

Tredjepartsverifikasjon IKT

Utført av Capgemini



Innhold

- Om Capgemini
- Bakgrunn
- Verifikasjonsmetode
- Verifikasjon
 - 1. Verifikasjon av byggherrens tilbudsunderlag
 - 2. Verifikasjon av leverandørens design
 - 3. Verifikasjon av leverandørens leveranser
- Forslag til tiltak

Capgemini

En av verdens ledende leverandører av Consulting, Technology og Outsourcing tjenester

- Antall ansatte: 61.000 globalt
3 000 i Norden
550 i Norge
- Omsetning 2005: 6,954 milliarder euro
- Omsetning 1. halvår 2005: 3,5 milliarder euro
- Hovedkontor: Paris, Frankrike
- CEO Norge: Kjell Ulmfeldt
- Kontorer i Norge: Oslo, Trondheim, Bergen, Stavanger, Fredrikstad



Bransjefokus

- Olje & Gass
- Maritim
- Offentlig
- Finans
- Telecom

Kompetanse

- Bransjespisskompetanse
- Metoder, verktøy og teknikker
- Gjenbruk av kunnskap og erfaringer
- Stort partnernettverk
- Stadig utvikling av nye tjenester og konsepter

Om Collaborative Business Experience

- Capgemini, en av verdens mest innovative leverandører av tjenester innenfor Consulting, Technology og Outsourcing, samarbeider med sine kunder på en unik måte vi kaller Collaborative Business Experience.
- Basert på over tre tiår med erfaring fra industrien og tjenesteleveranser, er Collaborative Business Experience utviklet for å hjelpe våre kunder til å oppnå bedre, raskere og mer varige resultater gjennom full tilgang til vårt nettverk av ledende teknologipartnere og samarbeidsrettede metoder og verktøy.
- Gjennom en forpliktelse om gjensidig suksess og varig verdiskapning, hjelper vi virksomheter til å implementere vekststrategier og utnytte teknologier gjennom god samarbeidsånd.
- Capgemini sysselsetter omlag 55.000 mennesker verden over, og omsatte i 2003 for totalt 5.7 mrd. euro.
- Kontorer i Norge: Oslo, Trondheim, Bergen, Stavanger, Fredrikstad
Ansatte i Norge:550



Oppgave: Vurdering av tilgjengelighet i datanettverket

- Datamatrix ble etablert i 1982.
- 128 ansatte, fordelt på avdelinger i Norge, Sverige og Danmark.
- Samlet omsetning for 2005 var 360 MNOK.
- Selskapet eies av konsernet Tele2 AB.

- **Datamatrix er Cisco gullpartner**

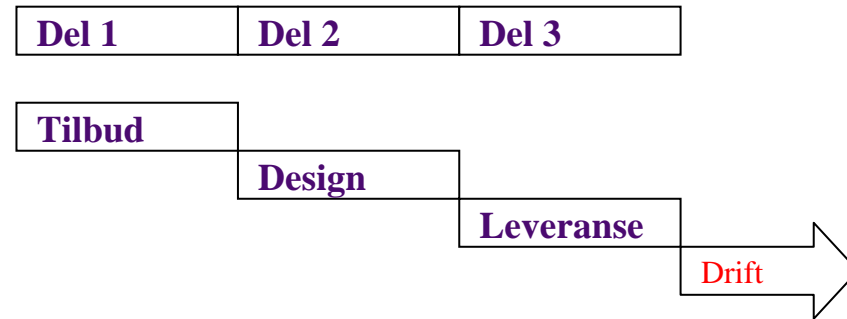


Bakgrunn

- Verifikasjonen tar utgangspunkt i dokument
*720-8001 Tredjeparts-verifikasjon IKT, YTELSSES- OG
RAPPORTERINGSSPESIFIKASJON*

”Helsebygg Midt-Norge ønsker å få verifisert datanettets funksjonalitet og egnethet fra ide og ned til komponenters godhet i den valgte strukturen. For å kunne holde oversikt og fokus gjennom verifiseringen deles oppgaven inn i tre hoveddeler med rapportering for hver del som samles og gis en endelig utforming i felles sluttrapport.”

- Verifikasjonen gjøres i 3 deler:
 1. Verifikasjon av byggherrens tilbudsunderlag
 2. Verifikasjon av leverandørens design
 3. Verifikasjon av leverandørens leveranser



- Verifikasjonen har fokus på B6 Datanett, og St. Olavs Hospital som er den brukeren med størst krav til datanettet
- Det leveres rapport for hver delgjennomgang. Rapportene blir oppsummert i en sluttrapport.

Verifikasjonsmetode

For å besvare spørsmålene har vi

- benyttet dokumentasjon som var input til prosessene (f.eks. anbudsforespørsel)
- benyttet dokumentasjon som ble produsert i prosessene (f.eks. design)
- hatt møter, telefonsamtaler og mailkorrespondanse med personer fra Telenor (inkl. HP og EDB), HBMN, NTNU og St. Olavs Hospital

Delrapportene har følgende mal:

- Sammendrag
- For hvert spørsmål:
 - Kilde: formelt navnet på dokumentasjonen vi legger til grunn for å besvare spørsmålet
 - Beskrivelse av observasjoner i forhold til spørsmålet
 - Svar: kortversjon av svaret

I sammendrag og sluttrapport er svarene i tillegg gitt "karakter" etter følgende skala:

- 😊 - Ingen avvik
- 😐 - Mindre avvik
- 😞 - Større avvik

Presentasjon av resultat (forklaring)

Gjennomgangen dekker utvalgte områder av IKT leveransen.
Disse er visualisert som grønne sirkler

I gjennomgangen avdekkes mindre avvik (gult punkt) og større avvik (rødt punkt)

I rapporten er svarene gitt et symbol

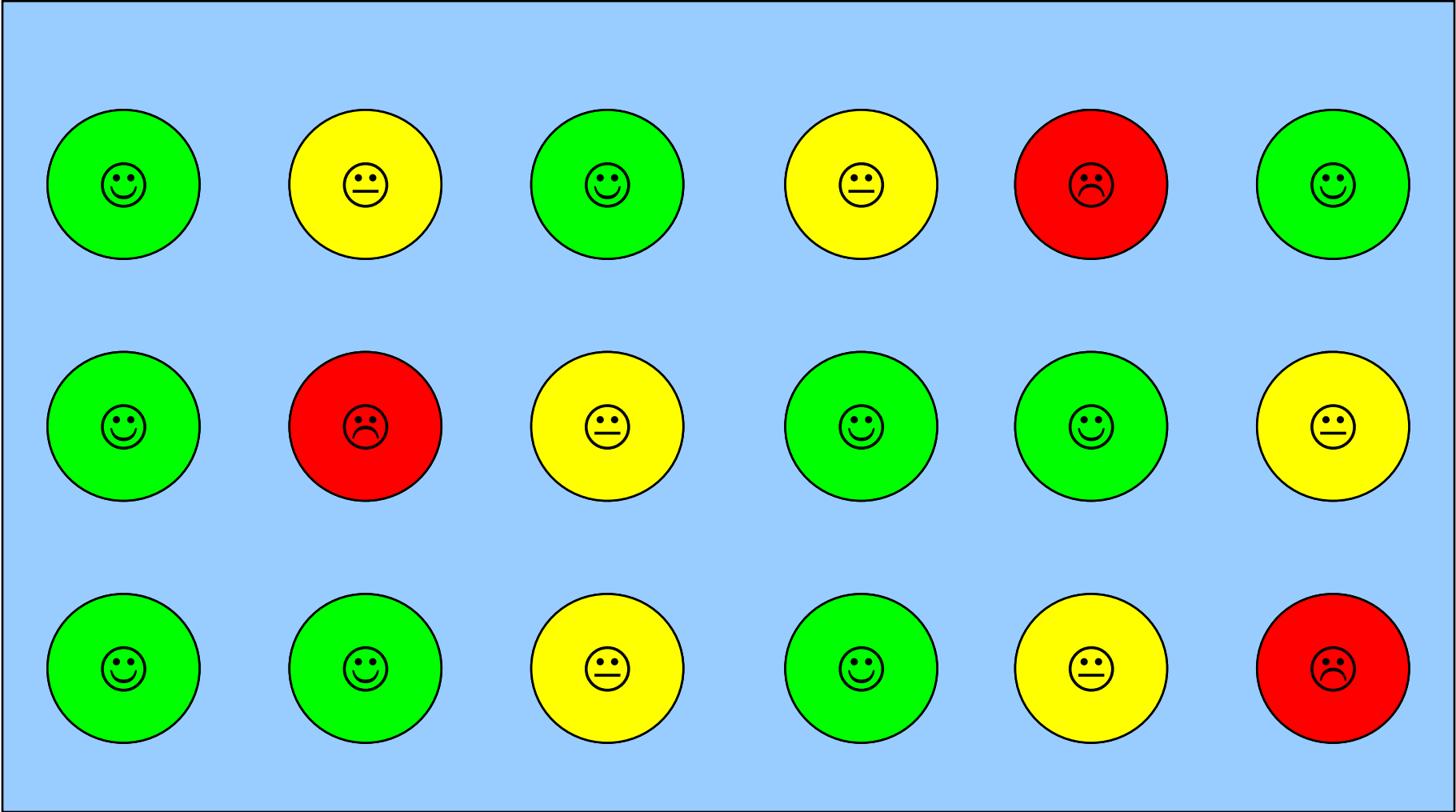
😊 ingen avvik

😐 mindre avvik

😞 større avvik

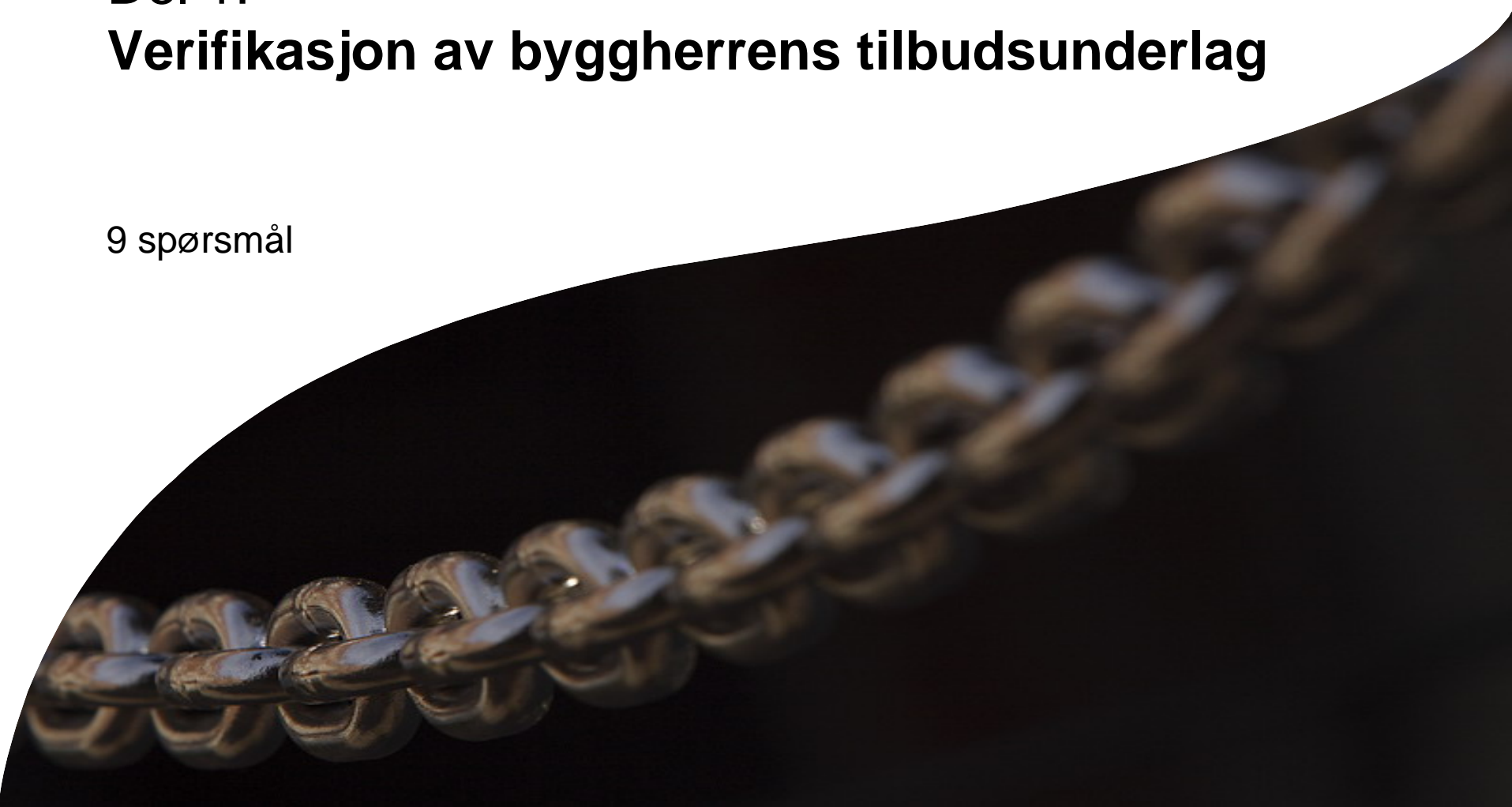
Hele området som dekkes av svaret får farge og et gult eller rødt symbol selv om bare ett avvik er avdekket.

Presentasjon av resultat (symbolsk)



Del 1: Verifikasjon av byggherrens tilbudsunderlag

9 spørsmål



Del 1: Kilder

Som underlag for vurderingen i del 1 har vi hatt tilgang til følgende dokumentasjon:

- Strategidokumenter og handlingsplaner
- Anbudsforespørsel
- Evalueringsrapport av tilbud
- Kontraktdokumenter
- Sikkerhetsgjennomganger
- Møtereferater

Vi har konsentrert innsatsen rundt dokumenter relatert til datanettverk og drift.

Del 1: Verifikasjon av byggherrens tilbudsunderlag

| | Spørsmål | Svar |
|---|---|--|
| 1 | <u>Var ambisjonsnivået i visjon/strategi for omfattende i forhold til det som er teknisk mulig?</u> |  |
| 2 | <u>Gjenspeilte visjon/strategi tilsvarende visjon og strategi for St.Olavs Hospital?</u> |  |
| 3 | <u>Var spesifikasjonene entydige og klar nok?</u> |  |
| 4 | <u>Stemte spesifikasjonen med det som er nedfelt i visjon og strategi?</u> |  |
| 5 | <u>Var de innledende føringer på funksjonalitet forenlig med tilgjengelig teknologi og kompetanse?</u> |  |
| 6 | 1) <u>Ble risiko og sårbarhet vurdert, kompensert og godt nok ivaretatt, og</u> 2) <u>ble failover og alternative løsninger vurdert for å eventuelt kompensere for situasjoner der datanettet ikke fungerer tilfredsstillende?</u> | 1)  2)  |
| 7 | <u>Var dette (ROS analyser) godt nok kommunisert til beslutningstakerne da beslutninger om datanettet ble fattet?</u> |  |
| 8 | <u>Var visjonen for datanettleveransen avstemt med sannsynlig virkelighet på det tidspunktet det skulle tas i bruk av sykehuset?</u> |  |
| 9 | <u>Var det hensiktsmessig å benytte en totalentreprise kontraktsform i dette prosjektet, og hvilke fordeler og ulemper ga kontraktsformen for dette prosjektet?</u> <u>Ble det introdusert risikoer gjennom kontraktsformen?</u> |  |

Del 1: Spørsmål 1 (av 9)

Var ambisjonsnivået i visjon/strategi for omfattende i forhold til det som er teknisk mulig?

Svar: 😊

Ambisjonsnivået i visjon/strategi var ikke for omfattende i forhold til det som var teknisk mulig.



Del 1: Spørsmål 2 (av 9)

Gjenspeilte visjon/strategi tilsvarende visjon og strategi for St.Olavs Hospital?

Svar: 😊

Visjon/strategi gjenspeilte tilsvarende visjon og strategi for St.Olavs Hospital.



Del 1: Spørsmål 3 (av 9)

Var spesifikasjonene entydige og klar nok?

Svar: 😊

Vi har funnet krav som kunne vært nærmere presisert, dette bl.a. begrunnet i besvarelsen fra leverandøren.



Del 1: Spørsmål 4 (av 9)

Stemte spesifikasjonen med det som er nedfelt i visjon og strategi?

Svar: 😊

I hovedsak er det overensstemmelse mellom spesifikasjonen og visjon og strategi. Spesifikasjonen forutsetter nettverksutstyr som rutere og kjernesvitsjer fra Cisco. Konsekvensen av dette er bl.a. at en alvorlig programvarefeil i en kjernesvitsj levert av Cisco kan gi alvorlige driftforstyrrelser i nettverket.



Del 1: Spørsmål 5 (av 9)

Var de innledende føringer på funksjonalitet forenlig med tilgjengelig teknologi og kompetanse?

Svar: ☺

De innledende føringer på funksjonalitet slik disse fremkommer i B6 var forenlig med tilgjengelig teknologi i denne fasen av prosjektet.

Etter vår mening burde det reises tvil om de innledende føringer på funksjonalitet slik disse fremkommer i B6 var forenlig med tilgjengelig kompetanse i denne fasen av prosjektet.



Del 1: Spørsmål 6 (av 9)

1) Ble risiko og sårbarhet vurdert, kompensert og godt nok ivaretatt?

Svar 1: 😞

Ut fra tilgjengelig dokumentasjon kan vi ikke se at ROS for teknisk løsning har vært systematisk gjennomført og fulgt opp i tilbudsfasen.

2) Ble failover og alternative løsninger vurdert for å eventuelt kompensere for situasjoner der datanettet ikke fungerer tilfredsstillende?

Svar 2: 😊

Det ble tatt høyde for å benytte alternative løsninger for eventuelt å kompensere for situasjoner der datanettet ikke fungerer tilfredsstillende.



Del 1: Spørsmål 7 (av 9)

Var dette (*ROS-analyser*) godt nok kommunisert til beslutningstakerne da beslutninger om datanettet ble fattet?

Svar: 😊

Beslutning om valg av løsning (kravspesifikasjon) for datanettet ble tatt uten at det var gjort formelle ROS-analyser. Beslutningstakerne ved Prosjektstyret fikk presentert overordnede risikobetraktninger med forslag til risikoreduserende tiltak. Vi vurderer det slik at beslutningsgrunnlaget ikke var fullstendig, men at man ved de foreslåtte tiltakene (bl.a. Proof of concept, Fall back) kunne argumentere for beslutningen ved at man utsetter vurdering av risiko for løsningen til et senere tidspunkt.



Del 1: Spørsmål 8 (av 9)

Var visjonen for datanettleveransen avstemt med sannsynlig virkelighet på det tidspunktet det skulle tas i bruk av sykehuset?

Svar: 😊

Visjonen for datanettleveransen var avstemt med sannsynlig virkelighet på det tidspunktet det skulle tas i bruk av sykehuset.



Del 1: Spørsmål 9 (av 9)

Var det hensiktsmessig å benytte en totalentreprise kontraktsform i dette prosjektet, og hvilke **fordeler og ulemper** ga kontraktsformen for dette prosjektet? Ble det introdusert risikoer gjennom kontraktsformen?

Svar: 😊

Det er etter vår vurdering optimalt å benytte en samordnet entreprisemodell for å plassere alt ansvar hos en leverandør, gitt kompleksiteten og mangfoldet av IKT-systemene som skulle leveres og som skulle integreres med eksisterende IKT-system. Det er etter vår oppfatning også en klok avgjørelse å la samme entreprenør få ansvaret for driften.

Vi mener at kontraktsformen muliggjør introduksjon av enkelte risikoer, selv om det ikke er avdekket noen avvik i prosjektet.



Del 2: Verifikasjon av leverandørens design

3 spørsmål



Del 2: Kilder

Som underlag for vurderingen i del 2 har vi hatt tilgang til følgende dokumentasjon:

- Kontraktdokumenter;
- PDR (Preliminary design review) og FDR (Final design review) dokumenter;
- Møtereferater og statusrapporter.

Vi har konsentrert innsatsen rundt dokumenter relatert til datanettverk og drift.

Del 2: Verifikasjon av leverandørens design

| | Spørsmål | Svar |
|---|---|---|
| 1 | <u>Stemmer beskrevet design/arkitektur/konsept med funksjonsspesifikasjonen?</u> |  |
| 2 | <u>Vil beskrevet løsning gi en god og driftssikker implementering i et operativt sykehus?</u> |  |
| 3 | <u>Hvilke risikoer er forbundet med de foreslåtte løsningene - hvor sårbar er løsningen?</u> |  |

Del 2: Spørsmål 1 (av 3)

Stemmer beskrevet design/arkitektur/konsept med funksjonsspesifikasjonen?

Svar: 😊

Dokumentasjonen viser at beskrevet design/arkitektur/konsept stemmer med funksjonsspesifikasjonen i betydningen at det foreligger design av samtlige krav i B6. Vi er likevel av den oppfatning at designet av kravet til tilgjengelighet kunne vært gitt en mer omfattende beskrivelse samt begrunnelse.



Del 2: Spørsmål 2 (av 3)

Vil beskrevet løsning gi en god og driftssikker implementering i et operativt sykehus?

Svar: 😊

Beskrevet løsning kan gi en god og driftssikker implementering i et operativt sykehus, selv om det i denne fasen av prosjektet mangler driftsdesign av noen ITIL prosesser. Dette er mangler som vi forutsetter kommer på plass av en leverandør som ønsker å basere sin drift på ITILs rammeverk.



Del 2: Spørsmål 3 (av 3)

Hvilke risikoer er forbundet med de foreslåtte løsningene - hvor sårbar er løsningen?

Svar: ☹️

Dokumentasjonen viser at kartlegging av risiko og sårbarhet ble gjennomført hos de forskjellige partene. De viktigste områdene ble avdekket og noen områder ble behandlet formelt, andre områder mindre formelt. Informasjon om risiko og sårbarhet fra leverandøren Telenor til HBMN og videre til St. Olavs Hospital har ikke vært tilstrekkelig, selv om St. Olavs Hospital hadde et selvstendig ansvar for å vurdere risiko og sårbarhet for løsningen.

Behovet for oppdatering av beredskapsplaner hos St. Olavs Hospital var avdekket i prosjektet, men forståelsen for å gjennomføre dette ville vært mye større med bedre informasjon om risiko i løsningen.



Del 3: Verifikasjon av leverandørens leveranser

6 spørsmål





Del 3: Kilder

Som underlag for vurderingen i del 3 har vi hatt tilgang til følgende dokumentasjon:

- Kontraktdokumenter;
- PDR (Preliminary design review) og FDR (Final design review) dokumenter;
- As built dokumenter;
- Rapporter fra sikkerhetsgjennomganger;
- Evalueringsrapporter etter innflytting
- Testplaner og testrapporter
- Servicenivå rapporter
- Møtereferater og statusrapporter.

Vi har konsentrert innsatsen rundt dokumenter relatert til datanettverk og drift.

Del 3: Verifikasjon av leverandørens leveranser

| | Spørsmål | Svar |
|---|---|---|
| 1 | <u>Stemmer levert løsning med prosjektets visjon og strategi, byggherrens og rådgivernes funksjonsspesifikasjon og leverandørens design?</u> |  |
| 2 | <u>Fanget kravanalysen som ble gjennomført ved starten av designfasen opp de kravene som var vitale for prosjektet, og ble oppfyllelsen av disse kravene verifisert før datanettet ble satt i drift?</u> |  |
| 3 | <u>Var testregime og den testingen som ble gjennomført egnet til virkelig å avdekke svakheter med løsningen, og dekket testene hele leveransen?</u> <u>Var testing og verifikasjon før idriftsettelse tilstrekkelig?</u> |  |
| 4 | <u>Var klargjøring for drift tilstrekkelig for å sette løsningen i drift?</u> |  |
| 5 | <u>Er nettet konstruert på en slik måte at kontraktskravet 99.999 % pr. måned kan oppnås?</u> |  |

Del 3: Spørsmål 1 (av 5)

Stemmer levert løsning med prosjektets visjon og strategi, byggherrens og rådgivernes funksjonsspesifikasjon og leverandørens design?

Svar:

Se svar i Del 1 rapport, spørsmål 4 og Del 2 rapport, spørsmål 1.



Del 3: Spørsmål 2 (av 5)

Fanget kravanalysen som ble gjennomført ved starten av designfasen opp de kravene som var vitale for prosjektet, og ble oppfyllelsen av disse kravene verifisert før datanettet ble satt i drift?

Svar: Kravsporingsprosessen tok sitt utgangspunkt i samtlige 214 krav i B6 Datanett. I første del av prosessen ble det skilt ut 74 krav for videre utredning for å komme frem til en felles kravforståelse mellom HBMN og leverandøren. Etter en gjennomgang av saksbehandlingen av disse 74 kravene slik denne er dokumentert i B06-FDR Vedlegg 2 Sporing er vår oppsummering som følger:

Starten på kravanalysen fanget opp alle vitale krav, men vi er ikke sikre på at kravanalysen ble avsluttet med en omforent forståelse av disse kravene ut fra tilgjengelig dokumentasjon. Begge parter er imidlertid enige om at det var en omforent forståelse av kravene .



Del 3: Spørsmål 3 (av 5)

Var testregime og den testingen som ble gjennomført egnet til virkelig å avdekke svakheter med løsningen, og dekket testene hele leveransen?

Svar:

- 3.1. Testregimet og den testingen som ble gjennomført var ikke egnet til virkelig å avdekke svakheter med løsningen. Vår begrunnelse for dette er at testene bare var designet for å sjekke at systemene virket som forutsatt. Eierne av systemer innen de forskjellige systemområder fikk ikke spørsmål om å beskrive hvilke hendelser som opplevdes som alvorlige driftsforstyrrelser med sikte på at denne informasjonen kunne legges til grunn for å lage reserveløsninger.
- 3.2. Testene dekket ikke hele leveransen. Vår begrunnelse for dette er:
 - Mangler ved testene til leverandør
 - Mangler ved testene til HBMN
- 3.3. Testing og verifikasjon før idriftsettelse var ikke tilstrekkelig.
 - Den definerte prosessen for verifikasjon av løsningen var god, men gjennomføringen fulgte ikke prosessen godt nok.
 - De testene HBMN var ansvarlig for var ikke formelt planlagt og dokumentasjon av testresultater i form av testrapporter eksisterer ikke.



Del 3: Spørsmål 4 (av 5)

Var klargjøring for drift tilstrekkelig for å sette løsningen i drift?

Svar: Klargjøring for drift var tilstrekkelig for å sette løsningen i drift.

Vi ønsker likevel å påpeke følgende:

- Leverandøren hadde ikke spesifikke planer hva angår implementering av Continuity management prosessen hos St. Olavs Hospital og NTNU.
- I forbindelse med FSAT savner vi en akseptansetest av IDS-systemet med utgangspunkt i virusangrep, hackerangrep og andre trusler samt hard trafikk belastning. Proxycom og leverandøren utførte sikkerhetstester av datanettet. Vi kan ikke se at Proxycoms test er en akseptansetest av IDS. Rapporten fra leverandørens sikkerhetstest er ikke stilt til vår disposisjon, referanse til møte med testleder, og kan derfor ikke uttale oss om denne testen var en akseptansetest av IDS.



Del 3: Spørsmål 5 (av 5)

Er nettet konstruert på en slik måte at kontraktskravet 99.999 % pr. måned kan oppnås?

Svar:

Beregninger og design-vurderinger tilsier at kontraktskravet på 99,999% tilgjengelighet kan oppfylles.



Forslag til tiltak



Forslag til tiltak for HBMN

| | Tiltak | Prioritet |
|---|--|-----------|
| 1 | <p>Gjennomfør ny ROS analyse for drift med minimum følgende aktiviteter:</p> <ul style="list-style-type: none">• Intervju eierne av systemer innen de forskjellige systemområder om hvilke hendelser som opplevses som alvorlige driftsforstyrrelser og katastrofer for at denne informasjon kan legges til grunn for å lage reserveløsninger og katastrofeberedskapsløsninger• Kartlegging, analyse av risiko og forslag til risikonedsettende tiltak• St. Olavs Hospital må ha sterkt eierskap til denne prosessen | Høy |
| 2 | Utarbeide bedre beskrivelse av rutiner for test og godkjenning av IKT-leveransen fase 2 | Middels |
| 3 | <p>Gjennomfør ny ROS analyse spesielt for nettverk og telefoni med minimum følgende aktiviteter:</p> <ul style="list-style-type: none">• Vurder beredskapsløsninger for alvorlige driftsforstyrrelser og katastrofer nettverk og telefoni• Vurder flere backupløsninger for nettverk og telefoni | Middels |
| 4 | Inkluder krav om ROS analyser ved en eventuell revisjon av IT-strategidokumentet | Lav |
| 5 | Ved en eventuell revisjon av IT-strategidokumentet bør det inkluderes krav om valg av stabil og velprøvd IT-teknologi. I tillegg bør det defineres hva som skal forstås med stabil, velprøvd og moden teknologi | Lav |