BILAG 3a – Transitions- og transformationsplan

**Vejledning til tilbudsgiver i forbindelse med udarbejdelse af tilbud**

*Tilbudsgiver skal udfylde dette Bilag 3a med tilbudsgivers besvarelse af evalueringskravene (”EK”) i Bilag 3 ”Transition og Transformation”.* ***Bilaget må maksimalt fylde 30 A4-sider ekskl. den anførte støttetekst****.*

*Tilbudsgivers besvarelse bedes indsættes i de anførte brackets* [*Indsæt beskrivelse*].

*Det er vigtigt, at tilbudsgiver udførligt beskriver, hvilke dele af evalueringskravene, der er opfyldt henholdsvis ikke-opfyldt, idet manglende eller upræcise oplysninger vil blive tillagt negativ vægt ved tilbudsvurderingen.*

*I Bilag 3 er der i kolonnen ”Positiv vægtning i evaluering” i kravtabellen angivet, hvad der vægter positivt i tilbudsgiverens besvarelse af hver enkelt EK, hvilket tilbudsgiver bedes lægge vægt på i besvarelsen af dette Bilag 3a. Tilbudsgiver skal være opmærksom på, at By & Havn alene er berettiget til at lægge vægt på de ved tilbuddet indkomne oplysninger, og at By & Havn vil tage alle oplysninger i tilbuddet i betragtning ved vurdering af, om et krav er opfyldt.*

*Det betyder blandt andet, at tilbudsgivers besvarelse i et Bilag vil kunne indgå ved vurderingen af, om et krav i et andet Bilag er opfyldt. Tilbudsgiver bør derfor altid sikre, at tilbudsgivers besvarelse i ét Bilag ikke fører til, at et krav må anses for ikke-opfyldt i et andet Bilag.*

*Denne vejledning og tekst angivet med kursiv i Bilaget slettes inden Kontraktens underskrivelse.*

Indholdsfortegnelse

[1 Transitionsplan 4](#_Toc168586098)

[2 Krav til transition 4](#_Toc168586099)

[B3-4 Transitionsplan 4](#_Toc168586100)

[B3-14 Baseline 4](#_Toc168586101)

[B3-24 Storage-typer 5](#_Toc168586102)

[B3-31 WAN til By & Havns interne netværk 5](#_Toc168586103)

[B3-36 Perimetersikkerhed 6](#_Toc168586104)

[B3-37 Scanning og logning af web-trafik 6](#_Toc168586105)

[B3-38 Beskyttelse mod angreb og skadelig kode 6](#_Toc168586106)

[3 Krav til tranformationsplan 9](#_Toc168586107)

# Transitionsplan

Dette Bilag 3a indeholder Leverandørens beskrivelse af evalueringskravene (EK) i Bilag 3 ”Transition og Transformation”.

# Krav til transition

## B3-4 Transitionsplan

Leverandøren skal i samarbejde med By & Havn udarbejde en transitionsplan, der som minimum indeholder følgende punkter:

* Aktivitets- og tidsplan
* Betragtninger om contingency og roll-back
* Testplan
* Nødvendig kundeinvolvering

Transitionsplanen skal indeholde de Prøver og tests, der er beskrevet i tabel 1 i Bilag 3c Prøver i transitions- og transformationsfasen.

Transitionsplanen skal beskrive, hvordan performance og Servicemål sikres i forbindelse med overtagelse af drift, support og vedligehold af Systemet.

Derudover skal transitionsplanen beskrive de ressourcer, som By & Havn forventes at afsætte og bidrage med, med angivelse af de ønskede kompetencer og antal timer, i de forskellige aktiviteter og faser i planen.

Det er By & Havns forventning, at varigheden for transitionen er maksimalt 3 måneder. Leverandøren skal angive tidsplan med start på dag 0 (dvs. ikke en datospecifik opstartsdato).

Tidsplanen skal anvende kalenderdage som mindste tidsenhed, og arbejde udenfor normal arbejdstid skal specifikt synliggøres.

*Tilbudsgiver bedes indsætte forslag til transitionsplan baseret på ovenstående krav. Tilbudsgiver bedes derudover i Bilag 3.c beskrive de prøver, der er indeholdt i tilbudsgivers transitionsplan.*

[*Indsæt beskrivelse*]

## B3-14 Baseline

Som udgangspunkt for at vurdere, om Leverandøren leverer et tilstrækkeligt højt-ydende driftsmiljø, skal der i eksisterende miljø foretages en baseline for udvalgte applikationer/systemer, hvor performance i form af svartider ved forskellige transaktionstyper måles. Listen over systemer/applikationer for hvilke der skal gennemføres baseline målinger fastlægges i analysefasen. Denne baseline vil blive udgangspunkt for de krav der stilles til det nye driftsmiljø, hvor minimum tilsvarende performance kræves.

*Tilbudsgiver bedes beskrive sin tilbudte løsning til at foretage performancemålinger.*

[*Indsæt beskrivelse*]

## B3-24 Storage-typer

Leverandøren kan benytte en storage-løsning med flere performanceniveauer (tiering) – eksempelvis høj/medium/standard performance – med henblik på at sikre performance jf. Bilag 7 ”Servicemål”.

Performanceniveauerne kan baseres på den teknologi Leverandøren ønsker. Det vil f.eks. være fuldt ud acceptabelt at anvende en niveauopdeling baseret på storagepolitikker og optimering af placeringen af data gennem disse.

Leverandørens priser på storage (datalagring) er indeholdt i Bilag 6.1, Tabel 3 ”Leverandørens priser”.

Leverandøren skal afregne storage ud fra ”anvendt storage”, som defineres som den del af den tildelte storage, der er anvendes af de virtuelle servere, som Leverandøren leverer til By & Havn fra sine datacentre under i Kontraktens løbetid. Dette svarer til de to kolonner ”tildelt storage” og ”anvendt storage” i serveroversigten i Bilag 2.1.

Det er Leverandørens ansvar at sikre, at storagesystemerne udnyttes, så systemerne overholder performancemål.

Til den initielle dimensionering af storage skal der regnes med 4 TB af den samlede storage skal være på tier 1 (højeste perfomanceniveau); og 8,5 TB på tier 2. By & Havns nuværende samlede storagekapacitet på de servere, der skal flyttes til Leverandøren, er ved udarbejdelsen af dette materiale beregnet til ca. 12,5 TB.

Den endelige fordeling af storage-tiering afdækkes i forbindelse med Analysefasen for at sikre, at Servicemål jf. Bilag 7 overholdes.

*Tilbudsgiver bedes beskrive den storageløsning som tilbydes By & Havn.*

[*Indsæt beskrivelse*]

## B3-31 WAN til By & Havns interne netværk

Der skal etableres WAN forbindelse fra Leverandørens datacenter til By & Havns netværk med en kapacitet på 1 Gbit/s.

Der skal etableres redundans på denne forbindelse. Redundans skal etableres, så en enkelt kabelfejl ikke vil medføre afbrydelse af forbindelsen mellem Leverandørens datacenter og By & Havns MPLS netværk.

Omkostninger til etablering og drift af WAN-forbindelse er indeholdt i Bilag 6.1 ”Leverandørens priser” i henholdsvis tabel 2 ”Samlet fast pris for Leverandørens Leverancer under etablering, transition og idriftsættelse” og i tabel 3 ”Månedligt vederlag for drift, support og vedligehold af WAN-linje fra Leverandør til By & Havn - redundant 1 Gbps.”

*Tilbudsgiver bedes beskrive den tilbudte redundante forbindelse, herunder hvilken WAN-teknologi der tænkes anvendt for både den primære og den sekundære forbindelse. Tilbudsgiver bedes desuden beskrive hvordan det sikres, at fejl på enkeltkomponenter eller et kabel ikke vil medføre afbrydelse af forbindelsen imellem tilbudsgiverens datacenter og By & Havn.*

[*Indsæt beskrivelse*]

## B3-36 Perimetersikkerhed

Leverandøren skal i Leverandørens datacenter etablere perimetersikkerhed til By & Havns it-miljø svarende til en firewall-løsning. Inkluderet i ydelsen skal som minimum være:

* IPS/IDS
* SecureDNS
* Malware-filtrering

Perimetersikkerheden skal driftes, administreres og vedligeholdes af Leverandøren. Løsningen skal kunne filtrere trafik fra By & Havns forskellige netværkssegmenter samt til og fra internettet.

*Tilbudsgiver bedes beskrive sin perimetersikkerhed i datacentret, herunder brug af FW services som anført ovenfor. Herudover bedes tilbudsgiver beskrive, hvordan perimetersikkerheden overvåges og hvordan events håndteres.*

[*Indsæt beskrivelse*]

## B3-37 Scanning og logning af web-trafik

Leverandøren skal etablere et SWG-system (Secure Web Gateway) til løbende scanning af trafik på By & Havns internetforbindelser.

Løsningen skal som minimum inkludere URL-filtrering, detektion og filtrering af ondsindet kode, applikationskontrol for udbredte webbaseret applikationer og logning og rapportering af brugeraktivitet.

*Tilbudsgiver bedes beskrive sin Secure Web Gateway funktion, og hvilke funktioner løsningen har i forhold til nærværende krav.*

[*Indsæt beskrivelse*]

## B3-38 Beskyttelse mod angreb og skadelig kode

Leverandøren skal i transitionen etablere en løsning, der samlet set sikrer, at der kontinuerligt forefindes en både aktiv og opdateret (med seneste tilgængelige version fra producenten) beskyttelse af By & Havns samlede it-infrastruktur, herunder på alle By & Havns server-operativsystemer.   
  
Beskyttelsen skal som minimum indeholde:

* Realtime beskyttelse/scanning
* Spamfilter
* Anti-phishing
* Firewall
* Beskyttelse mod spyware
* Beskyttelse mod malware

*Tilbudsgiver bedes beskrive sin løsning for nærværende krav, herunder tilbudsgivers proces, der sikrer, at løsningen holdes opdateret, samt hvordan løsningen løbende tilpasses i forhold til nye trusler.*

[*Indsæt beskrivelse*]

**B3-40 Etablering af VPN (Remote adgang for brugere)**

Leverandøren skal etablere en ny VPN-løsning til remote adgang for Brugere, som skal erstatte den eksisterende. Leverandøren skal i forbindelse med transitionen sikre, at By & Havns pc’er får installeret den nødvendige software til at anvende løsningen. VPN-forbindelsen skal både kunne anvendes af By & Havns ansatte og af By & Havns eksterne leverandører og samarbejdspartnere.

Omkostninger til drift, support og vedligehold af VPN-løsningen er indeholdt i det faste månedlige vederlag for drift, support og vedligehold af Systemet, som fremgår af Bilag 6.1 ”Leverandørens priser” tabel 3.

*Tilbudsgiver bedes beskrive hvordan og med hvilken teknologi en ny VPN-løsning vil blive etableret, og hvordan de nødvendige tilpasninger bliver installeret på By & Havns pc´er.*

[*Indsæt beskrivelse*]

**B3-42 Sporbarhed og overvågning – etablering af Security information and event management (SIEM)**

Leverandøren skal etablere overvågning og sporbarhed på By & Havns systemer inklusive servere i By & Havns datacentre. Overvågningen skal sikre, at der etableres sporbarhed for alle Brugeres it-sikkerhedsrelaterede aktiviteter, afvigelser og sikkerhedshændelser via logning, herunder:

* Log over alle afviste adgangsforsøg.
* Log over sikkerhedshændelser (konstaterede brud på sikkerheden samt ændringer i By & Havns it-miljø med relevans for it-sikkerheden).
* Log over tilgang og afgang af Leverandørens personale med adgange til By & Havns it-miljøer eller andele af shared infrastructure.
* Løbende overvågning og detektering af unormal brugeradfærd, der kan udgøre en sikkerhedsrisiko.
* Log over tilgang og afgang af personer (navne, konti) med privilegerede rettigheder på By & Havns systemer.
* Log over anvendelse af privilegerede konti.
* Log over alle ændringer i rettigheder for konti med privilegerede rettigheder (f.eks. indmelding og udmelding af rettighedsgrupper, oprettelse/nedlæggelse af adminkonti etc. på både AD-niveau og på enkeltsystemer.
* Opdateret overblik over alle privilegerede konti og de systemer/produkter, som de har rettighederne på.
* Log og statistikker over forekomster af vira på servere og pc’er samt udførte actions/respons (sletning, karantæne, manuelle handlinger etc.) på disse.
* Liste/matrix over alle oprettede sikkerheds/rettighedsgrupper (standard ”built-in” grupper i AD som f.eks. ”Domain Admin” er undtaget), der anvendes til at tildele privilegerede rettigheder samt en beskrivelse/definition af de adgange til systemer og data grupperne giver.

Log skal opbevares i en periode på minimum 13 mdr. af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.

*Tilbudsgiver bedes beskrive den løsning som By & Havn tilbydes. Tilbudsgiver bedes som en del af sin besvarelse redegøre for, hvad tilbudsgiveren er i stand til at logge, og hvad der logges som en del af ydelsen, hvilke regler og procedurer der gælder for opfølgning på logning, samt hvem logningen er tilgængelig for.*

[*Indsæt beskrivelse*]

**B3-43 Security Operations Center (Option)**

Leverandøren skal som Option kunne levere et full service Security Operations Center (SOC) dækkende alle dele af By & Havns it-miljøer, der overvåger Systemet for potentielle trusler, angreb og sikkerhedsbrud. Leverandøren skal med det leverede Security Operations Center kunne opretholde et sikkerhedsniveau, der kan understøtte det til enhver tid værende trusselsbillede.

SOC skal være døgnbemandet og proaktivt overvåge netværk, infrastruktur, platforme, og applikationer og arbejde for at stoppe og forebygge cyberangreb, før de når at forvolde skade på data og it-miljøer.

SOC skal understøtte By & Havn med anbefalinger til at løbende gennemførelse af sikkerhedsmæssige opdateringer af By & Havns It-miljø, så disse tilpasses i henhold til det gældende trusselsbillede.

Leverandøren skal desuden komme med anbefalinger til ændringer ved introduktion af ændrede krav i lovgivningen, så By & Havn rettidigt efterlever gældende regler på sikkerhedsområdet, eksempelvis i forhold til NIS2.

Sikkerhedsmæssige opdateringer af denne type gennemføres som projekter uden for de faste vederlag for etablering og drift.

Leverandørens SOC skal som udgangspunkt indeholde følgende:

* Overvågning og detektion
* Incidenthåndtering og respons
* Overvågning af trusler og sikkerhedsrisici
* Sårbarhedsstyring
* Overvågning af compliance og rapportering

*Tilbudsgiver bedes beskrive sin SOC løsning, hvordan den er bemandet, hvordan det sikres at relevante events bliver identificeret hurtigt og hvordan events vurderes og relevante aktiviteter bliver igangsat. Det bør ligeledes beskrives, hvem der udføre igangsatte aktiviteter og hvordan SOC funktionen sikrer, at aktiviteter bliver udført i overensstemmelse med den gældende Security Incident proces.*

[*Indsæt beskrivelse*]

**B3-44 Beredskab i forbindelse med major security incidents**

Leverandøren skal i transitionsfasen i samarbejde med By & Havn etablere en proces for beredskab i forbindelse med major security incidents. Processen skal indarbejdes i driftshåndbogen.

*Tilbudsgiver bedes beskrive sin proces for beredskab i forbindelse med major security incidents, herunder redegøre for, hvordan tilbudsgiver vil sikre By & Havns data i forbindelse med et evt. ransomware angreb (worst case scenarie). Tilbudsgiver bedes ligeledes redegøre for tilbudsgiverens beredskab og organisatoriske tilgang i forbindelse med et sådant worst case scenarie, herunder hvordan By & Havn bliver inddraget og opdateret.*

[*Indsæt beskrivelse*]

**B3-47 Tilpasning af it-systemerne**

Leverandøren skal, som en del af transitionen tilpasse de i Bilag 2.1. ”Konfigurationer” anførte it-systemer og underliggende servere (inklusive systemer og servere, der varetages som Remote drift) til driftsmiljøet, således at:

* Eksisterende software til backup, antivirus, overvågning og software deployment afinstalleres
* Leverandørens software til varetagelse af driftsansvaret installeres, herunder backup, antivirus, konfigurationsstyring og deployment, logning samt overvågning.
* Servernes ip-konfiguration tilrettes, hvis nødvendigt, iht. Leverandørens ip-adresseplan
* Relationer internt mellem servere og eksterne systemer genoprettes.

*Tilbudsgiver bedes beskrive hvordan alle relevante og nødvendige tilpasninger af it-systemerne bliver identificeret og de tilhørende tilpasninger bliver sikret gennemført.*

[*Indsæt beskrivelse*]

# Krav til tranformationsplan

Kontrakten inkluderer ingen transfomation.