Københavns Kommune

Revision af generelle IT-kontroller 2025

Økonomiforvaltningen
Att.: Adm. direktør Søren Hartmann Hede
Direktør Nicolai Kragh Petersen
Københavns Rådhus
1599 København V

Intern Revision

Building a better working world

1. Formål, omfang mv. 3
1.1. Revisionens formål 3
1.2. Revisionens omfang og afgrænsning 3
1.3. Revisionsarbejdets udførelse 5
2. Ledelsesresumé og konklusion 6
2.1. Lovpligtige revision 6
2.2. Forvaltningsrevision med fokus på informationssikkerhed 6
3. Observationer, risikovurdering og anbefaling 8
3.2 Bemærkninger og observationer fra tidligere år, og hvortil det vurderes, at disse videreføres i indeværende år 10
3.3 Bemærkninger og observationer fra sidste år, der i forbindelse med IT-revisionen er konstateret lukket 13
4 Afslutning 14
Bilag - Formidling af risiko og væsentlighed mv. 15

1. Formål, omfang mv.

Som led i den løbende revision af Københavns Kommunes regnskab for 2025 har vi foretaget revision af generelle IT-kontroller, som understøtter kommunes regnskabsaflæggelse.

Rapporten skal ses i sammenhæng med revisionsrapporten "Regnskabsføring, forretningsgange og interne kontroller", hvor en række forhold relateret til brugerstyringen i Kvantum er opsummeret.

1.1. Revisionens formål

Revisionen af de generelle IT-kontroller er en del af den lovpligtige revision og indgår i grundlaget for vores påtegning af Københavns Kommunes årsregnskab. De generelle it-kontroller skal forstås som kontroller, som ledelsen har etableret for at understøtte og sikre funktionen af forretningssystemer, it-baserede kontroller, og underliggende it-infrastruktur, som har betydning for Københavns Kommunes regnskabsaflæggelse. Som en del af revisionen udvælges desuden enkelte IT-områder til den lovpligtige forvaltningsrevision.

Hovedformålet med gennemgangen af de generelle it-kontroller omkring Kvantum, KMD Opus Debitor, KMD Opus Løn, KY og KSD, er dels at understøtte valget af revisionsstrategi samt påtegningen af årsregnskabet og dels at understøtte den lovpligtige forvaltningsrevision. Gennemgangen er derfor ikke foretaget med henblik på at identificere og evaluere effektiviteten af alle generelle it-kontroller eller potentielle forbedringer i etablerede processer og kontroller, men alene de kontroller som har betydning for regnskabsaflæggelsen.

Det bedste værn mod uregelmæssigheder er hensigtsmæssige forretningsgange og gode interne kontroller, hvorfor vores revision i vidt omfang har baseret sig på efterprøvelse af forretningsgange og interne kontroller, men ikke undersøgelser specielt med henblik på opdagelse af uregelmæssigheder.

Det påhviler ledelsen at tilrettelægge kontrolsystemer og forretningsgange, der er betryggende efter forvaltningens forhold, og det påhviler revisor at gennemgå disse forretningsgange og interne kontroller som et led i revisionen af årsregnskabet.

1.2. Revisionens omfang og afgrænsning

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for fejl.

Det er ledelsens ansvar at tilrettelægge niveauet for hensigtsmæssige og betryggende interne kontroller i overensstemmelse med god it-skik og kommunens kasse- og regnskabsregulativ mv.

Revisionen er baseret på en forventning om, at der er tilrettelagt et velfungerende internt kontrolsystem og en pålidelig bogføring. Dette indebærer, at det overordnede kontrolmiljø og de organisatoriske rammer understøtter et velfungerende ledelses- og kontrolsystem, og at der på de enkelte aktivitetsområder er beskrevet og implementeret interne kontroller, som reducerer risikoen for væsentlige fejl til et acceptabelt niveau.

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for væsentlige fejl i regnskabsaflæggelsen.

Vi skal gøre opmærksom på, at revisionen først anses for afsluttet, når vi har underskrevet erklæringen på årsregnskabet.

Lovpligtig revision:

Revisionen er tilrettelagt således, at ikke alle områder gennemgås hvert år; dog således, at alle for regnskabets væsentlige områder bliver gennemgået årligt, samt væsentlige kontrolsvagheder altid bliver fulgt op ved efterfølgende års revision. Revisionen har omfattet en vurdering af de generelle IT-kontroller inden for følgende områder for Kvantum, KMD Opus Debitor, KMD Opus Løn, KY og KSD:

Logiske adgangskontroller:

- Processer for Brugeradministration, herunder oprettelse, nedlæggelse og periodisk gennemgang af brugeradgange
- Sikkerhedsindstillinger
- Krav til adgangskoder
- Privilegerede adgange, herunder funktionsadskillelse i adgangskontrollerne
- Adgange til kritisk it-funktionalitet

Ændringshåndtering:

- Processer for vedligeholdelse af KMD Opus Debitor, KMD Opus Løn, KY og KSD, herunder at ændringer inden implementering i de produktive miljøer er;
  - Autoriseret
  - Testet
  - Godkendt
  - Samt at der er funktionsadskillelse processen

Operations:

- Patch management

Revisionen af de generelle IT-kontroller har ikke omfattet en vurdering af kontrol- og sikkerhedsniveauet i de enkelte brugersystemer, herunder automatiske kontroller i de administrative processer og logiske adgangsrettigheder til udførsel af forretningsaktiviteter i brugersystemerne.

Københavns Kommune har aftale med KMD omkring drift af Kvantum, KMD Opus Debitor & KMD Opus Løn, samt tilhørende platforme. Yderligere har kommunen en aftale med Kombit omkring drift af applikationerne KY og KSD.

Der modtages årligt en revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser, samt en årlig specifik erklæring for Kvantum, KMD Opus Debitor & KMD Opus Løn. For så vidt angår KY og KSD-applikationerne modtages der også årligt specifikke erklæringer. Revisionserklæringerne forventes modtaget primo Q2 2026 dækkende 2025.

Forvaltningsrevision:

Forvaltningsrevisionen har omfattet følgende områder:

- Organisering af informationssikkerhed og styrkelse af ISMS (opfølgning på tidligere observationer)
- Ibrugtagning af IT-systemer (opfølgning på tidligere observationer)

1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2025, og ved interviews af relevante personer hos Københavns Kommune samt ved observation og stikprøvevis gennemgang af udleveret materiale.

2. Ledelsesresumé og konklusion

2.1. Lovpligtige revision

Den lovpligtige revision af IT-området har blandt andet haft fokus på brugerstyringen i de IT-systemer, som vurderes kritiske for regnskabsaflæggelsen.

Vi kan konstatere, at KK generelt har et velfungerende kontrolmiljø omkring kritiske rettigheder, som tildeles midlertidigt ("PIM-løsningen").

Vi har konstateret enkelte områder omkring brugeradministration og sikkerhedsopsætning som bør styrkes i Kvantum.

Der henvises til afsnit 3 for uddybning af ovenstående og andre relevante forhold.

2.2. Forvaltningsrevision med fokus på informationssikkerhed

Truslerne på informationssikkerhedsområdet er konstant stigende og antallet af virksomheder og myndigheder, der har været udsat for alvorlige hændelser som følge af cyberangreb eller andre alvorlige IT-sikkerhedsmæssige hændelser er tilsvarende stigende.

Siden 2021 har revisionen løbende påpeget behovet for styrkelse af informationssikkerheden i KK, herunder etablering af et passende ledelsessystem for informationssikkerhed (ISMS) baseret på ISO27001, og et tilhørende SoA-dokument.

Et velfungerende ledelsessystem, og implementering af passende sikkerhedsforanstaltninger, baseret på konkrete og aktuelle risikovurderinger, er med til at underbygge om det aktuelle informationssikkerhedsniveau er tilstrækkeligt ift. kommunens risikoappetit og kan ligeledes bidrage til at styre økonomien forbundet med at opretholde det sikkerhedsniveau, som ledelsen har besluttet. Styrer man efter ISO-27001 kan der derfor også skabes indblik i, om de økonomiske rammer anvendes bedst muligt ift., hvor der skabes mest værdi for de overordnede informationssikkerhedsmæssige beslutninger.

Etableringen af et ISMS er desuden blevet mere aktuelt efter at kommunerne er blevet omfattet af NIS-lovgivningen. NIS 2-loven er Danmarks implementering af EU´s NIS 2-direktiv som skærper kravene til cybersikkerhed i enheder og organisationer på tværs af EU.

Københavns Kommune er som helhed omfattet af NIS2, og klassificeret som væsentlig enhed og er derfor underlagt tilsyn og sektoransvar hos Styrelsen for Samfundssikkerhed (SAMSIK). Kommunerne blev omfattet af NIS2-lovgivningen den 1. juli 2025.

ØKF har igangsat et ISMS-projekt i erkendelse af, at der er behov for yderligere styrkelse og forbedringer i forhold til drift og vedligeholdelse af kommunens ledelsessystem.

Vi har noteret os, at status på dette arbejde i november 2025 er følgende:

- Styrkelse af ledelsessystemet for informationssikkerhed baseret på ISO 27001 (ISMS).

Tværgående handleplan

Implementeringen af et ISMS i KK følger den vedtagne handleplan. Arbejdet ledes af CISO-funktionen i ØKF, og der er nedsat en række arbejdsgrupper med repræsentanter fra forvaltningerne med ansvar for at omsætte de af ledelsen udpegede fokusområder til konkrete initiativer, der skal implementeres i forvaltningerne.

Der er udarbejdet en handleplan for første fase frem til marts 2026, der afsluttes med et 'stop and go' med beslutning om næste fase. Det er forventningen, at ISMS-implementeringen vil forløbe over 3 år, hvor delelementer løbende vil overgå til drift og øge den ledelsesmæssige gennemsigtighed omkring informationssikkerheden.

Vi henstiller, at man fortsætter og intensiverer arbejdet med at etablere et samlet ISMS for hele KK, der sikrer både fuldstændighed og nøjagtighed og dermed identificerer restrisikoen, i forhold til det nuværende trusselsbillede. Et fuldt implementeret ISMS vil kunne dokumentere, at KK er i stand til at styre informationssikkerheden forsvarligt og professionelt ligesom det vil sikre at KK lever op til de krav, der kommer med NIS2-loven.

- Vurdering af, hvorledes styring af informationssikkerhed mest hensigtsmæssigt organiseres og styrkes

Sikkerhedsvurdering af IT-systemer

Af Forretningscirkulæret for IT-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt IT-system skal sikkerhedsvurderes, inden det idriftsættes. En sikkerhedsvurdering tager stilling til, at alle krav til informationssikkerhed og databeskyttelse er opfyldt. På baggrund af sikkerhedsvurderingen udstedes en ibrugtagningstilladelse. IT-systemer skal have en ibrugtagningstilladelse, inden de idriftsættes.

Det er forbundet med stor risiko for kommunen at idriftsætte et IT-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse.

Vi har noteret os, at KK i 2024 og 2025 har udført et stort arbejde med at få udarbejdet sikkerhedsvurdering af et stort antal systemer, i forlængelse af revisionens bemærkning herom fra 2023. Vores opfølgning i 2025 viser, at man ikke er helt i mål med arbejdet i forhold til at sikre, at kommunens regler er efterlevet fuldt ud.

Der henvises til afsnit 3 for uddybning af ovenstående og andre relevante forhold.

3. Observationer, risikovurdering og anbefaling

For nærmere beskrivelse af kategoriernes prioritet henvises til Bilag 1 - Formidling af væsentlighed og risiko mv.

3.1 Nye kritiske bemærkninger og væsentlige observationer i forbindelse med den udførte IT-revision

Forvaltning	ØKF	Revisionsområde	Brugeradministration	Væsentlighedsniveau
Reference	3.1.1	Revisionsemne	Tildeling af autorisationer (Kvantum)	
Observation	Vi har ved revisionen konstateret at en bruger har tildelt sig selv rettigheder (roller) i maj 2025 direkte i Kvantum og udenom IGA-løsningen. Det er oplyst at brugeren sidder i brugerstyring og har rettigheden til at tildele roller direkte i Kvantum. Tildeling af rettigheder direkte i Kvantum er endvidere ikke omfattet af ledelsestilsynet. Der er risiko for uautoriseret tildeling af rettigheder, hvilket kan resultere i funktionsadskilles risici, tilsigtet og utilsigtet fejl m.v.			2025
Revisionsbemærkning	Vi henstiller til at tildeling af rettigheder i Kvantum sker gennem IGA-løsningen.			

Forvaltning	ØKF	Revisionsområde	Brugeradministration	Væsentlighedsniveau
Reference	3.1.2	Revisionsemne	Adgang til at administrere batchjobs (Kvantum)	
Observation	Vi har ved revisionen konstateret en række brugere (4 fra KS og 22 fra KMD_UDV) med adgang til at administrere batchjobs i Kvantum. Der er efterfølgende modtaget dokumentation for at der er foretaget en rolleændring efter vores analyse, samt det er oplyst at rolleændringen har reduceret adgangen til at administrere batchjobs i Kvantum. Brugere med adgang til at administrere batchjobs har mulighed for at oprette, ændre eller slette jobs, hvilket medfører risiko for tilsigtet og/eller utilsigtet fejl, som kan påvirke forretningskritiske data.			2025
Revisionsbemærkning	Vi henstiller til at adgangen begrænses og primært søges udført gennem PIM-løsningen.			

Forvaltning	ØKF	Revisionsområde	Brugeradministration	Væsentlighedsniveau
Reference	3.1.3	Revisionsemne	Password opsætning (Kvantum)	
Observation	Vi har ved revisionen konstateret at en gruppe brugere (ZAUM_XXXXX) ikke følger København Kommunes passwordpolitik. Brugerne er tilknyttet en special sikkerhedspolitik i Kvantum (BAC_USER), som er underlagt følgende profilparametre i Kvantum: ► "login/password_expiration time": Password udløb er sat til 999 dage. ► "login/password history size": Minimum password history er sat til 3 Manglende skift af password gør det nemmere for uautoriserede personer at gætte eller bryde adgangskoderne ved hjælp af brute force-angreb eller andre metoder. Et brute force-angreb er en metode, hvor en hacker forsøger at få adgang til en konto ved systematisk at prøve alle mulige kombinationer af adgangskoder, indtil den rigtige kombination findes.			2025
Revisionsbemærkning	Det anbefales, at passwordopsætningen følger Københavns Kommunes passwordpolitik, som stiller krav om at password skal skiftes efter maksimum 365 dage, og at password ikke kan genbruges før efter 24 password skift. Vi vil anbefale at I styrker adgangskodeparametrene, da der er en risiko for, at brugere kan tilgå SAP GUI direkte og få adgang til ZAUM_XXXX brugerne. SAP GUI (Graphical User Interface) er den primære grænseflade, som brugere anvender til at interagere med SAP-systemet. Det er et program, der installeres på brugerens computer og giver adgang til SAP-applikationer og data. Hvis brugerne omgår Single Sign-On (SNC) og logger ind direkte på SAP GUI, kan de potentielt undgå de sikkerhedsforanstaltninger, der er forbundet med Single Sign-On via AD. Derfor er det vigtigt at sikre, at adgangskoderne i SAP GUI også er stærke og komplekse for at beskytte systemet mod uautoriseret adgang, herunder at generiske brugere med svage password i Kvantum misbruges.			

3.2 Bemærkninger og observationer fra tidligere år, og hvortil det vurderes, at disse videreføres i indeværende år

Forvaltning	ØKF	Revisionsområde	ISMS	Væsentlighedsniveau
Reference	3.2.1	Revisionsemne	Organisering af informationssikkerhed og styrkelse af ISMS	
Observation	Siden 2021 har revisionen løbende påpeget behovet for at styringen og gennemsigtigheden af arbejdet med informationssikkerhed i KK, skal styrkes væsentligt. Dertil kommer, at nye lovgivninger og reguleringer (aktuelt NIS2, AI Act og forventede yderligere reguleringer de kommende år) kræver en større grad af gennemsigtighed, hvor ledelsen vil blive afkrævet svar om prioriteringer, dokumentation og det ledelsesmæssigt vedtagne sikkerhedsniveau hvilket bl.a., kræver at KK har et ISMS. Opfølgning 2025 Der er udarbejdet en handleplan for første fase frem til marts 2026, der afsluttes med et 'stop and go' med beslutning om næste fase. Det er forventningen, at ISMS-implementeringen vil forløbe over 3 år, hvor delelementer løbende vil overgå til drift og øge den ledelsesmæssige gennemsigtighed omkring informationssikkerheden.			2025 2024
Revisionsbemærkning	Det henstilles, at arbejdet gennemføres hurtigst muligt således, at den periode hvor den øverste ledelse må acceptere et, "uklart" billede af den samlede informationssikkerhed, herunder manglende viden om foranstaltninger og effektiviteten af kontroller samt residualrisikoen, reduceres mest muligt.			

Forvaltning	ØKF	Revisionsområde	Brugeradministration	Væsentlighedsniveau
Reference	3.2.2	Revisionsemne	Gennemgang af rettigheder (Kvantum)	
Observation	Tildelingen af rettighederne "Lederhat" og "Prokuraværdi" sker manuelt via brugeradministration i Kvantum. Disse rettigheder er ikke omfattet af den automatiske tildelingsproces, der håndteres af Omada. Dette betyder, at tildelingen af disse specifikke roller ikke følger den samme automatiske proces som andre roller, der administreres automatisk. Vi har fået oplyst, at Omada indeholder oplysninger om de tildelte rettigheder, og at det periodiske ledelsestilsyn af de nævnte rettigheder basere sig på en rapport fra Omada og ikke fra Kvantum. Det har i forbindelse med revisionen ikke været muligt for os at opnå overbevisning om at udtrækket fra Omada er fuldstændigt og nøjagtigt i forhold til de nævnte rettigheder. Det er derfor ikke muligt at vurdere om listen som anvendes til gennemgangen, er fuldstændighed og nøjagtighed. Opfølgning 2025 Der er ved revisionen konstateret at "Lederhat" og "Prokuraværdi" fortsat ikke er inkluderet i ledelsestilsynet, dog er der foretaget en manuel kontrol forud for ledelsestilsynet, hvor brugere med "Lederhat" og "Prokuraværdi" er gennemgået. For den manuelle kontrol der er udført, foreligger ikke dokumentation for fuldstændighed og nøjagtighed af datagrundlaget der er anvendt til kontroludførslen. Vi er endvidere blevet informeret om at der arbejdes på at implementere løsning for tildelinger via IGA.			2025 2024
Revisionsbemærkning	Vi anbefaler, at der som led i den periodiske gennemgang laves en afstemning af oplysningerne i Omada og Kvantum for de nævnte rettigheder, da der en forhøjet risiko for fejl i integrationen ved manuelle tildelinger direkte Kvantum.			

Forvaltning	ØKF og SOF	Revisionsområde	Ibrugtagningstilladelser på IT-systemer	Væsentlighedsniveau
Reference	3.2.3	Revisionsemne	Sikkerhedsvurdering af systemer	
Observation	*Sikkerhedsvurdering af systemer* Af Forretningscirkulæret for IT-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt IT-system skal sikkerhedsvurderes, inden det idriftsættes. I 2023 konstaterede vi at der er, jf. oplysningerne i FISKK, er mange systemer, som er anskaffet før 1. november 2018, der ikke har en ibrugtagningsstatus, og at flere systemer har en "ikke godkendt" status. Forvaltningernes har igangsat en handleplan som omfatter: 1. KIT foretager en tilpasset sikkerhedsvurdering af a. it-systemer i drift fra før 2018, *der har undergået væsentlige ændringer*, *b.* it-systemer ibrugtaget før 2018 uden ibrugtagningstilladelse, men hvor der efterfølgende er foretaget en risikovurdering, 2. KIT gennemgår systemer registreret som "ikke godkendt" i FISKK og går i dialog med relevante forvaltninger om nødvendighed af eskalation, ny sikkerhedsvurdering eller udfasning af ikke-godkendte it-systemer. Status 2025 ØKF oplyser, at handleplanen næsten er gennemført. Forvaltningerne mangler at klarmelde 2 systemer til sikkerhedsvurdering hos KIT. I Q4 2025 vil ØKF eskalere systemer med status "Ikke godkendt".			2025 2024 2023 2022
Revisionsbemærkning	I lighed med tidligere år henstilles det, at ► der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018, samt, ► de systemer, der har status "ikke godkendt" eskaleres, jf. anskaffelsescirkulæret, og der træffes de nødvendige foranstaltninger, bl.a. om udfasning, idet disse, jf. kommunes regler, udgør en sikkerhedsrisiko.			

3.3 Bemærkninger og observationer fra sidste år, der i forbindelse med IT-revisionen er konstateret lukket

I 2025 er der lukket 3 væsentlige observationer fra 2024 og 2 væsentlige observationer er overført til anden bemærkning.

- (3.1.2) Risikovurdering af systemer. Ved revisionen i 2024 blev der konstateret mangler i forhold til de nuværende risikovurderinger af systemer. Revisionen henstillede, at de nuværende risikovurderinger af systemer styrkes, så det sikres, at:
  - alle relevante systemer bliver omfattet og med afsæt i opdaterede trusselsvurderinger
  - der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt
  - der udarbejdes en plan, der viser, hvor mange systemer, der fremover risikovurderes, og hvor tit det vil blive foretaget. Planen bør ligeledes omfatte et overblik over det efterslæb, som der er pt.at risikovurderinger af systemer ikke foretages for alle systemer, men kun de systemer der enten har været i drift i minimum fire år, eller hvor forvaltningen er usikker på om informationssikkerhedsniveauet er tilstrækkeligt, samt for systemer, der anvendes tværgående i KK's forvaltninger.

  Denne bemærkning er i 2025 overført til bemærkning 3.2.1 hvor revisionen påpeger behovet for, at styringen og gennemsigtigheden af arbejdet med informationssikkerhed i KK, skal styrkes væsentligt. Risikovurderinger af infrastruktur og systemer vil indgå som en væsentlig foranstaltning i forbindelse med KKs samlede tilgang til risikostyring og accept.
- (3.1.3) Ændringshåndtering. Ved revisionen i 2024 blev det konstateret, at det produktive miljø for klient 000 var åben for programændringer. Vi har ikke konstateret sådanne forhold i 2025.
- (3.1.4) Ændringshåndtering. Ved revisionen i 2024 blev det konstateret, at for to ændringer i produktive miljø for klient 950, blev der ikke sat logning på ved åbning af Kvantum. Vi har ikke konstateret sådanne forhold i 2025.
- (3.1.5) Brugeradministration. Ved revisionen i 2024 blev det konstateret, at passwordopsætning i Kvantum ikke fulgte København Kommunes passwordpolitik for to parameter vedr. længde og kompleksitet. Password længde er ændret fra 8 til 15 og der er nu sat krav om kompleksitet.
- (3.2.1) Ledelsestilsyn med brugerautorisationer. Ved revisionen i 2024 blev det konstateret, at beslutningen om, at it-systemer med adgangsstyring, som håndterer person- eller værdi-oplysninger, skal integreres med kommunens til enhver tid anvendte brugerstyringsløsning ikke er efterlevet. Der er igangsat et arbejde med at få onboardet flere systemer i IGA-løsningen og arbejdet fortsætter i 2025. Denne bemærkning er i 2025 overført til bemærkning 3.2.1 hvor revisionen påpeger behovet for, at styringen og gennemsigtigheden af arbejdet med informationssikkerhed i KK, skal styrkes væsentligt. Brugerstyring vil indgå som en væsentlig foranstaltning i forbindelse med KKs samlede tilgang til risikostyring og accept.

4 Afslutning

De konstaterede forhold har været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

Yderligere spørgsmål eller kommentarer til rapporten kan rettes til EY, Ulrik B. Vassing på telefon 25 29 45 54 eller Intern Revision, Jesper Andersen på telefon 20 42 90 88.

København, den 18. december 2025

EY	Københavns Kommune
Ulrik B. Vassing statsautoriseret revisor	Jesper Andersen revisionschef
Rasmus F. Andersen statsautoriseret revisor	Nicholai Mandrup intern revisor

Bilag - Formidling af risiko og væsentlighed mv.

Vi har i nærværende revision vurderet graden af risiko og væsentlighed for de enkelte observationer, og i tilknytning til den givne observation er påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med
▶ Prioritet 1 markeringer anvendes for forhold, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en revisionsbemærkning.
▶ Et forhold anses for kritisk, såfremt der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt og/eller har en betydelig udbredelse.
▶ Prioritet 1 markeringer rapporteres til ledelsen med påkrav om, at disse forelægges for det stående udvalg eller Økonomiudvalget.
Prioritet 2 – markeres med
▶ Prioritet 2 markeringer anvendes for forhold, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre revisionsbemærkninger i årsberetningen.
▶ Et forhold anses for væsentlig, såfremt der en middel grad af sandsynlighed for, at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse.
▶ Prioritet 2 markeringer rapporteres til ledelsen i den reviderede forvaltning.
Prioritet 3 – markeres med
▶ Anvendes for forhold, der ikke har givet anledning til omtale eller kun anses for mindre væsentlige, og som derfor kun rapporteres til ledelsen som opmærksomhedspunkter.
▶ En risiko anses for mindre væsentlig, såfremt der er en lille grad af sandsynlighed for, at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse.