

Kvalitetskrav kapittel 10 - 18

M (Mandatory) = Obligatorisk krav fra IT. Krav som skal være et A-krav i ethvert prosjekt.

O (Optional) = Valgfritt krav fra IT. Prosjektet må vurdere hvilken prioritet det skal ha.

Krav med blå tekst betyr at endret krav etter at siste signering av rammeavtaler mai 2015

10 Brukervennlighet og utseende

Forskningsrådet anbefaler å se på "Volere specification template" kap. 10 og 11 for eksempler.

A	Krav til utseende	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	En god brukeropplevelse er førende for utvikling av IT-systemene	M				Se nærmere informasjon i vedlegg
2	Ikonene i Ikonbank skal brukes i egenutviklede systemer.	M				Se nærmere informasjon på siden
3	Brukergrensesnittet skal utformes i henhold til universal utforming. WCAG 2.0 på nivå A og AA er obligatorisk for innhold på offentlige nettsider for Forskningsrådet	M				

11 Systemutvikling

A	Generelle krav	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Navngiving av felter, variabler, konstanter, klasser og metoder skal være informativ og konsistent. Forskningsrådets begrepskatalog på Confluence samt navnene i Forskningsrådets kodeverksmodulen brukes som utgangspunkt.	M				
2	På generell basis skal GUI og presentasjonslag lages som en integrert del av kallende systemet og bruke servertjenester til å hente/lagre data, jmfør Forskningsrådets arkitekturprinsipper (link til dokumentet)	M				Forskningsrådets arkitekturdokument vil følge vedlagt ved anbudsforespørsler
3	Logikk skal legges på lavest mulig lag/nivå	M				
4	Forretningslogikk, presentasjonslogikk og integrasjonslogikk skal som hovedregel holdes adskilt, for å få god lagdeling	M				
5	Egenutviklet kode skal skrives på norsk. Norske bokstaver æøå skal ikke benyttes. (æ=æ, ø=ø og å=å i variabelnavn, metoder ol.)	M				
6	Distribuert transaksjonshåndtering må unngås	M				

7	Sammensatte prosesser som består av flere atomære prosesser/steg må kunne kjøres separat. Atomære prosesser/steg må kunne startes separat. Dette gjelder asynkrone kall. Preferert løsning er asynkrone kall, jfr krav 11 E-1	M				
8	Ved lesing i databaser skal "nolock" og/eller medfølgende @Transactional (readOnly = true) benyttes så langt det er mulig.	M				
9	Oppslag i database skal bruke indekserte nøkler. I installasjonsbeskrivelse skal det beskrives forslag til indeksering av db felt (selv om DBA har ansvaret).	M				
B	Krav til Java utvikling	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Hver webapplikasjon må ha sin egen unike webapprootkey i web.xml for å unngå konflikter med andre webapplikasjoner	M				Eksempel: <pre><context-param> <param-name>webAppRootKey</param-name> <param-value>webapp.evurdering.indre.root</param-value> </context-param></pre>
2	Nye web-klienter skal baseres på HTML5, CSS/LESS og Javascript (preferert javascript.lib er ikke avklart)	M				
3	Alle stylesheet elementer skal legges i stylesheet filer for eksempel css skal legges i css-filer etc.	M				
4	Javascript og javascriptlogikk skal som hovedregel legges i egne javascript-filer, men der det er nødvendig kan kall til funksjoner i egne js-filer kan legges i html-filen feks. det å lytte på at lasting av siden er ferdig.	M				
5	Enhetstester skal skrives i form av testklasser for alle nye eller endrede Java metoder og Javascript metoder, jfr. hovedprinsipper i testreven systemutvikling.	M				
6	Koden skal dokumenteres på forklarende og forståelig norsk med vanlige java kommentarer og Javadoc. Javadoc skal benyttes for klasser og public metoder. Vanlige java kommentarer benyttes for private metoder og sentrale kodelinjer. Vanlige Java kommentarer er spesielt nødvendig der koden ikke er selvforklarende. En enkel metode som kun involverer retur av prosjektnummer trenger ingen vanlig kommentar om at prosjektnummer returneres hvis variablene er selvforklarende	M				
7	Leverandør må kunne dokumentere prefererte standarder og retningslinjer som den benytter for design og utvikling av web- og java-applikasjoner	M		X		
8	Automatiske enhetstester skal kjøres jevnlig for eksempel på byggeserver ved innsjekking av ny kode til kildecodesystemet for både master-branch og prosjekt-brancher. Utførte automatiske enhetstester skal dokumenteres i systemtestrapporten for eksempel i form av dekningsgrad av kildekoden og at eventuelle integrasjonstester som ikke kjøres ved hvert enkelt bygg er utført	M				
C	Generelle krav til web services (WS)	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse

1	Navne- og versjonerings-standard som skal benyttes ligger på Confluence: Navnestandard	M					
2	Tegnsett som skal benyttes er ISO10646/UTF-8 (ISO 8859-1 + 6 samiske tegn upper/lower case)	M					
3	Web service skal ivareta forretningslogikk for eget domene	M					
4	Web service skal ikke eksponere intern objektsmodell for domenet	M					
5	Web service skal legges på et medium nivå, ref. Forskningsrådets IT arkitektur dokument (link til dokumentet)	M					Forskningsrådets arkitekturdokument vil følge vedlagt ved anbudsforespørsler
D	Krav for egenutviklede web services (WS) for egenutviklede og integrerte systemer, unntatt web services for DVH	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	Integrasjon med andre applikasjoner forretningslag/systemer skal skje via web service-grensesnittet til den andre applikasjonen/systemet	M					
2	Konsumering av andre systemers data og integrasjon med andre systemers databaser skal skje via systemets web services	M					
3	Nye web service skal helst baseres på REST API og JSON datautveksling. SOAP kan benyttes i tilfeller hvor REST ikke dekker behovet eller er mindre egnet på grunn av for eksempel krav til sikkerhet. JAX-WS benyttes til å generere SOAP WS og JAX-RS til å generere REST WS.	M					
4	I tilfeller hvor synkrone web service kall feiler skal feilen spesifiseres i resultat, slik at kallende system enkelt kan finne feilen og presentere en informativ feilmelding til bruker. I slike tilfeller skal web servicen returnere feil i et eget exception response-objekt. Hensikten med dette er å tilrettelegge for en standardisert feilhåndtering slik at WS-konsument kan sjekke om et excetion response-objektet finnes, hvis objektet finnes kan exception tas tak i og viderebehandles / formidles. Hvis ikke slikt objekt finnes, kan det antas at retur er ok og ingen feil har intruffet	M					
E	Generelle krav til bruk av tjenestebuss for egenutviklede og integrerte systemer, unntatt web services for DVH	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	Tjenester skal settes opp og konsumeres asynkront. Unntak kun etter spesiell godkjenning fra IT-avdelingen.	M					
2	Asynkrone tjenester skal bruke tjenestebuss (Mule)	M					
3	Ved tjenester i form av typen broadcast skal en JMS-melding legges på tjenestebussens kø-system (ActiveMQ), interessenter abonnerer på hendelser. Applikasjonen utfører det som skal gjøres som et resultat av meldingen.	M					
4	IT-systemet som <u>tilbyr</u> en asynkron tjeneste er ansvarlig for å implementere logikk i Mule for å hente meldinger fra sin kø, og gjennomføre tjenestekall mot sin webservice-implementasjon. Se Asynkrone Tjenester	M					
5	Synkrone tjenester skal bruke Mule som integrasjonspunkt vha web service proxy. Se Synkrone Tjenester	M					

F	Krav for egenutviklede web services for Datavarehus (DVH)	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Web service for DVH skal være SOAP-basert	M				
2	Data skal avleveres på en flat form og tilpasset direkte til en rad i en tabell	M				
3	Web service skal ha en metode som returnerer nøkkel-ID på nye eller endrete forekomster. Nøkkel-ID'en benyttes igjen for oppslag i øvrige metoder. (Dette forutsetter at databaser har felt for endret dato som oppdateres.)	M				
4	For WS hvor det skal hentes et utvalg av data skal det kunne angis tidsperiode (fra dato og til dato) i request grensesnittet for eksempel alle prosjekter eller søknader for en gitt tidsperiode	M				
G	Krav til bruk av køer for egenutviklede og integrerte systemer, unntatt web services for DVH	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Meldinger mellom systemer/interaksjonspunkter skal legges på egne køer	M				
2	Når et ukjent antall systemer abonnerer på en gitt type hendelse skal avsendende system publisere en JMS-melding til en <i>topic</i> i Active MQ. For detaljer se Broadcast-base rte tjenester	M				
H	Krav til database design	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Ved opprettelse nye databaser skal Forskningsrådets navnestandard for databaser benyttes Navnestandard for databaser	M				
2	Leverandør skal anslå dimensjonering av database i form av beregninger av datamengde på ukentlig og årlig basis	M		X		
3	Nye sentrale databasetabeller skal ha felt for opprettet dato, opprettet av, endret dato og endret av for å sikre sporbarhet på sentrale data	M				
4	Alle nye tabeller skal ha konsistent navnebruk både på kolonner, attributter og nøkler samt PRE- og POST-FIX ihht Forskningsrådets begrepskatalog og generelle kodeverk (bruke samme ordlyd som tidligere krav)	M				
5	Nye tabell- og kolonnenavn skal ha medium lange, maks 32 tegn lange. De skal ha meningsfulle navn som er forståelig norsk, men ikke inneholde norske bokstaver, æøåÆØÅ, men benytte ae=æ, o=ø og a=å.	M				
6	Datavarehus (DVH) databasen skal være denormalisert (dvs stjernemodell og uten constraints)	M				

12 Ytelse og robusthet

A	Krav til kapasitet	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	<p>Systemet skal håndtere N aktive brukere samtidig og oppfylle krav om responstider (krav nedenfor). Dette skal kunne skje på samme tid som systemet utfører normale oppgaver.</p> <ul style="list-style-type: none"> N - Det er p.t. ca. 450 ansatte i Forskningsrådet. Det er størst bruk av systemene i ordinær arbeidstid (mandag - fredag kl 07:00 - 18:00) N - Det kan forventes opp til 2000 samtidige brukere på de eksterne nettsidene. Det er størst belastning like før søknadsfrister. 	M		X		<p>N vil variere avhengig av det er IT-systemer som utvikles for eksterne kunder eller interne brukere.</p> <p>N vil bli oppgitt i hver anbudsforespørsel</p>
2	<p>Systemet skal dimensjoneres slik at krav om responstider (krav nedenfor) er ivaretatt ved topp belastning og ytelsen på løsningen (responstid) skal være stabil og jevn ved økende antall brukere. (Dette skal dokumenteres via egne kapasitetstester). Kapasitetstester skal utføres for større leveranser og nye prosjekter. Leverandør skal i samarbeid med Forskningsrådet avklare hvilke områder som skal kapasitetstestes for hver gang. Leverandør skal dokumentere utførte kapasitetstester for utvalgte tilfeller. <i>Beskriv metode og mulighet.</i></p> <p><i>Alternativ kravtekst for standard systemer:</i></p> <p>Systemet skal dimensjoneres slik at krav om responstider (krav nedenfor) er ivaretatt ved topp belastning og ytelsen på Systemet (responstid) skal være stabil og jevn ved økende antall brukere. (Dette skal dokumenteres via egne kapasitetstester). Kapasitetstester skal utføres for større leveranser og nye prosjekter. Leverandør skal dokumentere utførte kapasitetstester for utvalgte tilfeller. <i>Beskriv metode og mulighet.</i></p>	M		X		
3	<p>Systemet skal ikke ha minnelekkasjer. (Dette må dokumenteres via lasttester på 48 - 72 t tester) Lasttester skal utføres for større leveranser og nye prosjekter. Leverandør skal i samarbeid med Forskningsrådet avklare hvilke områder som skal lasttestes for hver gang. Leverandør skal dokumentere utførte lasttester for utvalgte tilfeller. <i>Beskriv metode og mulighet.</i></p> <p><i>Alternativ kravtekst for standard systemer:</i></p> <p>Systemet skal ikke ha minnelekkasjer. (Dette må dokumenteres via lasttester på 48 - 72 t tester) Lasttester skal utføres for større leveranser og nye prosjekter. Leverandør skal dokumentere utførte lasttester for utvalgte tilfeller. <i>Beskriv metode og mulighet.</i></p>	M		X		
B	Krav til responstid	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	<p>Det er viktig at brukeren opplever rask respons og ikke behøver å vente på at data kommer frem i et skjermbilde. Responstid for oppdatering av skjermbilder skal være lavest mulig, som hovedregel skal den maksimalt være 2 sekunder. Hvis enkelt-funksjoner tar mer enn 2 sek. må dette dokumenteres, begrunnes samt oppgi gjennomsnittlig responstid ved lav, medium og høy systembelastning. Eksempel på slike funksjoner kan være dokumentgenerering, innhenting av store lister eller integrasjon med andre systemers tjenester.</p>	M				<p>Gjør et utvalg av bestemte skjermbilder som skal testes</p>
2	<p>Løsningen skal ha mulighet for å benytte standard testverktøy til automatisk ytelsestest og stresstesting. (Responstid ved lavt, middels og høyt antall brukere og belastning skal dokumenteres via ytelsestester og stresstester). <i>Beskriv mulighetene.</i></p> <p><i>Alternativ kravtekst for standard systemer:</i></p> <p>Responstid ved lavt, middels og høyt antall brukere og belastning skal dokumenteres via ytelsestester og stresstester.- <i>Beskriv muligheter</i></p>	M		X		
C	Krav til tilgjengelighet (og pålitelighet)	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	<p>Systemet, applikasjon og web service skal ikke stoppe, men skal være tilgjengelig selv om ett eller flere av integrerte systemer, tjenester og databaser ikke er tilgjengelige. Funksjoner som ikke er avhengig av integrerte systemer/tjenester skal kunne benyttes selv om integrerte systemer/tjenester ikke er tilgjengelige.</p> <p>Hensikten med dette kravet er at hvis omkringliggende og integrerte systemer blir utilgjengelige eller slutter å fungere som normalt, så skal et systems funksjonalitet som ikke har integrasjon mot slike systemer fungere som normalt. Dersom et system mister kontakt med sin database eller omkringliggende og integrerte systemer, så skal kontakten gjenopprettes når dette er mulig, uten at det er behov for en omstart av systemet.</p> <p>(Dette må dokumenteres via robusthetstester) <i>Beskriv metode og mulighet</i></p>	M		X		
2	<p>Operasjoner som feiler skal kunne restartes automatisk der det er mulig. Det må være lett å finne og restarte prosesser som må startes manuelt. Hvis en eller flere prosesser er utilgjengelige må disse kunne fortsette der det stoppet når de er tilgjengelige igjen uten at data går tapt.</p>	O				
3	<p>Løsningen skal kun være tilgjengelig internt på Forskningsrådets nettverk inkludert via VPN / Direct Access til enhver tid.</p>	M				<p>Unntatt for de eksterne kundeløsningene.</p>
4	<p>Autorisasjonsstyring av dataoverføring/datauttrekk</p> <p>Når det er funksjonelle krav til dataoverføring til annet format for eksempel XML eller .csv format til Excel så skal dataoverføringen styres av samme autorisasjonsmodell som tilgang til systemets andre brukergrensesnitt.</p>	M				
5	<p>"Ulovlige" karakterer/kontrolltegn skal ikke skape problemer i integrasjon og lagring. Det må utføres kontroll av data som legges inn og ulovlige tegn må fjernes.</p>	M				

6	Det skal ikke lagres blanke etter eller i begynnelsen av tekst/data. Kun en blank mellom tekst/data skal lagres. Dette gjelder spesielt nøkler og data som brukes i sammensatte nøkler, gjerne på tvers av moduler/systemer for eksempel brukernavn og aktivitetskode og kodeverkskoder. Dette kravet fravikes for tekstfelt der det er spesifisert funksjonelt at tekst skal kunne formateres dvs inneholde innrykk ol.	M					
D	Krav til skalerbarhet	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	Systemet skal være skalerbar både horisontalt og vertikalt slik at den håndterer økt antall brukere og økt datamengde. Beskriv hvilke tekniske og økonomiske konsekvenser skalering av Løsningen vil ha for Kunden.	M		X			
E	Krav til datautveksling	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	<u>E-post</u> All lagring av e-postadresser skal være korrekt i hht standarden RFC822. (Sending av e-post skal foregå via en egen tjeneste på tjenestebussen (p.t. Mule) der det er relevant.)	M					
2	<u>Filkopiering og filkonvertering</u> Dette skal foregå via en tjeneste for filkopiering på tjenestebussen. Tjenesten sjekker at operasjonen er vellykket.	M					P.t. er ikke denne tjenesten utviklet.
3	<u>Synkrone oppgaver</u> Ved synkrone oppgaver skal det gis en brukervennlig melding direkte til sluttbruker. Prosesser som feiler skal automatisk omstartes inntil X ganger. X skal kunne konfigureres. Det skal være ventetid mellom hvert forsøk som enkelt må kunne konfigureres og endres uten at IT-systemet må redployes. Hvis omstart ikke har lyktes etter X forsøk skal det sendes e-post til en konfigurert epostadresse. For asynkrone oppgaver henvises det til krav 12 E-4.	M					
4	<u>Asynkrone oppgaver</u> Ved asynkron utføring av oppgaver så skal køer brukes. Forsøk på å behandle meldinger på køer skal utføres X ganger. X skal kunne konfigureres. Det skal være ventetid mellom hvert forsøk som enkelt må kunne konfigureres og endres uten at IT-systemet må redployes. Dersom oppgaven ikke lar seg gjennomføre etter X forsøk så skal dette logges og varsel sende på e-post til en konfigurert epostadresse. Dette varselet skal inneholde nok informasjon til at mottager kan "ta nødvendig action" (se neste krav).	M					
F	Krav til sporbarhet	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	Utføring av sentrale funksjoner/oppgaver skal logges. Dette vil da være en form for logging av utført/kallet forretningslogikk. Naturlige tidspunkt for slik logging vil være ved oppretting/innsending, verifisering, tjenestekall, oppslag, etc.	M					
2	Det skal være logging når informasjon sendes over systemgrenser. For eksempel når data sendes til systemer som driftes eksternt, og med en gang de mottas av interne systemer.	M					
G	Krav til asynkrone oppgaver	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	Det skal foreligge dokumentasjon som viser bruken av køer (ref informasjonsflyt som en del av systemdokumentasjon), samt instruksjer/rutinebeskrivelser for hva som må gjøres dersom noe feiler.	M					Mal for dokumentasjon på Confluence.
H	Krav til bakgrunnsjobber og tjenester	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse	
1	Dersom det lages løsninger som utføres i bakgrunnen så skal kravene til feilmeldinger, sporbarhet og asynkrone oppgaver gjelde for disse også.	M					
2	Faste jobber skal automatiseres og dokumenteres.	M					

13 Integrasjon, IT-arkitektur og plattform

A	Krav	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Løsningen skal implementeres på Kundens infrastruktur slik den er beskrevet i "Teknisk beskrivelse av NFRs IT-systemer" og i tråd med øvrige tekniske krav i kvalitetskravene og retningslinjer for systemutvikling.	M		X		
2	Web sider skal fungere på netlesere ref. preferert plattform	M				

3	Leverandøren skal levere en detaljert løsningsbeskrivelse med figurer som gir oversikt over anbefalt teknisk arkitektur og driftsmiljø, samt angivelse av nødvendig antall servere, spesifikasjonskrav for servere og serverversjoner.	M				
4	Løsningen skal i størst mulig grad være modularisert og tjenesteorientert slik at de ulike delsystemene og tjenestene er uavhengige av hverandre og kan byttes ut dersom det skulle bli nødvendig grunnet for eksempel endringer i lovgivning eller organisasjon. For ytterligere beskrivelse av dette, se Forskningsrådets arkitekturprinsipper (link til dokumentet)	M				
5	Applikasjonen må kunne kjøres i flere instanser samtidig med en lastbalanser i front. Hensikten er bla å sikre tilgjengelighet	M		X		Leverandør må foreslå metode og løsning.
6	Løsningen skal kunne fungere med Windows klient operativsystem, ref. preferert plattform .	M				
7	Det skal ikke være krav om bruk av Microsoft klientprogramvare i moduler tilgjengeliggjort for eksterne brukere jfr. referansekatalogen for offentlige forvaltningsstandarder	M		X		Beskriv hvordan eksterne brukere (som ikke har en AD bruker hos Forskningsrådet) kan få tilgang til nødvendige deler av løsningen.
8	Hvis løsningen skal integreres med Microsoft Office produkter så skal dette gjøres med Microsoft Office 2010	M				
9	Hvis løsningen skal integreres med Microsoft Outlook så skal dette gjøres med Microsoft Outlook 2010 eller nyere	M				
10	Hvis løsningen skal integreres med Microsoft Exchange Server så skal dette gjøres med Microsoft Exchange Server 2010 eller nyere	M				
11	Applikasjonen skal kunne installeres på Windows 2008 eller nyere på virtuelle servere og være supportert på dette.	M				
12	Applikasjonen bør kunne kjøres fra Microsoft Terminal Server.	O				
13	Applikasjonen skal kunne benytte Microsoft SQL server 2008, 2012 eller nyere som database. Angi versjon i detaljert løsningsbeskrivelse.	M		X		
14	Systemet skal kommunisere over TCP/IP.	M				
15	ActiveMQ skal benyttes som køsystem for egenutviklede tjenester	M				
16	SOLR skal brukes som søkemotor internt i egenutviklede it-systemer	M				
17	Registre og registerdata skal gjenbrukes og ikke dupliseres på tvers av systemer/moduler, men kun ligge lagret i registersystemet som er ansvarlig for dataene. Andre moduler lagrer kun referanse som benyttes til å hente ut data fra registersystem. Hensikten med dette er at datasett skal ikke vedlikeholdes mer enn ett sted.	M				
18	Frittstående system som ikke skal integreres med andre IT-systemer ved Forskningsrådet, skal følge tekniske krav som gjelder i IT-avdelingen. (Dette kan være standardssystem som anskaffes eller system med lite antall brukere og ikke noen krav til oppetid.)	M				

14 Vedlikehold, drift og support

A	Krav til konfigurering og oppdatering av parametre	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referans
1	Miljøavhengige variabler som servernavn og portnummer ol. skal legges i en egen propertyfil for slike opplysninger. Dette for å oppnå at hvert konfigurasjonsparameter kun redigeres i en fil. Parametre som er like for ulike miljø skal legges i en properties-fil som kan benyttes for ulike miljø for eksempel test og produksjon. For flere detaljer se retningslinjer for systemutvikling.	M				
2	Alle konstanter som det kan tenkes at de kan endre seg over tid eller som kan ha ulike verdier skal trekkes ut i konfigurerbare egenskaper enten i form av property-filer eller databasetabeller slik at verdiene kan endres der. Dette gjelder for eksempel brukernavn, brukerid'er, passord, maks antall av noe, navn på filkataloger og filer, navn på servere, ip-adresser, etc	M				
3	Kravet er flyttet til dokumentasjon kap 17, 36					
4	All kommunikasjon mellom moduler/systemer skal sende med et brukernavn for logging og endringshåndtering. Der hvor operasjonen igangsettes av en innlogget bruker skal dennes brukernavn benyttes, der hvor operasjonen settes i gang av systemet skal egne systembrukere (hvert system/modul får sin systembruker) benyttes.	M				

5	Leverandøren må bidra til at oppsett, konfigurering og vedlikehold av servere og applikasjoner medfører lavest mulig risiko for sikkerhetsbrudd.	M					
B	Krav til installasjon/driftssetting	ITs krav	Prioritet	Utdypes	Oppfylles	Komment / Referans	
1	Leveranser skal være mest mulig automatisert og enkle å installere uten at det oppstår feil. Autodeploy-script må logge trinnene som utføres og hvis mulig gi en fornuftig feilmelding om noe feiler	M					
2	Alle leveranser må ha et unikt og stigende versjonsnummer	M					
3	Applikasjonskoden skal ligge separert fra applikasjonsserverens filer.	M					
4	Installasjoner skal scriptes og alle properties-filer skal parametriseres.	M					
5	Liquibase skal brukes til å holde orden på leveranseinnhold mht databaseendringer	M					
6	Leveransescripts for manuell opprettelse av databaseobjekter (tabeller, prosedyrer, indekser osv.) skal ikke referere til databasenavn (f.eks. navn på databaser i test/utviklingsmiljø). Dette for å forenkle opprettelse i forskjellige de miljøene.	M					
7	Leveransescripts for <u>manuell</u> opprettelse av databaseobjekter (tabeller, prosedyrer, indekser osv.) må inneholde drop- og create-statements sånn at de kan kjøres flere ganger. Rollback-script av endringene som kommer med leveransen	M					Kravet gjelder der man ikke benytter liquibase:
8	I leveransescripts for manuelle endringer av allerede opprettede databaseobjekter må det tas hensyn til at objektene allerede eksisterer, og at det kan være data i dem.	M					
9	Alt som skal gjøres i produksjonsmiljøet skal følge Forskningsrådets ITILs changeorder-prosess.	M					
C	Krav til feilmeldinger og feilhåndtering	ITs krav	Prioritet	Utdypes	Oppfylles	Komment / Referans	
1	Alle feilmeldinger som vises til sluttbruker skal presenteres i klartekst. Dersom koder eller forkortelser brukes så skal disse i tillegg forklares i klartekst. Brukernavn, dato og klokkeslett skal vises der det er mulig (brukere sender ofte skjermdumper til support, og dette vil lette arbeidet for alle parter).	M		X			
2	Løsningen skal tilby funksjonalitet som beskriver at noe har feilet, samt bør om mulig gi instruksjoner til sluttbruker om hvordan dette kan løses. Eksempel: hvis bruker forsøker å publisere et dokument, men dette feiler fordi bruker ikke har tilgang til å arkivere dokumentet til elektronisk arkiv, kan feilmelding være som følger: <i>"Publisering av dokument feilet pga manglende tilgang til arkiv. Kontakt systemansvarlig for elektronisk arkiv og be om å få tilgang til å lagre dokumentet. Deretter kan publisering gjøres på nytt"</i>	M		X			
3	For alle feil skal sammenheng hvor feil har oppstått logges sammen med selve feilen. I loggen skal det i tillegg til selve feilmeldingen angis en kontekst slik at det er mulig å utføre feilsøking og feilhåndtering. Dette skal være (så fremt mulig) informasjon som identifiserer: <ul style="list-style-type: none"> Når feilen oppsto (timestamp) Hvor feilen oppsto (Modul/Tjeneste/Database/Tabell/Entitet?) Hvem som utførte en oppgave/kalte en funksjon eller da feilen oppsto Hva ble "bearbeidet" da feilen oppsto (Prosjektnummer/Rapport/Søknadsnummer/ Annen nøkkelinformasjon) Alle feilmeldinger som vises til sluttbruker i brukergrensesnittet skal logges. Beskrivelsen ovenfor om logginhold gjelder også feilmeldinger som vises til sluttbruker i brukergrensesnittet. Feilmeldinger som vises til sluttbruker i brukergrensesnittet og feilmeldinger som skrives til logg må kunne "kobles sammen med en Id. Hvis hensiktsmessig kan feilmeldinger logges i en applikasjonslogg	M		X			
4	Alarmer om alvorlige feil bør gis støtte for å bli sendt på e-post, slik at man unngår å lete i loggfiler/databaser etter tilstrekkelig informasjon til å adressere feilen.	M		X			
5	Leverandøren er ansvarlig for å utarbeide, implementere og verifisere feilhåndtering	M					
6	Leverandøren skal utarbeide og implementere re-kjøring av operasjoner i feilsituasjon der det er hensiktsmessig	O					
7	Tekniske detaljer fra detaljerte feilmeldinger, debug informasjon, "stack traces" eller lignende skal ikke vises til sluttbruker i produksjon, slike opplysninger skal kun skrives til log. Visning av "stack traces" fra web-applikasjoner skal dog kunne slås av og på ved hjelp av en konfigureringsparameter.	M					
8	I nye løsninger bør det lages en egen egen knapp i feilmeldingen "send til IT-avd" som sender en mail til IT-7100 med feilmelding og teknisk tilgjengelig nøkkelinformasjon fra prosessrinnnet/dialogen/sesjonen om situasjonen samt tidspunkt	O					
D	Krav til logging og overvåking	ITs krav	Prioritet	Utdypes	Oppfylles	Komment / Referans	
1	Auditing/Sporing Med 'auditing' menes alle brukerinitierte CRUD-operasjoner som berører søknader, prosjekter, brukere skal være sporbare. Auditing skal skrives som en egen logg. Eksempler: operasjon=logg-inn operasjon=soknad-hent-fra-database-start	M		X			
2	For egenutviklede løsninger skal logger bygges opp slik at dataene er lett lesbare maskinelt med informative opplysninger som tidspunkt for feil, unik nøkkel for fagområdet el.og andre sentrale dataelementer. I tillegg skal tidsbruk for sentrale/viktige kall til mottatt retur logges som en del av logg-entriet. Eksempel på syntaks for logg-entry: soknadsnummer=<soknadsnummer>, prosjektnummer=<prosjektnummer>, brukerid=Bxx, PrsId=<skattefunnid>, operasjon=Oxx, <Melding>, tidsbruk=10 (i millisekunder o.s.v.	M		X			Det må vurderes i hvert enkelt tilfelle hva s er informativ opplysninge

3	<p>Format på loggmeldinger:</p> <p>Formatet på loggmeldingene skal være generisk slik at de består av et antall "feltnavn-verdi"-par (bortsett fra "loggnivå" og "timestamp"):</p> <p>felt1="verdi for felt1", felt2=42, felt3=konferansesenter ...</p> <p>Merk: Tekst som inneholder mellomrom må settes i frutter eller avsluttes med komma (dvs da kan ikke komma forekomme inne i teksten)</p> <p>Bakgrunn for oppdelinga i "navn-verdi"-par:</p> <p>Når loggfilene indekseres av Splunk, trekker Splunk automatisk ut felter fra meldingene når de er på "Navn=verdi"-formen. Det gjør at man kan søke i Splunk slik:</p> <p>Eksempelsøk1: Modul=eVurdering AND Operasjon=eVrd-SøknadMottatt</p> <p>Eksempelsøk2: soknadsnummer=455555</p> <p>Loggmeldingens utsende:</p> <pre><Loggnivå> [2010.05.03 22:17:45,135] Modul=<modul>, Klasse=<klasse>[, soknadsnummer=<soknadsnummer>][, prosjektnummer=<prosjektnummer>][, brukerdid=<brukerid>][, PrsId=<skattefunnid>][, operasjon=<Operasjon>][, Navn_i="<et-eller-annet>][, melding="<ei melding>"][, tidsbruk=<n>]</pre> <p>Loggmeldingsnivåer og felt som skal være med:</p> <pre><Loggnivå> ::= FATAL ERROR WARN INFO DEBUG ... <Modul> ::= eVurdering eAdmin Merkning Prosjektrapportering OrgReg MittNettsted SkatteFUNN inWeb Avtalemal ... <Klasse> ::= 'Klassa som skrev meldinga' (for eksempel EsoknadServertjenester.getSoknadInfo) <Operasjon> ::= soknad-lagre-slutt eAdm-SoknadRegistrert eAdm-SoknadMottatt WS-SakOpprettet FRS-prosjektOpprettet ...</pre> <p>NB! <Operasjon> må være "kort og konsis", og uten mellomrom i teksten</p> <p>Tidsbruk, for eksempel: 31 (i millisekunder)</p> <p>Tidsbruk skal logges for alle operasjoner over integrasjonspunkter og operasjoner som man forventer kan ta noe tid, for eksempel:</p> <ul style="list-style-type: none"> - databaseoperasjoner - kall til webservicer - kall til andre systemer - ... <p>Felt-navnstandard når feltet er med i loggmeldingen:</p> <pre>feilmelding eksempel: "Brukernavn er ugyldig" prosjektnummer soknadsnummer eksempel: 542160 (dvs søknadsnummeret skal IKKE prefikses med 'ES') brukerid eksempel: baat bruker eksempel: "Bård Tørustad", torustad2011@rcn.no prsid (gjelder SkatteFUNN)</pre> <p>Feltnavn kan finnes på etter behov:</p> <pre><Navn_i> ::= "navn-verdi"-par</pre> <p>Eksempler:</p> <pre>Melding='tekst etter ønske' Adresse='Kongens gate 42' Stilling='Konsulent med opprykk'</pre> <p>Når et felt i en gitt modul vanligvis har verdi, skal den angis som 'null' når den ikke har verdi (for eksempel: innsendingsfrist=null)</p> <p>Eksempel på loggmelding fra Mittnettsted:</p> <pre>INFO [06.01.2015 10:47:42] message.LOGGER - SoknadEJB.lagreSoknad bruker=terje.finstad@ntnu.no, soknadsnummer=542160, innsendingsfrist=null, prosjektnummer=null, operasjon=soknad-lagre-slutt, tidsbruk=31</pre>	M		X			
4	Ved feilsøking skal det være mulig å aktivere og deaktivere logging og loggnivå for utvalgte deler av systemet uten restart av systemet	M		X			
5	Det skal leveres overvåkingsprober (for eksempel url) til å teste om server og tjeneste/service er tilgjengelig	M					
6	Ved leveranse må Leverandøren fremlegge forslag til hvilke viktige logg-entries som skal overvåkes og kunne settes alarm på	M					
E	Krav til driftsstøtte	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referans	
1	Administrasjonskonsollet ProssessAdminKonsoll (PAK) skal brukes til å administrere eSak applikasjoner og tjenester. Leverandøren skal bidra til at PAK kan brukes som et driftsadministrasjonsgrensesnitt mot alle eSak applikasjoner og tjenester.	M					
2	Leverandøren skal utarbeide en oversikt over overvåkningspunkter for løsningen som kan legges inn i driftsadministrasjonsgrensesnittet (PAK)	M					
3	Leverandøren skal utarbeide hensiktsmessige helsesjekker for løsningen.	M					
4	Leverandøren skal utarbeide hensiktsmessige diagnostester for løsningen.	M					
5	Leverandør skal ved migrering av data benytte systemets bruker og ikke en personlig bruker i felt som "sist endret av" og i logger.	M					
6	Leverandør skal bidra til at HTTP TRACE skal være deaktivert på web servere i produksjon. Leverandør er ansvarlig for å legge dette inn i installasjonsbeskrivelsen	M					

15 Sikkerhet

A	Krav til autentisering	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Windows Active Directory (AD) skal benyttes som brukerkatalog for autentisering ved oppstart av applikasjoner i indre sone.	M				
2	Applikasjoner i ytre sone skal benytte Forskningsrådets brukerkatalog og ikke db til autentisering. pt benyttes eDir.	M				
3	Løsningen skal støtte Single Sign On (SSO). <i>Beskriv løsning.</i>	M		X		
4	Det skal ikke være mulig fra en klient å hente ut en liste med/informasjon om andre brukere så fremt dette ikke er en spesifisert del av løsningen (ref OWASP)	M				
5	Fullt navn skal presenteres i brukerdialogen, ikke påloggingsid	M				
6	Autentisering og autorisasjon skal ligge på server-siden og ikke på klient-siden	M				
7	Det skal benyttes et eget godkjent tegnsett for innloggingssider. Godkjent tegnsett er ISO10646/UTF-8	M				
B	Krav til autorisasjon	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Brukertilganger til og i applikasjoner skal kunne styres av systemforvaltere hos Kunden.	M				
2	Brukertyper / roller skal implementeres i AD	M				
3	Brukerne skal gis tilgang til ulike faglige områder som tilordnes via en eller flere av følgende brukergrupper. <ul style="list-style-type: none"> • Hele Forskningsrådet • En bestemt divisjon • En bestemt avdeling • En betemt brukergruppe • En bestemt bruker • Et program • En utlysning • En søknad 	O				Må vurderes om kravet er relevant for det gitte IT-systemet
4	Det finnes følgende brukertyper <ul style="list-style-type: none"> • Systemadministratorer (Systemeier for applikasjon) • Saksbehandlere med tilgang til alle objekter innenfor et gitt område • Lesebrukere 	O				Systemadministrator vil kun være interne brukere. Lesebrukere og saksbehandlere kan i gitte tilfeller være eksterne brukere.
5	Systembrukere skal ha lavest mulig nødvendige tilgangsnivå. Eksempel fra applikasjon til applikasjon og administratorkontoen (sa) skal aldri benyttes av web-applikasjonen ved lesing fra databasen.	M				
6	Brukere skal ha lavest mulig mulige tilgangsnivå. (Need to know prinsippet)	M				
C	Krav til sikkerhet for egenutviklede systemer og tjenester	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	All programmering inkl. Javakode skal følge beste praksis med hensyn til informasjonssikkerhet og for sikker programmering uavhengig om programmeringsspråket heter C#, PHP, Java, HTML oa. Kravene er nærmere beskrevet på følgende web sider. https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide <i>Utdypes</i>	M		X		Leverandøren må i besvarelsen si hvordan dette følges opp og hvilke rutiner de har
2	Forskningsrådets webapplikasjoner og web services skal ikke ha sårbarheter som er beskrevet i OWASP Top 10. (https://www.owasp.org/index.php/TopTen). Det skal ikke være mulig å utføre Injections (for eksempel sql-injection) (A1), Cross-Site Scripting (XSS) (A3), Cross-Site request Forgery (CSRF) (A8), Reflected XSS eller Dom-basert XSS fra input-felter. Sesjonshåndteringen må være slik at man unngår "Broken Authentication" (A2), "Insecure Direct Object references" (A4), "Security Misconfiguration" (A5), "Sensitive Data Exposure" (A6), "Missing Function Level Access Control" (A7), "Using Components with Known Vulnerabilities" (A9) og "Unvalidated Redirects and Forwards" (A10) samt ClickJacking må unngås. Leveranseansvarlig leverandør er ansvarlig for å utføre sikkerhetstester av leveransen.	M				
3	All input som kommer inn via inputfelt i URL, web sider, webapplikasjoner og i request til web services skal ha input-validering med hensyn til lovlige tegn,. Hvilke tegn som er lovlig i inputfelt må spesifiseres i funksjonelle krav. Hensikten med dette kravet er å gjøre applikasjonen sikker og robust (ref kvalitetskrav 15, C-1).	M				
4	Nye Web applikasjoner skal bruke standard sikkerhetsrammeverk som for eksempel OWASP rammeverk og Spring WebSecurity ol. Sikkerhetsrammeverket skal godkjennes av IT avdelingen før det tas i bruk.	M		X		(Dette må brukes i nye utviklingsprosjekt)

5	Det skal gjøres sikker vasking av ALLE inputfelt og alle andre felt i databasen eller adressefelt som hentes/benyttes. Dersom en verdi skal leses/sendes videre for behandling så skal den vaskes slik at vi er sikre på at det ikke sendes inn uønsket data/kode. Dette innebærer at felt som bruker ikke kan endre, men som vises i webGUI også skal vaskes da disse ofte kan endres via andre former for post enn i webGUI. Egne rutiner for vasking av URL som inneholder ID, kode, annet som referanseverdi som kan endres/misbrukes må lages da disse ofte er unike mht antall tegn som f.eks. representerer sesjonsID osv. (om verdien er for lang, for kort har feil tegnsett osv så skal den forkastes).	M				
6	Det skal kun benyttes parameteriserte SQL spørringer (for å unngå SQL injection)	M				
7	iFrames skal ikke benyttes verken i nye moduler eller nye applikasjoner. Der iFrames allerede finnes, men ikke kan tas bort umiddelbart skal applikasjonen ha med "X-Frame-Options"-headeren i responsen fra server. "DENY" skal brukes om man ønsker å forhindre all innramming eller "SAMEORIGIN" for å tillate innramming bare fra nettsider som har samme domene som responsen. Alternativt må det spesifiseres nøyaktig hvilken kilde som kan bli innrammet ved å benytte seg av "ALLOWFROM uri". (blant annet for å unngå ClickJacking)	M				
8	Det skal brukes referanser til objekter og ikke databaseID på objektet som er knyttet til en spesifikk bruker eller sesjonen, ref. retningslinjer for Java systemutvikling, for flere detaljer se retningslinjer for systemutvikling VI-9	M				
9	Skjema-ID (på mitt Nettsted) må genereres og sendes fra serveren for hver gang. Serveren må sjekke at ID kommer fra serverene og ikke fra brukeren. ID-genereringsmønsteret må være tilfeldig slik at det ikke er lett å gjette algoritmen/mønsteret.	M				
10	Automatiske sikkerhetstester/scanning skal utføres og dokumenteres for hver leveranse	M				
D	Øvrige krav til sikkerhet	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Nettsider som tilbyr innlogging/sending av brukerdata skal kryptere disse	M				
2	Alle nettsider skal være kryptert, dvs det skal ikke være mulig å besøke noen sider med bruk av HTTP:	M				
3	HTTP data skal ikke vises på HTTPS sites.	M				
4	Det skal være umulig å manipulere nettstedet på en slik måte at det kan endres fra en side med kryptering til å få opp samme side ukryptert. Ukryptert trafikk skal ikke være mulig mot hele/deler av nettstedet som krever kryptering.	M				
5	Secure-flag og HttpOnly-flag skal settes på sesjons-cookiene i alle webtjenester.	M				
6	AutocompleteOff må være satt for å unngå at passord lagres i browser	M				
7	Directory browsing på system-diskene til tjenesten skal være avslått. (kravet gjelder ikke diskene som er tilgjengelig lokalt)	M				
8	Versjonsnummer på rammeverk og serverprogramvare (f.eks Glassfish, Apache o.l.) skal ikke være synlig for sluttbrukeren	M				
9	Sikring av web services bør gjøres med kryptering der det er mulig (transportsikring)	O				
10	Web servicene skal minimum sikres med brukernavn og passord (kryptert). Det skal ikke skal være mulig å kjøre en WS direkte utenfor applikasjonen uten autorisering (mot AD eller eDir). Serverne/applikasjonen som tar i mot en forespørsel skal sjekke at avsender er godkjent til å gjøre spørringen.	M				
11	Alle appservere/webservere som tilbyr kryptert kommunikasjon skal gjøre dette via TLS, og da TLS 1.1 og TLS 1.2.SSL 1.0, SSL 2.0 og SSL 3.0 skal ikke benyttes. Svake Chiper som f.eks. 40, 56 og 112 skal ikke benyttes og skal skrus av på serveren og i applikasjonen. Chiper på minimum 128 eller 256 skal benyttes.	M				
12	Brukernavn og passord skal ikke hard-kodes					
13	Passord skal ikke lagres i applikasjoner.					
14	Det skal stilles krav til passord som brukere kan velge å benytte. Passord bør være 10 tegn eller mer, og et minimumskrav er at ett passord skal inneholde både tall og bokstaver (både store og små).	M				
15	Systembrukeres passord skal være kryptert og ikke være representert i klartekst i kode eller konfigurasjonstabeller	M				
16	Dersom brukerpasord lagres så skal dette krypteres (hashes og saltes) før det lagres med en enveisalgoritme som betyr at det ikke er mulig å reversere det som ligger lagret for å få frem passord. Mer om å gjøre dette rett finnes her: http://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/	M				

17	<p>Forskningsrådet forutsetter at leverandørens utviklingsgruppe har utviklere som har et minstenivå av kunnskaper om sikker koding. Dette for å unngå gjengangere som Cross-site scripting (XSS) og SQL injections. Disse utviklere skal minimum ha kunnskap/kjennskap om følgende:</p> <ol style="list-style-type: none"> 1. Input Validation 2. Output Encoding 3. Authentication and Password Management (includes secure handling of credentials by external services/scripts) 4. Session Management 5. Access Control 6. Cryptographic Practices 7. Error Handling and Logging 8. Data Protection 9. Communication Security 10. System Configuration 11. Database Security 12. File Management 13. Memory Management 14. General Coding Practices <p>Mer på: https://security.berkeley.edu/content/application-software-security-guidelines</p> <p>OWASP Secure Coding Practices - Quick Reference Guide i PDF og DOC: https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide</p> <p><i>Alternativ kravtekst for standard systemer: (første del)</i></p> <p>Kunden forutsetter at Leverandørens IT-system tilfredsstiller sikker koding. Dette for å unngå gjengangere som Cross-site scripting (XSS) og SQL injections. Dvs at følgende ikke kan forekomme:</p>	M		X		
----	--	---	--	---	--	--

16 Tilganger

A	Krav til tilganger	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Systemet skal ha innebygget tilgangskontroll/autorisasjon av enkelt brukere og brukergrupper. Brukertilgangen må også være differensiert og gi ulike tilgang til systemets funksjoner (les, skriv og slett funksjon), ref kvalitetskrav kap 15, B	M				
2	For alle systemer skal det implementeres superbruker-tilgang (potensielt flere autorisasjonsnivåer) som gir superbrukere tilgang til alle funksjoner samt gir mulighet for å tilrettelegge for spesialfunksjoner/utvidede rettigheter for superbruker.	M				
3	Autorisasjonskontroll skal gjøres på nytt for hvert system. Dette gjelder både for bruk av systemet gjennom systemets brukergrensesnitt, og for bruk av datauttrekk fra systemet samt tilganger igjennom andre systemer.	M				
B	Krav til integritet	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	Det skal finnes en oversikt over hvilket eller hvilke tidsrom en brukerident har vært aktiv. Hensikten med dette er at det skal være sporbart når tid en bruker har vært pålogget et system.	O				
2	Funksjon for permanent sletting av informasjon skal kun være tilgjengelig for administrator, untatt innhold i redigerbare tekstfelt som skal kunne slettes av brukere med tilgang til skrive funksjon	M				

17 Dokumentasjon

A	Krav	ITs krav	Prioritet	Utdypes	Oppfylles	Kommentar / Referanse
1	All dokumentasjon skal være på norsk	M				
2	Dokumentasjonen kan utformes på Confluence. I tillegg skal all dokumentasjon overleveres elektronisk i pdf-format. Hvis Confluence ikke benyttes skal dokumentasjonen være i redigerbar form.	M				
3	Systemets standard systemdokumentasjon skal medfølge der IT-systemet er egenutviklet.	M				

4	Leveransedokument skal overleveres før installasjon i akseptansetestmiljø.	M				
5	Leveransedokument skal bl.a. inneholde beskrivelse av endringer i properties-fil og en detaljert installasjonsbeskrivelse som på forhånd er kvalitetstestet i testmiljøet. Denne skal være så utfyllende at det er mulig for driftspersonell i Forskningsrådet å kunne foreta en full installasjon uten leverandørens tilstedeværelse eller bistand.	M				
6	Installasjonsbeskrivelsen skal være spesifikk for hver enkelt leveranse/ending.	M				
7	Installasjonsbeskrivelsen skal inneholde det som er nødvendig for å gjennomføre installasjonen, hverken mer eller mindre.	M				
8	Installasjonsbeskrivelse skal inneholde detaljert og punktvis oversikt over nøyaktig hva som må gjøres og i hvilken rekkefølge, for å installere denne leveransen. For eksempel hvilke scripts skal kjøres i hvilke databaser, hvilke filer som skal kopieres hvor, hva skal deployes på hvilken server, osv.	M				
9	Installasjonsbeskrivelsen skal inkludere oppretting av database(r) med innlegging av tilhørende grunnlagsdata, eventuelle tilpasninger av omliggende systemer (tilgangsstyring, epostserver, etc)).	M				
10	Installasjonsbeskrivelsen skal kunne videresendes uten endringer til ekstern driftsleverandør, som skal kunne gjøre installasjonen på egen hånd.	M				
11	Det skal medfølge driftsdokumentasjon som beskriver alle aspekter som må håndteres for å kunne drive systemet på en sikker og effektiv måte. Dette inkl. bl.a. en oversikt over type backup-rutiner, periodiske jobber som skal utføres, start/stopp rutiner, hva som bør overvåkes, kjente feil og mangler osv. Denne kan være som separat dokumentasjon eller inngå som en del av systemdokumentasjon.	M				
12	Systemdokumentasjonen skal beskrive alle aspekter som man må forstå for å kunne forvalte og drifte systemet på en sikker og effektiv måte.	M				
13	Eventuelle systemtilpasninger i for eksempel prosesser og teknisk arkitektur skal være dokumentert i systemdokumentasjonen	M				
14	Norges forskningsråds standardmal for systemdokumentasjon benyttes. Denne oversendes ved kontraktsinngåelse. (link til Confluence side Generell systemdokumentasjonsmal for IT-prosjekter)	M				
15	Det skal overleveres dokumentasjon på hvilke brukergrupper som finnes i løsningen og hva de ulike rollene kan gjøre i systemet.	O				Hvis det finnes flere roller er kravet Mandatory
16	Det skal overleveres funksjonell dokumentasjonen som dekker alle områder i systemet og som viser hvordan løsningen skal brukes	M				
17	All dokumentasjon som leveres fra leverandøren skal godkjennes av Forskningsrådet	M				
18	Funksjonell dokumentasjonen skal finnes tilgjengelig på web-format slik at den kan publiseres på Forskningsrådets intranett.	M				
19	Forskningsrådet kan vederlagsfritt videreutvikle, tilpasse, kopiere og distribuere dokumentasjonen for løsningen ut fra egne behov.	M				
20	Løsningen skal ha hjelpfunksjon som gir mulighet både for å slå opp på emner og/eller kontekstavhengige (context sensitive) hjelpetekster dvs hjelp ut fra hvilken funksjon, skjerm bilde og felt brukeren befinner seg i.	M				
21	Leverandøren bes å beskrive løsningens hjelpfunksjon nærmere	M		X		
22	Leverandøren bes å beskrive hvilke muligheter virksomheten har for å supplere og evt. definere egne hjelpetekster og elektroniske brukerveiledningstekster.	M		X		
23	Forskningsrådet må kunne legge inn egne hjelpetekster.	M				
24	Egne hjelpetekster må overleve versjonsoppdateringer.	M				
25	Løsningens hjelpfunksjon må støtte mulighet flerspråklige hjelpetekster for eksterne brukere	M				
26	Det må finnes hjelpfunksjoner som gir brukerne informasjon om hvordan de enkelte felt i skjemaet skal fylles ut. Nivå av hjelpfunksjon må spesifiseres for hvert system.	M				
27	Ved nye releaser, skal alle endringer være dokumentert. For eksempel så skal funksjonelle endringer beskrives i brukerdokumentasjonen, prosessendringer, arkitekturendringer og systemendringer skal beskrives i systemdokumentasjonen.	M				
28	Ved leveranse av nye versjoner, skal oppdatert dokumentasjon overleveres.	M				

29	Manuelle testscript skal legges på Confluence på en subside under hvert system/modul som nås via systemoversikten (IT-Systemoversikt). Automatiske testscript kan legges i bygge- og testsystem som benyttes for eksempel Hudson	M				
30	Leverandøren er ansvarlig for å oppdatere testscript i Confluence ved endring av funksjon	M				
31	Forskningsrådet står fritt til å endre/tilpasse dokumentasjonen etter installasjonen.	M				
32	Nye prosesser skal spesifiseres og dokumenteres, eksisterende skal oppdateres i Enterprise Architect (EA). Tekstlig beskrivelse skal sammen med for eksempel UseCase diagrammer være en del av systemdokumentasjonen.	M				
33	Enterprise Architect skal benyttes til modellering og Kunden skal ha tilgang til EA-modellen(e) i Enterprise Architect.	M				
34	Web Services skal dokumenteres på en egen Confluence-side på standard form i henhold til Forskningsrådets standard mal. Tjenestetilbyder/-leverandør/-utvikler har ansvar for dette og forvaltningsteamet har overordnet ansvar for oppfølging av dette. <ul style="list-style-type: none"> • Det lages underområder for hvert enkelt IT-system/IT-modul som den enkelte leverandør skal oppdatere • Wsdl skal vise til systemtest-/akseptansetest-miljø • Tjenestene skal ha følgende informasjon: Navn på tjeneste, tjenesteleverandør, tjeneste-wsdl, kort beskrivelse, konsument(er), innført i versjon (it-system), målsystem 	M				
35	Jira benyttes til feilhåndtering mellom Kunden og Leverandøren. Alle avklarings spørsmål skal inn i Jira, og valgte løsninger/avklaringer skal dokumenteres i systemdokumentasjonen. Avklaringer som er dokumentert i møtereferat skal linkes inn fra Confluence til JIRA og avklaringer i epost skal legges inn i Confluence eller jira	M				
36	Innføring av nye tabeller, tabell endringer og databasescript i forbindelse med leveranser skal dokumenteres på Confluence	M				
37	Testscript skal så langt det er mulig bygges opp av små atomære tester som kan gjenbrukes i ulike leveranser hvor det leveres endringer innen samme funksjon	M				

18 Juridiske krav

A	Krav	ITs krav	Prioritet	Utdypes	Oppfylles	Kor / Re
1	<p>Formelle krav i henhold til regelverk og lover skal oppfylles. Eksempler på aktuelle lover og regelverk er personopplysningsloven, arkivloven, forvaltningsloven og offentlighetsloven.</p> <p>Forskningsrådet har ansvaret for at lover overholdes i spesifikasjoner og leverandør har ansvar for at lover overholdes i koden, for eksempel at personnummer ikke er tilgjengelig i browser ("view-source"/F12) når det er spesifisert at personnummer ikke skal vises eller skal presenteres med *****</p> <p><i>Tilleggstekst for standard systemer som driftes eksternt. (på slutten)</i></p> <p>Leverandøren må beskrive i tilbudet hvordan systemet er sikret for å ivareta konfidensialitet, integritet og tilgjengelighet, jf. personopplysningslova § 13, jf. forskrift til personopplysningslova kap. 2</p> <p>Forskningsrådet er eier av personopplysningene i systemet, og leverandøren blir databehandlarer vår for de aktuelle opplysningene. Databehandlaravtale må inngås for systemer som driftes eksternt og som behandler og lagrer personopplysninger.</p> <p><i>Krav til sky-løsninger og eksternt drift</i></p> <p>Ved opphør av avtale med eksternt driftsleverandør, skal leverandøren overføre personopplysningene og andre data i systemets database til Forskningsrådet i henhold til nærmere anvisninger fra Forskningsrådet</p>	M				
2	<p>Der Løsningen kan anses som et forsystem til et økonomisystem skal SSØ sine krav til økonomisystemer følges.</p> <p>Kravene finner man konkretisert i "Funksjonell kravspesifikasjon for statlige økonomisystem". Denne er forankret i "Reglement for økonomistyring i staten" og tilhørende "Bestemmelser om økonomistyring". http://www.regjeringen.no/nb/dep/fin/tema/Statlig_ekonomistyring/Reglement-for-okonomistyring-i-staten.html?id=438887</p>	M				
3	<p>Kunden får full eiendoms- og disposisjonsrett til resultatet av arbeid utført for Kunden, herunder eksklusiv opphavsrett i den grad resultatet har opphavsrettslig vern.</p> <p>Metodikk, rutiner, kompetanse mv. som Leverandøren bringer inn i oppdraget og evt. videreutvikler gjennom utførelse av oppdraget, forblir Leverandørens eiendom.</p>	M				