

Servicegruppen for Dataudstyr A/S

**Uafhængig revisors rapport om
generelle it-kontroller hos Servicegrup-
pen for Dataudstyr A/S**

Erklæring pr. 31. december 2010

Indholdsfortegnelse

	<u>Side</u>
Indledning	1
Afgrænsning	2
Den udførte revision	2
Konklusion	3
Bilag 1: Kontrolområder og kontrolmål	4

Servicegruppen for Dataudstyr A/S
Att.: Leverancechef Martin Høyer
Baldersbuen 40
2640 Hedehusene

Uafhængig revisors erklæring om generelle it-kontroller i Servicegruppen for Dataudstyr A/S' it-driftsmiljø

Indledning

Servicegruppen for Dataudstyr A/S (herefter SG) har indgået aftale med en række kunder om drift af kundernes it-miljø. Kunder hvis platform driftes af SG er som udgangspunkt omfattet af SGs fælles processer, kontroller og sikkerhedspolitikker. En række kunder har dog aftalt individuelle processer på et eller flere områder, og kan have afvigende sikkerhedsmæssige opsætninger. Disse individuelle aftaler er ikke omfattet af nærværende erklæring.

Vi har indgået aftale med SG om at revidere de generelle it-kontroller, som SG varetager for det omfattede it-miljø.

De generelle it-kontroller omfatter, jf. Revisionsvejledning 3411, følgende områder:

- Drift af datacentre og netværk
- Anskaffelse, ændringer og vedligeholdelse af systemssoftware
- Adgangssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af applikationssystemer

Det er SGs ledelses ansvar at sikre opretholdelsen af relevante kontroller og at udarbejde beskrivelser af disse. Det er vores opgave, baseret på vores arbejde, at udtrykke en konklusion om, hvorvidt vi er enige i, at de etablerede kontroller er tilfredsstillende opretholdt hos SG.

Erklæringen er udelukkende beregnet til brug for SG, SGs kunder og deres revisorer.

Afgrænsning

Revisionen har til formål at vurdere, om de generelle it-kontroller for det generelle driftsmiljø, som SGs kunder er omfattet af hos SG, er tilfredsstillende tilrettelagt, og om de har fungeret i revisionsperioden.

Der er i bilag 1 vedlagt en oversigt over de kontrolmål og revisionshandlinger, som revisionen har omfattet.

Vi har som led i revisionen udvalgt centrale tekniske platforme, for hvilke vi har testet overensstemmelse med SGs overordnede sikkerhedsretningslinjer. Vores stikprøve omfatter følgende:

- Windows 2003 (Administrativt domæne)
- Windows 2003 (Stikprøve på tilfældigt udvalgte kundeservere)
- Central firewall

Gennemgangen omfatter ikke:

- Kontroller, der udføres lokalt af SGs kunder på de af SG driftede platforme
- Kontroller i de brugersystemer, der kører på platforme hos SG
- Kontroller, som relaterer sig til kundespecifikke applikationer eller platforme
- Logisk sikkerhed på kundespecifikke servere, databaser, firewalls o. lign.

Den udførte revision

Vores revision af kontrolmiljøet hos SG er udført i overensstemmelse med den danske revisionsstandard for it-erklæringer (RS3411 type B) og således, at der opnås en høj, men ikke fuldstændig sikkerhed for vores konklusioner.

Revisionen er foretaget ved interview, observationer samt vurdering af udleveret/forevist materiale. Vi har stikprøvevis efterprøvet de beskrevne kontrolforanstaltninger.

Vores revisionshandlinger omfatter perioden 1. januar 2010 – 31. december 2010.

Vi har som vurderingsgrundlag anvendt Deloitte's opfattelse af "god it-skik".

Eventuelle kontrolsvagheder er beskrevet i en selvstændig rapport til SG; dog vil væsentlige enkeltstående kontrolsvagheder, eller hvor flere kontrolsvagheder i forening udgør en væsentlig svaghed, være beskrevet i konklusionsafsnittet.

Det er vores opfattelse, at det udførte arbejde giver et tilstrækkeligt grundlag for vores konklusion.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdekkes af vort arbejde. Endvidere vil en anvendelse af vor konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, eller i SG' overholdelse af de beskrevne politikker og procedurer, hvorved vor konklusion muligvis ikke længere vil være gældende.


Konklusion

På grundlag af den udførte revision er det vores vurdering, at de generelle it-kontroller hos SG i det væsentligste har været opretholdt i perioden 1. januar 2010 til 31. december 2010.

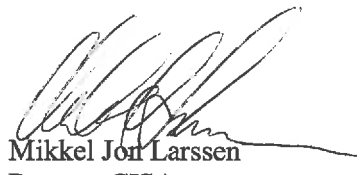
København, den 10. januar 2011

Deloitte

Statsautoriseret Revisionsaktieselskab



Mikkel Schøning
statsautoriseret revisor, CISA



Mikkel Jon Larssen
Partner, CISA

Bilag 1: Kontrolområder og kontrolmål

Nedenfor vises Deloitte's kontrolområder og kontrolmål for generelle it-kontroller.

Områder markeret med hvidt er omfattet fuldt ud af vores revision, mens gråt indikerer, at kontrolmålet ikke er omfattet.

Kontrolområder/Kontrolmål
1000 Datacenter og netværksdrift
Driftsrutiner og -opgaver administreres hensigtsmæssigt for at understøtte planlægning, udførelse, monitorering og kontinuitet af it-programmer og processer for nøjagtig, fuldstændig og gyldig behandling og registrering af finansielle transaktioner.
Data administreres hensigtsmæssigt for at skabe rimelig overbevisning for at finansielle data forbliver nøjagtige, fuldstændige og gyldige gennem opdaterings- og lagringsprocessen.
Faciliteterne, herunder de komponenter af it-infrastrukturen som håndterer finansielle informationer, administreres hensigtsmæssigt med henblik på at beskytte integriteten af finansielle informationer.
En beredskabsplan er indgået mellem kunden og outsourcingleverandøren. Denne testes og opdateres løbende, for at afspejle resultaterne af sådanne tests.
2000 Adgangssikkerhed
Konfigurationen af program- og systemsikkerhed i change management-processen administreres hensigtsmæssigt for at sikre mod uautoriserede modifikationer til programmer og data, som kan resultere i ufuldstændig, unøjagtig, eller ugyldig behandling eller registrering af finansiell information.
Systemsikkerhed er hensigtsmæssigt implementeret, administreret og logges, for at sikre mod uautoriseret adgang til, eller modifikationer i, applikationer og data, som resulterer i ufuldstændig, unøjagtig, eller ugyldig behandling eller registrering af finansiell information.
3000 Anskaffelse, Ændringer og Vedligeholdelse af Systemsoftware
Ny systemsoftware og modifikationer til eksisterende systemsoftware implementeres hensigtsmæssigt, og fungerer i overensstemmelse med ledelsens forventninger.
4000 Programændringer
Program- og systemændringer bliver administreret hensigtsmæssigt, for at minimere sandsynligheden for forstyrrelser, uautoriserede ændringer og fejl, som påvirker nøjagtig, fuldstændig og gyldig behandling og registrering af finansielle data.
5000 Anskaffelse, Udvikling og Vedligeholdelse af Applikationer
Nye applikationer og modifikationer til eksisterende applikationer implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.
Eksisterende data, som konverteres til nye applikationer i forbindelse med implementering af disse, er nøjagtige, fuldstændige og gyldige.

Kontrolområder/Udførte revisionshandlinger	
1000 Datacenter og netværksdrift	Konklusion
<p>Vi har, i det omfang SG har ansvaret herfor, stikprøvevist kontrolleret, at beskrevne opgaver er ansvarsmæssigt placeret i organisationen.</p> <p>Vi har endvidere stikprøvevist kontrolleret, at der løbende overvåges og rapporteres på om de indgåede aftaler overholdes.</p>	<p>Vi har ikke konstateret væsentlige svagheder på området.</p>
<p>Vi har, i det omfang SG har ansvaret herfor, stikprøvevist kontrolleret, at relevante systemer er omfattet af backupaftalen, herunder at konfigurationen af backup er i overensstemmelse med den godkendte backupaftale. Vi har stikprøvevist sikret, at backup foretages i overensstemmelse med aftalen, og at ændringer til aftalen afspejles korrekt i systemkonfigurationen.</p> <p>Vi har såfremt det er aftalt i kontrakten stikprøvevist verificeret, at der foretages løbende test af læsbarheden af backupmedier, samt at disse opbevares betryggende.</p>	<p>Vi har ikke konstateret væsentlige svagheder på området.</p>
<p>Vi har, i det omfang SG har ansvaret herfor, stikprøvevist kontrolleret adgangskontrolmekanismen til det centrale serverrum, samt den fysiske sikring mod indbrud i serverrum.</p> <p>Vi har endvidere, i det omfang SG har ansvaret herfor, kontrolleret, at serverrummet er beskyttet tilstrækkeligt mod brand, vandskade, strømsvigt mv. Vi har herunder verificeret eksistensen samt vedligeholdelsesgraden af brandslukningsudstyr, klimaanlæg, UPS, fugt- og varmemålere.</p>	<p>Vi har ikke konstateret væsentlige svagheder på området.</p>

2000 Adgangssikkerhed	Konklusion
<p>Vi har, i det omfang SG har ansvaret herfor, kontrolleret, at SG har modtaget gældende it-sikkerhedspolitik, og at denne efterleves af Servicegruppen i alle, for den indgåede aftale, relevante, henseender. Vi har endvidere kontrolleret følgende ved observation, samt stikprøvevis gennemgang:</p> <ul style="list-style-type: none"> • Relevante logningskrav er defineret og opsat korrekt på de tekniske platforme. • Kritiske logfiler gennemgås periodisk. • Standardpasswords er ændret på relevante systemer, platforme og kritiske netværkskomponenter. • Unikke brugerid'er er krævet for personlige brugere. • Screensaver, hvor relevant, anvendes og er opsat således, at timeout-settings ikke kan disables/ændres af brugeren. • Dokumentation for anvendelsen af åbne netværk eksisterer, og relevant krypteringsmetode er implementeret. • Relevante krav til passwords er defineret og implementeret på relevante tekniske platforme. • Administratorrettigheder tildeles alene på baggrund af en formel godkendelse. • Tilføjelser, ændringer og nedlæggelser af brugere, sker på baggrund af behørig godkendelse. • Periodisk revurdering af brugere og tilhørende rettigheder foretages. • Der er etableret beskyttelse som sikrer relevante servere og klienter mod virus, herunder at virussignatur er up to date samt at Servicegruppen gennemfører periodisk kontrol heraf. • Firewall-regler er opsat hensigtsmæssigt. 	<p>Vi har ikke konstateret væsentlige svagheder på området.</p>
<ul style="list-style-type: none"> • 3000 Anskaffelse, Ændringer og Vedligeholdelse af Systemsoftware 	Konklusion
<p>Vi har i relation til udvikling og vedligeholdelse af netværks- og systemsoftware kontrolleret følgende ved observation, samt stikprøvevis gennemgang:</p> <ul style="list-style-type: none"> • Der foreligger dokumentation for gennemførelse af test og godkendelse heraf før implementering i produktionsmiljø. • Ændringer planlægges, godkendes og implementeres, således at idriftsættelsen sker uden væsentlige konsekvenser for den daglige drift. • Dokumentation for kritiske netværkskomponenter og systemsoftware opdateres som følge af ændringer. • Fallback-planlægning indgår i overvejelserne i forbindelse med implementering af ændringer. • Større udviklingsprojekter følger en formel change procedure. 	<p>Vi har ikke konstateret væsentlige svagheder på området.</p>

• 4000 Programændringer	Konklusion
<p>Vi har i relation til programændringer kontrolleret følgende ved observation samt stikprøvevis gennemgang:</p> <ul style="list-style-type: none">• Anskaffelser, udvikling, ændringer og vedligeholdelse af projekter defineres, evalueres og godkendes af ledelsen i opstartsfasen.• Alle beslutninger om anskaffelse, udvikling, ændring og vedligeholdelse af applikationer, databaser, netværk og kommunikationssoftware, evalueres og godkendes af ledelsen.• Udviklingsprojekter følger en formel change procedure.	<p>Vi har ikke konstateret væsentlige svagheder på området.</p>