Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C
Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

Københavns Kommune

Revision af generelle it-kontroller 2011

Indholdsfortegnelse

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C
Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

10.05.2012

Københavns Kommune
Att.: Lars Henningsen
Ottiliavej 3
2500 Valby

Revision af generelle it-kontroller

Indledning

Deloitte har som et led i revisionen af årsrapporten for 2011 revideret de generelle it-kontroller hos Københavns Kommune (herefter KK). Nærværende rapport indeholder vores observationer, anbefalinger og prioriteringer. Rapporten er kun til kommunens egen interne brug.

Nærværende rapport vedrører vores revision af generelle it-kontroller hos Koncernservice (herefter KS) og deres aktiviteter i relation til drift, sikkerhed og vedligeholdelse af den fælles infrastruktur for kommunen.

KK har aftale med KMD omkring drift af mainframe applikationer (KKI-systemer), KØR, Udbudsportalen og WAN forbindelser samt drift vedrørende print og distribution. Vedligeholdelse af KKI systemer varetages af KMD.

De generelle it-kontroller, omfattende de outsourcede platforme og systemer, er ikke omfattet af nærværende rapport, idet vi forventer at modtage revisionserklæring om generelle it-kontroller fra KMD ift. de fælles kommunale systemer. I relation til KK´s specifikke systemer i "hjørneløsningen" (KKI), forventer vi at foretage en gennemgang af teknisk sikkerhed på udvalgte platforme og gennemgang af ændringskontroller primo 2012.

Formål

Generelle it-kontroller er de kontroller, som ledelsen har etableret i og omkring kommunens væsentlige it-platforme med henblik på at opnå en velkontrolleret og sikker it-anvendelse og dermed understøtte en pålidelig databehandling i it-baserede forretningsprocesser.

Som led i revisionen af KK, har Deloitte revideret den del af de generelle it-kontroller, som vi vurderer relevante for aflæggelse af en årsrapport, der giver et retvisende billede uden væsentlig fejlinformation, og som er i overensstemmelse med de lovgivningsmæssige krav.

Formålet har været at vurdere, om ovennævnte generelle it-kontroller dels er udformet på en hensigtsmæssig måde og dels opretholdes og dokumenteres som tilsigtet for regnskabsåret.

Sammenfatning

På baggrund af vores revision af de generelle it-kontroller, som vi har vurderet relevante for at understøtte revisionen af årsrapporten for Københavns Kommune, har vi identificeret følgende væsentlige områder til forbedring:

- It-beredskabsplanen for Københavns Kommune og for Koncernservice er ikke endelig færdigudarbejdet. Vi har noteret en væsentlig fremdrift i arbejdet med at færdiggøre planen i revisionsperioden.
- En formel it-risikoanalyse har været under udarbejdelse i revisionsperioden og er primo 2012 udarbejdet i et endeligt oplæg. I perioden frem til juni 2012 undergår it-risikoanalysen endelig færdiggørelse.
- Kontroller for periodisk opfølgning på tildelte rettigheder udføres ikke konsekvent, hvilket gennemgangen af oprettede brugere i Windows lokalnetværket bekræfter (ansvaret for forholdet ligger i forvaltningerne for egne brugere).
- Vi har ved gennemgang af KK firewall konstateret, at proceduren for konfiguration og vedligeholdelse af firewall regelsættet på en række områder ikke er betryggende.

KK har outsourcet væsentlige områder af de generelle it-kontroller til KMD. KK har for de outsourcede områder rekvireret systemrevisionserklæring til verifikation af, at de outsourcede kontroller gennemføres betryggende for de fælles kommunale systemer. Vi har gennemgået erklæringen, og vores gennemgang heraf har ikke givet anledning til væsentlige bemærkninger.
Revision af teknisk sikkerhed på udvalgte platforme samt revision af ændringer på KKI systemer hos KMD er foretaget af Deloitte på vegne af KK for indeværende regnskabsår.

Vi har i forbindelse med revisionen hos KMD identificeret en række svagheder relateret til den logiske sikkerhed på operativsystemer og databaser, herunder enkelte væsentlige observationer relateret til Oracle, Sun Solaris og z/OS. Der henvises til særskilt erklæring udarbejdet for det vedr. KMD udførte arbejde.

Afsluttende bemærkninger

Vi har konstateret, at der i året er gennemført en række tiltag i overensstemmelse med KS-ledelsens anførte handlingsplaner for 2011. Ved årets udgang er alle handlingsplaner endnu ikke færdigimplementeret, og således udestår arbejdet med implementering af ny sikkerhedsstandard, fælles adgangssystem og nyt ledelsessystem forsat. De nævnte områder vil efter det oplyste blive implementeret i 2. kvartal 2012.

Det er vores vurdering, at det samlede niveau for de generelle it-kontroller i KS forsat bør forbedres i forhold til nuværende status. Vi har konstateret en øget ledelsesfokus og indsats for udbedring af kontrolmanglerne i kommunens it-kontroller og vurderer, at kommunen vil få løftet kvaliteten af de generelle it-kontroller væsentligt, hvis implementering af de anførte tiltag foretages som planlagt. Det bemærkes, at denne vurdering udelukkende omhandler KS, dvs. IKKE observationer og anbefalinger omhandlende TMF Navision og KØR.

Vi har efterfølgende beskrevet revisionens indhold og omfang samt anført de detaljerede observationer og anbefalinger, som revisionen har givet anledning til.

Vi står naturligvis til disposition, såfremt De måtte have spørgsmål eller kommentarer til rapporten.

Deloitte
Statsautoriseret Revisionspartnerselskab

Lynge Skovgaard
statsautoriseret revisor

Mikkel Jon Larssen
partner, CISA

Revisionens indhold og omfang

Revisionen er fokuseret på den del af de generelle it-kontroller, som er væsentlige i forhold til de brugersystemer og tilhørende tekniske platforme, som vi vurderer som væsentlige og risikofyldte i revisionsmæssigt henseende. Udvælgelsen af de generelle it-kontroller er således baseret på en vurdering af omfang, kompleksitet og afhængighed af it-baserede forretningsprocesser samt risikoen for væsentlig fejlinformation ved aflæggelse af årsrapporten.

Vi har således valgt at gennemgå væsentlige, revisionsrelevante generelle it-kontroller, som understøtter den tekniske infrastruktur og de systemer, som afvikles hos Koncernservice. Det er Koncernservice, som har ansvaret for datakommunikation og en sikker adgang til kommunens systemer, uanset om disse er placeret i kommunes egne serverrum eller hos outsourcingleverandører som KMD.

Vores gennemgang har således omfattet generelle it-kontroller inden for områderne it-drift, it-sikkerhed og håndtering af ændringer i infrastruktur og netværkskomponenter, som understøtter de brugersystemer, som driftes hos Koncernservice. Vi har herunder bl.a. gennemgået sikkerheden i kommunens Windows baserede lokalnetværk.

Vi har endvidere revideret de generelle it-kontroller, som understøtter brugersystemerne:

- KØR
- Navision – TMF (Rapporteret i bilag 1)

samt sikkerheden på de tekniske platforme, som brugersystemerne er placeret på:

- SQL-servere for TMF Navision
  - KS-NAV01-TMF
- Windows domains:
  - KS-DC01-KULTUR; KS-DC01-OF; KS-DC01-SUND;
  - KS-DC01-TMF; KS-DC01-UUF; KS-DC01-FAF; KS-DC01

Skraverede anbefalinger vedrørende øvrigt udestående dokumentation bestilt hos kommunen.

Den samlede revision baseres for en dels vedkommende på relevante interne kontroller i kommunen, herunder både manuelle kontroller og kontroller, der automatisk udføres af de brugersystemer, kommunen anvender. 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 udførelse af forretningsaktiviteter i brugersystemerne.

For hvert af de udvalgte brugersystemer og tilhørende tekniske platforme, udvælges og gennemgås de relevante generelle it-kontroller indenfor følgende kontrolområder:

Hovedområde	Delområde
A. It-drift	A1. Jobschedulering A2. Sikkerhedskopiering A3. Fysisk adgang og sikring A5. Nødberedskab
B. It-sikkerhed	B1. It-sikkerhedsledelse B2. It-sikkerhedsadministration B3. Logisk sikkerhed
C. Implementering og vedligeholdelse af netværk og systemsoftware	C1. Ændringskontrol – Netværks- og kommunikationssoftware C2. Ændringskontrol – Systemsoftware
D. Programændringer	D1. Change Governance
E. Implementering og vedligeholdelse af applikationer og databaser	E1. Ændringskontrol – Applikationer E2. Ændringskontrol – Databaser E3. Ændringskontrol – Datakonvertering

Relevante områder revideres i løbet af en flerårig periode (højst 3 år), således at ikke alle områder revideres i samme omfang alle år. Vi følger dog altid op på tidligere rapporterede svagheder samt væsentlige identificerede kontroller inden for de enkelte områder.

For områder, hvor væsentlige kontroller er outsourcet til eksterne leverandører, baserer vi vores revision heraf på modtaget revisionserklæring, der udarbejdes af leverandørens revisor efter anmodning fra KK's ledelse.

Revisionen er udført ved interview af personale hos KK samt ved observation, gennemgang af udleveret materiale samt stikprøvevis gennemgang af tekniske sikkerhedsopsætninger på de udvalgte platforme. De stikprøver, som vi har udvalgt til at teste kontrollernes operationelle effektivitet dækker regnskabsåret 2011.

Udvikling i rapporterede anbefalinger

Overordnet kan udviklingen i antallet af anbefalinger fra it-revisionen anskueliggøres således:

	Prioritet 1	Prioritet 2	Prioritet 3	I alt
Antal anbefalinger fra 2010 revisionen	10	40	8	58
Anbefalinger lukket i indeværende år	-9	-12	-5	-26
Nye anbefalinger ved årets revision	0	12	5	17
Status 2011 (åbne anbefalinger)	**1**	**40**	**8**	**49**

Kontrolmålsoversigt og detailvurderinger

I skemaet på side 7 er i oversigtsform angivet vores vurderinger af faktiske forhold imod kontrolmål for de kontrolområder, som vi har revideret i indeværende år. Skemaet indeholder tillige vores vurderinger for de kontrolområder, som er revideret i tidligere år, såfremt der er blevet fulgt op på disse.

I skemaet er resultatet for hvert kontrolmål angivet ved anvendelse af følgende symboler:

Symbol	Betydning
	De interne kontroller vurderes ikke at fungere effektivt og kræver omgående fokus fra ledelsen. Der er behov for flere væsentlige forbedringer.
	Kontrolniveauet vurderes ikke at fungere tilstrækkeligt effektivt og kræver ledelsens fokus. Der er behov for forbedringer, hvoraf enkelte kan være væsentlige.
	Kontrolniveauet vurderes som relativt højt, og der er alene behov for forbedringer af mindre væsentlig karakter.
	Revisionen af kontrolmålet har ikke givet anledning til bemærkninger.

Skemaet fungerer som en indholdsfortegnelse til de detaljerede observationer og anbefalinger, og det er ud for kontrolmålet angivet, på hvilken side i den detaljerede rapport de pågældende forhold er nærmere beskrevet. Såfremt revisionen af et kontrolmål *ikke* har givet anledning til bemærkninger, er en detaljeret beskrivelse af kontrolmålet således ikke medtaget.

Klassifikation af anbefalinger

For de detaljerede observationer og tilhørende anbefalinger er angivet en prioritet baseret på følgende opdeling:

Prioritet	Betydning
1	**Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol** Anvendes for svagheder i de interne kontroller, der medfører en forøget risiko for, at der opstår eller ikke opdages væsentlig fejlinformation i regnskabsaflæggelsesprocessen - eksempelvis utilstrækkelig adgangsbegrænsning i it-systemer, mulighed for at omgå etablerede kontrolprocedurer samt manglende overordnet stillingstagen til omfang af it-sikkerhed og tilsvarende krav til det interne kontrolmiljø. De interne kontroller vurderes ikke at fungere effektivt, og kræver omgående fokus fra ledelsen og yderligere handlinger for at afdække den identificerede risiko.
2	**Anbefalinger til udbedring af svagheder i den interne kontrol** Anvendes for svagheder i de interne kontroller, der medfører en forøget risiko for, at der opstår eller ikke opdages fejlinformation i regnskabsaflæggelsesprocessen – eksempelvis manglende formalisering af kontrolprocedurer samt utilstrækkelig dokumentation for udførte kontroller. De interne kontroller vurderes ikke at fungere tilstrækkeligt effektivt og kræver ledelsens fokus.
3	**Anbefalinger til forbedring af den interne kontrol i øvrigt** Anvendes for svagheder i de interne procedurer, som - i revisionsmæssigt henseende - ikke medfører en forøget risiko for fejlinformation i indeværende regnskabsår. Forholdet medtages alene som en information til ledelsen om mulig forbedring af de interne kontroller.

Observationer og anbefalinger for Fælles Forhold

Ref.	Kontrolmål	Vurdering 2010	Side	Vurdering 2011
A1	Alle nødvendige jobs og kørsler, såvel online som batch, afvikles rettidigt og korrekt, og kommunen kontrollerer, at dette sker til normal fuldførelse og med forventet resultat.	!		✓
A2	Data sikkerhedskopieres, opbevares og kan fremskaffes i overensstemmelse med gældende lovgivning og kommunens behov.	!	8	!
A3	Den fysiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kommunens behov.	!		✓
A5	En plan for genoptagelse af kommunens primære it-baserede forretningsprocesser efter en katastrofe er udarbejdet, afprøvet og ledelsesgodkendt og vedligeholdes løbende.	X (1)	9	!
B1	En ledelsesgodkendt it-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse og kommunikeret til hele kommunen.	X (1)	10	!
B2	Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kommunens behov.	X (1)	10	!
B3	Den logiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kommunens behov.	X (5)	18	X (1)
C1	Netværk- og kommunikationssoftware kan vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med kommunens behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.	!	26	!
C2	Systemsoftware kan vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med kommunens behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.	!	26	!
D1	Program- og systemændringer bliver administreret hensigtsmæssigt, prioriteret og vurderet, og gennemførelse af ændringer følger en af ledelsen valgt projektmodel.	✓		✓
E1	Tilretninger til applikationer er tilfredsstillende testet, godkendt og implementeret, og de tilrettede funktioner i applikationen er i overensstemmelse med ledelsens og brugernes forventninger.	!	30	!
E2	Tilretninger til databaser er tilfredsstillende testet og implementeret, og databaser fungerer i overensstemmelse med ledelsens forventninger.	✓		✓
E3	Konvertering af eksisterende data til nye eller ændrede applikationer er dokumenteret, og det er sikret, at eksisterende data kan genskabes i tilfælde af fejl ved konvertering.	✓		✓

A. It-drift			
Kontrolmål A2 Data sikkerhedskopieres, opbevares og kan fremskaffes i overensstemmelse med gældende lovgivning og kommunens behov.		**Risiko** Utilstrækkelige backupprocedurer øger risikoen for, at kommunen lider unødige økonomiske tab som følge af, at data ikke kan retableres efter et nedbrud, eller at gældende lovgivning på området ikke overholdes.	
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-01	*Sikkerhedskopiering – strategi* Vi har fået udleveret en meget kortfattet, uformel og overordnet strategi for backup af systemer og data, som KS har ansvaret for. Vi har fået oplyst, at der foreligger godkendte backup aftaler med de enkelte systemejere, men vi har ikke modtaget dokumentation herfor. Manglende eller utilstrækkelig dokumenteret, overordnet backupstrategi medfører risiko for, at den efterfølgende udarbejdelse/konfiguration af backup ikke etableres i overensstemmelse med lov- eller ledelseskrav. **Status 2011** Vi har modtaget en backupstrategi. Denne er dog endnu ikke ledelsesgodkendt. Forholdet reduceres til prioritet 3.	Vi anbefaler, at der udarbejdes en overordnet ledelsesgodkendt backupstrategi, som efterfølgende lægges til grund for etableringen af backup for de relevante systemer. For de enkelte systemer bør backupkrav endvidere godkendes i samarbejde med de enkelte systemejere. **Ledelsens kommentar 2010** Implementering af ny backupløsning på basis af Netback fra Symantec indbefatter definition af et antal backupprogrammer, som vil blive forelagt til ledelsesgodkendelse. Systemejere kan herefter vælge at benytte et standard backupprogram (cyklus og retensionperiode) eller bestille særligt job. Backupstrategi er godkendt af ledelsen i april 2011.	3
11-01	*Sikkerhedskopiering – test* Vi har konstateret, at det med den tilgængelige dokumentation ikke er muligt at kontrollere, om de registrerede restoretests er udført, da der ikke registreres dato eller anden information for testen, som kan identificerer handlingen i OpsCenter systemet. Desuden har vi konstateret, at der ved generelle restores oprettes en ticket i Remedy, men at der i denne ikke er link til OpsCenter. Manglende eller utilstrækkelig kontrol af mulighederne for at anvende den etablerede backupløsning medfører risiko for, at backupløsningen ikke kan anvendes som forventet.	Vi anbefaler, at test af restore samt generel restores dokumenteres på en måde, som muliggør efterfølgende kontrol af handlingen. **Ledelsens kommentar 2011** Der afventes udtalelse fra Intern revision, men indtil denne foreligger, vil testrestore blive registreret som en særlig produktkategori i sagsstyringssystemet "Remedy", således at gennemførte testrestore kan dokumenteres via sagsudtræk. Ændringen i sagsstyringssystemet forventes gennemført inden 15.5.2012.	3

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

A. It-drift

Kontrolmål A5
En plan for genoptagelse af kommunens primære it-baserede forretningsprocesser efter en katastrofe er udarbejdet, afprøvet og ledelsesgodkendt og vedligeholdes løbende.

Risiko
Utilstrækkelige, uafprøvede eller ikke-godkendte nødplaner for håndtering af større nedbrud i it-anvendelsen øger risikoen for, at retablering tager længere tid, end ledelsen forventer, og at kommunen som følge heraf lider ikke kalkulerede eller unødige økonomiske tab.

Pkt.	Observation	Anbefaling	Pri.
09-44	*Beredskabsplanlægning* Vi har fået oplyst, at der ikke er gennemført en risikovurdering og med udgangspunkt heri etableret en formel, godkendt og testet beredskabsplan. Manglende eller utilstrækkelig fastlæggelse og godkendelse af omfanget af beredskabsplanlægningen (systemer, platforme, acceptable retableringstider og lignende) medfører risiko for, at retableringsforanstaltninger ikke er i overensstemmelse med ledelsens forventninger hertil. **Status 2011** Vi har konstateret at en beredskabsplan er under udarbejdelse. Vi har efterfølgende fået oplyst, at beredskabsplanen er blevet præsenteret, og skabelonen er accepteret af ledelsen på et møde primo februar 2012. Vi har verificeret dette ved gennemgang af mødereferat. Grundet beredskabsplanens nuværende stadie og fremskridt mht. implementeringen, så nedprioriteres punktet til prioritet 2.	Vi anbefaler, at grundlaget for og formålet med beredskabsplanlægningen fastlægges og godkendes formelt af ledelsen, samt at opfyldelsen af kravene pr. system og platform efterfølgende dokumenteres og rapporteres til ledelsen. **Ledelsens kommentar 2010** KS forventer at afslutte BIA for KS medio marts 2011. Der vil herefter blive lagt en tidsplan for gennemførelse af risikoanalyse i forvaltningerne, som forventes afsluttet i løbet af 2. halvår 2011. Beredskabsplanen i kommunen bliver udbygget i takt med, at risikoanalysen bliver gennemført i forvaltningerne i 2. halvår 2011. Se i øvrigt 09-05. **Ledelses kommentar 2011** KS har afholdt møde med Deloitte, hvor igangværende aktiviteter for etablering af Beredskabsplan er blevet fremvist og dokumenteret. Ligeledes er der fremsendt dokumentation til Deloitte for ledelsens accept af igangværende aktiviteter.	2
11-02	*Beredskabsplaner – test* Det oplyses, at der ikke foreligger en endelig it-beredskabsplan, hvorfor denne ikke regelmæssigt testes. Efter det oplyste fandt man i forbindelse med skybruddet ud af, at den nuværende plan ikke var tilstrækkelig og havde en række huller. Vi har efterfølgende modtaget ajourført beredskabsplan med beskrivelse af skrivebordstests samt kriterier og defineret krav til test af beredskabsplanen. Planen er dog stadig ikke endelig færdigudarbejdet og afstemt med bl.a. systemejerne. Manglende eller utilstrækkelig koordinering med systemejerne mht. test af den etablerede beredskabsplanlægning medfører risiko for, at væsentlige systemer og platforme i kommunens opgavevaretagelse ikke kan retableres i overensstemmelse med forventningerne.	Vi anbefaler, at der som minimum gennemføres skrivebordstest af kritiske forudsætninger i beredskabsplanlægningen, samt at kritiske delelementer i denne - f.eks. retablering via backupmedier - tillige afprøves og vurderes. Gennemførte test bør dokumenteres og godkendes samt koordineres med systemejerne, og identificerede ændringsbehov på baggrund af testen bør indarbejdes i den samlede beredskabsplanlægningen. **Ledelsens kommentar 2011** KS planlægger at teste Beredskabsplanen, når denne foreligger.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Kontrolmål B1

En ledelsesgodkendt it-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse og kommunikeret til hele kommunen.

Risiko

Manglende overordnet it-sikkerhedspolitik, udarbejdet med udgangspunkt i en it-risikoanalyse og kommunikeret til medarbejderne, medfører risiko for, at den etablerede sikkerhed i forbindelse med it-anvendelsen ikke i tilstrækkelig grad opfylder kommunens behov.

Pkt.	Observation	Anbefaling	Pri.
09-05	*It-risikoanalyse* Vi har fået oplyst, at der ikke er udarbejdet en overordnet og ledelsesgodkendt it-risikoanalyse, som dækker KS. En manglende eller utilstrækkelig it-risikoanalyse medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante. **Status 2011** Det er oplyst, at it-risikoanalysen endnu ikke er færdigudarbejdet. Vi har dog modtaget risikoanalyse fase 2 med aktivitetsliste for 1. samt 2.kvartal 2012. Nuværende oplæg til risikoanalysen, behandler højrisiko områder og kommer med anbefalinger til tiltag. Vi har endvidere modtaget ledelsespræsentation vedr. risikoanalyse og beredskabsplan 2011. En af aktiviteterne fra risikoanalysen er, at opdaterer it-beredskabsplanen på baggrund af observationer fra risikoanalysen planlagt til 1/6 2012. Punktet nedgraderes til prioritet 2.	Vi anbefaler, at arbejdet med nuværende it-risikoanalyse færdiggøres i 2. kvartal 2012, og prioriterede tiltag med henblik på fastlæggelse af it-sikkerhedsniveauet i kommunen implementeres i it-beredskabsplanen. Endvidere anbefaler vi, at it-risikoanalysen derefter opdateres periodisk - minimum én gang årligt - samt når andre faktorer indikerer nødvendigheden heraf, f.eks. større planlagte ændringer eller uventede hændelser af it-sikkerhedsmæssig karakter. **Ledelses kommentar 2011** It-risikoanalyse er udarbejdet. KS arbejder i øjeblikket med aktionsplan på lukning af "findings".	2

Kontrolmål B2

Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kommunens behov.

Risiko

Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov.

Pkt.	Observation	Anbefaling	Pri.
10-03	*Brugerrettigheder – nedlæggelser* Vi har fået oplyst, at der ikke er etableret en kontrol, som sikrer, at KS-BA konsekvent bliver orienteret om medarbejderes fratrædelse eller ændring i arbejdsopgaverne. I de tilfælde, hvor KS-BA bliver informeret om en brugers fratrædelse, foreligger der formelle procedurer for håndtering af nedlæggelse af disse brugere. Vi har supplerende fået oplyst, at KK er i gang med et projekt omkring sammenkøring af AD adgang og lønsystemet, hvorved ændring af adgang initieres via ændring i ansættelsesforholdet. Manglende eller utilstrækkelig kontrol med fratagelse af brugeres rettigheder medfører øget risiko for, at brugere misbruger disse rettigheder, f.eks. efter en afskedigelse. **Status 2011** Forholdet er uændret. Vi har fået oplyst, at KS-BA fortsat ikke bliver informeret om alle fratrædelser eller ændringer af medarbejdernes adgang. Sammenkøring af AD adgang og lønsystem er ikke endelig implementeret, hvorved der stadig er risiko for, at ændringer og fratrådte medarbejdere ikke bliver opdateret i AD.	Vi anbefaler, at proceduren for nedlæggelser bliver fulgt, og alle ændringer/nedlæggelser af medarbejdere i de enkelte enheder bliver meldt ind til KS-BA. Vi anbefaler tillige, at sammenkøring af AD og lønsystemet bliver færdigimplementeret således, at ændringer af medarbejderforhold bliver afspejlet i deres systemmæssige adgang til kommunen. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
10-04	*Brugerrettigheder – periodisk revurdering* Vi har fået oplyst, at der ikke periodisk foretages gennemgang og revurdering af tildelte rettigheder til brugere på applikationerne, herunder f.eks. KØR og Netværket (Domain adgang). Vi har endvidere fået oplyst, at det er de enkelte forvaltninger der er ansvarlige for periodisk gennemgang af rettigheder. Manglende eller utilstrækkelig periodisk revurdering af tildelte rettigheder til brugere medfører risiko for, at brugeres rettigheder bliver utidssvarende og ikke afspejler deres arbejdsmæssigt betingede behov. **Status 2011** Vi har modtaget dokumentation for udførsel af en brugergennemgang, hvor de enkelte it-sikkerhedsledere har kommenteret på lister over brugerautorisationer. Det er dog oplyst, at der ikke har været kontrol med, om alle it-sikkerhedsledere returnerede deres lister. Dog er det oplyst, at KK er i gang med at implementere et Identity Management system. Prioriteten reduceres til prioritet 2.	Vi anbefaler, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere for relevante systemer og platforme. Ansvaret herfor ligger i forvaltningerne for egne brugere. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive mulighederne for, at fremtidige revurderinger foretages af de daglige ledere og sikre mulighederne for kontrol af, at revurderingerne foretages. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2
09-06	*It-sikkerhedslogning* Vi har konstateret, at der i it-sikkerhedspolitikken stilles krav om logning af brugeres handlinger med henblik på at opdage forsøg på uautoriserede handlinger, herunder forsøg på uautoriseret tilgang til systemer. Vi har endvidere fået oplyst, at der ikke er etableret en kontrol med henblik på at sikre, at specificerede logningskrav implementeres på relevante platforme. Vores gennemgang af opsat logning på Windows platformen viser, at der ikke i alle tilfælde er opsat en betryggende logning. Endvidere har vi fået oplyst, at der ikke periodisk sker gennemgang af relevante logs eller alarmer på baggrund af disse. Manglende eller utilstrækkelig sikkerhedsmæssig logning medfører risiko for, at forsøg på uautoriserede handlinger ikke opdages og imødegås i tilstrækkeligt omfang. **Status 2011** Vi har konstateret, at der i it-sikkerhedspolitikken fortsat er beskrevet, at sikkerhedshændelser løbende skal registreres og følges op på. Ved gennemgang af Windows platformen, har vi dog konstateret, at der fortsat ikke i alle tilfælde er opsat en betryggende logning. Bl.a. bliver uautoriserede adgangsforsøg ikke logget. Der er i risikovurderingen ikke en stillingstagen til fra KK, om hvorvidt risikoen for denne form for sikkerhedslogning kan forsvares. Endvidere er det oplyst, at disse logs anvendes reaktivt og dermed ikke gennemgås og følges op på periodisk, som kravene foreskriver i it-sikkerhedspolitikken.	Vi anbefaler, at der i risikovurderingen tages stilling til krav til sikkerhedslogning, og risici vurderes bl.a. for logning af uautoriserede adgangsforsøg. Baseret på risikovurderingen bør sikkerhedslogning implementeres og følges op hos KK ifølge kravene i overensstemmelse med kommunens it-sikkerhedspolitik. **Ledelses kommentar 2011** It-sikkerhed har grundet stort tidspres i forbindelse med udarbejdelse af beredskabsplan, risikoanalyse mv. nedprioriteret opgaven vedr. eftersynet af alle systemers overholdelse af logningskontrol. Det forventes, at indsamling af data kan genoptages medio 2012 med afslutning ultimo 2012. Efter en relancering af systemoversigten FISKK.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
11-03	*Brugerrettigheder - udvidede rettigheder* Det er oplyst, at it-serverdriften selv tildeler administrative rettigheder. Dog udfyldes der ingen blanket for oprettelsen af administrator brugeren. Manglende eller utilstrækkelig kontrol med tildeling af administrative rettigheder medfører risiko for, at sådanne rettigheder ikke tildeles tilstrækkeligt restriktivt.	Vi anbefaler, at tildeling af administrative rettigheder kun sker på baggrund af formelle og dokumenterede autorisationer. **Ledelsens kommentar 2011** KS er enige i revisionens anbefaling.	2

Observationer og anbefalinger relateret til gennemgang af platform:			
Windows 2003 – it-sikkerhedslogning			
Windows 2003 – KS-DC01-UUF (Børn og Ungdoms Forvaltningen)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-08	På serveren KS-DC01-UUF har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • Policy Change (Success) • System Events (Success) • Account Management (Success) • Account Logon Events (Success) • Logon Events (Success) • Directory Service Access (Success) • Object Access (No auditing) • Privilege Use (No auditing) Manglende eller utilstrækkelig logning medfører risiko for, at hændelser - eller forsøg herpå - ikke registreres i fornødent omfang. **Status 2011** Forholdet er uændret.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Management (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events(Success + Failure) • Directory Service Access (Failure) • Object Access (Failure) • Privilege Use (Failure) **Ledelses kommentar 2011** På grund af fejl i opsætning af policy har indstillinger på eventlog ikke slået igennem. Der er change under udarbejdelse med henblik på at aktivere logningen 100% i overensstemmelse med anbefalingen og nedenstående i pkt. 09-08 på alle DC'ere. Der forventes implementeret nedenstående: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Management (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events(Success + Failure) • Directory Service Access (Failure) • Object Access (Success + Failure) • Privilege Use (Failure)	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Windows 2003 – KS-DC01-TMF (Teknik og Miljø Forvaltningen)

Pkt.	Observation	Anbefaling	Pri.
09-10	På serveren KS-DC01-TMF har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • Policy Change (Success) • System Events (Success) • Account Logon Events (Success) • Logon Events (Success) • Directory Service Access (Success) • Object Access (No auditing) • Privilege Use (No auditing) Manglende eller utilstrækkelig logning medfører risiko for, at hændelser - eller forsøg herpå - ikke registreres i fornødent omfang. **Status 2011** Forholdet er uændret.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events (Success + Failure) • Directory Service Access (Failure) • Object Access (Failure) • Privilege Use (Failure) **Ledelses kommentar 2011** På grund af fejl i opsætning af policy har indstillinger på eventlog ikke slået igennem. Der er change under udarbejdelse med henblik på at aktivere logningen 100% i overensstemmelse med anbefalingen og i pkt. 09-08 på alle DC'ere. Der forventes implementeret nedenstående: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Management (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events(Success + Failure) • Directory Service Access (Failure) • Object Access (Success + Failure) • Privilege Use (Failure)	2

Windows 2003 – KS-DC01-SUND (Sundhed og Omsorgs Forvaltningen)

Pkt.	Observation	Anbefaling	Pri.
09-12	På serveren KS-DC01-SUND har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • Account Logon Events (Failure) • Directory Service Access (No auditing) • Object Access (No auditing) • Privilege Use (No auditing) Manglende eller utilstrækkelig logning medfører risiko for, at hændelser - eller forsøg herpå - ikke registreres i fornødent omfang. **Status 2011** Forholdet er uændret.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • Account Logon Events (Success + Failure) • Directory Service Access (Failure) • Object Access (Failure) • Privilege Use (Failure) **Ledelses kommentar 2011** På grund af fejl i opsætning af policy har indstillinger på eventlog ikke slået igennem. Der er change under udarbejdelse med henblik på at aktivere logningen 100% i overensstemmelse med anbefalingen og i pkt. 09-08 på alle DC'ere. Der forventes implementeret nedenstående: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Management (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events(Success + Failure) • Directory Service Access (Failure) • Object Access (Success + Failure) • Privilege Use (Failure)	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Windows 2003 – KS-DC01-OF (Økonomiforvaltningen)

Pkt.	Observation	Anbefaling	Pri.
09-15	På serveren KS-DC01-OF har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • System Events (No auditing) • Account Logon Events (Success) • Directory Service Access (Success) • Object Access (No auditing) Manglende eller utilstrækkelig logning medfører risiko for, at hændelser - eller forsøg herpå - ikke registreres i fornødent omfang. **Status 2011** Forholdet er uændret.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • System Events (Success + Failure) • Account Logon Events (Success + Failure) • Directory Service Access (Failure) • Object Access (Failure) **Ledelses kommentar 2011** På grund af fejl i opsætning af policy har indstillinger på eventlog ikke slået igennem. Der er change under udarbejdelse med henblik på at aktivere logningen 100% i overensstemmelse med anbefalingen og i pkt. 09-08 på alle DC'ere. Der forventes implementeret nedenstående: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Management (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events(Success + Failure) • Directory Service Access (Failure) • Object Access (Success + Failure) • Privilege Use (Failure)	2

Windows 2003 – KS-DC01-KULTUR

Pkt.	Observation	Anbefaling	Pri.
11-04	På serveren KS-DC01-KULTUR har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • Logon Events (Failure) Manglende eller utilstrækkelig logning medfører risiko for, at hændelser - eller forsøg herpå - ikke registreres i fornødent omfang.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • Logon Events (Success + Failure) **Ledelses kommentar 2011** Der forventes implementeret nedenstående: • Policy Change (Success + Failure) • System Events (Success + Failure) • Account Management (Success + Failure) • Account Logon Events (Success + Failure) • Logon Events(Success + Failure) • Directory Service Access (Failure) • Object Access (Success + Failure) • Privilege Use (Failure)	3

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Sårbarhedsscanning

Platform - kontrolmål	Risiko
Platformen (operativsystem) er konfigureret sikkert og vedligeholdes, således at platformen forbliver sikker og stabil. Sikkerheden omkring platformen omfatter: - Konfiguration af services - Kryptering relateret til administration og dataoverførsel - Adgangskontrol til administration - Sikkerhedsopdatering af operativsystemer	Manglende konfiguration og vedligeholdelse af platformen kan føre til manglende sikkerhed og driftsstabilitet for de services, som it-infrastrukturen er afhængig af. Sikkerheden i applikationer og database software er ikke effektiv, hvis den underliggende platform har sårbarheder, hvorfor sikkerhedsniveauet på platformniveau er centralt for hele infrastrukturen.

Pkt.	Observation	Anbefaling	Pri.
11-05	*Konfigurationsmæssige sårbarheder, SSL opsætning* Vi har under scanning af de interneteksponerede servere, observeret, at følgende IP-adresser er sårbare overfor en kendt SSL-relateret sårbarhed: • 193.169.155.8 (Citrix Netscaler) • 193.169.155.9 (Citrix Netscaler) • 193.169.155.10 (Citrix Netscaler) Sårbarheden omfatter: • CVE-2009-3555: SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection Vi har endvidere observeret, at følgende IP-adresser er sårbare overfor en anden SSL-relateret sårbarhed_ • 193.169.155.9 (Citrix Netscaler) • 193.169.155.10 (Citrix Netscaler) Sårbarheden omfatter: • CVE-2011-1473: SSL / TLS Renegotiation DoS Vi har yderligere fået oplyst, at der kører en krypteret tunnel inde i SSL-tunnelen. Vi vurderer, at der er lav risiko for tab af fortrolighed, da det kræver stor teknisk viden at udnytte sårbarheden samt adgang til datatrafikken.	Vi anbefaler, at de pågældende SSL servere konfigureres til kun at understøtte SSLv3 og TLSv1 og krypteringsalgoritmer med en nøglelængde på mindst 128 bit. **Ledelses kommentar 2011** KS er enige i observationen, og ændringen vil blive implementeret.	3
11-06	*Konfigurationsmæssige sårbarheder, SSL opsætning* Vi har under gennemgangen af de interneteksponerede servere konstateret, at svage SSL-krypteringsalgoritmer er tilladte på følgende ip-adresser: • 193.169.154.111 (KS-WEBHOTEL01_public) • 62.242.41.29 Brug af svage krypteringsalgoritmer udgør en risiko for, at krypteringen kan brydes. Hvis sårbarhederne udnyttes af en angriber, kan det betyde tab af fortrolighed. Vi vurderer, at der er øget risiko for, at en angriber vil kunne gøre brug af disse svagheder, da det dels kræver stor teknisk indsigt at udnytte sårbarheden, og dels kræver adgang til datatrafikken.	Vi anbefaler, at de pågældende SSL servere konfigureres til kun at understøtte stærke krypteringsalgoritmer med en nøglelængde på mindst 128 bit. **Ledelses kommentar 2011** KS er enige i observationen, og ændringen vil blive implementeret.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
11-07	*Konfigurationsmæssige sårbarheder, SSL opsætning* Vi har under scanning af de interneteksponerede servere, observeret, at SSLv2 understøttes på følgende ip-adresser: • 193.169.154.111 (KS-WEBHOTEL01_public) • 62.242.41.29 • 193.169.154.125 Brug af SSLv2 udgør en særlig risiko, da der eksisterer kendte sårbarheder til denne version, hvormed en angriber kan opnå adgang til oplysninger, som udveksles mellem servere og klienter. Hvis sårbarhederne udnyttes af en angriber, kan det betyde tab af fortrolighed. Vi vurderer, at der er øget risiko for, at en angriber vil kunne gøre brug af disse svagheder, da det dels kræver stor teknisk indsigt at udnytte sårbarheden og dels kræver adgang til datatrafikken.	Vi anbefaler, at de pågældende SSL servere konfigureres til kun at understøtte SSLv3 og TLSv1. **Ledelses kommentar 2011** KS er enige i observationen, og ændringen vil blive implementeret.	2
11-10	*Interne IP-adresser offentligt tilgængeligt* Vi har under scanning af de interneteksponerede servere konstateret, at en intern LAN-IP-adresse er synlig for brugerne på IP-adressen: • 62.242.41.29 (StormP_og_Biblioteksbase_ext) svarer til den interne adresse 10.47.151.51 Vi vurderer, at der er lav risiko for, at information om interne IP-adresser i sig selv kan føre til en sikkerhedshændelse, men det kan give en angriber information om den bagvedliggende netværksinfrastruktur, hvilket kan bruges til mere avancerede angreb.	Vi anbefaler, at interne IP-adresser ikke benyttes i kode - ej heller sider, der eksponeres på internettet. **Ledelses kommentar 2011** KS er enige i anbefalingen. Anbefalingen vil blive formidlet til systemejer, som har ansvaret for applikationens sikkerhed.	3

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Applikation – kontrolmål	Risiko
Applikationen er programmeret sikkert og beskyttet mod uautoriseret adgang. Applikationssikkerhed omfatter: - Adgangskontrol i forhold til applikation og administration - Sessionshåndtering og kryptering - Datavalidering og applikationslogik	Manglende sikkerhed omkring autentifikation, autorisation og sessionshåndtering i applikationer kan føre til uautoriseret adgang til applikationer og administrativ funktionalitet. Manglende datavalidering kan føre til SQL injection og Cross Site Scripting (XSS) angreb, der typisk benyttes i relation til målrettede hacker- og virusangreb. Applikationslaget er det mest komplekse lag i infrastrukturen og udgør den største risiko for tab af fortrolighed, integritet og tilgængelighed af data.

Pkt.	Observation	Anbefaling	Pri.
	Vedligeholdelse – PHP Vi har observeret, at serveren på følgende IP-adresse: • 193.169.154.125 har sårbarhederne: • php-cve-2011-1148 PHP use-after-free in substr_replace() • php-cve-2011-1938 Fixed stack buffer overflow in socket_connect() • php-cve-2011-2202 File path injection vulnerability in RFC1867 File upload filename • php-cve-2011-2483 PHP Updated crypt_blowfish to 1.2	Vi anbefaler, at alle relevante sikkerhedsopdateringer fra leverandøren af den pågældende platform installeres hurtigst muligt. Vi anbefaler, at der indarbejdes procedurer, der sikrer, at kritiske sikkerhedsopdateringer løbende installeres. **Ledelses kommentar 2011** KS er enige i observationen. Systemejer vil blive tilskrevet om svagheden i applikationen. Risikomæssigt er kontrolmanglen mindre væsentlig, idet serveren ikke er medlem af kommunens domain og kan betragtes som en stand alone løsning i DMZ.	
11-12	Vi har fået oplyst, at serveren KS-VALHALLA på den interne IP-adresser ligger bag ved 193.169.154.125. Vi har endvidere fået oplyst, at serveren benyttes til at kontrollere og kommunikere med tilforordnede til folketingsvalg. Vi vurderer, at der er forøget risiko for, at en angriber vil kunne udnytte de fundne sårbarheder til at sætte webserveren ud af drift eller i værste fald udføre kommandoer på serveren. Det kan føre til tab af tilgængelighed og fortrolighed og kan potentielt påvirke de valgtilforordnede og dermed afviklingen af folketingsvalg. **Status 2011** Da sårbarhederne ikke direkte har indvirkning på Kbh. Kommunes regnskabsaflæggelse, har Deloitte revurderet risiko-kategoriseringen af anbefalingen også set i lyset af Kbh. Kommunes kommentar.		3

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Kontrolmål B3	Risiko
Den logiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kommunens behov.	Svagheder i den logiske sikkerhed øger risikoen for, at interne eller eksterne personer får uautoriseret adgang til it-ressourcerne og dermed mulighed for at slette, ændre eller kopiere programmer eller data eller i øvrigt kompromittere kommunens it-anvendelse. Endvidere øger svagheder risikoen for, at adgangen til it-systemerne ikke understøtter den i kommunen etablerede organisatoriske funktionsadskillelse.

Observationer og anbefalinger relateret til gennemgang af platform:

Windows 2003 – it-sikkerhedskonfiguration

Windows 2003 – KS-DC01-UUF (Børn og Ungdoms Forvaltningen)

Pkt.	Observation	Anbefaling	Pri.
09-07	På serveren KS-DC01-UUF har vi observeret følgende: • 1459 aktive brugerprofiler, der er undtaget fra brug af passwords. • 520 aktive brugerprofiler, hvor password aldrig udløber. • 149 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 2903 aktive brugerprofiler, der aldrig har været logget på Windows. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 768 aktive brugerprofiler, hvor password aldrig udløber. • 878 aktive brugerprofiler, som ikke har fået ændret deres password. • 1235 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 1399 aktive brugerprofiler, der aldrig har været logget på Windows. • 1861 aktive brugerprofiler, som ikke har ændret password i mere end 90 dage. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Windows 2003 – KS-DC01-TMF (Teknik og Miljø Forvaltningen)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-09	På serveren KS-DC01-TMF har vi observeret følgende: • 228 aktive brugerprofiler, der er undtaget fra brug af passwords. • 389 aktive brugerprofiler, hvor password aldrig udløber. • 90 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 960 aktive brugerprofiler, der aldrig har været logget på Windows. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 9 aktive brugerprofiler, der er undtaget fra brug af passwords. • 650 aktive brugerprofiler, hvor password aldrig udløber. • 258 aktive brugerprofiler, som ikke har fået ændret deres password. • 745 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 479 aktive brugerprofiler, der aldrig har været logget på Windows. • 1105 aktive brugerprofiler, som ikke har ændret password i mere end 90 dage. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Windows 2003 -- KS-DC01-SUND (Sundhed og Omsorgs Forvaltningen)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-11	På serveren KS-DC01-SUND har vi observeret følgende: • 445 aktive brugerprofiler, der er undtaget fra brug af passwords. • der findes 495 aktive brugerprofiler, hvor password aldrig udløber. • 403 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 3129 aktive brugerprofiler, der aldrig har været logget på Windows. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 28 aktive brugerprofiler, der er undtaget fra brug af passwords. • 561 aktive brugerprofiler, hvor password aldrig udløber. • 1632 aktive brugerprofiler, som ikke har fået ændret deres password. • 2607 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 1471 aktive brugerprofiler, der aldrig har været logget på Windows. • 2698 aktive brugerprofiler, som ikke har ændret password i mere end 90 dage. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Windows 2003 – KS-DC01-OF (Økonomiforvaltningen)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-13	På serveren KS-DC01-OF har vi observeret følgende: • 608 aktive brugerprofiler, der er undtaget fra brug af passwords. • 304 aktive brugerprofiler, hvor password aldrig udløber. • der findes 98 aktive brugerprofiler, som ikke har fået ændret deres password. • 185 aktive brugerprofiler har ikke været logget på i et længere tidsrum. • 269 aktive brugerprofiler har aldrig været logget på Windows. • 409 aktive brugerprofiler har ikke skiftet password i et længere tidsrum. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 189 aktive brugerprofiler, der er undtaget fra brug af passwords. • 431 aktive brugerprofiler, hvor password aldrig udløber. • 103 aktive brugerprofiler, som ikke har fået ændret deres password. • 422 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 315 aktive brugerprofiler, der aldrig har været logget på Windows. • 667 aktive brugerprofiler, som ikke har ændret password i mere end 90 dage. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2
09-14	På serveren KS-DC01-OF har vi observeret, at der findes 21 aktive Administrator konti, hvilket bl.a. inkluderer kontoen "AfSys". Tildeling af administrative privilegier til for mange brugerprofiler medfører risiko for, at sikkerheden ikke kan opretholdes på systemet. **Status 2011** Forholdet er uændret. Antallet af administratorkonti er dog steget til 26.	Vi anbefaler, at antallet af brugerprofiler med administrative privilegier revurderes og nedbringes såfremt muligt. **Ledelses kommentar 2011** KS er enig i observationen. Der arbejdes fortsat på reduktion, men KBH Brand har behov for et antal administratorer på grund af egen administration af eget netværk.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Windows 2003 – KS-DC01-KULTUR (Kultur og Fritids Forvaltningen)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-16	På serveren KS-DC01-KULTUR har vi observeret følgende: • 14 aktive brugerprofiler er undtaget fra brug af passwords. • 213 aktive brugerprofiler, hvor password aldrig udløber. • der findes 147 aktive brugerprofiler, som ikke har fået ændret deres password. • 364 aktive brugerprofiler har ikke været logget på i et længere tidsrum. • 310 aktive brugerprofiler har aldrig været logget på Windows. • 601 aktive brugerprofiler har ikke skiftet password i et længere tidsrum. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 282 aktive brugerprofiler, hvor password aldrig udløber. • 128 aktive brugerprofiler, som ikke har fået ændret deres password. • 525 aktive brugerprofiler, der ikke har været logget på i et længere tidsrum. • 207 aktive brugerprofiler, der aldrig har været logget på Windows. • 661 aktive brugerprofiler, som ikke har ændret password i mere end 90 dage. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2
09-17	På serveren KS-DC01-KULTUR har vi observeret, at der findes 21 aktive Administrator konti, hvilket bl.a. inkluderer fællesbrugerkontoen "bibedb". Tildeling af administrative privilegier til for mange brugerprofiler medfører risiko for, at sikkerheden ikke kan opretholdes på systemet. **Status 2011** Forholdet er uændret. Antallet af administratorkonti er dog faldet til 16. Brugeren 'bibedb' er fortsat aktiv og medlem af administratorgruppen.	Vi anbefaler, at antallet af brugerprofiler med administrative privilegier revurderes og nedbringes, såfremt muligt. **Ledelses kommentar 2011** KS er enig i observationen. Der pågår arbejde med reduktion af administratorkonti.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Windows 2003 – KS-DC01 (Koncern Service)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-18	På serveren KS-DC0 har vi observeret følgende: • 374 aktive brugerprofiler er undtaget fra brug af passwords. • 109 aktive brugerprofiler, hvor password aldrig udløber. • der findes 82 aktive brugerprofiler, som ikke har fået ændret deres password. • 90 aktive brugerprofiler har ikke været logget på i et længere tidsrum. • 157 aktive brugerprofiler har aldrig været logget på Windows. • 184 aktive brugerprofiler har ikke skiftet password i et længere tidsrum. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 236 aktive brugerprofiler, hvor password aldrig udløber. • 209 aktive brugerprofiler, som ikke har fået ændret deres password. • 459 aktive brugerprofiler har ikke været logget på i et længere tidsrum. • 247 aktive brugerprofiler har aldrig været logget på Windows. • 452 aktive brugerprofiler har ikke skiftet password i et længere tidsrum. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2
09-19	På serveren KS-DC01 har vi observeret, at der findes 25 aktive Administrator konti, hvilket bl.a. inkluderer kontoen "PHPWebUserADReadWrit", samt 108 aktive brugerprofiler der er medlem af gruppen "Account Operators" og dermed er tildelt administrative privilegier. Dette inkluderer bl.a. kontoen "SD-TEST". Tildeling af administrative privilegier til for mange brugerprofiler medfører risiko for, at sikkerheden ikke kan opretholdes på systemet. **Status 2011** Forholdet er uændret. Antallet af Account Operators er faldet til 64 dog er antallet af administratorer steget til 36.	Vi anbefaler, at antallet af brugerprofiler med administrative privilegier revurderes og nedbringes såfremt muligt. **Ledelses kommentar 2011** KS er enig i observationen og følger ledelsesbeslutning om, at alle teknikere skal være accountoperator.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Windows 2003 – KS-DC01-FAF (Social, Beskæftigelses og Integrations Forvaltningerne)			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-21	På serveren KS-DC01-FAF har vi observeret følgende: • 8199 aktive brugerprofiler er undtaget fra brug af passwords. • 236 aktive brugerprofiler, hvor password aldrig udløber. • 461 aktive brugerprofiler har ikke været logget på i et længere tidsrum. • 3632 aktive brugerprofiler har aldrig været logget på Windows. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har observeret følgende: • 1446 aktive brugerprofiler, hvor password aldrig udløber. • 2038 aktive brugerprofiler, som ikke har fået ændret deres password. • 3548 aktive brugerprofiler har ikke været logget på i et længere tidsrum. • 3300 aktive brugerprofiler har aldrig været logget på Windows. • 5262 aktive brugerprofiler har ikke skiftet password i et længere tidsrum. Forholdet er således uændret.	Vi anbefaler, at der foretages en gennemgang af brugere, således at det sikres, at alle brugere følger de overordnede retningslinjer for skift af passwords. Vi anbefaler endvidere, at brugere, som ikke længere benyttes, gennemgås og slettes eller disables. **Ledelses kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive den fremtidige vedligeholdelsesproces for brugerdata og brugerprofiler. Projektets arbejde med vedligeholdelsesprocessen forventes afsluttet i 2. kvt. 2012.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Firewall – FW_OTT_Cluster1			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
10-06	Vi har konstateret, at der tillades usikre administrative services (f.eks. ftp, telnet og http) mod 2. level firewall modulerne fra interne og eksterne IP adresser. Følgende regler medvirker til dette: 6, 12, 20, 159, 185 Vi vurderer, at manglende kryptering af data, der sendes imellem administrator og firewall-moduler medfører risiko for, at data, som sendes i klar tekst over netværket opsnappes og misbruges. **Status 2011** Vi har konstateret, at der stadig tillades usikre administrative services mod firewall-modulerne. Minimum regel 25 medvirker til dette. Vi vurderer stadig, at manglende kryptering af data, der sendes imellem administrator og firewall-moduler medfører risiko for, at data, som sendes i klar tekst over netværket opsnappes og misbruges. Dette er specielt kritisk i pågældende netværkssegment, da dette er firewall-administration. Observationen opretholdes. **Status 2011** Der tillades usikker tjeneste i form af telnet adgang på det interne net. Dog har Deloitte revurderet anbefaling, da der er tale om det interne net hos KK, hvor andre sikkerhedsforanstaltninger, såsom etablering af adgangskontrol, gør, at risikoen ikke kan udnyttes bredt. Punktet nedprioriteres til prioritet 3.	Vi anbefaler, at adgang til firewallen begrænses til sikre, krypterede og autoriserede services. Dette er f.eks. Check Points services og ssh. **Ledelses kommentar 2011** KS er enig i observationen men gør opmærksom på, at det kun er indenfor netværket på Ottiliavej, at der kan tilgås de administrative services.	3
10-08	Vi har observeret flere tekniske forhold på den gennemgåede firewall, der indikerer, at procedurer for konfiguration og vedligeholdelse af firewall regelsættet ikke er veldefinerede og effektive. Det er f.eks. konstateret at: 1) flere aktive regler er markeret som værende 'unused', 'midlertidige' ol. 2) flere aktive regler er oprettet uden kommentarer eller reference til RFC 3) ANY service tillades mellem forskellige sikkerhedszoner (Outside, Inside, DMZ) Vi vurderer, at ineffektive procedurer vedrørende konfiguration og vedligeholdelse af firewall regelsættet øger risikoen for, at firewallen ikke opretholder den forventede netværkssegmentering. Der er herved øget risiko for, at vira eller orme kan spredes, eller at der kan opnås uautoriseret adgang på tværs af netværkssegmenterne. **Status 2011** Vi har konstateret, at der stadig forefindes flere aktive regler markeret som værende "test" og "midlertidige" fra 2009. Vi har yderligere konstateret, at der stadig findes regler, der tillader ANY service mellem forskellige sikkerhedszoner. Observationen opretholdes.	Vi anbefaler, at kommunen gennemgår og forbedrer procedurerne omkring konfiguration og vedligeholdelse af firewalls og tilhørende regelsæt. Vi anbefaler desuden, at der etableres et mere effektivt kontrolsystem til periodisk test, der sikrer, at firewalls er opsat betryggende og i overensstemmelse med det forventede. **Ledelses kommentar 2011** KS er i gang med planer for en større udskiftning, som adresserer alle disse punkter. Dette forventes implementeret i 2. kvt. 2012.	1

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

C. Implementering og vedligeholdelse af netværk og systemsoftware			
Kontrolmål C1 Netværks- og kommunikationssoftware kan vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med virksomhedens behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.		**Risiko** Utilstrækkelige eller svage procedurer i relation til vedligeholdelse og support af netværks- og kommunikationssoftware medfører risiko for, at dette ikke sker i overensstemmelse med virksomhedens behov.	
10-10	*Ændringskontrol – test* Vi har fået oplyst, at ekstern leverandør (NetDesign) i forbindelse med ændringer til netværkskomponenter gennemfører kvalitetskontrol af ændringen samt ved kritiske ændringer bistår Københavns Kommune i implementeringen heraf. Vi har dog også fået oplyst, at kvalitetssikringen og implementeringsassistancen ikke dokumenteres. Manglende eller utilstrækkelig kvalitetssikring af ændringer til netværksmiljøet medfører øget risiko for, at ændringer til netværksmiljøet ikke kan gennemføres tilfredsstillende. **Status 2011** Forhold er uændret. Anbefalingen opretholdes.	Vi anbefaler, at eksterne leverandørers kvalitetssikring og assistance i forbindelse med implementering af ændringer til netværksmiljøet dokumenteres. **Ledelses kommentar 2011** KS er enige i, at dokumentationen skal styrkes. KS har skiftet leverandør på netværksudstyret til Conscia, som er rådgiver på de ændringer, der foretages - processen omkring kvalitetskontrol er på plads – men det at få anbragt anbefalingerne i remedy-sagen udestår.	2
11-15	*Ændringskontrol – fallback* Vi har fået oplyst, at der i forbindelse med alle netværksændringer beskrives en fallback plan i Remedy, samt at der ved større ændringer udarbejdes en drejebog, som beskriver, hvilke forhold, som skal testes, og hvad fallback proceduren er. Ved udvælgelse af stikprøver har vi dog konstateret, at der ikke i alle tilfælde er beskrevet en fallback plan." Manglende eller utilstrækkelig planlægning af fallback medfører risiko for, at fejlagtige ændringer til kritiske netværkskomponenter ikke kan fjernes igen uden uhensigtsmæssige konsekvenser for driften og sikkerheden af netværket.	Vi anbefaler, at overvejelserne omkring fallback formelt dokumenteres og godkendes i forbindelse med implementeringen af ændringer til kritiske netværkskomponenter, og at den nødvendige kontrol af forudsætningerne for gennemførelse af fallback tillige dokumenteres. **Ledelses kommentar 2011** KS er enige i observationen. Eksisterende roll/fallback dokumentation skal styrkes.	2
Kontrolmål C2 Systemsoftware kan vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med kommunens behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.		**Risiko** Utilstrækkelige eller svage procedurer i relation til vedligeholdelse og support af systemsoftware medfører risiko for, at dette ikke sker i overensstemmelse med kommunens behov.	
Pkt.	**Observation**	**Anbefaling**	**Pri.**
10-11	*Nyanskaffelse – beslutninger* Vi har fået oplyst, at der er etableret overordnede krav og retningslinjer i relation til, hvorledes beslutninger om indkøb af nyt systemsoftware skal ske. Vi har ydermere fået oplyst, at der har været indkøb af systemsoftware i 2010, herunder et nyt system til HR-området, men vi har ikke modtaget dokumentation på beslutninger omkring indkøbene. Manglende eller utilstrækkelig dokumentation for beslutninger vedr. nyindkøb og/eller nyudvikling medfører risiko for, at beslutninger om indkøb eller udvikling tages på et utilstrækkeligt grundlag. **Status 2011** Vi har fået oplyst, at de etablerede retningslinjer for beslutningstagen i relation til nyanskaffelser, ikke altid følges. Anbefalingen opretholdes.	Vi anbefaler, at overvejelser omkring, hvorvidt der skal ske anskaffelse af nyt systemsoftware, beslutning samt godkendelse heraf dokumenteres. **Ledelses kommentar 2011** KS er enige i observationen.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Observationer og anbefalinger for TMF Navision

Ref.	Kontrolmål	Vurdering 2010	Vurdering 2011
B2	Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kommunens behov.	✓!	!
B3	Den logiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kommunens behov.	X (2)	!
D1	Program- og systemændringer bliver administreret hensigtsmæssigt, prioriteret og vurderet, og gennemførelse af ændringer følger en af ledelsen valgt projektmodel.	✓	✓
E1	Tilretninger til applikationer er tilfredsstillende testet, godkendt og implementeret, og de tilrettede funktioner i applikationen er i overensstemmelse med ledelsens og brugernes forventninger.	!	!
E3	Konvertering af eksisterende data til nye eller ændrede applikationer er dokumenteret, og det er sikret, at eksisterende data kan genskabes i tilfælde af fejl ved konvertering.	✓	✓

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed

Kontrolmål B2	Risiko
Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kommunens behov.	Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov.

Pkt.	Observation	Anbefaling	Pri.
TMF-11-01	*It-sikkerhedslogning* Vi har fået oplyst, at der ikke periodisk sker gennemgang af relevante logs. Manglende eller utilstrækkelig monitorering af logs medfører risiko for, at forsøg på uautoriserede handlinger ikke opdages og imødegås i tilstrækkeligt omfang.	Vi anbefaler, at der etableres kontroller, der sikrer, at krav til sikkerhedsmæssig logning på relevante platforme og systemer implementeres og overholdes, samt at der gennemføres en dokumenteret periodisk gennemgang af relevante logs fra disse platforme og systemer. **Ledelsens kommentar 2011** KS er enige i observationen.	2

Kontrolmål B3	Risiko
Den logiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kommunens behov.	Svagheder i den logiske sikkerhed øger risikoen for, at interne eller eksterne personer får uautoriseret adgang til it-ressourcerne og dermed mulighed for at slette, ændre eller kopiere programmer eller data eller i øvrigt kompromittere kommunens it-anvendelse. Endvidere øger svagheder risikoen for, at adgangen til it-systemerne ikke understøtter den i kommunen etablerede organisatoriske funktionsadskillelse.

Observationer og anbefalinger relateret til gennemgang af platform:

SQL 2005 – it-sikkerhedskonfiguration

Pkt.	Observation	Anbefaling	Pri.
TMF-10-04	Vi har observeret, at funktionen "Force Encryption" er implementeret således, at SSL kryptering af data, sendt imellem klient og server, ikke er slået til. Manglende kryptering af data, der sendes imellem klient og server, medfører risiko for, at data, som sendes i klar tekst over netværket, opsnappes og misbruges. **Status 2011** Forholdet er uændret, anbefalingen opretholdes.	Vi anbefaler, at SSL kryptering slås til, således at data, der sendes imellem klient og server, ikke umiddelbart kan opsnappes og misbruges. **Ledelses kommentar 2011** KS er enige i observationen.	3
TMF-10-07	Vi har observeret, at PUBLIC er tildelt udvidede systemprivilegier i form af EXECUTE rettighed på følgende stored procedures på master databasen: xp_instance_regread, xp_revokelogin, xp_grantlogin, xp_sprintf og xp_regread. Tildeling af systemprivilegier til PUBLIC på databasen medfører risiko for, at brugere har adgang til funktioner og privilegier, som de ikke har et arbejdsmæssigt betinget behov for, og dermed risiko for, at sikkerheden ikke kan opretholdes på databasen. **Status 2011** Forholdet er uændret, anbefalingen opretholdes.	Vi anbefaler, at de til PUBLIC tildelte systemprivilegier revurderes og fjernes, såfremt muligt. **Ledelses kommentar 2011** KS er enige i observationen.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
TMF-10-08	Vi har konstateret, at de anvendte services (såsom SQL Server service account (KS-NAV01-TMF)) logger på med Local System eller en anden account med administrative privilegier. Anvendes Local System eller en anden account med administrative privilegier til at køre MS SQL serverens services, øges risikoen for, at sikkerheden på Windows systemet - som databasen kører på - kan kompromitteres, idet denne account har administrative privilegier, der potentielt vil kunne lægge hele systemet ned. **Status 2011** Forholdet er uændret. Punktet opretholdes.	Vi anbefaler, at MS SQL serverens services køres under en Domain User account (alternativt Local Service eller Network Service account), der ikke har administrative privilegier på systemet. **Ledelses kommentar 2011** KS er enige i observationen.	2
TMF-11-02	Vi har konstateret, at MS SQL Server er konfigureret således, at der tillades mixed mode autentifikation. Brugen af mixed mode autentifikation tillader login med SQL profiler, hvilket medfører dårligere sikkerhed end anvendelse af Windows autentifikation, da password policy egenskaber og account locks kan undlades ved brug af SQL login autentifikation.	Vi anbefaler, at MS SQL serveren sættes op således, at der kun anvendes login med Windows autentifikation. **Ledelsens kommentar 2011** KS er enige i observationen.	2
TMF-11-03	Vi har konstateret, at der er 7 (ikke disablede) brugerprofiler, som ikke har fået sat CHECK_EXPIRATION på deres profil. Endvidere har vi konstateret, at der er 2 (ikke disablede) brugerprofiler, som ikke har fået sat CHECK_POLICY på deres profil. Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov.	Vi anbefaler, MS SQL Server 2005 sættes op således, at parameteren CHECK_EXPIRATION enables. Endvidere anbefaler vi, at krav til kvaliteten af passwords for SQL Login profiler overvejes og implementeres i nødvendigt omfang ved at enable CHECK_POLICY. **Ledelsens kommentar 2011** KS er enige i observationen.	2
TMF-11-04	Vi har konstateret, at et stort antal brugere har administrative privilegier på MS SQL serveren via medlemskab af kritiske grupper på operativsystemet, såsom BUILTIN\Administrators. Ikke alle brugere har efter det oplyste behov for sådanne administrative privilegier. Tildeling af administrative privilegier til medarbejdere, som ikke har et arbejdsmæssigt betinget behov herfor, medfører øget risiko for fejl og uautoriserede handlinger på databasen.	Vi anbefaler, at antallet af brugere i de kritiske grupper på Windows operativsystemet revurderes og begrænses til medarbejdere med et arbejdsmæssigt betinget behov for administrativ adgang til MS SQL serveren. **Ledelsens kommentar 2011** KS er enige i observationen.	2
TMF-11-05	Vi har konstateret 3 personer, som er tildelt administrative rettigheder til SQL databasen med mindst 2 brugerprofiler: TMF\hhanse = KS\AS36 KS\AU59 = KS\BK7W KS\ZY94 = KS\BK7X Manglende eller utilstrækkelig kontrol med oprettelse og nedlæggelse af bruger medfører risiko for uautoriseret adgang til systemer og data.	Vi anbefaler, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere for relevante systemer og platforme. **Ledelsens kommentar 2011** KS er enige i observationen.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

E. Implementering og vedligeholdelse af applikationer og databaser			
Kontrolmål E1 Nye applikationer udvikles/indkøbes, og tilretninger til applikationer testes, godkendes og implementeres således, at applikationerne fungerer i overensstemmelse med ledelsens og brugernes forventninger og således, at væsentlige applikationer kan vedligeholdes og supporteres.		**Risiko** Utilstrækkelige eller svage procedurer i relation til indkøb af eller styring af tilretninger til applikationer øger risikoen for, at applikationer eller ændringer heraf sættes i drift uden fornøden dokumentation, kvalitetssikring eller ledelsesgodkendelse, og at applikationer dermed ikke fungerer eller i længden ikke kan vedligeholdes og supporteres i overensstemmelse med kommunens behov.	
Pkt.	**Observation**	**Anbefaling**	**Pri.**
TMF-10-10	*Ændringskontrol – kvalitet af testmiljø* Vi har fået oplyst, at det i forbindelse med gennemførelsen af test i testmiljøet overordnet vurderes, hvorvidt data og programmer i testmiljøet er repræsentative for produktionsmiljøet. Vi har via stikprøver observeret, at sådanne overvejelser ikke er dokumenteret. Manglende eller utilstrækkelig kontrol af kvaliteten af testmiljøet forinden gennemførelsen af test medfører risiko for, at testresultater kan være fejlagtige eller på anden vis ikke være repræsentative for, hvorledes en ændring vil fungere i produktionsmiljøet. **Status 2011** Forholdet er uændret. Punktet opretholdes.	Vi anbefaler, at det i forbindelse med igangsætningen af testforløb formelt vurderes, hvorvidt kvaliteten af testmiljøet er tilstrækkelig, og at vurderingen dokumenteres og godkendes. **Ledelses kommentar 2011** KS er enige i observationen.	2
TMF-10-11	*Ændringskontrol – fallback* Vi har fået oplyst, at der i forbindelse med implementering af ændringer til produktionsmiljøet uformelt tages stilling til, hvorledes fallback kan gennemføres, såfremt ændringerne mod forventning skulle medføre problemer i produktionsmiljøet. Overvejelserne dokumenteres dog ikke, ligesom det ikke fremgår, hvorvidt eventuelle forudsætninger for fallback kontrolleres, f.eks. at der er taget en sikkerhedskopi forinden implementering af ændringerne. Manglende eller utilstrækkelig planlægning af fallback medfører risiko for unødige komplikationer i forbindelse med, at fejlbehæftede ændringer, implementeret i produktionsmiljøet, forsøges fjernet igen. **Status 2011** Forholdet er uændret. Punktet opretholdes.	Vi anbefaler, at overvejelserne omkring fallback dokumenteres og godkendes i forbindelse med implementeringen af ændringer til produktionsmiljøet, og at eventuel kontrol af forudsætningerne for fallback tillige dokumenteres. **Ledelses kommentar 2011** KS er enige i observationen.	2
TMF-10-12	*Support – vedligeholdelse af dokumentation* Vi har fået oplyst, at der i forbindelse med implementering af ændringer til Navision tages stilling til, hvorvidt ændringen har betydning for den eksisterende system-, drifts- og brugerdokumentation, og at denne tilrettes såfremt nødvendigt. Vi har dog fået oplyst, at denne stillingtagen ikke formelt dokumenteres og godkendes forinden idriftsættelse. Manglende eller utilstrækkelig opdatering af system-, drifts- og brugerdokumentation i forbindelse med implementering af ændringer medfører risiko for, at systemet ikke i længden kan vedligeholdes, supporteres og anvendes i overensstemmelse med forventningerne. **Status 2011** Forholdet er uændret. Punktet opretholdes.	Vi anbefaler, at der i forbindelse med implementering af ændringer konkret sker en dokumenteret godkendelse af, at overvejelserne i relation til opdatering af system-, drifts- og brugerdokumentation er gennemført, og at dokumentationen er opdateret, hvor dette vurderes nødvendigt. **Ledelses kommentar 2011** KS er enige i observationen.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

E. Implementering og vedligeholdelse af applikationer og databaser			
TMF-10-13	*Ændringskontrol – testplaner og godkendelser* Vi har fået oplyst, at formelle testplaner og -scenarier kun anses som nødvendige ved større funktionelle ændringer. Ved mindre ændringer dokumenteres foretaget test samt resultat heraf ikke. Manglende eller utilstrækkelig anvendelse og godkendelse af testplaner og -scenarier i forbindelse med test af ændringer medfører risiko for, at kvaliteten og omfanget af gennemførte test og resultaterne heraf ikke er i overensstemmelse med forventningerne og dermed, at der idriftsættes fejlbehæftede ændringer. **Status 2011** Forholdet er uændret. Punktet opretholdes.	Vi anbefaler, at der i forbindelse med alle ændringer til idriftsættelse sker dokumentation af den gennemførte tests omfang og godkendelse af resultatet. Såfremt test i den enkelte situation ikke vurderes relevant, bør denne beslutning endvidere godkendes og dokumenteres. **Ledelses kommentar 2011** KS er enige i observationen.	2
TMF-10-14	*Ændringskontrol – timing af idriftsættelse* Vi har fået oplyst, at alle ændringer til Navision, som udgangspunkt, idriftsættes inden for de aftalte servicevinduer, som generelt er udenfor normal arbejdstid. Vi har tillige fået oplyst, at der ikke foreligger dokumentation af det aftalte idriftsættelsestidspunkt på ændringerne. Manglende eller utilstrækkelig kontrol med tidspunktet for idriftsættelsen af ændringer medfører risiko for, at ændringer implementeres på tidspunkter, hvor dette kan have uheldige følger for den normale driftsafvikling. **Status 2011** Forholdet er uændret. Punktet opretholdes.	Vi anbefaler, at overvejelserne omkring idriftsættelsestidspunkter dokumenteres og godkendes. **Ledelses kommentar 2011** KS er enige i observationen.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Observationer og anbefalinger for KØR

Ref.	Kontrolmål	Vurdering 2011
B2	Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kommunens behov.	
B3	Den logiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kommunens behov.	
D1	Program- og systemændringer bliver administreret hensigtsmæssigt, prioriteret og vurderet, og gennemførelse af ændringer følger en af ledelsen valgt projektmodel.	
E1	Tilretninger til applikationer er tilfredsstillende testet, godkendt og implementeret, og de tilrettede funktioner i applikationen er i overensstemmelse med ledelsens og brugernes forventninger.	
E3	Konvertering af eksisterende data til nye eller ændrede applikationer er dokumenteret, og det er sikret, at eksisterende data kan genskabes i tilfælde af fejl ved konvertering.	

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

B. It-sikkerhed			
Kontrolmål B2 Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kommunens behov.		**Risiko** Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov.	
Pkt.	**Observation**	**Anbefaling**	**Pri.**
KØR-11-01	*Brugerrettigheder – oprettelse og ændringer* Vi har for en stikprøve konstateret, at der ikke i alle tilfælde kunne fremskaffes dokumentation for brugeroprettelser. Manglende eller utilstrækkelig kontrol med tildelingen af rettigheder til brugere medfører risiko for, at brugeres rettigheder ikke er i overensstemmelse med deres arbejdsmæssigt betingede behov.	Vi anbefaler, at tildeling af rettigheder til brugere sker på baggrund af formelle og dokumenterede autorisationer. **Ledelsens kommentar 2011** Ændring/fratagelse af autorisationer er fastlagt, idet det er forvaltningernes autorisationsansvarlige (daglige leder), som skal sikre, at ændrede autorisationer indberettes til KS brugeradministration.	2
KØR-11-02	*Brugerrettigheder – periodisk revurdering* Vi har fået oplyst, at der periodisk foretages en revurdering af tildelte rettigheder til brugere. Det foregår ved, at afdelingslederne selv skal gennemgå brugerlister og melde tilbage til brugeradministrationen, såfremt der er ændringer til listen. Der følges dog ikke op på, om alle afdelingslederne vender tilbage til brugeradministrationen. Manglende eller utilstrækkelig periodisk revurdering af tildelte rettigheder til brugere medfører risiko for, at brugeres rettigheder bliver utidssvarende og ikke afspejler deres arbejdsmæssigt betingede behov.	Vi anbefaler, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere for relevante systemer og platforme. Samt at det kontrolleres, at alle involverede melder tilbage. **Ledelsens kommentar 2011** KK har iværksat et projekt, der skal identificere og beskrive mulighederne for, at fremtidige revurderinger foretages af de daglige ledere og sikre mulighederne for kontrol af, at revurderingerne foretages. Projektets arbejde med vedligeholdelsesprocesserne forventes afsluttet i 2. kvt. 2012.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukket observationer i 2011

Ved vores gennemgang i 2011 har vi afsluttet følgende observationer, som er blevet afhjulpet af Københavns Kommune.

Lukkede observationer på Fælles Forhold			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
09-04 a	*Sikkerhedskopiering – ekstern arkivering* Vi har fået oplyst, at den nuværende backupløsning sikrer, at der opbevares en kopi af data på to forskellige lokationer – (fremover kaldet primær serverrum og backup serverrum). Der eksisterer ifølge det oplyste ikke sikkerhedskopier på bånd, som opbevares eksternt i forhold til ovennævnte lokationer. Manglende eller utilstrækkelig kontrol med den eksterne opbevaring af datamedier medfører risiko for, at disse ikke arkiveres tilstrækkelig sikkert, eller at datamedier ikke bringes til arkivering som forventet. **Status 2011** Vi har modtaget dokumentation for ekstern arkivering. Punktet lukkes.	Vi anbefaler, at det som en del af beredskabsplanlægningen sikres, at der opbevares en "disaster sikkerhedskopi" på en ekstern lokation, hvortil kun særligt udvalgte medarbejdere tildeles adgang. Der bør etableres en formel procedure, som styrer, hvorledes håndteringen af sikkerhedskopier foregår. **Ledelsens kommentar 2010** Det fremgår af it-sikkerhedsreg. § 73. "Den it-ansvarlige skal sikre, at der sker lagring og backup af oplysninger på serverudstyr. Det skal sikres, at der efter behov og i henhold til aftale tillige opbevares en sikkerhedskopi på en ekstern lokation. Den it-ansvarlige fastsætter nærmere retningslinjer for sikkerhedskopieringen. Retningslinjerne skal revideres mindst hvert 4. år." Da den nuværende backupløsning sikrer, at der opbevares en kopi af data på to forskellige lokationer, anses kravet for opfyldt. KS vil i løbet af 2011 implementere en digital (disk) løsning for backup. KS betragter herefter pkt. som lukket.	3
09-04 b	*Sikkerhedskopiering - ekstern arkivering* Vi har fået oplyst, at den nuværende backupløsning sikrer, at der opbevares en kopi af data på to forskellige lokationer – (fremover kaldet primær serverrum og backup serverrum). Da flere af KS' medarbejdere har adgang til både primær serverrum og backup serverrum, kan der være en risiko for, at en person kan ødelægge data begge steder. Manglende eller utilstrækkelig kontrol med den eksterne opbevaring af datamedier medfører risiko for, at disse ikke arkiveres tilstrækkelig sikkert, eller at datamedier ikke bringes til arkivering som forventet. **Status 2011** Vi har modtaget dokumentation for ekstern arkivering. Punktet lukkes.	Vi anbefaler, at det som en del af beredskabsplanlægningen sikres, at der opbevares en "disaster sikkerhedskopi" på en ekstern lokation, hvortil kun særligt udvalgte medarbejdere tildeles adgang. Der bør etableres en formel procedure, som styrer, hvorledes håndteringen af sikkerhedskopier foregår. **Ledelsens kommentar 2010** Der eksisterer ingen krav i kommunens it-sikkerhedsregulativ om opbevaring af Disaster sikkerhedskopi. For så vidt angår medarbejderes adgang til serverrum henvises til: "Procedure vedr. adgang til kritiske lokationer – primært serverrum vil blive udarbejdet og forventes indarbejdet i "Driftshåndbog for serverdrift", der forventes færdig Q1, 2011. Endvidere henvises til "ITAS_It-sikkerhedsforskrift - fysisk sikkerhed_20100305_1.0_AE_TT39" (eDoc: 2010-165184).	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på Fælles Forhold			
10-01	*Sikkerhedskopiering – opbevaring internt* Vi har fået oplyst, at backupbånd opbevares i båndmaskinen. Disse flyttes ikke til f.eks. internt brandskab eller andet. Båndene fjernes kun fra maskinen, når de er slidt og skal skiftes ud. Manglende eller utilstrækkelig kontrol med arkiveringen af backupmedier medfører risiko for, at disse ikke arkiveres i overensstemmelse med forventningerne og derfor kan gå tabt. **Status 2011** Vi har modtaget dokumentation for passende intern opbevaring. Punktet lukkes.	Vi anbefaler, at der etableres en procedure for sikker opbevaring af bånd på selve lokationen. **Ledelsens kommentar 2010** KS vil i løbet af 2011 implementere en digital (disk) løsning for backup. Pkt. lukkes.	2
09-36	*Adgang til kritiske lokationer – primært serverrum* Vi har konstateret, at adgange til nyt og gammelt serverrum samt hovedkrydsfelt er tildelt til over 100 medarbejdere, herunder er en række af disse fra eksterne firmaer. En del udleverede adgangskort er ikke direkte personhenførbare, eksempelvis. "GÆSTEFLYTTEFOLK". Manglende eller utilstrækkelig kontrol med tildelingen af adgange til centrale it-ressourcer - herunder serverrum - medfører risiko for, at for mange adgange tildeles og dermed risiko for misbrug af adgange. **Status 2011** Vi har modtaget periodisk udført dokumenteret gennemgang af adgange til serverrum. Punktet lukkes.	Vi anbefaler, at antallet af adgange revurderes, samt at adgange til serverrum kun tildeles på baggrund af formelle dokumenterede autorisationer. Endvidere anbefales det, at der periodisk foretages en revurdering af tildelte adgange til kritiske lokationer. **Ledelsens kommentar 2010** KS vil sikre, at antallet af adgange vil blive gennemgået med sigte på reduktion og størst mulig grad af personificering. Gennemgangen vil være gennemført inden 01.04.2011. Tildelte adgange er i øvrigt vurderet i januar 2011 og forventes således yderligere reduceret. Procedure vedr. adgang til kritiske lokationer – primært serverrum - vil blive udarbejdet og forventes indarbejdet i "Driftshåndbog for serverdrift", der forventes færdig Q1, 2011. Endvidere henvises til "ITAS_It-sikkerhedsforskrift - fysisk sikkerhed_20100305_1.0_AE_TT39" (eDoc: 2010-165184).	2
09-37	*Adgang til kritiske lokationer – sekundært serverrum* Vi har konstateret, at adgange til serverrum er tildelt 79 medarbejdere, herunder er en række af disse fra eksterne firmaer. En del udleverede adgangskort er ikke direkte personhenførbare, eksempelvis "Dong Energy". Manglende eller utilstrækkelig kontrol med tildelingen af adgange til centrale it-ressourcer - herunder serverrum - medfører risiko for, at for mange adgange tildeles og dermed risiko for misbrug af adgange. **Status 2011** Vi har modtaget periodisk udført dokumenteret gennemgang af adgange til serverrum. Punktet lukkes.	Vi anbefaler, at antallet af adgange revurderes, samt at adgange til serverrum kun tildeles på baggrund af formelle dokumenterede autorisationer. Endvidere anbefales det, at der periodisk foretages en revurdering af tildelte adgange til kritiske lokationer. **Ledelsens kommentar 2010** Problemstillingen vil blive behandlet som en del af det under punkt 09-36 nævnte. Tildelte adgange er vurderet i januar 2011 og forventes således yderligere reduceret. Procedurer udarbejdes og forventes indarbejdet i "Driftshåndbog for serverdrift", der forventes færdig Q1, 2011. Endvidere henvises til "ITAS_It-sikkerhedsforskrift - fysisk sikkerhed_20100305_1.0_AE_TT39" (eDoc: 2010-165184).	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på Fælles Forhold			
10-02	*It-sikkerhedspolitik* Vi har noteret, at der foreligger udkast til nyt it-sikkerhedsregulativ, som blandt andet tager udgangspunkt i DS484. Ved anvendelsen af DS484 kan der være en risiko for, at der besluttes et sikkerhedsniveau, som ikke fuldt ud er tilpasset kommunens behov, da der ikke umiddelbart tages udgangspunkt i en fuldstændig risikovurdering af kommunens behov. **Status 2011** Vi har konstateret, at Københavns Kommune er i færd med at overgå til ISO27002. Punktet lukkes.	Det anbefales, at kommunen overvejer anvendelsen af ISO27000 til fastsættelse af it-sikkerhedspolitikker mv., idet der herved tages udgangspunkt i kommunens reelle behov for it-sikkerhed. **Ledelsens kommentar 2010** KS er enig i revisionens bemærkning og vil arbejde videre med revisionens anbefaling.	3
09-20	På serveren KS-DC01 har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • Directory Service Access (Success) • Object Access (No auditing) • Privilege Use (No auditing) Manglende eller utilstrækkelig logning medfører risiko for at hændelser - eller forsøg herpå - ikke registreres i fornødent omfang. **Status 2011** Vi har konstateret, at der nu logges i overensstemmelse med vores anbefalinger. Punktet lukkes.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • Directory Service Access (Failure) • Object Access (Failure) • Privilege Use (Failure) **Ledelsens kommentar 2010** KS betragter pkt. som lukket, jf. pkt. 09-06.	3
09-26	*Anvendelse af fælles brugerprofiler* Vi har konstateret, at der anvendes en del fællesbrugerprofiler til administration af bl.a. antivirussoftware og backupsystem (EMC Networker). Vi har endvidere fået oplyst, at anvendelsen af disse profiler - herunder hvem der har kendskab til passwordet for disse - ikke er dokumenteret og godkendt. Anvendelse af fællesbrugerprofiler medfører øget risiko for, at handlinger gennemført på systemet ikke kan spores tilbage til en ansvarlig person (manglende kontrolspor). **Status 2010** Vi har fået oplyst, at der ikke er etableret dokumentation for fællesprofiler, men at disse uformelt er godkendt. Password til disse konti er kun tildelt medarbejdere, som organisatorisk er tilknyttet enheden Serverdrift samt en medarbejder i udviklingsafdelingen, som indgår i serverdrifts rådighedsvagt. Endvidere har vores gennemgang af anvendte brugernavne på Windows AD vist, at der anvendes enkelte fællesprofiler. I 2010 er der gennemført en oprydning (Grunddata projektet), der har fjernet en stor del af fællesprofilerne, hvorfor vi nedgraderer prioriteten til **2**. **Status 2011** Vi har ved gennemgang af Windows AD ikke konstateret kritiske fælles brugerprofiler. Punktet lukkes.	Vi anbefaler, at det i videst muligt omfang sikres, at der kun anvendes personlige brugerprofiler ved administration af netværk og udstyr. Hvis der er behov for anvendelse af fælles brugerprofiler skal dette dokumenteres - herunder med angivelse af hvilke medarbejdere, som har kendskab til passwordet for disse - samt at anvendelsen af de dokumenterede profiler godkendes. **Ledelsens kommentar 2010** Det er som udgangspunkt ikke korrekt, at der ikke foreligger godkendelse af, hvem der kender password til "fællesbrugerprofiler". Disse kendes alene af medarbejdere, som organisatorisk er tilknyttet enheden Serverdrift samt en medarbejder i udviklingsafdelingen, som indgår i serverdrift rådighedsvagt. Ansvaret for øvrige brugerprofiler i AD, som kan være "fælles" ligger hos den enkelte sikkerhedsleder, eller for så vidt der er tale om lokale konti på servere hos systemejer. Fællesbrugerprofiler må ikke forveksles med systemkonti, som anvendes til afvikling af et systeminitieret job, f.eks. backupjob og lignende. Antallet af "upersonlige" konti med administrative rettigheder på servere vil blive dokumenteret og reduceret inden 01.06.2011. KS betragter herefter pkt. som lukket.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på Fælles Forhold			
09-27	*Anvendelse af passwords* Vi har konstateret, at der i it-sikkerhedspolitikken stilles krav om anvendelse af passwords ved brug af systemer og platforme. Vi har endvidere fået oplyst, at der ikke er etableret en kontrol med henblik på at sikre, at dette krav implementeres på relevante platforme. Ovenstående understøttes af de tekniske gennemgange af Windows domænerne for Københavns Kommune, som viser, at passwords ikke er implementeret konsistent henover alle domæner. Manglende eller utilstrækkelig kontrol med passwords implementering på systemer og platforme medfører risiko for, at passwords ikke anvendes i det omfang, som det forventes, og dermed øger risiko for brud på sikkerheden. **Status 2010** Vi har fået oplyst, at der ikke er etableret en kontrol med henblik på at sikre, at passwordkrav implementeres på relevante platforme. Endvidere har vi fået oplyst, at der ikke foreligger dokumentation for, hvilke systemer, der har undtagelser til passwordkrav. **Status 2011** Vi har ved gennemgang af password opsætning på Windows AD konstateret væsentlige forbedringer siden 2010. Tilbageværende afvigelser rapporteres for sig. Punktet lukkes.	Vi anbefaler, at det dokumenteres, at de specificerede krav til passwords er implementeret på relevante platforme og systemer, og at denne dokumentation løbende vedligeholdes. **Ledelsens kommentar 2010** På platformen, forstået som styresystem på servere, er der implementeret fuld anvendelse af brugerkonti og password. Ansvaret for implementering på systemer ud over OS henhører under systemejer og skal sikres i forbindelse med godkendelse af system. KS betragter herefter ovenstående som lukket. It-sikkerhedsfunktionen vil i februar/marts mdr. 2011 udsende høring til forvaltningernes 400 + systemejere, med henblik på: 1) kontrol af, at passwordvejledning overholdes 2) evt. tiltag, hvis manglende overholdelse Resultatet rapporteres til forvaltningernes direktioner.	2
09-28	På serveren KS-DC01-UUF har vi observeret, at: • Minimum Password Age er konfigureret til 0 • Account Lockout Threshold er konfigureret til 0 • Account Lockout Duration ikke er konfigureret • Reset Account Lockout Counter ikke er konfigureret Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har konstateret, at password parametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at de nævnte passwordparametre konfigureres i overensstemmelse med nedenstående security baseline: • Minimum Password Age = 1 • Account Lockout Threshold = 3 • Account Lockout Duration min. 30 min. • Reset Account Lockout Counter min. 30 min. **Ledelsens kommentar 2010** Problemet med konti, undtaget for brug af PSW og mgl. udløbsdato på passwordskift, er løst i forbindelse med implementering af policy til sikring for overholdelse af politik for password, jf. pkt. 09-27. KS betragter herefter pkt. som lukket.	1
09-29	På serveren KS-DC01-TMF har vi observeret, at: • Password Complexity ikke er enabled • Minimum Password Age er konfigureret til 0 Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har konstateret, at password parametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at de nævnte passwordparametre konfigureres i overensstemmelse med nedenstående security baseline: • Password Complexity = enabled • Minimum Password Age = 1 **Ledelsens kommentar 2010** Problemet med konti, undtaget for brug af PSW og mgl. udløbsdato på passwordskift, er løst i forbindelse med implementering af policy til sikring for overholdelse af politik for password, jf. pkt. 09-27. KS betragter herefter ovenstående som lukket.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på Fælles Forhold			
09-30	På serveren KS-DC01-SUND har vi observeret, at: • Account Lockout Threshold er konfigureret til 0 • Account Lockout Duration ikke er konfigureret • Reset Account Lockout Counter ikke er konfigureret Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har konstateret, at password parametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at de nævnte passwordparametre konfigureres i overensstemmelse med nedenstående security baseline: • Account Lockout Threshold = 3 • Account Lockout Duration min. 30 min. • Reset Account Lockout Counter min. 30 min. **Ledelsens kommentar 2010** Problemet med konti, undtaget for brug af PSW og mgl. udløbsdato på passwordskift, er løst i forbindelse med implementering af policy til sikring for overholdelse af politik for password, jf. pkt. 09-27. KS betragter herefter ovenstående som lukket.	1
09-31	På serveren KS-DC01-OF har vi observeret, at: • Minimum Password Age er konfigureret til 0 • Password History Size er konfigureret til 6 • Account Lockout Duration er konfigureret til 5 minutter • Reset Account Lockout Counter er konfigureret til 5 minutter Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har konstateret, at password parametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at de nævnte passwordparametre konfigureres i overensstemmelse med nedenstående security baseline: • Minimum Password Age = 1 • Password History Size = 8 • Account Lockout Duration min. 30 min. • Reset Account Lockout Counter min. 30 min. **Ledelsens kommentar 2010** Problemet med konti, undtaget for brug af PSW og mgl. udløbsdato på passwordskift, er løst i forbindelse med implementering af policy til sikring for overholdelse af politik for password, jf. pkt. 09-27. KS betragter herefter ovenstående som lukket.	2
09-32	På serveren KS-DC01-KULTUR har vi observeret, at: • Minimum Password Age er konfigureret til 0 • Account Lockout Threshold' er konfigureret til 5 • Reset Account Lockout Counter er konfigureret til 5 minutter Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har konstateret, at password parametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at de nævnte passwordparametre konfigureres i overensstemmelse med nedenstående security baseline: • Minimum Password Age = 1 • Account Lockout Threshold = 3 • Reset Account Lockout Counter min. 30 min. **Ledelsens kommentar 2010** Problemet med konti, undtaget for brug af PSW og mgl. udløbsdato på passwordskift, er løst i forbindelse med implementering af policy til sikring for overholdelse af politik for password, jf. pkt. 09-27. KS betragter herefter ovenstående som lukket.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på Fælles Forhold			
09-33	På serveren KS-DC01 har vi observeret, at: • Account Lockout Threshold er konfigureret til 5 Manglende eller svage procedurer, vedrørende administration, overvågning og vedligeholdelse af adgang til systemer, data og andre it-ressourcer, medfører øget risiko for uautoriseret adgang til disse og dermed risiko for, at it-sikkerheden ikke er i overensstemmelse med kommunens behov. **Status 2011** Vi har konstateret, at password parametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at de nævnte passwordparametre konfigureres i overensstemmelse med nedenstående security baseline: • Account Lockout Threshold = 3 **Ledelsens kommentar 2010** Problemet med konti, undtaget for brug af PSW og mgl. udløbsdato på passwordskift, er løst i forbindelse med implementering af policy til sikring for overholdelse af politik for password, jf. pkt. 09-27. KS betragter herefter ovenstående som lukket.	3
09-22	På serveren KS-DC01-FAF har vi observeret, at der ikke foretages tilstrækkelig logning af hændelserne: • Directory Service Access (No auditing) • Object Access (Success) • Privilege Use (No auditing) Manglende eller utilstrækkelig logning medfører risiko for, at hændelser - eller forsøg herpa - ikke registreres i fornødent omfang. **Status 2011** Vi har konstateret, at logningsparametre nu er sat op i overensstemmelse med det anbefalede. Punktet lukkes.	Vi anbefaler, at logning implementeres i overensstemmelse med nedenstående Windows security baseline: • Directory Service Access (Failure) • Object Access (Failure) • Privilege Use (Failure) **Ledelsens kommentar 2010** KS betragter pkt. som lukket, jf. pkt. 09-06.	2
10-09	*Ændringskontrol - patchmanagement, timing og fallback* Vi har fået oplyst, at alle ændringer som udgangspunkt bliver håndteret i Remedy og følger KS' Change Management proces, herunder stillingtagen til patchmanagement, timing og fallback. Vi har modtaget et screenshot, der viser, at der er gennemført 71 ændringer på netværksområdet i 2010, men vi har ikke modtaget en specificeret liste med de 71 ændringer, hvorfor det ikke har været muligt at udtage stikprøver. Manglende eller utilstrækkelig kontrol med patchmanagement, timing og fallback medfører øget risiko for, at ændringer til netværksmiljøet ikke kan gennemføres tilfredsstillende. **Status 2011** Det var i år muligt at modtage liste over ændringer. Punktet lukkes.	Vi anbefaler, at det fremadrettet sikres, at det er muligt at udtrække en specificeret liste over ændringer foretaget på netværksmiljøet. **Ledelsens kommentar 2010** Enig i, at dokumentation bør styrkes, og ønsket om mere detaljeret dokumentation vil blive indarbejdet, men at dokumentationen mangler i Remedy er mere en indikation for "manglende registreringspraksis" end manglende planlægning eller kvalitet i udførelsen af ændringer. Følgende handling vil blive iværksat og forventet gennemført umiddelbart efterfølgende (uge 10). Undervisning i registreringspraksis i changesager i Remedy samt opfølgning/kontrol i forbindelse med ledergodkendelse af changesager herefter. KS betragter herefter ovenstående pkt. som lukket.	2
10-05	Vi har fået oplyst, at der ikke foreligger dokumentation for kørende services på de enkelte domain controllere. Vi har endvidere observeret services, som ikke bør være kørende på domain controllere, f.eks.: • Printspooler • Wireless configuration Ingen eller utilstrækkelig kontrol med kørende services på systemerne øger risikoen for, at uautoriserede (ikke godkendte) services - for eksempel som følge af installation af uautoriserede programmer - ikke opdages og fjernes. **Status 2011** Vi har konstateret, at der har været udført oprydning af kritiske services. Punktet lukkes.	Vi anbefaler, at kørende services er underlagt en dokumenteret periodisk gennemgang, og at unødvendige services er deaktiveret, såfremt det er muligt. **Ledelsens kommentar 2010** Der er grundlæggende ikke tale om uautoriserede services, idet de 2 anførte services er en del af standardinstallationen samtidig med, at der ikke pt. er fastlagt retningslinjer for, hvilke services, som er en del af styresystemet, der skal være aktiveret. Der vil i løbet af 2011 blive etableret en standard for, hvilke services der skal være installeret, og hvilke der skal være aktiverede. KS foretager opfølgning på status 01.09.2011.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på Fælles Forhold			
10-07	Vi har konstateret, at der er oprettet en (fælles) VPN brugerprofil (NetDesign-Support), der anvendes til ekstern adgang til firewall, SafeLog, RealSecure og router for TDC it-sikkerheds ansatte (jf. regel 27). Vi vurderer, at anvendelse af fælles-brugerprofiler medfører øget risiko for, at handlinger gennemført på systemet ikke kan spores tilbage til en ansvarlig person. **Status 2011** Vi har konstateret, at brugerprofilen NetDesign-Support er fjernet. Observationen lukkes.	Vi anbefaler, at det sikres, at etablerede fælles-brugerprofiler er dokumenteret, herunder hvilke eksterne og interne medarbejdere, der har kendskab til passwordet for disse profiler. Der bør endvidere tages stilling til, om der skal etableres periodisk gennemgang af handlinger gennemført af sådanne brugere på kritiske systemer som f.eks. FW_OTT_Cluster1. **Ledelsens kommentar 2010** Enig - KS ønsker selv at nedlægge fællesadgange, og der pågår arbejde med et setup, for at rettigheder fremover bliver personlige og differentieret og naturligvis mere traceable. Vær opmærksom på, at kun meget få og relevante/kompetente personer i KS har adgang til firewall miljøet. Der vil blive taget kontakt til Netdesign med henblik på at undersøge muligheden for at oprette personlige adgange til deres vagtteknikere til firewall miljøet. Med hensyn til adgang til TDC's routerudstyr, så vil dette opklaringspunkt blive videresendt til TDC med henblik på at afdække, hvordan dette håndteres, men vær opmærksom på, at KS teknikere samt Netdesign "kun" har læseadgang til disse routere. Læs mere om Tuffin som nævnt i 10-08. Pkt. forventes afsluttet 01.06.2011.	1
11-11	*Konfigurationsmæssige sårbarheder - Kryptografisk usikre protokoller* Vi har observeret, at der er adgang til følgende IP-adresse via ukrypteret telnet: • 195.41.120.213 Vi vurderer, at der er øget risiko for, at dette kan medføre tab af fortrolighed, da det kræver, at en angriber har adgang til datatrafikken. Er disse omstædigheder til stede, vil det være muligt at udtrække brugernavne og adgangskoder, som transmitteres via telnet. Status 2011 Vi har modtaget dokumentation for, at telnet nu er fjernet fra IP adressen. Punktet lukkes.	Vi anbefaler, at adgang kun tillades via kryptografisk sikre protokoller, som f.eks. Secure Shell (SSH).	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.

Lukkede observationer på TMF			
Pkt.	**Observation**	**Anbefaling**	**Pri.**
TMF-10-02	Vi har observeret, at der kun er etableret logning på MS SQL databaseserveren af fejlslagne login-forsøg. Manglende eller utilstrækkelig logning medfører, at det ikke er muligt at følge op på uautoriserede hændelser. **Status 2011** Da Symantec Security Information Manager sørger for logning af succesfulde logins, vurderes forholdet som passende. Punktet lukkes.	Vi anbefaler, at audit konfigureres således, at logning for Failed og Successful Logins etableres, samt at der etableres retningslinjer for, hvorledes logning periodisk gennemgås, således at gentagne fejlslagne loginforsøg vurderes, og nødvendige handlinger foretages. **Ledelsens kommentar 2010** Punktet er taget til efterretning og er delvis løst ved, at brugerne under punkt 10-01 og 10-03 er fjernet fra databasen. Servergruppen har et igangværende projekt/produkt Symantec Security Information Manager, som tager hånd om logning af successful login.	3
TMF-10-03	Vi har observeret 2 (ikke disablede) brugerprofiler, som har fået sat et password lig brugernavn. Det drejer sig om brugerne "pvalentest" og "godkend". Pvalentest er desuden med i SYSADMIN. Utilstrækkelige passwords for brugere på databasen eller manglende låsning/sletning af disse brugerprofiler medfører øget risiko for, at disse misbruges, hvorved databasen ikke længere er tilstrækkeligt sikret imod tab af data eller uautoriserede handlinger. **Status 2011** Vi har konstateret, at der ved seneste gennemgang ikke var brugere med password lig brugernavn. Punktet lukkes.	Vi anbefaler, at passwords for brugere i databasen implementeres således, at de underlægges en passwordpolitik, der sikrer, at kvaliteten af passwords overholder kommunens retningslinjer herfor. **Ledelsens kommentar 2010** Brugerprofilerne er slettet 25. januar 2011. Figurerede ikke på selve databasen. **KS bemærkning** Ansvaret for sikkerhedsopsætningen i en applikation henhører under systemejer. SSL kan slås til på bestilling fra systemejer, men der skal samtidig ske tilretning af klient og webinterface med fornødne certifikater. Løsning bør udarbejdes med applikationsudvikler. Tidshorisont for implementering vil være 4-6 uger, men afhænger af konkret analyse.	1
TMF-10-05	Vi har observeret, at 125 brugerprofiler er oprettet som DB_owner på master databasen og fået oplyst, at de fleste ikke skal have denne rettighed. Tildeling af administrative privilegier til mange brugerprofiler, herunder brugerprofiler, der ikke har arbejdsmæssigt behov herfor, medfører risiko for, at sikkerheden og den af ledelsen ønskede funktionsadskillelse ikke kan opretholdes på databasen. **Status 2011** Antallet er reduceret til brugeren DBO. Punktet lukkes.	Vi anbefaler, at antallet af brugerprofiler med administrative privilegier (Fixed Server Roles) revurderes og nedbringes, såfremt muligt. **Ledelsens kommentar 2010** Er taget til efterretning og nedbringes til en "bruger" DBO, der ejer skemaerne på databasen. De 124 øvrige brugere er fjernet på Master databasen den 22. februar 2011.	1
TMF-10-06	Vi har observeret, at 8 brugerprofiler har udvidede rettigheder via den tildelte Fixed Server Role sysadmin. Heraf er nogle af brugerne personlige brugere, som ikke har været anvendt i længere tid, og en af brugerne har fået sat et password lig brugernavn. Tildeling af administrative privilegier til mange brugerprofiler, herunder brugerprofiler, der ikke har arbejdsmæssigt behov herfor, medfører risiko for, at sikkerheden og den af ledelsen ønskede funktionsadskillelse ikke kan opretholdes på databasen. **Status 2011** Vi har konstateret, at brugere med administrative privilegier er blevet nedbragt, samt at der ikke længere er brugere med password lig brugernavn. Punktet lukkes.	Vi anbefaler, at antallet af brugerprofiler med administrative privilegier (Fixed Server Roles) revurderes og nedbringes, såfremt muligt. **Ledelsens kommentar 2010** De 4 databaselogins er fjernet. Det ene via punkt 10-03. Hermed er password lig brugernavn også fjernet. De øvrige 4 brugerprofiler, der har rettigheden er arbejdsbetinget, og antallet kan ikke nedbringes yderligere. Der anvendes personlige passwords, som følger Windows sikkerhedsforanstaltninger.	2

Prioritet 1: Anbefalinger til udbedring af væsentlige svagheder i den interne kontrol.
Prioritet 2: Anbefalinger til udbedring af svagheder i den interne kontrol.
Prioritet 3: Anbefalinger til forbedring af den interne kontrol i øvrigt.