INTERN REVISION

7. marts 2024

SÆRLIG UNDERSØGELSE

# IT-Anskaffelsesprocessen

## Økonomiforvaltningen

## 2024

**MODTAGER**

Adm. direktør Søren Hartmann Hede
Direktør Nicolai Kragh Petersen

# Indholdsfortegnelse

# 1. INDLEDNING

Intern Revision (IR) har i overensstemmelse med den vedtagne revisionsplan foretaget en undersøgelse af kommunens It-anskaffelsesproces som fremgår af kommunens Forretningscirkulære for it-anskaffelser.

Forretningscirkulære for it-anskaffelser har til formål at sætte rammerne for, at alle it-anskaffelser i Københavns Kommune understøtter kommunens og forvaltningernes forretningsbehov og dermed skaber mest mulig værdi for kommunen.

## Formål, metode og afgrænsning

Formålet med tilsynet er at undersøge, hvorvidt processen er designet hensigtsmæssigt og betryggende.

Observationerne bygger på den viden IR har oparbejdet på området, interview med relevante interessenter og review af regler og retningslinjer og materiale tilgængeligt i kommunens systemregister, FISKK. Kommunens eksterne revisor EY har givet sparring og rådgivning i forbindelse med undersøgelsen.

## Rapportering

Rapporten forelægges Revisionsudvalget.

Et udkast til rapporten har været i høring hos ledelsen i Økonomiforvaltningen. Vi har i rapporten alene forholdt os til de dele af de indkomne høringssvar, der vedrører de faktiske forhold, der beskrives i rapporten. Vi har således som udgangspunkt ikke inddraget bemærkninger til vores vurderinger.

## 2. KONKLUSION, SAMMENFATNING OG ANBEFALINGER

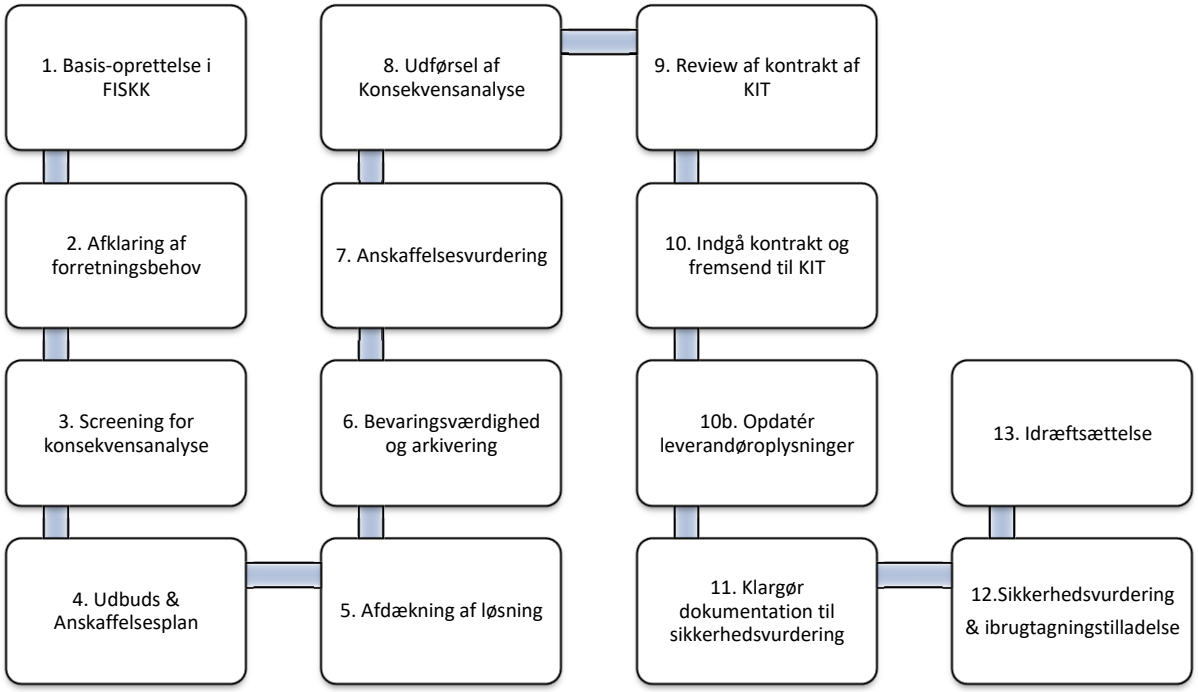
**Anskaffelsesprocessen**
It-anskaffelsesprocessen består af fire delprocesser:

1. Behovsafklaring
2. Analyse & planlægning
3. Gennemførsel
4. Afslutning

Processen skal overordnet sikre at:

1. It-anskaffelser foretages for at kunne understøtte kommunens enheders forretningsbehov på en måde, hvor arbejdsgange og forretningsbehov understøttes så effektivt som muligt.
2. Kommunens samlede it-portefølje skal være nem og kosteffektiv at anskaffe, anvende, drifte, vedligeholde og udfase.
3. Test af nye teknologier skal rammesættes, så der kan arbejdes fleksibelt og koordineret med nye teknologier på tværs i kommunen.
4. Sikkerheden i kommunens samlede it-portefølje skal fastsættes i balance mellem trusselsniveau og forretningsbehov for at sikre kommunen mod kompromittering af fortrolighed, integritet og tilgængelighed.

De fire delprocesser dækker over 13 aktiviteter som forvaltningerne skal igennem før Afslutning og idriftsættelse.



Aktiviteterne er i vid udstrækning fornuftige tiltag, som forvaltningerne kan og bør forholde sig til.

Den samlede proces er væsentligst et compliancetjek, som medvirker til, at Koncern IT (KIT) kan foretage en indledende anskaffelsesvurdering, en efterfølgende sikkerhedsvurdering og endelig, udstede en ibrugtagningstilladelse.

I aktivitet to, "Afklaring af forretningsbehov", ligger en Konsolideringsvurdering. Af hensyn til omfanget af kommunens samlede it-portefølje og investeringer foretaget i it-systemer, skal muligheden for at anvende eksisterende it-systemer i kommunen, frem for at anskaffe nye it-systemer, altid undersøges. KIT skal derfor vurdere, hvorvidt et allerede eksisterende it-system kan anvendes. Konsolideringsvurderingen er midlertidigt sat på pause, da forvaltningerne ikke er enige i KIT's vurderinger.

Anskaffelsesvurderingen afslutter delprocesserne "Behovsafklaring" og "Analyse & planlægning" og ligger således forud for selve købet. En anskaffelsesvurdering er en vurdering af, om anskaffelsen kan/bør/skal benytte specifikke løsningsbyggeblokke og datakilder, eller følge relevante regler, retningslinjer og lovgivning.

Anskaffelsesvurderingen ender typisk ud i flere afklaringspunkter som forvaltningerne bør iagttage i det videre arbejde, for at få en sikkerhedsvurdering og ibrugtagningstilladelse.

Den anskaffende forvaltning/enhed har overfor den respektive borgmester ansvaret for, at det anskaffede it-system overholder de til enhver tid gældende love og regler, og i flere tilfælde betaler forvaltningerne KIT for rådgivning og bistand i forbindelse hermed.

**Sikkerhedsvurdering**
Det er vigtigt, at vi beskytter vores data og systemer i Københavns Kommune. Derfor skal alle it-systemer overholde de gældende retningslinjer og principper indenfor informationssikkerhed og databeskyttelse, herunder fortrolighed, integritet og tilgængelighed.

Det anskaffede it-system skal derfor sikkerhedsvurderes forud for idriftsættelse. Sikkerhedsvurderingen foretages af KIT i samarbejde med den anskaffende forvaltnings Digitaliseringskontor.

Modsat anskaffelsesvurderingen, som er før anskaffelsen, er sikkerhedsvurderingen efter anskaffelsen og indeholder aktiviteterne "Review" og indgåelse af kontrakt med leverandøren samt klargøring af den dokumentation, der ligger grund for sikkerhedsvurderingen.

I forhold til de fire overordnede mål med Anskaffelsesprocessen er det vores vurdering, at Sikkerhedsvurderingen skal sikre det overordnede mål, som kan henføres til Økonomiudvalget/Økonomiforvaltningens ansvar:

- Sikkerheden i kommunens samlede it-portefølje skal fastsættes i balance mellem trusselsniveau og forretningsbehov for at sikre kommunen mod kompromittering af fortrolighed, integritet og tilgængelighed.

Økonomiforvaltningen (ØKF) har, efter koordinering med It-kredsen, ansvaret for at fastsætte de fælles retningslinjer og teknologier, der som standard anvendes i Københavns Kommune. Dette skal ske under hensyntagen til nationale og sektorspecifikke standarder.

Et af styringsprincipperne er bl.a. at sikre, at

> *Sikkerheden i kommunens samlede it-portefølje skal fastsættes i balance mellem trusselsniveau og forretningsbehov for at sikre kommunen mod kompromittering af fortrolighed, integritet og tilgængelighed.*

Sikkerhedsvurderingen omfatter en lang række punkter, som kan være vanskeligt at få et præcist overblik over. Bl.a. foreligger der en liste med 90 minimumskrav og flere "nice-to"-krav samt krav, som forvaltningerne kan vurdere, om er aktuelle. Herudover indgår forretnings- og lovgivningsmæssige aspekter i vurderingen, som er forvaltningernes ansvar.

Sikkerhedsvurderingen ender typisk ud i en ibrugtagningstilladelse med handlingsplan. En konklusion vil typisk være udformet som:

"Systemet er samlet set udsat for en risiko, der, på nuværende tidspunkt, er acceptabel, forudsat at der indgås aftale om følgende identificerede afklaringspunkter".

Det er vores opfattelse, at en sikkerhedsvurdering ikke kan sammenlignes med en risikovurdering. Sikkerhedsvurderingen er derfor ikke en garanti for, at systemerne på tidspunktet, hvor de bliver ibrugtaget, opfylder formålet med sikkerhedsvurderingens præmisser, som er, "at et it-system lever op til de it-sikkerhedsstandarder og -love, som gælder for Københavns Kommune".

Vi kan ligeledes ikke se, om der i sikkerhedsvurderingen bliver taget stilling til, hvordan det enkelte it-system eller anvendelsen påvirker kommunens infrastruktur. Ligesom den ikke håndterer leverandørrisici, som er yderst relevant, da mange af kommunens løsninger driftes af tredjeparter.

Herudover anføres "på nuværende tidspunkt". Der er således tale om et øjebliksbillede, og hvis væsentlige forhold ændrer sig efterfølgende og dermed risikoen, er det forvaltningernes ansvar at forholde sig til dette. KIT foretager årligt et begrænset antal risikovurderinger af igangværende systemer i et utidssvarende setup. I praksis følges der, efter vores vurdering, ikke tilstrækkeligt op på sikkerhedsvurderingerne.

At der ikke foretages en egentlig risikovurdering medfører, at der i de fleste tilfælde, kan være en "høj" risiko forbundet med anvendelsen af systemet, idet mange risici forsat vil være ukendte, selvom der er udstedt en ibrugtagningstilladelse.

Det er vores opfattelse, at anskaffelsesprocessen er omfattende med mange lag, uhensigtsmæssigt tilrettelagt og dermed unødigt ressourcekrævende.

**Anbefaling**
Det er vores vurdering, at der i relation til en it-anskaffelse, generelt er tre sikringsniveauer, der bør håndteres af ØKF/KIT:

- Beskyttelse af kommunens infrastruktur
- Sikkerheden i det konkrete system eller applikation
- Compliance ift. at overholde interne regler som sikrer passende sikkerhedsniveau

Det er vores opfattelse, at forvaltningerne bør kunne vælge anskaffelsesvurderingen til og fra, hvis de på baggrund af en vurdering af væsentlighed og risiko selv er i stand til at foretage vurderingen.

Anskaffelsesprocessen er et forudgående compliancetjek i forhold til love, regler og retningslinjer, som forvaltningerne selv er ansvarlige for at efterleve. Det anbefales derfor, at anskaffelsesvurderingen som et obligatorisk krav afskaffes.

Forvaltningerne skal understøttes af gode vejledninger fra KIT og have mulighed for at få rådgivning og sparring fra KIT, eventuelt mod betaling.

Det anbefales desuden, at sikkerhedsvurderingen afløses af en risikovurdering/ibrugtagningstilladelse, der udelukkende fokuserer på de tre sikringsområder, som Økonomiudvalget/Økonomiforvaltningen er ansvarlige for. I risikovurderingen bør systemet og leverandøren indgå, og der bør ligeledes være taget stilling til, hvilke minimumskrav der skal være opfyldt for at sikre et passende sikkerhedsniveau i Københavns Kommune. Det bør vurderes, på hvilket tidspunkt i anskaffelsesprocessen risikovurderingerne mest hensigtsmæssigt bør foretages.

Endelig bør KIT, som det allerede fremgår af cirkulæret, sikre at der er udarbejdet de nødvendige retningslinjer, vejledninger og skabeloner, som skal sikre at forvaltningerne kan løfte deres opgaver i anskaffelsesprocessen hensigtsmæssigt og betryggende. KIT bør herudover rådgive og udbyde kurser i anvendelsen af materialet.

Det er vores vurdering, at en ændring af anskaffelsesprocessen vil medføre en mere transparant og effektiv proces, som både vil kunne højne kvaliteten og effektivisere processen væsentligt.

## 3. OBSERVATIONER

### 3.1 Forretningscirkulære for IT-anskaffelser

Cirkulæret blev vedtaget 1. november 2018 og gælder for enhver anskaffelse af ny it eller teknologi er som udgangspunkt omfattet af anskaffelsescirkulæret. Definitionen er meget bred og gælder alt fra it-systemer til software, der skal være med til at understøtte forretningsbehov.

Forretningscirkulære for it-anskaffelser har til formål at sætte rammerne for, at alle it-anskaffelser i Københavns Kommunes understøtter kommunens og forvaltningernes forretningsbehov og dermed skaber mest mulig værdi for kommunen.

Sammen med de underliggende forretningsgange er Forretningscirkulære for it-anskaffelser rammesættende for samarbejdet på tværs af kommunens enheder. Forretningscirkulæret er udarbejdet i henhold til Informationssikkerhedsregulativet for Københavns Kommune og kommunens vision om: "Lovlig forvaltningsvirksomhed og tryghed for borgerne og virksomhederne i mødet med Københavns Kommune".

I forretningscirkulæret fastsættes de nærmere regler for kommunens anskaffelser af it med udgangspunkt i følgende principper:

1. It-anskaffelser foretages for at kunne understøtte kommunens enheders forretningsbehov på en måde, hvor arbejdsgange og forretningsbehov understøttes så effektivt som muligt.
2. Kommunens samlede it-portefølje skal være nem og kosteffektiv at anskaffe, anvende, drifte, vedligeholde og udfase.
3. Test af nye teknologier skal rammesættes, så der kan arbejdes fleksibelt og koordineret med nye teknologier på tværs i kommunen.
4. Sikkerheden i kommunens samlede it-portefølje skal fastsættes i balance mellem trusselsniveau og forretningsbehov for at sikre kommunen mod kompromittering af fortrolighed, integritet og tilgængelighed.

Herudover er følgende anført:

> *"Ovenstående principper søges opnået i dette forretningscirkulære ved at rammesætte overblik, standardisering og entydig fordeling af roller og ansvar mellem kommunens enheder. Med de underliggende forretningsgange sikres et fælles grundlag for et tæt og smidigt samarbejde mellem kommunens enheder om it-anskaffelser. Det fælles grundlag i dette forretningscirkulære tager udgangspunkt i de styringsprincipper, der er fastsat i Informationssikkerhedsregulativet"*

Nedenfor følger en forenklet gennemgang af anskaffelsescirkulærets overordnede faser.

**Behovsafklaring**

| | |
|---|---|
| Basisoprettelse i FISKK | Den anskaffende enhed er forpligtet til at indmelde nye it-systemer samt ændringer til eksisterende it-systemer i kommunens centrale systemregister efter de til enhver tid gældende retningslinjer. |
| Afdækning af forretningsbehov | Alle anskaffelser skal være baseret på et afdækket og dokumenteret forretningsbehov. Det er den anskaffende enheds ansvar at afdække forretningsbehovet forud for anskaffelsen. |
| Konsolideringshensyn og konsolideringsvurdering | Koncern IT har ansvaret for at identificere konsolideringspotentialer for it-anskaffelser baseret på det afdækkede forretningsbehov. Den anskaffende enhed er forpligtet til aktivt at forholde sig til eventuelle konsolideringspotentialer, som Koncern IT måtte identificere, jf. nedenstående. Det er dermed den anskaffende enhed, som i sidste ende beslutter, hvorvidt det er formålstjenstligt at anvende et allerede eksisterende it-system.<br><br>På nuværende tidspunkt foretages der ikke konsolideringsvurderinger. |
| Konsekvensanalyse, screening | Forvaltningen skal vurdere, hvorvidt der skal laves en GDPR konsekvensanalyse ift. den behandling der skal foretages i det system m.v. der påtænkes anskaffet. |

**Analyse & planlægning**

| | |
|---|---|
| Afdækning af løsning | I afklaringen af løsningsmuligheder er den anskaffende enhed forpligtet til, med afsæt i de gældende retningslinjer og teknologivalg i Københavns Kommune, at tage aktiv stilling til følgende aspekter af it-systemet forud for anskaffelsen:<br><br>• Konsolideringshensyn<br>• It-arkitektur, herunder integrationer til andre it-systemer<br>• Informationssikkerhed og databeskyttelse<br>• Udbudsjura og kontraktstyring<br>• Bevaringsværdighed/arkiveringsbehov<br>• Brugeradministration (se forretningscirkulære for informationssikkerhed)<br>• Drift (se forretningscirkulære for it-drift, -vedligehold og -udfasning) |
| Udbuds & anskaffelsesplan | Den anskaffende enhed er forpligtet til at lave en udbuds- og anskaffelsesplan i forbindelse med it-anskaffelser. Koncern IT har ansvaret for at udarbejde, vedligeholde og tilgængeliggøre retningslinjer for, hvorledes udbuds- og anskaffelsesplaner kan udformes i Københavns Kommune. |
| Bevaringsværdighed og arkivering | Den anskaffende enhed er forpligtet til at sikre, at gældende regler og love om arkivering og bevaringsværdighed overholdes. Københavns Stadsarkiv har ansvar for at tilbyde rådgivning herfor. |

| | |
|---|---|
| Anskaffelsesvurdering | *For at stille den anskaffende enhed bedst muligt gennemføres forud for anskaffelsen en vurdering af de beslutninger og overvejelser, enheden har foretaget. Vurderingen har til formål at sikre de bedste vilkår for den anskaffende enhed og kommunen som helhed samt at give enheden et overblik over de beslutninger, der skal tages og dokumenteres frem mod idriftsættelsen*.<br><br>Koncern IT har ansvar for at foretage vurderingen i samarbejde med de anskaffende enheders digitaliseringskontorer. Den anskaffende enhed har ansvar for at sikre, at der bliver foretaget en vurdering og at bidrage aktivt til udarbejdelsen af denne. Vurderingen af it-anskaffelsen tager afsæt i de afdækkede forretningsbehov og tekniske løsningsmuligheder. Vurderingen er en helhedsvurdering, som rummer følgende aspekter:<br>• It-arkitektur, herunder integrationer til andre it-systemer<br>• Informationssikkerhed og databeskyttelse<br>• Udbudsjura og kontraktstyring<br>• Brugeradministration<br>• Drift |
| Konsekvensanalyse, udførsel | Hvis screeningen viser behov, skal den egentlige konsekvensanalyse udføres og dokumenteres. |

**Gennemførsel**

| | |
|---|---|
| Review af kontrakt af KIT | Kontrakten skal sendes til gennemlæsning i Udbud og Kontraktstyring, inden den indgås eller ikke kan ændres. |
| Indgå kontrakt og fremsend til KIT | For at sikre muligheden for effektiv kontraktstyring er den anskaffende enhed forpligtet til at sørge for, at alle indgåede it-kontrakter, tillæg og ændringer hertil sendes til Koncern IT. Koncern IT er forpligtet til at opbevare disse.<br><br>Koncern IT er ligeledes forpligtet til at tilbyde kontraktstyring i forhold til indgåede kontrakter. |
| Leverandørdata | Systemet skal opmærkes med leverandører, fx driftsleverandør og systemleverandør. Hertil udfyldes oplysninger om evt. databehandleraftale er indgået og journaliseret samt aftale om tilsyn og revisionserklæring. |
| Klargør dokumentation | Den anskaffende enhed skal klargøre den nødvendige system- og driftsdokumentation forud for sikkerhedsvurderingen. |
| Sikkerhedsvurdering | Det anskaffede it-system skal sikkerhedsvurderes forud for idriftsættelse for at sikre at alle krav til informationssikkerhed og databeskyttelse er opfyldt. |

**Afslutning**

| | |
|---|---|
| Idriftsættelse | Systemer idriftsættes |

Ovenstående gennemgang er overordnet. Under de enkelte punkter, vil der være flere delpunkter, som skal sikres.

### 3.2 Anskaffelsesvurderingen

Forud for den endelige sikkerhedsvurdering foretages en anskaffelsesvurdering. Vurderingen er en overordnet helhedsvurdering, som rummer følgende aspekter:

- It-arkitektur, herunder integrationer til andre it-systemer
- Informationssikkerhed og databeskyttelse
- Udbudsjura og kontraktstyring
- Brugeradministration
- Drift

Det skal bl.a. også sikre, at

- at kommunens samlede it-portefølje er tilstrækkelig sikret mod kompromittering af fortrolighed, integritet og tilgængelighed,
- at anskaffelsen overholder kommunens fælles regler og retningslinjer på it-området,

Anskaffelsesvurderingen ligger før selve udbudsfasen, og der kan derfor være ukendtheder til det aktuelle system på tidspunktet. I det eksempel, vi har set, er det de samme ting, man forholder sig til i den indledende anskaffelsesvurdering, som den endelige sikkerhedsvurdering.

### 3.3 Sikringsniveauer

Det er vores vurdering, at der i relation til en it-anskaffelse, er tre sikringsniveauer, der bør håndteres.

- Beskyttelse af kommunens infrastruktur
- Sikkerheden i det konkrete system eller applikation
- Compliance ift. overholde interne regler og lovgivning

**Ad. 1.** Vi kan ikke se, om dette sikres igennem anskaffelsesprocessen.

**Ad. 2.** Sikres ikke igennem anskaffelsesprocessen, men håndteres af KIT igennem de årlige risikovurderinger. Disse er dog ikke dækkende for hele kommunens it-landskab. Der har ligeledes været udfordringer den forhenværende metode, som der er ved at blive håndteret. For de fleste systemer vil der derfor ikke være tilstrækkelige risikovurderinger.

**Ad. 3.** Sikres delvist igennem anskaffelsesprocessen. Den lovgivning, som bliver vurderet i anskaffelsesvurderingen synes udelukkende at være databeskyttelseslovgivningen.

### 3.4 Ansvarsfordeling i KK

I henhold til kommunens informationssikkerhedsregulativ har Økonomiforvaltningen bl.a. ansvaret for

- Kommunens overordnede og tværgående informationssikkerhed
- Tilsyn med overholdelse af kommunens informationssikkerhedsbestemmelser.

De øvrige forvaltninger har bl.a. ansvaret for,

- At fastlæggelsen af informationssikkerhedsniveauet i egen forvaltning sker inden for rammerne af kommunens overordnede og tværgående bestemmelser vedr. kommunens informationssikkerhedsniveau samt med ansvar for, at forvaltningens informationssikkerhedsniveau ikke indebærer risiko for negativ påvirkning af kommunens samlede risiko på tværs af forvaltningerne.
- At forvaltningens behandling af personoplysninger efterlever den til enhver tid gældende lovgivning, herunder databeskyttelseslovgivningen og kommunens fastsatte rammer og retningslinjer herfor.

### 3.5 Definition af It-systemer

I den nedenstående gennemgang er et skal et it-system betragtes i henhold til kommunens definition i anskaffelsescirkulæret.

> *"It-systemer klassificeres i Københavns Kommune som værende infrastruktur, generiske administrative it-systemer, fagsystemer, generiske administrative hjælpeværktøjer og fagspecifikke hjælpeværktøjer."*

Definitionen dækker således over alt, der er understøttet it-baseret, drives over et netværk eller understøtter kommunens infrastruktur.

### 3.6 Sikkerhedsvurdering

Sikkerhedsvurderingen er det sidste trin i processen, før der kan gives tilladelse til at tage systemet i brug. Det anskaffede it-system skal sikkerhedsvurderes forud for idriftsættelse, så det sikres, at alle krav til informationssikkerhed og databeskyttelse er opfyldt.

På baggrund af sikkerhedsvurderingen kan KIT udstede en ibrugtagningstilladelse, hvis KIT vurderer, at risikoniveauet er acceptabelt. Det er kun tilladt at idriftsætte it-systemer, som har en gyldig ibrugtagningstilladelse.

En sikkerhedsvurdering består af:

- En systembeskrivelse, der opridser den udledte systemforståelse, med angivelse af forretningsformål, dataklassifikation, kritikalitet og arkitektur, som sætter konteksten for risikoanalysen.
- En risikoanalyse, der gennemgår de sikkerhedsdomæner som Serviceområde Sikkerhed har vurderet som særligt vigtige med henblik på at tegne et risikobillede for systemet.
- En konklusion, der beskriver udstedelsen af ibrugtagningstilladelsen samt den videre proces.

Sikkerhedsvurderingen giver et øjebliksbillede af, om sikkerheden af et it-system lever op til de it-sikkerhedsstandarder og -love, som gælder for Københavns Kommune. Sikkerhedsvurderingen danner grundlag for udstedelse af den ibrugtagningstilladelse, der er obligatorisk for at have tilladelse til at idriftsætte it-systemet.

Et af styringsprincipperne i forretningsgangen er bl.a. at sikre, at

> *Sikkerheden i kommunens samlede it-portefølje skal fastsættes i balance mellem trusselsniveau og forretningsbehov for at sikre kommunen mod kompromittering af fortrolighed, integritet og tilgængelighed.*

Det er vores vurdering, at sikkerhedsvurderingerne mangler gennemsigtighed i forhold til de tekniske krav, som er gældende i henhold til kommunens interne regler, ligesom der mangler en tydelig sammenhæng mellem sikkerhedsvurderingerne og de egentlige risici, der forsøges håndteret.

Det er vores opfattelse, at grænsen for et acceptabelt risikoniveau er svær at vurdere, idet sikkerhedsvurderingerne dels er et øjebliksbillede, samt at der ikke foretages egentlige risikovurderinger. De vurderinger, der ligger til grund for sikkerhedsvurderingen, er en gennemgang af den, på tidspunktet, tilgængelige information, vurderet op imod de tekniske krav, der følger af Københavns kommunes interne regler.

Det er vanskeligt at følge, hvordan de enkelte sikkerhedskonsulenter finder frem til, hvilket vurderingskriterie der er relevant for det enkelte system, eller applikation. Vi har set et eksempel, hvor et system med kritikalitet 2 (desto højre tal, jo mere kritisk er systemet for forvaltningen) er blevet vurderet efter nærmest identiske vurderingskriterier, som et system med kritikalitet 4.

Det er vores vurdering at sikkerhedsvurderingerne er meget personafhængige, og at der er stor variation i de konkrete sikkerhedsvurderinger.

Systemer, der ikke efterlever vurderingskriterierne på tidspunktet for sikkerhedsvurderingen, kan trods dette godt få en ibrugtagningstilladelse. I så fald gives der en ibrugtagningstilladelse med krav om handleplaner for

håndteringen af de identificerede risici. Disse handleplaner kan være åbentstående i længere tid, uden at det har en egentlig betydning for det enkelte system.

Sikkerhedsvurderingen er derfor ikke en garanti for, at systemerne på tidspunktet, hvor de bliver ibrugtaget, opfylder formålet med sikkerhedsvurderingens præmisser, som er, *at et it-system lever op til de it-sikkerhedsstandarder og -love, som gælder for Københavns Kommune*.

Det er vores vurdering, at sikkerhedsvurderingerne i al væsentlighed skal anses som en compliance gennemgang, der er relateret til en række tekniske minimumskrav, der følger af kommunens regelgrundlag, samt databeskyttelsesreglerne.

Desuden udarbejdes sikkerhedsvurderingerne efter, at kontrakterne er underskrevet. Dette er særligt uhensigtsmæssigt, idet kontrakten muligvis ikke kan ændres, uden det får økonomisk betydning. Der er ligeledes en risiko for, at du kan stå med et system, der ikke kan anvendes, idet det ikke kan efterleve kravene i KK. Hvis skabes gennemsigtighed i omkring sikkerhedsvurderingerne fra start, vil forvaltningerne kunne tage dialogen med leverandøren meget tidligt i processen.

Det at man kalder det en sikkerhedsvurdering, og anvender ord som risikoanalyse, kritikalitet m.v. er, efter vores vurdering, misvisende i forhold til det faktisk produkt. Vi ser en væsentlig risiko for, at dette kan være med til at skabe en falsk tryghed hos forvaltningsledelserne, som muligvis forventer, at deres løsninger bliver vurderet i større omfang, end hvad det er tilfældet, samt at der mitigeres egentlige risici i it-systemet.

Det faktum, at der ikke foretages en egentlig risikovurdering, medfører, at der i de fleste tilfælde, kan være en "høj" risiko forbundet med anvendelsen af systemet, idet mange risici forsat vil være ukendte, selvom der er udstedt en ibrugtagningstilladelse.

ØKF påtager sig således en ikke uvæsentlig risiko, hvis der indtræder en it-sikkerhedshændelse, samt når der gives ibrugtagningstilladelser med handleplaner (dispensationer).

### 3.7 Krav repositorium

I vores interview med KIT, bliver kommunens krav repositorium (efterfølgende kaldet KravBanken) nævnt, som et sted forvaltningerne kan danne sig overblik over tekniske krav.

Det følger af forretningcirkulæret, at,

> *"I udarbejdelsen af udbudsmaterialer og kravspecifikationer er den anskaffende enhed forpligtet til at tage udgangspunkt i Københavns Kommunes standard, non-*

> *funktionelle krav, som beskrevet i kommunens kravrepositorium. Koncern IT har ansvaret for at styre og koordinere udarbejdelse af indhold i kravrepositoriet."*

På kommunens intranet står der:

> *"Non funktionelle krav beskriver rammen omkring løsningen, f.eks. hvilken lovgivning, standarder og it-sikkerhedsregler løsningen skal overholde såsom at være GDPR-compliant eller skal kunne integreres og hostes i kommunens infrastrukturmiljø.*
>
> *[...] KravBanken er en hjælp til at få samlet de relevante non-funktionelle krav til en it-løsning og består af en samling af de mest almindelige non-funktionelle krav til en it-løsning.*
>
> *Hvis din anskaffelse skal i udbud, skal du tage udgangspunkt i Københavns Kommunes standard, non-funktionelle krav, som beskrevet i kommunens kravrepositorium – det vil sige KravBanken. Selv hvis din anskaffelse ikke skal i udbud, er det alligevel en rigtig god ide at tage udgangspunkt i KravBanken. Derved øger du chancen for at dit it-system lever op til de krav, der er til it-systemer i Københavns Kommune og at din løsning virker teknisk."*

Der kan søges løbede rådgivning, hos KIT. KIT skriver selv, at

> *"Mange oplever dette som en udfordrende og kompleks opgave, fordi det kan være svært at gennemskue hvilke krav der er relevante. Derfor kan du tilkøbe rådgivning hos Koncern IT's it-arkitekter, såfremt du vil være sikker på, at du får alle relevante krav med.*
>
> *Når du har fundet frem til, hvilke krav du skal have med, skal kravene samles i et bilag og indgå i udbudsmaterialet for din anskaffelse."*

Der er også en disclaimer

> *KravBanken er stillet til rådighed af Koncern IT som et hjælpeværktøj til de anskaffende enheder. Når du bruger KravBanken har du fortsat selv ansvaret for at sikre, at du får stillet de rigtige krav til dit it-system, og at it-systemet dermed har de bedste forudsætninger for at kunne implementeres i Københavns Kommune.*

Det er vores umiddelbare vurdering, at der er mange gode elementer i kravBanken. Derfor er vi også uforstående overfor, hvorfor værktøjet er frivilligt, hvis det indeholder tekniske minimumskrav til de systemer der skal anskaffes i KK.

En gennemgang af værktøjet har vist, at det ikke er færdig udarbejdet.

På kravbank.kk.dk bliver man ligeledes mødt med beskeden

> *"Der er desværre ikke udgivet en ny version i længere tid.*
> *Kontakt din forvaltningspartner for mere information."*

Materialet ses ikke at været opdateret siden 2021.

Det er vores anbefaling, at man gør værktøjet obligatorisk, samt at man gør det mere tilgængeligt.

Dette kan ske ved fx at låse de felter, som ikke kan fraviges, mulighed for skalering i forhold til mindre anskaffelser, samt udarbejde vejledning til anvendelsen.