CENTER FOR CYBERSIKKERHED

DIGITALISERINGSSTYRELSEN

Vejledning

Cybersikkerhed i leverandørforhold

Beskyt organisationen ved outsourcing af it-driften i hele forløbet - fra start til slut.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

DIGITALISERINGSSTYRELSEN

Landgreven 4
1301 København K
Telefon: + 45 3392 5200
E-mail: digst@digst.dk

Forsideillustration:
Iaroslav Neliubov/Shutterstock
2. udgave maj 2022.

Indledning

Mange myndigheder og virksomheder vælger at outsource hele eller dele af deres it-drift til eksterne leverandører. Det skyldes blandt andet, at outsourcing ofte kan give god mening ud fra et forretningsmæssigt synspunkt. Det kan være for at koncentrere sig om organisationens kerneforretning, sikre de fornødne kompetencer til it-driften, frigøre ressourcer til andre formål eller noget fjerde. Til gengæld er der også væsentlige risici forbundet med outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed. Derfor er leverandørstyring en vigtig del af enhver organisations gode cyberforsvar og styring af informationssikkerhed.

Fremmede stater og kriminelle angriber jævnligt deres mål gennem forsyningskæden ved at kompromittere leverandører. Hackere udnytter altså sårbarheder hos leverandører som et springbræt til at kompromittere deres egentlige mål. Det er derfor vigtigt, at organisationen stiller de relevante sikkerhedskrav til leverandøren og løbende fører kontrol med leverandørens efterlevelse heraf i aftaleperioden.

Cybertruslen mod forsyningskæden
Læs mere om cybertruslen mod forsyningskæden i CFCS' trusselsvurderinger "Cyberangreb mod leverandører" og "Cybertruslen mod it-serviceudbydere" (CFCS 2019 og 2020).

Desuden sker outsourcing ofte på bekostning af organisationens direkte kontrol med de driftsopgaver, der overlades til leverandøren. Selvom udvalgte it-systemer outsources til en leverandør, er det stadig organisationens ansvar at beskytte egne systemer og informationer, hvilket leverandørstyring bidrager til.

Denne vejledning omhandler organisationers styring af cyber- og informationssikkerhed i kunde-leverandørforhold ved outsourcing af it. Vejledningen giver en række anbefalinger til, hvordan organisationer kan styre cyber- og informationssikkerheden i de forskellige faser af et outsourcing-forløb. Andre aspekter af kundens samarbejde med leverandøren såsom indkøbs-, udbuds- og kontraktstyring berøres ikke i vejledningen.

Cyber- og informationssikkerhed bør være en integreret del af organisationens styring af samarbejdet med leverandøren og omfatte alle faser af outsourcing-forløbet. Derudover bør kundens styring af samarbejdet med leverandøren altid bero på en risikovurdering af den konkrete leverance og leverandør. Enhver organisation har begrænsede ressourcer og bør derfor arbejde risikobaseret ved at fokusere på de mest kritiske it-systemer. Desuden kan der gælde særlige krav for myndigheder ved outsourcing af eksempelvis samfundskritiske it-systemer.

Vejledningen henvender sig primært til statslige myndigheder, der outsourcer - eller planlægger at outsource - deres it til en eller flere leverandører, herunder i forbindelse med større it-anskaffelser. Vejledningen kan også anvendes af andre offentlige myndigheder og af virksomheder, der har besluttet at outsource deres it. Målgruppen er først og fremmest de medarbejdere, der har ansvaret for at styre organisationens leverandører. Dele af vejledningen henvender sig også til ledelsen, der bør træffe de strategiske beslutninger om outsourcing.

Overordnede anbefalinger

Nedenfor ses de overordnede anbefalinger til organisationers styring af cyber- og informationssikkerheden ved outsourcing af it. Anbefalingerne er opdelt efter faserne i et outsourcing-forløb og nummereret. De uddybes enkeltvist i vejledningen.

På specifikke forretningsområder og i visse sektorer eller brancher kan der være særlige risici, standarder eller sikkerhedskrav, som ikke berøres i vejledningen. Nedenstående anbefalinger skal derfor ikke opfattes som en udtømmende liste.

Fase	Anbefaling
1. Planlægning	1.1 Dokumentér interne og eksterne forhold vedrørende den planlagte outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed.
	1.2 Kortlæg organisationens forretningsprocesser med fokus på den underliggende it-infrastruktur, herunder datastrømme og indbyrdes afhængigheder.
	1.3 Foretag en risikovurdering med fokus på særlige risici ved den planlagte outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed.
	1.4 Formulér en separat politik for organisationens styring af cyber- og informationssikkerhed i kunde-leverandørforhold ved outsourcing af it.
	1.5 Etablér en intern organisation egnet til leverandørstyring med veldefinerede roller, de fornødne ressourcer og kompetencer, dokumenterede processer og den nødvendige it-understøttelse.
2. Kravstillelse	2.1 Stil relevante krav til leverandørens cyber- og informationssikkerhed på baggrund af en risikovurdering.
	2.2 Stil krav til leverandørens cyber- og informationssikkerhed med fokus på den ønskede effekt frem for den præcise løsning.
	2.3 Vurdér behovet for ekstern rådgivning og bistand, herunder inddragelse af CFCS, i forbindelse med udarbejdelsen af sikkerhedskrav til leverandøren.
3. Leverandørvalg	3.1 Vælg leverandør ud fra relevante kriterier og på baggrund af en grundig vurdering af leverandørens samlede evne til at opfylde sikkerhedskravene og de øvrige krav til opgaveløsningen.
4. Aftalen	4.1 Aftal en klar rolle- og ansvarsfordeling med leverandøren i forhold til parternes styring af cyber- og informationssikkerhed i kunde-leverandørforholdet.
	4.2 Etablér en samarbejdsorganisation og formaliseret proces for håndtering af dialogen med leverandøren, som både omfatter den daglige dialog og kommunikation i tilfælde af sikkerhedshændelser og i en beredskabssituation.
5. Styring	5.1 Dokumentér organisationens behov for at føre kontrol med leverandøren.
	5.2 Udpeg en dedikeret rolle med ansvar for organisationens leverandørstyring i forhold til opfyldelsen af sikkerhedskravene i kontrakten.
	5.3 Før løbende kontrol med leverandørens opfyldelse af sikkerhedskravene i kontrakten efter behov og på baggrund af en risikovurdering.
	5.4 Gennemfør løbende risikovurderinger med input fra leverandøren og eventuelle underleverandører.
	5.5 Håndtér evt. sikkerhedshændelser og væsentlige ændringer hos kunden, leverandøren eller i omgivelserne, der kan påvirke sikkerheden i leverancen.
6. Afslutning	6.1 Bevar cyber- og informationssikkerheden under afviklingen af kunde-leverandørforholdet.

Læsevejledning

Der er flere forhold i samarbejdet mellem en organisation og dens leverandører, der kan påvirke organisationens cyber- og informationssikkerhed. Denne vejledning fokuserer på aspekter af cyber- og informationssikkerhed i kunde-leverandørforhold ved outsourcing af it.

Vejledningen henvender sig først og fremmest til de medarbejdere, der har ansvaret for den daglige styring af organisationens leverandører. Indledningen og afsnittet om planlægningsfasen henvender sig også til ledelsen, der har det overordnede ansvar for organisationens cyber- og informationssikkerhed og derfor bør være bevidst om deres rolle og ansvar i forbindelse med outsourcing.

Vejledningen er struktureret efter faserne i et outsourcing-forløb. For hver fase er der særlige aspekter vedrørende cyber- og informationssikkerhed, der skal adresseres i forholdet mellem kunde og leverandør. Vejledningen kan således anvendes uanset hvor, organisationen befinder sig i et konkret outsourcing-forløb. For eksempel kan vejledningen både benyttes ved igangsættelsen af et nyt outsourcing-forløb og i forbindelse med leverandørstyring med udgangspunkt i en eksisterende kontrakt.

Outsourcing af it
I vejledningen defineres outsourcing af it som det forhold, at en organisation får varetaget hele eller dele af it-driften af en anden virksomhed eller myndighed. Outsourcing kan omfatte it-systemer, applikationer, it-infrastruktur og -services, hvor leverandøren varetager den daglige drift og eventuelt opgaver som vedligeholdelse, support og videreudvikling. Hvis disse opgaver varetages af forskellige leverandører, bør organisationen følge op på sikkerheden hos alle leverandørerne. Organisationers almindelige indkøb af it-udstyr og -produkter er som udgangspunkt ikke omfattet af definitionen, medmindre der er tale om større it-anskaffelser, hvor driftsopgaver også overdrages til leverandøren i forbindelse med anskaffelsen af den pågældende it-løsning.

Den organisation, der outsourcer, bliver benævnt kunden, mens den organisation, der varetager opgaven på vegne af kunden, betegnes leverandøren. For enkelthedens skyld anvendes betegnelserne konsistent i vejledningen, selvom kunde og leverandør også benævnes henholdsvis ordregiver og tilbudsgiver i visse dele af en eventuel udbudsproces.

Nedenstående figur illustrerer den typiske fordeling af opgaver og ansvar i et kunde-leverandørforhold ved outsourcing af it. Kunden beholder altid ansvaret for at beskytte egne it-systemer og informationer, selvom den daglige it-drift overdrages til en leverandør. Det er derfor vigtigt, at kunden løbende fører kontrol med leverandøren i aftaleperioden.

Figur 1. Opgave- og ansvarsfordeling i et kunde-leverandørforhold.

Da vejledningen omhandler styring af cyber- og informationssikkerhed ved outsourcing af it generelt, gælder anbefalingerne også ved outsourcing til leverandører af cloud-services. For specifikke anbefalinger til styringen af cloud-leverandører henvises til "Vejledning i anvendelse af cloudservices" (CFCS og Digitaliseringsstyrelsen 2020).

Myndigheder er ofte forpligtet til at gennemføre udbud i forbindelse med outsourcing. Hvis driftsopgaven skal i udbud, er det myndighedens ansvar at overholde reglerne i udbudsloven. Myndighedens eventuelle forpligtelser i forhold til udbudsreglerne beskrives ikke i denne vejledning.

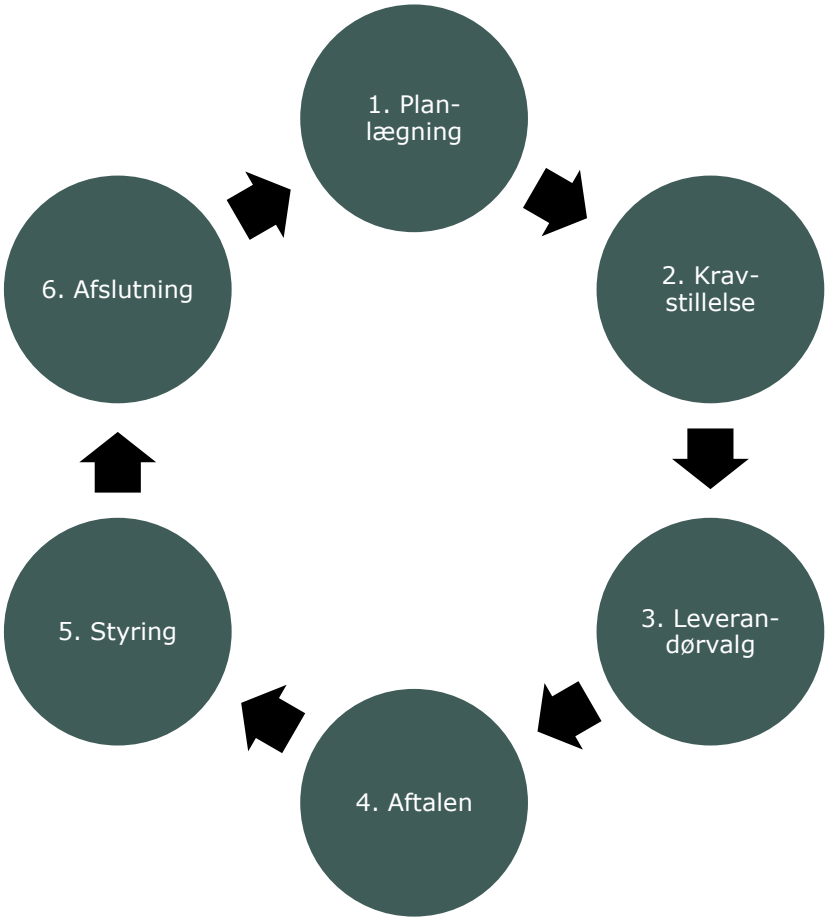
Dog anvender myndigheder ofte rammeaftaler gennem Staten og Kommunernes Indkøbsservice (SKI) eller Statens Indkøb (SI) i forbindelse med it-anskaffelser. Det kan skabe tvivl om parternes ansvar i forhold til at kontrollere leverandørens efterlevelse af rammeaftalen og leveranceaftalen. Bilag 1 beskriver derfor ansvarsfordelingen mellem parterne i relation til leverandørstyring, når myndigheder anvender rammeaftaler gennem SKI eller SI.

Forsyningskæden er ikke stærkere end det svageste led
Ofte indgår kunden og leverandøren i en længere række af kunde-leverandørforhold, hvor også underleverandører kan være involveret. Det kaldes også en forsyningskæde. Forsyningskæder er som regel vidt forgrenede, da kunder ofte anvender flere leverandører, ligesom leverandører ofte har mange kunder.

Leverandører benytter ofte underleverandører i forbindelse med deres opgaveløsning, hvilket i sidste ende kan påvirke kundens cyber- og informationssikkerhed. Det er derfor vigtigt, at kunden har overblik over leverandørens brug af underleverandører. I bilag 2 beskrives en række forhold relateret til forsyningskæden, som kunden bør være opmærksom på.

Faser i et outsourcing-forløb

Ethvert outsourcing-forløb følger en cyklus, der kan inddeles i en række faser. Denne vejledning er struktureret efter de seks faser, der vises i figuren herunder. Overvejelser om cyber- og informationssikkerhed er relevante i alle faser af outsourcing-forløbet, fra den indledende planlægningsfase til afslutningen på kunde-leverandørforholdet. CFCS' anbefalinger til de enkelte faser uddybes enkeltvist i de følgende afsnit.



Figur 2. Faser i et outsourcing-forløb.

Myndigheder har ikke altid mulighed for selv at tildele kontrakten til en leverandør ved outsourcing. En del myndigheder er nemlig forpligtet til at anvende en bestemt leverandør, som ofte er en anden offentlig myndighed. Eksempelvis har mange statslige myndigheder overdraget driftsansvaret til Statens IT (SIT) ved kongelig resolution. Som udgangspunkt gælder anbefalingerne i vejledningen uanset, om myndigheden selv har valgt eller er forpligtet til at anvende en bestemt leverandør. Ved outsourcing til SIT gælder dog en række særlige forhold, der har betydning for myndighedens styring af cyber- og informationssikkerheden i kunde-leverandørforholdet. Disse forhold er beskrevet i bilag 3.

1. Planlægning

1.1 Dokumentér interne og eksterne forhold vedrørende outsourcing

Når en kunde planlægger at outsource hele eller dele af organisationens it til en leverandør, er der en række forhold af betydning for organisationens cyber- og informationssikkerhed, som ledelsen kan tage med i overvejelserne. Kunden kan dokumentere disse sikkerhedsmæssige overvejelser i en outsourcing-plan eller lignende, da overvejelserne indgår i organisationens generelle styring af cyber- og informationssikkerhed. Ledelsen bør både tage stilling til relevante interne (såsom organisationens behov, risikoappetit og organisering) og eksterne forhold (såsom gældende regulering og andre kontraktlige forpligtelser). Disse forhold uddybes i det følgende.

I planlægningsfasen bør kunden først og fremmest tage stilling til kritikaliteten af de it-systemer, som potentielt skal outsources. It-systemernes kritikalitet - i forhold til kundens forretning - spiller nemlig en afgørende rolle for, dels hvilke sikkerhedskrav kunden bør stille til leverandøren, og dels hvordan kunden efterfølgende følger op på leverandørens efterlevelse af kravene. I vurderingen af it-systemers kritikalitet kan kunden hente en definition i "Vejledning til model for porteføljestyring af statslige it-systemer" (Digitaliseringsstyrelsen 2021).

Kunden bør også tage udgangspunkt i sine forretningsbehov, når beslutningen om at outsource skal træffes. Kunden bør foretage en behovsafdækning og beskrive formålet med den planlagte outsourcing under inddragelse af relevante interessenter i organisationen. Der kan være både strategiske og operationelle fordele ved at outsource, som kunden bør overveje. Figuren herunder giver eksempler herpå.

Strategiske fordele	Operationelle fordele
• Frigørelse af ressourcer til andre formål • Prioritering af organisationens kerneforretning • It-anskaffelser, som ikke kan udvikles internt til samme pris • Effektivisering af it-driften • Forbedre organisationens cyber- og informationssikkerhed	• Mere stabil it-drift • Adgang til leverandørens faglige ekspertise og erfaring • Bedre vedligeholdelse, it-support og videreudvikling • Øget brugervenlighed • Adgang til ny og bedre teknologi • Hjælp til dokumentation og rapportering

Figur 3. Potentielle fordele ved outsourcing af organisationens it.

Outsourcing indebærer ofte, at kunden må afgive direkte kontrol med de it-driftsopgaver, der overlades til leverandøren. Inden beslutningen om at outsource træffes, bør ledelsen derfor overveje, om der er dele af organisationens it, der ikke kan outsources. Kunden kan eksempelvis have forretningskritiske it-systemer eller særligt følsomme

informationer, som kunden ønsker at bevare fuld kontrol over, såfremt risikoen ved outsourcing vurderes for høj. Det afhænger blandt andet af kundens risikoappetit.

I vurderingen af it-systemernes væsentlighed bør ledelsen ligeledes tage stilling til, om den planlagte outsourcing omfatter kritisk it-infrastruktur eller samfundskritiske it-systemer. Hvis dette er tilfældet, bør kunden vurdere behovet for selv at træffe særlige sikkerhedsforanstaltninger og stille yderligere krav til leverandørens cyber- og informationssikkerhed.

Definition af kritisk it-infrastruktur
Den delmængde af kritisk infrastruktur, der omfatter den digitale infrastruktur, der er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner.

Definition af samfundsvigtige funktioner
Samfundsvigtige funktioner omfatter de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed.

Definition af samfundskritiske it-systemer
De it-systemer, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet som helhed. Utilgængelighed og ustabil drift i it-systemerne kan få markante følger for samfundet og for opretholdelsen af samfundskritiske processer.

Af eksterne forhold kan der være forpligtelser i kundens kontrakter med andre leverandører eller særlig regulering på området, som ledelsen bør overveje i forbindelse med outsourcing. Lovkrav, anden regulering og kontraktlige forpligtelser kan have indflydelse på, hvilke it-systemer kunden kan outsource driften af, hvor it-driften kan outsources til, eller hvordan bestemte typer af informationer skal behandles og beskyttes. Eksempelvis kan der være forhold vedrørende klassificerede oplysninger, personoplysninger, lokationskrav og eksportkontrol, som kunden bør tage med i overvejelserne. Outsourcing af kritisk infrastruktur kan desuden være underlagt et krav om tilladelse fra Erhvervsstyrelsen efter investeringsscreeningsloven.

Dokumentér interne og eksterne forhold vedrørende den planlagte outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed.

1.2 Kortlæg organisationens forretningsprocesser, it-infrastruktur og data
Hvis kunden outsourcer et it-system uden at have overblik over organisationens forretningsprocesser, it-infrastruktur og datastrømme, kan der opstå nye sårbarheder og dermed introduceres cyber- og informationssikkerhedsrisici, som kunne være forudset og dermed undgået.

Inden beslutningen om at outsource træffes, bør kunden derfor kortlægge, hvordan it-infrastrukturen er sammensat, hvordan datastrømmene løber, og hvordan de indbyrdes afhængigheder og grænseflader mellem organisationens it-systemer ser ud. Kortlægningen gør det nemmere for kunden at udvælge de rette segmenter af it-infrastrukturen og hvilke lag af teknologistakken, der skal outsources, samt at beskrive

dem over for leverandøren. Hvis der tidligere er foretaget en kortlægning, bør kortlægningen opdateres, så den giver et revisende billede af kundens forretningsprocesser og den underliggende it-infrastruktur.

Kortlæg organisationens forretningsprocesser med fokus på den underliggende it-infrastruktur, herunder datastrømme og indbyrdes afhængigheder.

1.3 Foretag en risikovurdering og tag stilling til risikohåndteringen

I planlægningsfasen bør kunden fortage en risikovurdering med fokus på særlige risici ved outsourcing af organisationens it, der kan påvirke fortroligheden, integriteten og tilgængeligheden af kundens informationer. Outsourcing kan nemlig introducere nye cyber- og informationssikkerhedsrisici og dermed ændre organisationens risikobillede. Derudover er risikovurderingen en forudsætning for, at kunden efterfølgende kan stille relevante sikkerhedskrav til leverandøren, der bidrager til at imødegå konkrete risici ved outsourcing.

Risikovurderingen af den planlagte outsourcing kan være integreret i organisationens generelle risikostyring og gennemføres med udgangspunkt i en dokumenteret proces og metode. For hjælp til udarbejdelsen af risikovurderinger se ISO/IEC 27005 eller "Vejledning til risikostyring inden for Informationssikkerhed" (Digitaliseringsstyrelsen 2020a).

Nedenfor er listet en række forhold ved outsourcing, som kunden kan inddrage i risikovurderingen. Listen er ikke udtømmende, og vurderingen af disse forhold bør indgå i kundens samlede beslutning om at outsource:

- Væsentlige forandringer hos leverandøren, der kan påvirke leverancen. Leverandøren kan eksempelvis flytte til et andet land, gå konkurs, skifte underleverandør eller blive opkøbt af en anden virksomhed.
- Ved outsourcing overlades dele af kundens risikohåndtering til leverandøren. Kunden bør derfor sikre, at leverandøren løbende bidrager til kundens risikovurdering, eksempelvis med særlig viden om relevante trusler og sårbarheder.
- Der kan være uoverensstemmelse mellem kundens sikkerhedsbehov og leverandørens risikoappetit og sikkerhedsniveau, hvilket kan føre til utilstrækkelig risikohåndtering. Omvendt kan outsourcing potentielt forbedre kundens sikkerhed afhængig af niveauet af leverandørens cyber- og informationssikkerhed.
- Cybertruslen fra cyberkriminalitet og cybespionage, da outsourcing kan øge kundens angrebsflade for hackere. Der er blandt andet risiko for supply chain-angreb, hvor hackere forsøger at kompromittere kunden ved at udnytte sårbarheder hos leverandøren eller leverandørens andre kunder.
- Medarbejdere hos leverandøren og eventuelle underleverandører, som kunden ikke har ledelsesretten over, kan få fysisk og logisk adgang til kundens aktiver.
- Leverandøren kan få kendskab til kundens organisation, forretningsprocesser, it-infrastruktur, sikkerhedsforanstaltninger, interne procedurer m.m.
- Leverandørens villighed til at levere den efterspurgte dokumentation og kundens mulighed for at føre kontrol med leverandøren kan være begrænset.
- Eventuelle lovkrav og anden regulering på området, der kan medføre risici for kunden ved manglende efterlevelse heraf hos kunden eller leverandøren.

- Kritikaliteten og væsentligheden af de outsourcede it-systemer og informationernes følsomhed.
- Udfordringer forbundet med at afslutte samarbejdet med leverandøren og videreføre it-driften såsom at verificere sletning af kundens data hos leverandøren.
- Potentielle risici ved outsourcing, der kan få utilsigtede konsekvenser for kundens samarbejde med andre leverandører. Især ved multisourcing, hvor kunden outsourcer til flere forskellige leverandører.

Når kunden har afdækket relevante risici ved den planlagte outsourcing, bør kunden udarbejde en plan for, hvordan disse risici skal håndteres i kunde-leverandørforholdet og dermed nedbringes til et acceptabelt niveau for kunden. De identificerede risici håndteres blandt andet ved at stille relevante sikkerhedskrav til leverandøren i kontrakten og de medfølgende bilag (se afsnit 2 om kravstillelse). Alle sikkerhedsforanstaltninger bør dokumenteres i en risikohåndteringsplan. En del af kundens risikohåndtering vil ofte overgå til leverandøren, men der vil være visse områder, som kunden stadig har ansvar for. Kunden bør derfor overveje ansvarsfordelingen mellem parterne, inden der træffes en endelig beslutning om, hvilke konkrete opgaver der outsources.

Foretag en risikovurdering med fokus på særlige risici ved den planlagte outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed.

Multisourcing stiller større krav til kundens risiko- og leverandørstyring
Mange organisationer vælger at outsource deres it til flere leverandører frem for at have hele it-porteføljen samlet hos én leverandør. Det kan f.eks. skyldes de økonomiske fordele, fleksibiliteten og adgangen til mere specialiserede ydelser ved at multisource. Til gengæld vokser kompleksiteten i kundens it-arkitektur, ligesom organisationens angrebsflade øges for hackere. Multisourcing stiller derfor større krav til organisationens processer for risiko- og leverandørstyring, hvilket bør indgå i den samlede beslutning om at multisource.

Hvis en organisation planlægger at multisource, bør ledelsen formulere en outsourcing-strategi og etablere en standardiseret proces og livscyklus for håndtering af samarbejdet med leverandører, hvor sikkerhed indgår fra start til slut.

1.4 Formulér en politik for cyber- og informationssikkerhed ved outsourcing
Kunden kan også formulere en separat politik for cyber- og informationssikkerhed i kunde-leverandørforhold med afsæt i organisationens risikovurdering og overordnede cyber- og informationssikkerhedspolitik. Formålet med politikken er at fastsætte de overordnede rammer for organisationens styring af cyber- og informationssikkerhed ved outsourcing af it.

Politikken bør definere organisationens målsætninger og overordnede krav til styringen af cyber- og informationssikkerhed i kunde-leverandørforhold, herunder de generelle processer, retningslinjer og procedurer som både kunde og leverandør skal implementere. Derudover bør politikken beskrive opgave- og ansvarsfordelingen mellem relevante roller i kundens organisation relateret til leverandørstyring og styring af cyber-

og informationssikkerhed (se afsnit 1.5 og bilag 4). Dermed bidrager politikken også til at sikre, at kundens organisation egner sig til at styre cyber- og informationssikkerheden i kunde-leverandørforhold.

Formulér en separat politik for organisationens styring af cyber- og informationssikkerhed i kunde-leverandørforhold ved outsourcing af it.

1.5 Etablér en intern organisation egnet til leverandørstyring

Leverandøren kan besidde kompetencer, der nedbringer risici, frem for hvis kunden selv skulle stå for driften af it-systemet. Det er under alle omstændigheder en vedvarende og tværfaglig opgave at styre cyber- og informationssikkerheden i et kunde-leverandørforhold. Ledelsen bør derfor sørge for at have en intern organisation på plads, der egner sig til at føre kontrol med organisationens leverandører. Leverandørstyring forudsætter nemlig, at der i organisationen findes veldefinerede roller og de fornødne ressourcer med kompetencer inden for blandt andet jura, økonomi, it og sikkerhed. I organisationens håndtering af samarbejdet med leverandøren indgår ofte en række forskellige roller og funktioner, herunder:

- Ledelsen
- Informationssikkerhedskoordinator/it-sikkerhedsansvarlig
- Kontraktansvarlig
- Jura
- It-ansvarlig
- Data- og systemejer
- Databeskyttelsesrådgiver (DPO)

I bilag 4 beskrives en mulig opgave- og ansvarsfordeling mellem ovenstående roller i forhold til organisationens styring af cyber- og informationssikkerhed i forbindelse med outsourcing. Afhængig af organisationens størrelse og organisering kan en medarbejder udfylde én eller flere roller på samme tid.

God leverandørstyring forudsætter ledelsesmæssig prioritering og samarbejde på tværs af organisationen.

I planlægningsfasen bør ledelsen også tage stilling til, hvilke ansvarsområder og kompetencer inden for cyber- og informationssikkerhed, der skal beholdes i organisationen, og hvilke opgaver der skal overføres til leverandøren. Kunden kan eksempelvis vælge at outsource en række tekniske sikkerhedsopgaver for at få adgang til leverandørens ekspertise og udnytte organisationens interne ressourcer mere effektivt. Der kan således være væsentlige fordele ved at outsource konkrete opgaver til en leverandør, som har særlige kompetencer på området. Dog bør kunden være opmærksom på, at det kræver viden og erfaring at styre sikkerheden i et kunde-leverandørforhold, og at kunden stadig har ansvaret for organisationens it-systemer og informationer, selvom driften outsources til en leverandør.

Ved outsourcing bør ledelsen derfor sikre, at organisationen bevarer de fornødne sikkerhedskompetencer og dermed har nogle af de rette forudsætninger for at styre sine leverandører. Ledelsen bør også sikre, at organisationen har dokumenterede processer og den nødvendige it-understøttelse på plads til at foretage leverandørstyring.

Etablér en intern organisation egnet til leverandørstyring med veldefinerede roller, de fornødne ressourcer og kompetencer, dokumenterede processer og den nødvendige it-understøttelse.

2. Kravstillelse

2.1 Stil relevante krav til leverandørens cyber- og informationssikkerhed
Det er vigtigt at stille relevante krav til potentielle leverandører, så kunden har et fyldestgørende grundlag at vælge leverandør ud fra og et godt udgangspunkt for den efterfølgende leverandørstyring. Kunden bør stille krav til leverandørens cyber- og informationssikkerhed, der bidrager til at nedbringe risici til et acceptabelt niveau for kunden og sikrer et tilstrækkeligt sikkerhedsniveau forbundet med leverancen. Kravene til leverandørens sikkerhed bør ledsages af krav vedrørende kontrol og opfølgning, der understøtter leverandørens efterlevelse af sikkerhedskravene i aftaleperioden.

Kunden bør stille krav til leverandørens sikkerhed på baggrund af en risikovurdering af den planlagte outsourcing, en risikohåndteringsplan og en politik for organisationens styring af cyber- og informationssikkerhed i kunde-leverandørforhold (se afsnit 1 om planlægningsfasen). Kunden bør nøje overveje alle aspekter af cyber- og informationssikkerhed, herunder organisatoriske, adfærdsmæssige, fysiske og tekniske sikkerhedsforanstaltninger. Derudover kan kravene omfatte såvel forebyggende som opdagende og korrigerende sikkerhedsforanstaltninger.

Kunden bør også sikre, at sikkerhedskravene afspejler informationernes følsomhed og væsentligheden af de outsourcede it-systemer i forhold til kundens forretning. Hvis kunden outsourcer kritisk it-infrastruktur eller samfundskritiske it-systemer, bør kunden stille større krav til leverandørens cyber- og informationssikkerhed, end hvis leverancen omfatter mindre væsentlige it-systemer. Desuden bør kunden overveje, om kravene til informationers fortrolighed, integritet og tilgængelighed er lige vigtige i forhold til leverancen og kundens forretning, eller om der skal prioriteres mellem dem.

I udarbejdelsen af sikkerhedskravene bør kunden tage udgangspunkt i best practice og internationale standarder for cyber- og informationssikkerhed såsom ISO/IEC 27001 og 27002 eller tilsvarende. Kunden bør udarbejde en kravspecifikation, hvor alle sikkerhedskravene til leverancen er tydeligt beskrevet, så leverandøren kender kundens forventninger til sikkerhedsniveauet ved tilbudsafgivelsen. Det kan være en styringsmæssig fordel at samle alle sikkerhedskravene i en separat sikkerhedskravspecifikation og sikre tydelig henvisning til relevante krav fra andre dele af kravspecifikationen.

Stil 'smarte' sikkerhedskrav til leverandøren
Det er vigtigt at stille veldefinerede sikkerhedskrav, som egner sig til at evaluere løsningsbeskrivelser fra potentielle leverandører. Derudover bør kravene egne sig til kontrol og opfølgning i aftaleperioden.

I bilag 5 beskrives, hvordan kunden kan formulere bedre sikkerhedskrav til leverandøren ved hjælp af SMART-princippet, der indebærer, at kravene så vidt muligt bør være *Specifikke, Målbare, Anvisende, Relevante* og *Tidsbestemte.*

Kunden bør sikre, at kravene til leverandøren omfatter følgende forhold vedrørende cyber- og informationssikkerhed samt leverandørstyring.

Forhold vedrørende cyber- og informationssikkerhed	Forhold vedrørende leverandørstyring
• Relevante lov- og myndighedskrav, herunder de tekniske minimumskrav, katalog over kontraktbestemmelser for samfundskritiske it-systemer, lokationskravet, sikkerhedscirkulæret og databeskyttelsesreglerne. • Leverandørens risikostyringsproces og opretholdelse af et ledelsessystem for informationssikkerhed baseret på ISO 27001 eller tilsvarende. • Rolle- og ansvarsfordelingen mellem kunde og leverandør (se afsnit 4). • Behovet for at indgå en databehandleraftale med leverandøren. • Uddannelse og træning af relevante medarbejdere hos leverandøren og evt. underleverandører med adgang til kundens aktiver. • Behovet for sikkerhedsgodkendelse af relevante medarbejdere hos leverandøren og evt. underleverandører med adgang til kundens aktiver. • Parternes gensidige tavshedspligt, der også omfatter underleverandører. • Parternes håndtering af cyber- og informationssikkerhed i overgangsperioden fra en evt. tidligere leverandør. • Gennemførelse af sikkerhedstests og sårbarhedsscanninger (af kunden, leverandøren eller en tredjepart). • Leverandørens adgangsstyring ift. adgangen til kundens aktiver, herunder at leverandøren skal understøtte kundens klassifikationssystem. • Parternes procedurer for hændelseshåndtering, forretningsvidereførelse og beredskab, herunder regelmæssig test af beredskabsplaner. • Leverandørens underretningspligt over for kunden om forhold, der kan påvirke sikkerheden forbundet med leverancen, herunder sikkerhedshændelser. • Sikker kommunikation mellem parterne, herunder f.eks. brug af TLS og DMARC. For flere anbefalinger herom se CFCS' vejledninger på cfcs.dk.	• Leverandørens rapportering, herunder rapporteringens form og indhold samt struktur og frekvens for statusmøder mellem parterne. • Kundens ret til at føre kontrol med leverandørens efterlevelse af kontrakten og gældende regulering på området (compliance). • Leverandørens brug af underleverandører (se bilag 2). • Leverandørens forpligtelse til at udpege relevante nøglepersoner i organisationen, der er centrale ift. leverandørens opfyldelse af kontrakten. • Leverandørens etablering af en samarbejdsorganisation (se afsnit 4). • Leverandørens forpligtelse til at samarbejde med kundens øvrige leverandører. • Kundens mulighed for at inddrage tredjeparter til støtte ifm. leverancen og ved aftalens ophør (f.eks. teknisk eller juridisk bistand). • Leverandørens forpligtelse til at levere retvisende, fyldestgørende og til enhver tid ajourført dokumentation for udførelsen af leverancen. • Parternes proces for håndtering af ændringer ift. løbende at tilpasse cyber- og informationssikkerheden i aftaleperioden (se afsnit 4). • Bestemmelser, der tager højde for et evt. salg, ændring i ejerforhold eller ophør af leverandørens virksomhed. • Bestemmelser vedrørende leverandørens forpligtelse til at afhjælpe fejl og mangler i leverancen. • Leverandørens forpligtelser til rettidigt at træffe supplerende eller udbedrende sikkerhedsforanstaltninger ved misligholdelse af sikkerhedskrav. • Procedurer for håndtering af tvister. • Konsekvenser ved leverandørens misligholdelse af sikkerhedskrav, der bør kunne medføre bod og give kunden ret til straks at ophæve kontrakten. • Ophørsbestemmelser ved afvikling af kunde-leverandørforholdet (se afsnit 6).

Kunden kan søge inspiration til udarbejdelsen af sikkerhedskrav i materialet på Digitaliseringsstyrelsens hjemmeside (digst.dk). Her findes bl.a. en række værktøjer og skabeloner, der kan hjælpe kunden med at stille relevante sikkerhedskrav i kontrakter, herunder K04 Standardkontrakt for it-drift, et klausulbibliotek og et kravkatalog (Digitaliseringsstyrelsen 2016; 2017; 2020b). På sikkerdigital.dk findes bl.a. også et katalog over kontraktbestemmelser for samfundskritiske it-systemer og et appendiks med tilføjelser til operationalisering af kataloget (Digitaliseringsstyrelsen 2022a; 2022b).

Stil relevante krav til leverandørens cyber- og informationssikkerhed på baggrund af en risikovurdering.

2.2 Stil krav til leverandørens sikkerhed med fokus på den ønskede effekt

Når kunden stiller krav til leverandørens cyber- og informationssikkerhed, bør detaljeringsgraden på kravene nøje overvejes. Kunden bør generelt formulere sikkerhedskrav, der udtrykker en ønsket effekt, frem for at stille meget specifikke og detaljerede krav til leverandørens konkrete opgaveløsning. Dét skyldes, at leverandøren med sit kendskab til egne medarbejdere, interne processer og egen it-infrastruktur ofte er bedre i stand til at designe og implementere sikkerhedsforanstaltninger i sin organisation, end kunden er. Leverandøren kan som regel også se andre og måske bedre måder at løse en given opgave på. Desuden kan specifikke og detaljerede krav vedrørende tekniske sikkerhedsforanstaltninger blive forældet i løbet af aftaleperioden.

Hvis leverandøren kan dokumentere opfyldelsen af et effektkrav, vil det ofte være at foretrække frem for at holde fast i specifikke krav til selve opgaveløsningen. I visse tilfælde kan kunden dog have behov for at stille helt specifikke krav til eksempelvis tekniske sikkerhedsforanstaltninger hos leverandøren. Det kan blandt andet skyldes gældende regulering eller særlige ønsker til leverancen fra kundens side.

Kravkatalog
Organisationen kan udarbejde et katalog med generelle sikkerhedskrav, der kan indsættes i alle kontrakter med leverandører uanset leverancen. Kravene bør gøres generelle, så de er relevante i alle kontrakter og kan tilpasses til den konkrete leverance, hvilket bidrager til at sikre et grundlæggende sikkerhedsniveau på tværs af organisationens leverandører. Hvis organisationen anvender et klassifikationssystem, bør der udarbejdes et kravkatalog for hvert klassifikationsniveau. Organisationen kan dermed overføre sikkerhedskrav fra det relevante kravkatalog til kontrakten med leverandøren, således at sikkerhedsniveauet afspejler klassifikationsniveauet forbundet med leverancen.

Hvis opgaven skal i udbud, gælder en række særlige forhold, som kunden bør tage hensyn til. I udbudsreglerne er der blandt andet krav til, hvordan udbudsmaterialet skal udformes. Kunden bør derfor altid inddrage juridiske kompetencer i udbudsfasen.

I udarbejdelsen af udbudsmaterialet bør kunden overveje at stille udvalgte sikkerhedskrav som mindstekrav, der skal være opfyldt, før en tilbudsgiver kan komme i betragtning som leverandør. Alternativt kan kunden vælge at stille sikkerhedskravene som almindelige krav, hvilket giver tilbudsgivere bedre mulighed for at konkurrere på sikker-

heden forbundet med opgaveløsningen, såfremt kontrakten tildeles ud fra bedste forhold mellem pris og kvalitet, herunder sikkerhed. Eventuelle mindstekrav indgår derimod ikke i tilbudsevalueringen.

Det kan være hensigtsmæssigt at stille udvalgte sikkerhedskrav som mindstekrav, hvis kravene vurderes at være ufravigelige. Hvis udbuddet indeholder mange mindstekrav, kan mængden af mindstekrav dog afskrække potentielle leverandører fra at afgive et tilbud, ligesom de risikerer at få afvist deres tilbud som ukonditionsmæssigt på grund af manglende opfyldelse af mindstekrav. Desuden har kunden ikke mulighed for efterfølgende at justere i mindstekravene. Kunden bør derfor nøje overveje, hvilke krav, der eventuelt skal stilles som mindstekrav. Derudover bør det fremgår tydeligt af udbudsmaterialet, om kravene har karakter af mindstekrav eller almindelige krav.

Stil krav til leverandørens cyber- og informationssikkerhed med fokus på den ønskede effekt frem for den præcise løsning.

2.3 Vurdér behovet for rådgivning hos CFCS og anden ekstern bistand
Selvom kunden har bedst kendskab til sin forretning, herunder den underliggende it-infrastruktur og egne sikkerhedsforanstaltninger, har organisationen ikke altid de fornødne kompetencer til selv at identificere alle relevante sikkerhedskrav og øvrige bestemmelser i kontrakten. Kunden bør derfor vurdere behovet for ekstern bistand i form af eksempelvis juridisk eller it-sikkerhedsteknisk rådgivning.

Myndigheder bør søge rådgivning hos CFCS i forbindelse med udarbejdelsen af sikkerhedskrav til leverandøren ved outsourcing af kritisk it-infrastruktur eller samfundskritiske it-systemer.

Vurdér behovet for ekstern rådgivning og bistand, herunder inddragelse af CFCS, i forbindelse med udarbejdelsen af sikkerhedskrav til leverandøren.

Katalog over kontraktbestemmelser for samfundskritiske it-systemer
For statslige myndigheder med ansvar for outsourcing af samfundskritiske it-systemer gælder et nyt katalog over kontraktbestemmelser, der skal implementeres i fremtidige kontrakter efter følg-eller-forklar-princippet. Kataloget omfatter fire temaer: 1) driftsafvikling, 2) sikkerhed, 3) persondata og 4) kontrol. Kataloget findes på sikkerdigital.dk (Digitaliseringsstyrelsen 2022a).

Det er myndighedens ansvar at sikre, at katalogets bestemmelser indgår i fremtidige kontrakter med leverandører om outsourcing af samfundskritiske it-systemer. Myndigheden skal også vurdere behovet for at skærpe bestemmelserne og tilføje yderligere krav på baggrund af en risikovurdering af det pågældende it-system. Det er op til myndigheden at afgøre, om leverancen omfatter et samfundskritisk it-system. I vurderingen heraf kan myndigheden tage udgangspunkt i definitionen og hjælpespørgsmålene fra "Vejledning til model for porteføljestyring af statslige it-projekter" (Digitaliseringsstyrelsen 2021).

3. Leverandørvalg

3.1 Vælg leverandør ud fra relevante kriterier

Valget af leverandør har betydning for kvaliteten og sikkerheden forbundet med leverancen. Det er derfor vigtigt, at kunden vælger leverandør ud fra relevante kriterier og på baggrund af en grundig vurdering af leverandørens samlede evne til at opfylde kundens sikkerhedskrav og øvrige krav til opgaveløsningen. Dette har til hensigt at sikre, at leverandøren kan levere cyber- og informationssikkerhed på et tilstrækkeligt niveau i aftaleperioden og ved aftalens ophør.

Når kunden skal vælge leverandør, er der en række forhold vedrørende potentielle leverandører, som kunden bør overveje. Nedenstående liste giver et overblik over relevante forhold, som kunden kan medtage i sin vurdering af potentielle leverandører i forbindelse med leverandørvalget:

- Leverandørens evne til at levere den ønskede ydelse.
- Leverandørens evne til at leve op til de stillede sikkerhedskrav.
- Leverandørens geografiske placering.
- Leverandørens accept af eventuelle overgangsforhold, hvis opgaven tidligere har været outsourcet til en anden leverandør.
- Leverandørens villighed til at samarbejde og til at lade sig efterse/revidere.
- Leverandørens accept af ophørsbestemmelser, herunder forpligtelsen til at opretholde cyber- og informationssikkerheden i hele ophørsperioden (se afsnit 6).
- Leverandørens økonomiske forhold og ejerforhold.
- Leverandørens brug af underleverandører.
- Leverandørens integritet og eventuelle konstaterede tilfælde af væsentlig misligholdelse af tidligere offentlige kontrakter.
- Størrelses- og afhængighedsforholdet mellem kunde og leverandør.
- Risikoen for leverandørlåsning pga. omkostningerne ved senere at skifte leverandør, når kunden først er blevet afhængig af leverandørens ydelser.

Listen er ikke udtømmende, da der kan være særlige forhold forbundet med den konkrete leverance, som kunden også bør overveje i forbindelse med valget af leverandør. Flere af de nævnte forhold uddybes i det følgende.

Økonomi er som regel en væsentlig parameter, når kunden skal vælge leverandør. Ofte foretages en afvejning mellem pris og kvalitet, herunder sikkerhed, i vurderingen af potentielle leverandører. I forhold til sikkerhed bør kunden vurdere, om de sikkerhedsforanstaltninger, leverandøren forpligter sig til at levere, står i et rimeligt og realistisk forhold til prisen. Nogle leverandører vil muligvis slække på sikkerheden for at kunne give et bedre bud på prisen. Det kan derfor være en fordel at stille krav om, at prisen på sikkerheden i leverancen skal specificeres i udbud og kontrakt, så leverandøren har et økonomisk incitament til at levere det aftalte sikkerhedsniveau. Hvis den planlagte outsourcing omfatter kritisk it-infrastruktur, bør kunden generelt tillægge sikkerhed større vægt i afvejningen mellem pris og kvalitet i vurderingen af potentielle leverandører.

Kunden bør også overveje betydningen af størrelses- og afhængighedsforholdet mellem parterne for kundens mulighed for at styre leverandøren i aftaleperioden. Hvis der er tale om en lille kunde over for en stor leverandør, vil kunden alt andet lige have vanskeligere ved at stille særlige krav og efterfølgende styre leverandøren, frem for hvis det er en stor kunde over for en lille leverandør. Ved mindre leverandører skal kunden derimod være særligt opmærksom på risikoen for konkurs og ændringer i leverandørens ejerforhold i aftaleperioden. Kunden bør derfor overveje fordele og ulemper forbundet med valget af leverandør.

Kunden kan overveje, hvilket scenarie fra nedenstående figur, der bedst karakteriserer det pågældende kunde-leverandørforhold. Bemærk at figuren giver et forsimplet overblik over potentielle fordele og ulemper, der ikke nødvendigvis kan overføres direkte til et konkret kunde-leverandørforhold.

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">Kunde</th></tr>
<tr><th>Lille</th><th>Stor</th></tr>
<tr><td rowspan="2">Leverandør</td><td>Lille</td><td><u>Scenarie 1</u>: Kunden er én blandt relativt få andre kunder.
Fordele:
Kunden bliver prioriteret
God mulighed for at stille særlige krav og styre leverandøren
Ulemper:
Risiko for at leverandøren går konkurs eller skifter ejer
Begrænset udvalg af ydelser
Leverandøren har færre dokumenterede processer og procedurer</td><td><u>Scenarie 2</u>: Kunden er strategisk vigtig for leverandøren.
Fordele:
Kunden har høj prioritet
Rig mulighed for at stille særlige krav og styre leverandøren
Ulemper:
Risiko for at leverandøren går konkurs eller skifter ejer
Begrænset udvalg af ydelser
Leverandøren har færre dokumenterede processer og procedurer</td></tr>
<tr><td>Stor</td><td><u>Scenarie 3</u>: Kunden er uvæsentlig for leverandøren.
Fordele:
Valgfrihed inden for et stort udvalg af standardydelser
Leverandøren har flere dokumenterede processer og procedurer
Ulemper:
Kunden har lav prioritet
Det er vanskeligt at stille særlige krav og styre leverandøren
Risiko for leverandørlåsning</td><td><u>Scenarie 4</u>: Kunden er én blandt mange andre kunder.
Fordele:
Valgfrihed inden for et stort udvalg af standardydelser.
Leverandøren har flere dokumenterede processer og procedurer
Kunden prioriteres højere end leverandørens mindre kunder
Ulemper:
Det er vanskeligt at stille særlige krav og styre leverandøren
Risiko for leverandørlåsning</td></tr>
</table>

Figur 4. Potentielle fordele og ulemper forbundet med valget af leverandør.

Derudover bør kunden overveje leverandørens geografiske placering, da der kan være særlige forhold i udlandet, der påvirker kundens cyber- og informationssikkerhed. I visse dele af verden kan lokal lovgivning, myndigheders adgang til data, kriminalitetsraten, kulturelle forskelle, politiske forhold, naturkatastrofer og den sikkerhedspolitiske situation påvirke sikkerheden i leverancen. Eksempelvis kan der gælde særlige juridiske forhold for kunden og leverandøren, der skal tages højde for ved outsourcing til leverandører i udlandet. Derfor bør kunden blandt andet sikre, at de juridiske forhold,

som leverandøren er underlagt, ikke er i strid med kundens ønsker. Af samme grund bør kunden altid inddrage juridiske kompetencer i forbindelse med leverandørvalget.

Myndigheder skal desuden være opmærksomme på, at valget af leverandør ofte skal ske i overensstemmelse med udbudsreglerne. Myndigheder bør derfor sikre sig, at udbudsmaterialet så vidt muligt stiller relevante krav og betingelser til afhjælpning af ovenstående opmærksomhedspunkter under hensyntagen til udbudsreglerne.

Vælg leverandør ud fra relevante kriterier og på baggrund af en grundig vurdering af leverandørens samlede evne til at opfylde sikkerhedskravene og de øvrige krav til opgaveløsningen.

4. Aftalen

4.1 Aftal en klar rolle- og ansvarsfordeling med leverandøren
Når kunden har valgt eller er blevet pålagt en leverandør, skal der udarbejdes et aftalegrundlag mellem parterne. Aftalen bør sikre, at parterne kender deres roller og ansvar i forhold til at styre cyber- og informationssikkerheden i aftaleperioden. Det er vigtigt, at parternes opgaver og forpligtelser er klart defineret i aftalegrundlaget, så der ikke efterfølgende opstår tvivl om ansvarsfordelingen mellem parterne.

I aftalen bør det være klart for leverandøren, hvilke forventninger kunden har til leverandørens cyber- og informationssikkerhed. Sikkerhedskravene bør skrives ind i kontrakten, så de kan håndhæves på lige fod med andre krav i kontrakten. Hvis opgaven har været i udbud, bør kontrakten indeholde de sikkerhedskrav, der blev stillet i udbudsmaterialet, samt eventuelle ændringer som følge af leverandørens tilbud.

Aftalen bør også beskrive, hvordan det i aftaleperioden sikres, at leverandøren lever op til de fastsatte sikkerhedskrav. Bestemmelserne i aftalen bør blandt andet omfatte leverandørens forpligtelser i forhold til dokumentation og rapportering til kunden samt kundens ret til - enten selv eller ved hjælp af en tredjepart - at føre kontrol med leverandørens efterlevelse af kontrakten. Aftalen bør forpligte leverandøren til at afsætte de fornødne ressourcer til rapportering og kontrol, herunder tid til mødeforberedelse, udarbejdelsen af dokumentation og opfølgning.

Kundens ret til at føre kontrol med leverandøren bør omfatte alle forhold relateret til leverandørens opfyldelse af kontrakten, herunder forhold hos eventuelle underleverandører, der bidrager til opgaveløsningen. Kontrollen med leverandøren kan udføres på flere forskellige måder (se eksempler i afsnit 5 om styring). Leverandøren bør desuden være forpligtet til at bistå kunden i forbindelse med gennemførelsen af kontrollen, herunder ved at give kunden den fornødne fysiske og logiske adgang til leverandørens lokaliteter, it-systemer og data samt ved at udlevere alt relevant dokumentation.

Det er ikke altid de samme medarbejdere hos kunden og leverandøren, der har udarbejdet kontrakten, som har det efterfølgende driftsansvar, når samarbejdet går i gang. Efter indgåelsen af kontrakten bør parternes driftsansvarlige derfor afholde et opstartsmøde for at fastsætte de nærmere detaljer og drøfte eventuelle uklarheder i aftalen. Forventningsafstemningen kan bidrage til at sikre enighed om parternes respektive roller og forpligtelser samt forebygge misforståelser og tvister i aftaleperioden.

Aftal en klar rolle- og ansvarsfordeling med leverandøren i forhold til parternes styring af cyber- og informationssikkerhed i kunde-leverandørforholdet.

4.2 Etablér en samarbejdsorganisation og proces for dialog med leverandøren
Aftalen bør etablere en samarbejdsorganisation og formaliseret proces for håndtering af dialogen mellem kunde og leverandør. Processen bør fastlægge den daglige dialog mellem parterne, eskalationsveje til at løse eventuelle tvister og kommunikationsveje i tilfælde af, at der sker en sikkerhedshændelse eller opstår en beredskabssituation.

Kunden og leverandøren bør etablere en samarbejdsorganisation, som forankrer samarbejdet mellem parterne i en eller flere faste samarbejdsfora og dermed sikrer kontinuitet i dialogen. Denne samarbejdsorganisation bør etableres med udgangspunkt i kundens behov ud fra en vurdering af relevante parametre såsom it-systemernes kritikalitet, den samlede kontraktværdi og leverancens strategiske betydning for kundens forretning (se også afsnit 5 om styring).

Samarbejdsorganisationen kan eksempelvis bestå af en styregruppe og eventuelt en eller flere underliggende arbejdsgrupper, som enten er midlertidige eller permanente. I disse samarbejdsfora mødes relevante repræsentanter fra begge parter - eksempelvis på drifts- eller ledelsesniveau - regelmæssigt for at drøfte status for leverancen, herunder fremskridt, aktuelle problemstillinger og eventuelle ændringsforslag. Aftalen bør beskrive de enkelte samarbejdsforas sammensætning og ansvar, herunder deres mødefrekvens og dagsorden, hvor sikkerhed bør være et fast dagsordenspunkt.

Aftalen bør give begge parter mulighed for løbende at tilpasse sikkerhedsniveauet i kunde-leverandørforholdet.

Kunden bør desuden overveje, hvilke styringsmuligheder parterne skal have i forhold til løbende at kunne tilpasse cyber- og informationssikkerheden i leverancen. Forhold hos både kunden og leverandøren kan ændre sig og dermed introducere nye risici, ligesom trusselsbilledet er foranderligt. Aftalen bør derfor give parterne mulighed for løbende at justere sikkerhedsniveauet i takt med at risikobilledet ændrer sig, eksempelvis ved at kunden stiller supplerende sikkerhedskrav til leverandøren. Dog bør aftalen sikre, at kunden skal godkende eventuelle justeringer hos leverandøren og dermed i sidste ende fastsætte sikkerhedsniveauet forbundet med leverancen.

Etablér en samarbejdsorganisation og formaliseret proces for håndtering af dialogen med leverandøren, som både omfatter den daglige dialog og kommunikation i tilfælde af sikkerhedshændelser og i en beredskabssituation.

5. Styring

5.1 Dokumentér organisationens behov for at kontrollere leverandøren
Der kan være stor forskel på, hvor ofte og udførligt kunden har behov for at føre kontrol med sine leverandører. Omfanget og frekvensen af kontrollen bør derfor bero på en konkret vurdering af leverancens væsentlighed i forhold til kundens forretning og risici forbundet hermed. Denne vurdering bør dokumenteres og opdateres løbende afhængig af den konkrete leverance og eventuelle ændringer i risikobilledet.

Hvis kunden har flere leverandører, bør leverandørerne rangeres ud fra, hvor forretningskritiske de er. Kunden bør føre grundigere og hyppigere kontrol med de vigtigste leverandører på baggrund af en risikovurdering. Kunden kan udarbejde en prioriteret liste over leverandørerne ved at foretage en risikovurdering med udgangspunkt i relevante parametre såsom:

- Følsomheden og mængden af kundens informationer omfattet af leverancen.
- Om leverancen omfatter kundens forretningskritiske it-systemer eller processer.
- Om leverancen omfatter kritisk it-infrastruktur eller samfundskritiske it-systemer.
- Om der er tale om en standardiseret eller specialiseret leverance.
- Datas geografiske placering (hos kunden eller leverandøren, i ind- eller udland).
- Leverancens karakter, herunder leverandørens driftsansvar og adgangsrettigheder i forhold til kundens data (adgang til at se og/eller redigere i data).
- Den samlede kontraktværdi.
- Mængden af fejl og mangler i leverancen samt hændelser hos leverandøren.
- Leverandørens vilje til at samarbejde med kunden og kundens leverandører.

På baggrund heraf kan kunden udarbejde en tilsynsplan for sine leverandører og foretage en ressourcemæssig prioritering ved at fokusere på organisationens kritiske leverandører i udførelsen af kontrollen, så kundens leverandørstyring bliver risikobaseret og dermed giver størst mulig værdi.

Dokumentér organisationens behov for at føre kontrol med leverandøren.

Risici ved utilstrækkelig leverandørstyring
Manglende eller utilstrækkelig leverandørstyring kan blandt andet føre til:

- Utilstrækkelig risikohåndtering hos leverandøren.
- Flere fejl, forsinkelser og mangler i leverancen.
- Leverandørens manglende overholdelse af kontrakten.
- Kundens manglende håndhævelse af kontrakten.
- Leverandørens nedprioritering af kunden til fordel for andre kunder.
- Stigende leverandørafhængighed.

5.2 Udpeg en ansvarlig for den sikkerhedsmæssige leverandørstyring
Cyber- og informationssikkerhed er en integreret del af kundens leverandørstyring. Kunden bør derfor udpege en dedikeret rolle i organisationen med ansvar for at kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten (se bilag 4). Det er vigtigt, at rollen har de fornødne styringsmæssige og sikkerhedstekniske kompetencer til at udføre kontrollen og vurdere leverandørens opfyldelse af kravene. Da leverandørstyring er en tværfaglig opgave, der forudsætter kompetencer inden for bl.a. jura, økonomi, it og sikkerhed, bør rollen inddrage relevante medarbejdere fra andre afdelinger og funktioner i organisationen under udførelsen af kontrollen efter behov.

Kunden bør desuden sikre, at leverandøren ligeledes udpeger en rolle i sin organisation med ansvar for at varetage cyber- og informationssikkerheden forbundet med leverancen. Rollen bør blandt andet fungere som kundens kontaktperson ved forhold vedrørende cyber- og informationssikkerhed, herunder i forbindelse med kundens kontrol med leverandøren og i tilfælde af sikkerhedshændelser i aftaleperioden.

Udpeg en dedikeret rolle med ansvar for organisationens leverandørstyring i forhold til opfyldelsen af sikkerhedskravene i kontrakten.

5.3 Før kontrol med leverandørens efterlevelse af sikkerhedskrav efter behov
Når aftalen mellem parterne er underskrevet, og samarbejdet går i gang, bør kunden løbende kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten efter behov. Leverandørstyring giver kunden mulighed for at håndhæve kontrakten og bidrager dermed til at sikre, at leverandøren leverer den aftalte leverance og overholder sine forpligtelser i aftaleperioden.

Kunden bør altid styre leverandøren med udgangspunkt i kontrakten mellem parterne. Kontrakten bør derfor indgå aktivt i kundens leverandørstyring. Kunden kan f.eks. udvælge de sikkerhedskrav i kontrakten, som det er mest relevant at kontrollere leverandørens efterlevelse af, på baggrund af en risikovurdering. Hvis leverandøren ikke lever op til sikkerhedskravene, er det vigtigt, at kunden straks følger op på leverandørens afvigelser fra de aftalte krav og håndhæver kontrakten. Det er kundens ansvar at påpege leverandørens manglende efterlevelse af kravene og kontrollere, at leverandøren efterfølgende træffer de fornødne sikkerhedsforanstaltninger og udbedrer eventuelle fejl eller mangler i overensstemmelse med kontrakten. Kunden bør også sikre, at den gennemførte kontrol dokumenteres af hensyn til eventuel håndhævelse af kontrakten.

Eksempler på kontrol og opfølgning hos leverandøren
Kundens kontrol med leverandøren kan foregå på forskellige måder og omfatte flere former for dokumentation og rapportering. Leverandørens dokumentation kan blandt andet bestå af skriftlige rapporter, erklæringer, risikovurderinger og styringsdokumenter. Derudover kan kontrollen omfatte en række aktiviteter såsom:

- Statusmøder mellem kunde og leverandør (faste møder eller ad hoc).
- Skriftlig rapportering til kunden (fast afrapportering eller ved anmodning).
- Tilsyn hos leverandøren (enten varslet eller uanmeldt besøg).
- Intern audit/gennemgang eller egenkontrol foretaget af leverandøren.
- Ekstern audit/gennemgang foretaget af kunden eller en uvildig tredjepart.
- It-revision foretaget af certificerede revisorer.
- Beredskabsøvelser med kunden som deltager eller observatør.
- Sikkerhedstekniske undersøgelser (også kaldet penetrationstests).

Leverandørens rapportering og kundens kontrol med leverandøren skal gennemføres som beskrevet i aftalen. Det forudsætter, at parterne afsætter den fornødne tid til blandt andet forberedelse, dokumentation og opfølgning. Hvis parterne regelmæssigt holder statusmøder, bør sikkerhed være et fast dagsordenspunkt på disse møder. Der bør også altid tages referat ved vigtige møder, som godkendes af begge parter.

Desuden kan kunden overveje behovet for at inddrage en tredjepart under udførelsen af kontrollen med leverandøren. Myndigheder og virksomheder kan i visse situationer henvende sig til Digitaliseringsstyrelsen eller CFCS for rådgivning om leverandørstyring, herunder hjælp til at identificere relevante sikkerhedskrav i eksisterende kontrakter og kontrollere leverandørens efterlevelse heraf.

Før løbende kontrol med leverandørens opfyldelse af sikkerhedskravene i kontrakten efter behov og på baggrund af en risikovurdering.

5.4 Gennemfør løbende risikovurderinger med input fra leverandøren
Kunden bør løbende gennemføre risikovurderinger for at afdække, om sikkerhedsniveauet i kunde-leverandørforholdet skal justeres som følge af ændringer i risikobilledet. Risikovurderingen bør opdateres minimum årligt samt ved væsentlige sikkerhedshændelser, væsentlige ændringer (se afsnit 5.5.) og på baggrund af tilsyn med leverandøren. Herefter bør parterne aftale handleplaner for deres fælles risikohåndtering. Kunden bør følge op på, at de fælles risikohåndteringsplaner realiseres som aftalt.

Kunden bør sikre, at leverandøren samarbejder med kunden i udarbejdelsen af risikovurderingerne. Her bør kunden være opmærksom på parternes roller i forhold til risikostyring, og hvad de hver især kan bidrage med. Kunden bør tage stilling til de forretningsmæssige konsekvenser ved brud på informationers fortrolighed, integritet eller tilgængelighed. På baggrund af risikovurderingen bør kunden også afgøre, hvilke risici der accepteres, og hvordan ressourcerne prioriteres i forhold til håndteringen af risici.

Leverandøren bør bidrage til kundens forretningsmæssige risikovurdering ved at gennemføre risikovurderinger af leverancen med input fra eventuelle underleverandører i

forsyningskæden (se bilag 2). Leverandøren kan især bidrage til at identificere relevante risici og vurdere deres sandsynlighed og tekniske konsekvenser. Det skyldes, at leverandøren har større kendskab til egne sikkerhedsforanstaltninger og it-infrastrukturen, der understøtter leverancen. Kunden bør derfor sikre, at leverandøren bidrager med viden om relevante trusler og sårbarheder til kundens risikovurdering.

Gennemfør løbende risikovurderinger med input fra leverandøren og eventuelle underleverandører.

5.5 Følg op på eventuelle væsentlige ændringer og sikkerhedshændelser
I aftaleperioden kan der ske både uforudsete og planlagte ændringer hos kunden, leverandøren eller i deres omgivelser, som påvirker cyber- og informationssikkerheden forbundet med leverancen. Det er derfor vigtigt, at begge parter bidrager til at vedligeholde sikkerhedsniveauet i kunde-leverandørforholdet. Parterne bør løbende vurdere, dokumentere og håndtere væsentlige ændringer i aftaleperioden som en del af deres styring af cyber- og informationssikkerhed. Kunden bør sikre, at leverandøren følger rettidigt op på eventuelle ændringer ved at foretage fornødne justeringer og træffe supplerende sikkerhedsforanstaltninger i henhold til aftalen.

Der kan blandt andet ske ændringer i parternes organisation, forretningsprocesser og it-infrastruktur i aftaleperioden. Kunden bør være særlig opmærksom på forhold hos leverandøren, der kan påvirke sikkerheden i leverancen, såsom ændringer i leverandørens forretningsstrategi, økonomiske forhold og brug af underleverandører. I forhold til omgivelserne bør kunden især være opmærksom på den teknologiske udvikling, forandringer i trusselsbilledet og ændringer i den regulering, som parterne er underlagt.

Derudover bør kunden sikre, at leverandøren håndterer eventuelle sikkerhedshændelser i aftaleperioden i overensstemmelse med kontrakten. I aftaleperioden kan der desuden opstå behov for at opdatere aftalegrundlaget mellem parterne som følge af eventuelle ændringer. Kunden bør derfor gennemgå kontrakten med leverandøren minimum årligt for at sikre, at aftalen stadig opfylder kundens sikkerhedsbehov.

Håndtér eventuelle sikkerhedshændelser og væsentlige ændringer hos kunden, leverandøren eller i omgivelserne, der kan påvirke sikkerheden i leverancen.

6. Afslutning

6.1 Bevar cyber- og informationssikkerheden under hele afviklingsforløbet
Når aftalen ophører, bør kundens cyber- og informationssikkerhed bevares under afviklingen af kunde-leverandørforholdet. Dette gælder uanset om driften overdrages til en anden leverandør, eller om kunden vælger at overtage driftsopgaven (insourcing).

Ved indgåelsen af aftalen med leverandøren bør kunden sikre sig, at ophørsbestemmelserne i aftalen som minimum omfatter følgende forhold:

- Leverandørens forpligtelser og fortsatte servicemål i ophørsperioden, hvis aftalen frivilligt opsiges eller ophører som følge af tvister mellem parterne.
- Kundens krav til cyber- og informationssikkerhed i kunde-leverandørforholdet, mens opgaven overdrages til en anden leverandør eller overtages af kunden.
- En komplet liste over kundens aktiver (inklusiv backup) opbevaret hos leverandøren, der skal leveres tilbage til kunden, overdrages til en ny leverandør eller bortskaffes.
- Procedurer, der sikrer, at kundens aktiver leveres tilbage til kunden, overdrages til en anden leverandør eller bortskaffes, som beskrevet i aftalen.
- Parternes fortsatte tavshedspligt efter aftalens ophør.
- Leverandørens forpligtelse til at bidrage til en smidig overgang og videreførelse af driften, hvis opgaven skal i genudbud, overdrages til en ny leverandør eller hjemtages af kunden, herunder krav til leverandørens udlevering af dokumentation, overførsel af viden og samarbejde i overgangsperioden.

Derudover bør kunden og leverandøren udarbejde en plan for, hvordan det aftalte sikkerhedsniveau opretholdes under hele afviklingsforløbet. Planen bør beskrive de sikkerhedsforanstaltninger, der skal være til stede hos parterne, hvis driften føres tilbage til kunden eller overdrages til en ny leverandør. Kunden kan også vælge at udpege en rolle i organisationen med ansvar for at sikre, at kunde-leverandørforholdet afvikles i overensstemmelse med den aftalte plan for samarbejdets ophør, og at afviklingen er tilstrækkelig dokumenteret, inden samarbejdet formelt afsluttes.

Ved ophøret af samarbejdet med leverandøren bør kunden også sørge for rettidigt at fjerne alle leverandørens fysiske og logiske adgangsrettigheder til kundens aktiver, herunder kundens informationer, it-systemer og lokaliteter. Af kontrakten bør det fremgå, hvilke aktiver der skal leveres tilbage til kunden, bortskaffes eller overdrages til en ny leverandør. Aftalen bør ligeledes beskrive procedurer til at sikre leverandørens forsvarlige overdragelse og bortskaffelse af kundens aktiver med hensyn til format, fuldstændighed, dokumentation, verificering, sikkerhed med mere.

Parterne kan desuden aftale, at leverandøren fortsat opbevarer visse informationer for kunden i en periode efter samarbejdets formelle ophør. Leverandøren kan eksempelvis opbevare logfiler indsamlet i aftaleperioden, så det fortsat er muligt at foretage undersøgelser af potentielle it-sikkerhedshændelser hos leverandøren. I så fald bør kunden

tage stilling til, hvilke informationer leverandøren fortsat skal opbevare, og hvor længe disse informationer skal opbevares, inden de slettes eller overdrages til kunden.

Bevar cyber- og informationssikkerheden under afviklingen af kunde-leverandørforholdet.

Referencer

Center for Cybersikkerhed og Digitaliseringsstyrelsen (2020). *Vejledning i anvendelse af cloudservices.* https://digst.dk/data/vejledning-til-anvendelse-af-cloudservices/

Center for Cybersikkerhed (2017). *Undersøgelsesrapport: Outsourcing – hvem har ansvaret?.* https://www.cfcs.dk/da/cybertruslen/rapporter/arkiv/outsourcing---hvem-har-ansvaret/

Center for Cybersikkerhed (2019). *Trusselsvurdering: Cyberangreb mod leverandører.* https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/leverandorer/

Center for Cybersikkerhed (2020). *Trusselsvurdering: Cybertruslen mod it-serviceudbydere.* https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/it-serviceudbydere/

Digitaliseringsstyrelsen, Kommunernes Landsforening og Danske Regioner (2018). L*everandørstyring – en rejsefortælling om krav og opfølgning på sikkerhed.* https://www.sikkerdigital.dk/media/8785/leverandoerstyring-en-rejsefortaelling-om-krav-og-opfoelgning-paa-sikkerhed.pptx

Digitaliseringsstyrelsen (2016). *Klausuler til informationssikkerhed.* https://digst.dk/Styring/Standardkontrakter/Klausuler-til-informationssikkerhed

Digitaliseringsstyrelsen (2017). *Sådan stiller du krav til leverandører om informationssikkerhed – katalog.* https://digst.dk/styring/standardkontrakter/klausuler-til-informationssikkerhed/kravkatalog-til-leverandoerer/

Digitaliseringsstyrelsen (2020a). Vejledning til risikostyring inden for informationssikkerhed. https://sikkerdigital.dk/media/6835/vejledning_til_risikostyring-_nden_for_informationssikkerhed_2020.pdf

Digitaliseringsstyrelsen (2020b). *K04 Standardkontrakt for it-drift.* https://digst.dk/styring/standardkontrakter/k04-standardkontrakt-for-it-drift/

Digitaliseringsstyrelsen (2021). *Vejledning til model for porteføljestyring af statslige it-systemer.* https://digst.dk/styring/systemstyring/dokumenter-vejledninger-og-vaerktoejer/

Digitaliseringsstyrelsen (2022a). *Katalog over kontraktbestemmelser for samfundskritiske it-systemer.* https://sikkerdigital.dk/Media/637819816667401542/Katalog%20over%20kontraktbestemmelser_2022_web.pdf

Digitaliseringsstyrelsen (2022b). *Appendiks I: Tilføjelser til operationaliseringer af kontraktbestemmelser.* https://sikkerdigital.dk/Media/637819816660682223/Appendiks%20I%20-%202022.pdf

Finansministeriet (2017). *Vejledning om tilsynet med Statens It.* https://fm.dk/udgivelser/2017/december/vejledning-om-tilsynet-med-statens-it/

ISO/IEC 27036-1:2014 Informationssikkerhed – Sikkerhedsteknikker – Informationssikkerhed for leverandørrelationer – Del 1: Oversigt og begreber

ISO/IEC 27036-2:2014 Informationssikkerhed – Sikkerhedsteknikker – Informationssikkerhed for leverandørrelationer – Del 2: Krav

Bilag 1: Rammeaftaler

Udbud og anskaffelse af it gennem rammeaftaler
Myndigheder anvender ofte rammeaftaler gennem Staten og Kommunernes Indkøbsservice (SKI) eller Statens Indkøb (SI) i forbindelse med udbud og anskaffelse af it. En rammeaftale angiver hvilke varer eller ydelser, der kan købes på aftalen, på hvilke vilkår og betingelser samt til hvilken pris. Det er enten frivilligt eller forpligtende for myndigheder at benytte disse rammeaftaler.

Selvom kunden anvender en rammeaftale gennem SKI eller SI, er det altid kundens ansvar at kontrollere leverandørens efterlevelse af leveranceaftalen.

En af fordelene ved rammeaftaler er, at myndighedens udbudsforpligtelse løftes af SKI eller SI. Ud fra en række kriterier indgår SKI/SI en rammeaftale med en eller flere leverandører, som myndigheder kan benytte via rammeaftalen. Ved rammeaftaler med flere leverandører foregår kundens valg af leverandør enten ved direkte tildeling ud fra en vurdering af prisen og eventuelt kvaliteten af leverandørernes tilbud, eller gennem et miniudbud, hvor kunden kan stille supplerende krav til de prækvalificerede leverandører fra rammeaftalen. Myndigheden kan dog være forpligtet til at købe ind på en eneleverandøraftale, hvor myndigheden skal anvende en bestemt leverandør.

Nedenstående figur viser opgave- og ansvarsfordelingen mellem SKI/SI, kunden og leverandøren ved anvendelse af rammeaftaler i forbindelse udbud og anskaffelse af it.

SKI/SI	Kunde	Leverandør
• Indgår rammeaftale med en eller flere leverandører • Løfter kundens udbudsforpligtelse • Kontrollerer leverandørens efterlevelse af rammeaftalen, herunder sikkerhedskrav • Varetager kontraktstyring af rammeaftalen	• Vælger en leverandør fra rammeaftalen • Indgår en leveranceaftale med leverandøren på baggrund af rammeaftalen • Kontrollerer leverandørens efterlevelse af leveranceaftalen, herunder sikkerhedskrav	• Løser opgaven på vegne af kunden • Står til ansvar over for både SKI/SI og kunden i forhold til overholdelsen af henholdsvis ramme- og leveranceaftale

Figur 5. Fordeling af opgaver og ansvar ved outsourcing via rammeaftaler.

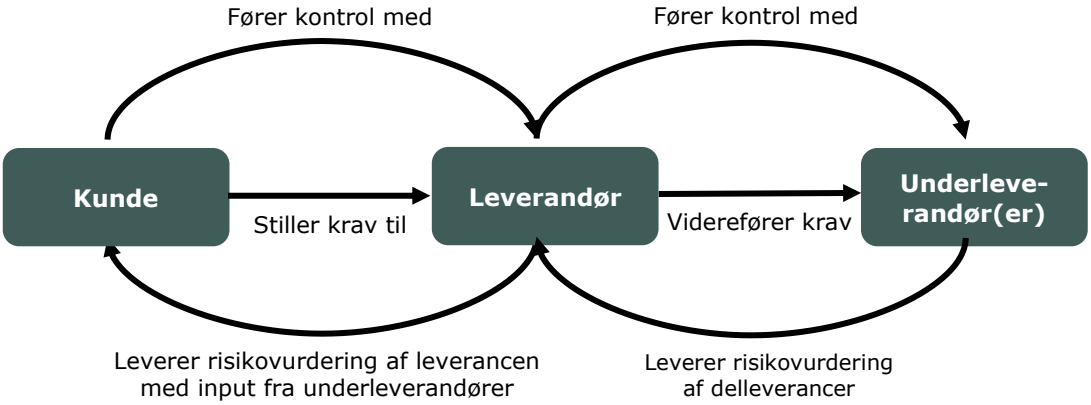
Selvom myndigheden benytter en rammeaftale, er det myndighedens ansvar at tildele kontrakten til den rette leverandør blandt leverandørerne på aftalen. Efterfølgende skal kunden også indgå en leveranceaftale med leverandøren på baggrund af rammeaftalen. Det er alene kundens ansvar at kontrollere leverandørens efterlevelse af denne leveranceaftale. Dette gælder uanset om der er tale om en forpligtende eller frivillig rammeaftale. Ved tvivlsspørgsmål bør kunden søge rådgivning hos SKI eller SI.

Bilag 2: Husk forsyningskæden

Hold styr på underleverandører i forsyningskæden ved outsourcing
Selvom kunden har valgt at outsource organisationens it til en specifik leverandør, vil leverandøren ofte anvende underleverandører i forbindelse med leverancen. Hvis leverandøren overlader dele af opgaveløsningen til en eller flere underleverandører, svækkes kundens kontrol med leverancen, og der opstår nye cyber- og informationssikkerhedsrisici for kunden. Det er derfor vigtigt, at kunden har overblik over forsyningskæden og tager stilling til risici forbundet med leverandørens brug af underleverandører.

Ved indgåelsen af aftalen med leverandøren bør kunden sikre, at der er taget højde for leverandørens eventuelle brug af underleverandører. Det bør fremgå af kontrakten, at kunden skal godkende leverandørens anvendelse af underleverandører i forbindelse med leverancen, og at leverandøren er forpligtet til at oplyse kunden herom. Derudover bør kundens krav til leverandørens cyber- og informationssikkerhed ligeledes gælde for de underleverandører, som leverandøren måtte benytte i forbindelse med leverancen. Det bør derfor også fremgå af kontrakten mellem kunde og leverandør, at leverandøren er forpligtet til som minimum at overføre de samme sikkerhedskrav og forpligtelser til eventuelle kontrakter med underleverandører relateret til leverancen.

Hvis leverandøren efter kundens godkendelse har overdraget dele af opgaveløsningen til en underleverandør, er det leverandørens ansvar at føre kontrol med de delleverancer, som underleverandøren leverer til kunden. Kunden bør derfor sikre, at kontrakten med leverandøren forpligter leverandøren til at føre kontrol med eventuelle underleverandørers opfyldelse af sikkerhedskravene og de øvrige krav fra den oprindelige kontrakt mellem kunde og leverandør. Af kontrakten bør det også fremgå, at leverandøren skal dokumentere udførte tilsyn med underleverandører over for kunden. Nedenstående figur illustrerer forholdet mellem kunde, leverandør og eventuelle underleverandører i forsyningskæden.



Figur 6. Forholdet mellem kunde, leverandør og underleverandør

Kunden bør sikre, at leverandøren fører tilstrækkelig kontrol med underleverandørernes overholdelse af de sikkerhedskrav, der stammer fra kontrakten mellem kunde og leverandør. Derudover bør kunden foretage en forretningsmæssig risikovurdering, der omfatter leverandører og eventuelle underleverandører i forsyningskæden. Kunden bør sikre, at leverandøren leverer risikovurderinger af leverancen til kundens forretningsmæssige risikovurdering med input fra underleverandører om relevante risici.

Bilag 3: Outsourcing til Statens IT

Særlige forhold ved outsourcing til Statens It
Statens It (SIT) varetager it-driften for mange statslige myndigheder, der har overdraget driftsansvaret til SIT ved kongelig resolution. Myndigheder kan vælge mellem en række forskellige driftsmodeller på systemniveau, der beskriver opgave- og ansvarsfordelingen mellem myndigheden og SIT ud fra de enkelte lag i teknologistakken. Her bør myndigheden vælge driftsmodellen med den mest hensigtsmæssige opgave- og ansvarsfordeling, hvilket blandt andet afhænger af organisationens forretningsbehov, sikkerhedstekniske kompetencer og risikoappetit.

For de statslige myndigheder, hvor ansvaret for organisationens it og driften heraf er ressortoverdraget til SIT, er tilsynet med SIT overgået til Finansministeriet (FM). FM's departement fører derfor blandt andet tilsyn med SIT's styring af cyber- og informationssikkerheden og deler resultaterne heraf med SIT's kunder. Dét fritager som udgangspunkt myndighederne for selv at føre tilsyn med SIT. I stedet bør myndighederne forholde sig til, om FM's løbende tilsynsrapporter og årlige tilsynsberetning fremhæver relevante risici eller indeholder bemærkninger til sikkerhedsniveauet hos SIT, der har betydning for sikkerheden forbundet med deres outsourcede it-systemer.

Afhængig af den valgte driftsmodel kan der være dele af teknologistakken, som ikke er omfattet af FM's tilsyn. I så fald vil denne tilsynsopgave påhvile den enkelte myndighed. Myndigheden bør derfor sørge for at føre tilsyn med SIT på de områder, hvor myndigheden selv har ansvaret for tilsynet. Derudover skal myndigheden sikre, at der følges op på de områder, som myndigheden selv har ansvaret for. Den præcise opgave- og ansvarsfordeling mellem FM og myndigheden i forhold til tilsynet med SIT ved de forskellige driftsmodeller er beskrevet i "Vejledning om tilsynet med Statens It" (Finansministeriet 2017). Da FM har overtaget tilsynsopgaven, bør myndigheden også orientere FM's departement, hvis SIT's risikohåndtering vurderes at være utilstrækkelig, eller der i aftaleperioden opstår tvister mellem SIT og myndigheden om konkrete forhold i kontrakten.

Selvom myndigheder kan være forpligtet til at outsource it-driften til SIT eller en anden myndighed, gælder anbefalingerne i vejledning som udgangspunkt fortsat. Ved outsourcing til SIT bør myndigheden også foretage en risikovurdering af det pågældende it-system. På baggrund heraf bør myndigheden vurdere, om sikkerhedsforanstaltningerne beskrevet i SIT's såkaldte varedeklaration tilsammen sikrer et tilstrækkeligt sikkerhedsniveau, eller om der er behov for yderligere sikkerhedsforanstaltninger.

Hvis myndigheden vurderer, at et it-system påkræver særlige sikkerhedsforanstaltninger, som ikke er dækket af SIT's standard sikkerhedsniveau, bør myndigheden stille yderligere krav herom til SIT. Herefter aftaler parterne, hvordan SIT skal opfylde og dokumentere opfyldelsen af disse yderligere sikkerhedskrav. Her bør myndigheden være opmærksom på, at eventuelle krav vedrørende særlige sikkerhedsforanstaltninger ikke er omfattet af FM's tilsyn. I stedet har myndigheden selv ansvaret for at kontrollere SIT's opfyldelse af de særlige sikkerhedskrav. Myndigheden bør derfor vurdere behovet for at følge op på disse krav og som minimum kræve skriftlig afrapportering.

Bilag 4: Roller og ansvar

Roller og ansvar i organisationen ved outsourcing

Herunder ses et eksempel på opgave- og ansvarsfordelingen mellem udvalgte roller, som generelt bør indgå i organisationens styring af cyber- og informationssikkerheden i et kunde-leverandørforhold ved outsourcing. Dertil kommer en række vigtige støttefunktioner såsom HR og Økonomi, der også bør inddrages i organisationens samarbejde med leverandøren. Listen over opgaver og ansvar er ikke udtømmende.

Roller	Opgaver og ansvar
Ledelsen	• Overordnet ansvarlig for organisationens styring af cyber- og informationssikkerhed, herunder den interne organisering, etablering af et ledelsessystem (ISMS) og fastsættelse af organisationens sikkerhedsniveau. • Ansvarlig for de strategiske beslutninger vedrørende outsourcing. • Skal godkende relevante styringsdokumenter såsom en politik for organisationens styring af cyber- og informationssikkerhed ved outsourcing. • Skal sikre, at organisationen har de fornødne ressourcer og kompetencer til leverandørstyring og styring af cyber- og informationssikkerhed. • Skal vurdere organisationens behov for ekstern rådgivning og bistand ved udarbejdelsen af kontrakten og den efterfølgende leverandørstyring. • Skal godkende risikovurderinger og risikohåndteringsplaner.
Informationssikkerhedskoordinator / it-sikkerhedsansvarlig	• Daglig ansvarlig for organisationens styring af cyber- og informationssikkerhed, herunder den tværgående koordination og kommunikation. • Skal sikre sammenhæng mellem sikkerhedskravene i kontrakten og organisationens politikker, procedurer og retningslinjer for cyber- og informationssikkerhed. • Skal sikre, at der føres tilstrækkelig kontrol med leverandørens efterlevelse af sikkerhedskravene i kontrakten. • Skal sikre, at der løbende gennemføres risikovurderinger og udarbejdes risikohåndteringsplaner i forbindelse med outsourcing.
Kontraktansvarlig	• Ansvarlig for den generelle styring og håndhævelse af kontrakten. • Skal sikre, at kontrakten opdateres ved ændringer i aftalegrundlaget. • Skal sikre, at leverandøren udbedrer evt. fejl og mangler i leverancen. • Skal håndtere evt. tvister med leverandøren og eskalere til ledelsen efter behov.
Jura	• Ansvarlig for organisationens efterlevelse af de udbudsretlige regler og overholdelse af andre relevante lov- og myndighedskrav ved outsourcing. • Skal bistå med juridisk rådgivning i forbindelse med outsourcing, herunder juridisk kvalitetssikring af sikkerhedskrav og kontrakten som helhed.
System- og dataejere	• Ansvarlig for cyber- og informationssikkerheden forbundet med it-systemer og data ved outsourcing, herunder leverandørstyring. • Skal klassificere it-systemer og data omfattet af kontrakten. • Skal identificere relevante sikkerhedskrav i kontrakten med udgangspunkt i organisationens sikkerhedsniveau og klassifikationssystem. • Skal kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten og følge op på eventuelle sikkerhedshændelser hos leverandøren. • Skal styre leverandørens adgang til organisationens it-systemer og data. • Skal gennemføre risikovurderinger i forbindelse med outsourcing og udarbejde risikohåndteringsplaner.
It-ansvarlig	• Skal bistå med teknisk rådgivning i forbindelse med outsourcing, herunder hjælp til at identificere relevante sikkerhedskrav i kontrakten.
Databeskyttelsesrådgiver (DPO)	• Skal bistå med rådgivning om beskyttelse af personoplysninger i forbindelse med outsourcing, herunder hjælp til at identificere relevante krav til databeskyttelse i kontrakten. • Skal kontrollere organisationens efterlevelse af databeskyttelsesreglerne. • Skal bistå med rådgivning ved indgåelse af en databehandleraftale med leverandøren og overvåge overholdelsen heraf i kontraktperioden.

Bilag 5: Stil bedre sikkerhedskrav

Stil smarte sikkerhedskrav til leverandøren
I udarbejdelsen af sikkerhedskrav til leverandøren kan kunden tage udgangspunkt i SMART-princippet (Specifik, Målbar, Anvisende, Relevant og Tidsbestemt). Tilsammen bidrager SMART-kriterierne til, at både tilbudsevalueringen i forbindelse med valget af leverandør og den efterfølgende leverandørstyring bliver lettere for kunden. De fem kriterier er tilpasset konteksten og uddybet med eksempler herunder.

- **Specifik: kravene bør være konkrete og formuleres klart og præcist, så det er tydeligt for leverandøren, hvordan kravene opfyldes.**

Undgå generelle og ukonkrete krav såsom *"Leverandøren skal foretage backup af systemet".* Stil klare og præcise krav, der er tilpas specifikke, eksempelvis ved at konkretisere omfanget og frekvensen af backuppen samt antallet af opbevarede sikkerhedskopier hhv. online og offline.

- **Målbar: leverandørens opfyldelse af kravene bør kunne måles, dokumenteres og evalueres.**

Undgå så vidt muligt krav, der efterlader et stort skøn i vurderingen af leverandørens opfyldelse og dermed ikke egner sig til opfølgning, såsom *"Leverandøren skal foretage tilstrækkelig logning".* Stil konstatérbare og entydige krav, som begge parter har let ved at vurdere opfyldelsen af. Eksempelvis ved at stille krav, der let kan dokumenteres og eventuelt kan besvares binært (ja/nej).

- **Anvisende: kravene bør være handlingsanvisende for leverandøren.**

Undgå lange, komplicerede og usammenhængende krav, der indeholder mange delkrav og helt eller delvist overlapper med andre krav. Formulér korte, konsistente og handlingsanvisende krav, der indledes med *"Leverandøren skal…".* Opdel eventuelt delkrav i separate krav uden overlap.

- **Relevant: kravene bør tilpasses den konkrete leverance, bygge på en risikovurdering og hænge sammen med kundens klassifikationssystem og fastsatte sikkerhedsniveau.**

Vær forsigtig med at genbruge krav fra gamle kontrakter, da kravene kan være forældede og irrelevante ift. den aktuelle kontrakt. Stil krav på baggrund af en risikovurdering, så kravene bidrager til at imødegå konkrete risici ved den planlagte outsourcing. Sørg også for at tilpasse "standardkrav" taget fra kravkataloger, rammeværker og standarder såsom ISO, NIST, CIS og SANS. Medtag gerne referencer til de specifikke sikkerhedskontroller, som kravene eventuelt svarer til.

- **Tidsbestemt: kravene bør fastsætte frekvenser eller indeholde præcise tidsangivelser for leverandørens aktiviteter og servicemål m.m.**

Begræns brugen af upræcise tidsbetegnelser såsom *"regelmæssigt, periodisk, jævnligt og hyppigt"*, da de er op til fortolkning. Brug så vidt muligt præcise tidsangivelser (f.eks. antal minutter/timer/dage) og frekvenser (f.eks. dagligt, ugentligt, månedligt, kvartalsvist og årligt).

For yderligere inspiration til udarbejdelsen af sikkerhedskrav henvises til præsentationsmaterialet "Leverandørstyring – en rejsefortælling om krav og opfølgning på sikkerhed", der kan findes på Sikkerdigital.dk.