DIGITALISERINGSSTYRELSEN

Krav til kontrakt- og leverandørstyring for samfundskritiske it-systemer

Januar 2023

2023

Katalog over krav til kontrakt- og leverandørstyring for myndigheder ved outsourcing af samfundskritiske it-systemer

For at sætte større fokus på myndigheders ansvar ved outsourcing af samfundskritiske it-systemer bliver der nu stillet krav til deres kontrakt- og leverandørstyring. Kravene udspringer af initiativ 1.2. fra den Nationale Strategi for Cyber- og Informationssikkerhed 2022-2024.

Målgruppen for kataloget er myndigheder, der:

i. Er ansvarlige for samfundskritiske it-systemer og
ii. Outsourcer driften af disse it-systemer.

Vurderingen af it-systemers kritikalitet skal foretages af myndigheden selv, og der findes definitioner på samfundskritiske it-systemer i "Vejledning til model for porteføljestyring af statslige it-systemer" (se digst.dk), som myndigheden kan benytte i sin vurdering.

Kravene i kataloget retter sig mod samfundskritiske it-systemer, hvor opgaven med drift af it-systemet er outsourcet til en ekstern leverandør. Kravene er opdelt i tre temaer:

1. Krav til kontraktstyring
2. Krav til organisering
3. Krav til leverandørstyring

Formål
Outsourcing af it-drift stiller både krav til leverandør og kunde. Myndigheden og leverandøren skal have et godt og professionelt samarbejde, hvor rollerne er kendte og fordelt mellem dem. Myndigheden skal bemande og styre arbejdet med it-systemet på en måde, som gør effektiv beslutningstagen og kontrolførelse med leverandøren muligt, samt rettidigt opfølgning på indberetninger og udbedringer af fejl eller mangler.

En forudsætning for god leverandørstyring er god kontraktstyring. Dette handler blandt andet om overblik over leverandører og kontrakternes livscyklus og dermed rettidighed i myndighedens tiltag, så eksempelvis genudbud bliver planlagt rettidigt. Derudover handler det om adgang til de dokumenter og oplysninger, som leverandøren udarbejder eller stiller til rådighed for myndigheden til at føre bedst mulig kontrol med leverancen og sikkerheden i det samfundskritiske it-system.

Formålet med kravene er, at myndigheden indretter sig på en sådan måde, at den er rustet til systematisk kontrakt- og leverandørstyring af de til enhver tid eksisterende kontrakter for samfundskritiske it-systemer for derigennem at bidrage til forsyningssikkerheden for samfundskritiske ydelser.

Implementering hos myndigheden
Det er myndighedens eget ansvar at sikre, at kravene implementeres, herunder at der indføjes relevante bestemmelser i myndighedens kontrakter, hvis dette er nødvendigt for at implementere kravene.

Myndigheden skal implementere kravene hurtigst muligt, dog senest ved udgangen af 2023.

For så vidt angår *eksisterende* kontrakter om outsourcing af samfundskritiske it-systemer skal myndigheden implementere nedenstående krav hurtigst muligt, dog senest ved udgangen af 2023 for så vidt, det er muligt. "For så vidt det er muligt" betyder, at nogle af de nedenstående krav kan forudsætte kontraktuelle beføjelser, som ikke nødvendigvis fremgår af eksisterende kontrakter med leverandører, og det kan derfor være vanskeligt for myndigheden at efterleve kravene uden ændringer af kontrakten. Dog kan flere af kravene implementeres i myndigheden uafhængig af kontrakten og dermed uden leverandørens medvirken, fx implementering af faste processer for leverandørstyring.

Kravenes opbygning
I nedenstående tabel er de krav oplistet, som myndigheder med ansvar for outsourcede samfundskritiske it-systemer skal følge.

1. Krav til kontraktstyring			
Område	**Formål**	**Krav**	**Operationalisering**

Figur 1: Sådan fremgår kravene

Yderst til venstre fremgår det, hvilket område kravet vedrører. Derefter følger en kolonne med formålet med kravet, og dernæst en beskrivelse af selve kravet. Yderst til højre er der forslag til, hvor myndigheden kan søge inspiration til efterlevelse af kravet.

Til hjælp for operationaliseringen af de enkelte krav er der udarbejdet et appendiks.

Sammenhæng til andre myndighedskrav og vejledninger
Kravene i tabellen vedrører samfundskritiske it-systemer, hvor opgaven med drift af it-systemet er outsourcet til en ekstern leverandør. For anbefalinger vedrørende

planlægning, udvælgelse af leverandør, udvælgelse af sikkerhedskrav og afslutning af samarbejdet med leverandøren se "Vejledning om cybersikkerhed i leverandørforhold" på sikkerdigital.dk.

Som led i den Nationale Strategi for Cyber- og Informationssikkerhed 2018-2021 blev der udarbejdet et "Katalog over kontraktbestemmelser for samfundskritiske it-systemer", som myndigheder skal følge ved indgåelse af nye kontrakter for samfundskritiske it-systemer. Kataloget kan findes på sikkerdigital.dk.

Med den Nationale Strategi for Cyber- og Informationssikkerhed 2022-2024 er myndigheder desuden forpligtet til at overveje inddragelse af CFCS i forbindelse med udarbejdelse af sikkerhedskrav ved indkøb og udbud af samfundskritiske it-systemer.

1. Krav til kontraktstyring			
Område	**Formål**	**Krav**	**Operationalisering**
1.1 Kontraktbibliotek	Formålet med et kontraktbibliotek er, at myndigheden til enhver tid har overblik over alle relevante kontraktdokumenter, herunder kontrakternes stamdata. Kontraktbiblioteket bidrager til at sikre, at myndigheden rettidigt igangsætter aktiviteter såsom transition ind/ud og genudbud.	Myndigheden skal etablere og vedligeholde et kontraktbibliotek til opbevaring af kontraktdokumenter vedrørende de samfundskritiske it-systemer. Kontraktbiblioteket skal som minimum indeholde stamdata på aftalen, selve aftalen samt tillæg og ændringer hertil. Myndigheden skal sikre, at dokumenter og oplysninger i kontraktbiblioteket til enhver tid er opdaterede.	I praksis kan et kontraktbibliotek antage mange former, og det er op til myndigheden selv at vælge det, der passer bedst. På Digitaliseringsstyrelsens hjemmeside kan myndigheden finde en informationsfolder om kontraktstyring, samt en udgave af et kontraktbibliotek, som frit kan benyttes. Se mere på https://digst.dk/styring/systemstyring/dokumenter-vejledning-og-vaerktoejer/

1. Krav til kontraktstyring			
1.2 Dokumentation	Formålet med dokumentation er at sikre myndigheden adgang til alle relevante dokumenter og oplysninger om det samfundskritiske it-system ved behov. Adgang til relevante dokumenter og oplysninger er en forudsætning for at kunne leverandørstyre.	Myndigheden skal sikre, at der er udarbejdet den fornødne dokumentation vedrørende leverancen og samarbejdet med leverandøren. Myndigheden skal opbevare alle relevante dokumenter og oplysninger vedrørende leverancen og samarbejdet med leverandøren i et tilgængeligt format.	Myndigheden har allerede adgang til et journaliseringssystem, som kan anvendes. Her kan myndigheden opbygge en systematik i opbevaringen og navngivningen af dokumenter og oplysninger, så de kan genfindes. Relevante dokumenter og oplysninger omfatter fx møde-referater, risikovurderinger, revisionserklæringer og rapporter fra leverandøren.

2. Krav til organisering			
Område	**Formål**	**Krav**	**Operationalisering**
2.1 Roller og ansvar	Formålet med at beskrive og fordele roller og ansvar i myndigheden er at sikre, at der tages ansvar og er ejerskab for alle de enkeltstående opgaver knyttet til kontrakt- og leverandørstyring.	Myndigheden skal etablere en intern organisation egnet til kontrakt- og leverandørstyring, herunder definere og fordele roller og ansvar relateret til kontrakt- og leverandørstyring. Denne organisering skal dokumenteres og ledelsesgodkendes.	Myndigheden kan søge inspiration til etableringen af en egnet organisation og hvilke roller, der er nødvendige på sikkerdigital.dk, i ISO 27001 og i vejledningen "Cybersikkerhed i leverandørforhold". Se mere på https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/roller-og-ansvar Opgaverne kan fordeles blandt de valgte roller efter den såkaldte RACI-model, som der kan læses mere om i rejsefortællingen, som kan findes under leverandørstyring her https://sikkerdigital.dk/myndighed/vejledninger-og-skabeloner Myndigheden kan også vælge at udarbejde en politik, der beskriver fordelingen af roller og ansvar i myndigheden.

2. Krav til organisering			
2.2 Faste processer for leverandørstyring	Mange myndigheder har flere leverandører og derfor forskellige aftaler med hver enkelt. Her vil effektiv styring af interne processer bidrage til systematik, så der på tværs af kontrakter etableres ensartede processer og igangsættes de fornødne aktiviteter over for leverandørerne. Det handler om at have et godt fundament af metoder og processer i organisationen.	Myndigheden skal etablere faste processer for styring af leverandører, som er dokumenterede og ledelsesgodkendte. Processerne skal som minimum omfatte planlægning af outsourcingforløb vedrørende samfundskritiske it-systemer, risikostyring, kontrol og opfølgning, transition ind/ud, afslutning af samarbejdet med leverandøren samt inddragelse af leverandører i beredskab og hændelseshåndtering.	Myndigheden kan overveje at udarbejde en samlet politik for organisering af arbejdet med leverandørstyring, der både dækker relevante processer og fordeling af roller og ansvar m.m. Se også vejledningen "Cybersikkerhed i leverandørforhold".
2.3 Kompetenceudvikling og overdragelse af viden	Formålet med kompetenceudvikling og overdragelse af viden er at sikre, at myndigheden til enhver tid har de fornødne interne kompetencer og viden til at styre myndighedens kontrakter og samarbejde med leverandører af samfundskritiske it-systemer.	Myndigheden skal sikre løbende kompetenceudvikling og etablere dokumenterede processer for overdragelse af viden om it-systemet i myndigheden, så der til enhver tid er tilstrækkelige ressourcer til stede med de fornødne kompetencer og viden om systemet, herunder også teknisk viden.	Myndigheden kan eksempelvis gennemføre sidemandsoplæring, teamopbygning (så der aldrig kun er én medarbejder tilknyttet systemet) og sende medarbejdere på mere formelle kurser om nødvendigt.

2. Krav til organisering			
2.4 Sammensætning af samarbejdsfora	Formålet med at beslutningsdygtige medarbejdere deltager i relevante samarbejdsfora med leverandøren er at kunne bruge møderne effektivt, så eventuelle ændringsforslag, aktuelle problemstillinger eller konflikter kan tages i rette tid og fora.	Myndigheden skal sikre, at der i sammensætningen af diverse samarbejdsfora med leverandøren indgår minimum én medarbejder med de fornødne beslutningskompetencer.	Myndigheden kan overveje at etablere og sammensætte samarbejdsfora på forskellige niveauer fx ledelse og drift. Myndigheden kan også overveje, om der skal være faste og ad-hoc medlemmer i disse fora. I "Katalog over kontraktbestemmelser for samfundskritiske it-systemer" stilles der et tilsvarende krav til leverandører (krav 1.2.1.), og det følger heraf, at myndigheden gør det samme.

3. Krav til leverandørstyring			
Område	**Formål**	**Krav**	**Operationalisering**
3.1 Risikostyring	Formålet med systematiske og løbende risikovurderinger er at sikre grundlaget for effektiv risikohåndtering. Ikke alle risici kan fjernes, men det er muligt at styre dem, idet en risikovurdering kan vise, om der er en uoverensstemmelse mellem myndighedens sikkerhedsbehov og leverandørens sikkerhedsniveau. Det er vigtigt at udarbejde risikovurderinger regelmæssigt og løbende genbesøge risikohåndteringen, da der kan opstå nye trusler og sårbarheder, der påvirker risikobilledet.	Myndigheden skal minimum årligt samt ved væsentlige ændringer, efter væsentlige sikkerhedshændelser og på baggrund af tilsyn med leverandøren gennemføre en risikovurdering af det samfundskritiske it-system med input fra leverandøren og eventuelle underleverandører. På baggrund af risikovurderingen skal myndigheden udarbejde en handleplan for håndtering af risici i samarbejde med leverandøren. Myndigheden skal løbende følge op på leverandørens håndtering af risici og inddrage resultaterne i myndighedens egen risikostyring.	Myndigheden kan søge inspiration til sin risikostyring i "Vejledning til risikostyring inden for informationssikkerhed" med tilhørende bilag, som kan findes under risikostyring her https://sikkerdigital.dk/myndighed/vejledninger-og-skabeloner Myndigheden kan søge inspiration til sin risikostyring i vejledningen om "Cybersikkerhed i leverandørforhold", som kan findes under leverandørstyring her https://sikkerdigital.dk/myndighed/vejledninger-og-skabeloner

3. Krav til leverandørstyring			
3.2 Beredskabsplanlægning	Formålet med at udarbejde beredskabsplaner er at være i stand til hurtigst muligt at få det samfundskritiske it-system genoprettet efter eksempelvis et nedbrud eller en sikkerhedshændelse, der påvirker systemet.	Myndigheden skal med input fra leverandøren udarbejde en beredskabsplan og sikre, at leverandørens it-beredskabsplan for det samfundskritiske it-system understøtter planen. Myndigheden skal sikre, at beredskabsplanerne indeholder kontaktoplysninger på relevante medarbejdere hos myndigheden og leverandøren, samt at oplysningerne er opdaterede. Myndigheden skal også sikre tilknyttede medarbejdere har kendskab til beredskabsplanens indhold og adgang til planen i en krisesituation.	Forpligtelsen til at udarbejde beredskabsplaner for at opretholde og videreføre samfundets funktioner på myndighedens område følger af beredskabsloven. Myndigheden kan søge inspiration til beredskabsplaner, herunder også fysiske miniberedskabsplaner på sikkerdigital.dk under beredskabsstyring her https://sikkerdigital.dk/myndighed/vejledninger-og-skabeloner
3.3 Beredskabsøvelse	Formålet med at udføre beredskabsøvelser er at være i stand til hurtigst muligt at få det samfundskritiske it-system genoprettet efter eksempelvis et nedbrud eller en sikkerhedshændelse, der påvirker systemet.	Myndigheden skal minimum årligt eller ved væsentlige ændringer teste beredskabsplanen og øve it-beredskabet for det samfundskritiske it-system i samarbejde med leverandøren.	Myndigheden kan overveje forskellige typer beredskabsøvelser afhængig af formålet med øvelsen. Myndigheden kan også vælge at teste hele eller dele af beredskabet, fx aktivering og mobilisering af beredskab.

3. Krav til leverandørstyring			
3.4 Drifts-opfølg-ning	Formålet med systematisk opfølgning på leverandø-rens leverancer, indberet-ninger, risikostyring, æn-dringer og sikkerhedshæn-delser er at sikre, at leve-randøren leverer det, denne er forpligtet til.	Myndigheden skal systematisk og kontinuerligt følge op på og kontrollere de leverancer i forhold til sikkerhedskravene, som leverandøren er forplig-tet til at levere.	Kravet om driftsop-følgning følger del-vist af ISO 27001. Myndigheden kan overveje at operatio-nalisere sikkerheds-kravene i kontrakten ved at opstille kon-krete målepunkter for kravenes opfyl-delse, som efterføl-gende anvendes til at følge op på leveran-dørens leverancer og indrapporteringer. Se mere for inspira-tion i rejsefortællin-gen på sikkerdigital under leverandørsty-ring her https://sik-kerdigital.dk/myn-dighed/vejledning-ger-og-skabeloner

3. Krav til leverandørstyring			
3.5 Skærpet tilsyn	Formålet med det skærpede tilsyn er at sikre et mere omfattende og formelt tilsyn af samfundskritiske it-systemer med henblik på at dokumentere leverandørens efterlever en høj sikkerhed iht. forpligtigelser.	Myndigheden skal foretage skærpet tilsyn hos leverandører af samfundskritiske it-systemer.	Myndigheden kan udarbejde en kontraktkalender, årshjul eller tilsvarende styringsdokument for sit tilsyn af det samfundskritiske it-system. Dette vil bidrage til at sikre gennemførelse af relevante tilsynsaktiviteter og opfølgning på revisionserklæringer – enten i løbet af et år eller i hele kontraktens levetid. Et skærpet tilsyn indebærer fx en kombination af skriftlige undersøgelser, test, revision og besøg hos leverandøren for at bekræfte kontrollers effektivitet. Se appendikset for eksempler på relevante styringsdokumenter.

Tjekliste

- [ ] **1. Krav til kontraktstyring**
- [ ] 1.1 Kontraktbibliotek
- [ ] 1.2 Dokumentation
- [ ] **2. Krav til organisering**
- [ ] 2.1 Roller og ansvar
- [ ] 2.2 Faste processer for leverandørstyring
- [ ] 2.3 Kompetenceudvikling og overdragelse af viden
- [ ] 2.4 Sammensætning af samarbejdsfora
- [ ] **3. Krav til leverandørstyring**
- [ ] 3.1 Risikostyring
- [ ] 3.2 Beredskabsplanlægning
- [ ] 3.3 Beredskabsøvelse
- [ ] 3.4 Driftsopfølgning
- [ ] 3.5 Skærpet tilsyn

digst.dk