gjelden vil forsvinne når systemet fases ut av bruk. Dette er en vanlig strategi som mange har god suksess med. For virksomhetskritiske systemer vil økende teknisk gjeld ved slutten av levetiden være økonomisk interessant å vurdere, men økt teknisk gjeld vil vanligvis også øke risiko for feil og problemer. Balansen mellom lav kostnad og høy kvalitet i IT-systemene er en klassisk utfordring. Virksomhetskritiske systemer i slutten av sin levetid som øker teknisk gjeld tar en risiko som kan være i konflikt med krav fra forretningssiden (dvs. brukere og eiere av systemet) innen dimensjoner som tilgjengelighet, integritet, konfidensialitet, økonomi og omdømme.

Det er ikke uvanlig at ved utfasing av et system vil (i) en måtte etablere ny funksjonalitet for å få flyttet data over i andre og overtagende systemer og (ii) integrasjoner mellom samhandlende systemer være i endring. I et IT-landskap med distribuert informasjon og tett integrerte systemer, slik man finner i mange større organisasjoner, viser det høy risikoappetitt om en øker teknisk gjeld i siste livsfase av et system. Slikt vil kreve spesiell oppfølging bl.a. fordi tilgrensende systemer også vil kunne bli skadelidende.
Tilsvarende vil det være risikosport å etablere informasjonsutveksling med andre organisasjoner hvor en ikke

	Tilsiktet, med overlegg, vet at man øker teknisk gjeld	Utilsiktet, uvitende om at man øker teknisk gjeld
Ingen plan for nedbetaling	Kjent risiko, kalkulert	Høy risiko
Har plan for kartlegging og nedbetaling	OK	Ukjent risiko, men har en plan/metode for å finne den

Figur 20, Teknisk gjeld og risiko-kvaderant

har kartlagt risikoer og muligheter på alle interoperabilitetslag.

Sammenheng mellom hvordan teknisk gjeld oppstår, hvordan gjelden er planlagt håndtert og risiko er forsøkt systematiser i figur 1. Matrisen er basert på Technical Debt Quadrant [3] og supplert med et risikofokus.

Forskjeller mellom økonomisk gjeld og teknisk gjeld.

En viktig forskjell er at den som etablerer økonomisk gjeld må stille sikkerhet og er ansvarlig for å betaler renter og nedbetale gjelden. Konsekvensen ved å ikke betale økonomisk gjeld kan være konkurs, eller at verdier og eiendeler blir inndratt. For teknisk gjeld er det ofte slik at den som tar opp gjeld kan overlate til andre å betale både renter og avdrag samt problemer ved størrelsen på gjelden. Dette gjør at lysten til å etablere teknisk gjeld for ofte er større enn det den burde være. Dette er ofte kjernen i utfordringene mellom suksess med en prosjektleveranse versus suksess gjennom hele levetid for et system.

Hvordan kan summen av teknisk gjeld håndteres

For å håndtere summen av teknisk gjeld trenger virksomheter å vite:

- Hvor stor gjeld en har til en hver tid
- Hvor gjelden befinner seg i systemet, systemene, grensesnitt, kravene, arkitekturen, IT-plattformen
- Hvilke deler av gjelden som er viktigst å betale ned og konsekvens ved ikke å betale ned
- Hva som er egnet tiltak for å nedbetale ulike deler av gjelden, eksempelvis:
    - Omskriving og opprydding (refactoring) av kode
    - Redesign av arkitektur

For å etablere oversikten nevnt i kulepunktene over vil bruk av risikoanalyser og risikostyring være godt egnet og velprøvde metoder.

Eksempler på forebyggende tiltak som kan iverksettes for å redusere oppbygging av gjeld kan være:

- Grundig og god behovs og kravspesifisering
- Vis høy risikoappetitt kun der du faktisk tåler det, og vit når du velger / ikke velger høy risikoappetitt.
- Etablere og bruke SW utviklingsmetoder
- Etablere og bruke kodestandarder og gjennomganger
- Testing, testing og atter testing

Kilder for dette appendix

1. Vurdering av Altinn II-plattformen. DNV rapport NR. 2011-1239. http://www.regjeringen.no/upload/NHD/Vedlegg/Rapporter_2012/altinn_sluttrapport_20120321.pdf
2. Managing Technical Debt, Eric Allman, Communication of the ACM May 2012. Og ACM Queue publikasjon: http://queue.acm.org/detail.cfm?id=2168798
3. Fowler, M. 2009. Technical debt. www.martinfowler.com/bliki/TechnicalDebtQuadrant.html