Deloitte.

Deloitte
Statsautoriseret
Revisionsaktieselskab
CVR-nr.: 24213714
Weidekampsgade 6
Postboks 1600
0900 København C
Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

IT Relation A/S

Erklæring fra uafhængig revisor vedrørende design og implementering af generelle it-kontroller til efterlevelse af sikkerhedspolitik

August 2011

Deloitte
Statsautoriseret
Revisionsaktieselskab
CVR-nr.: 24213714
Weidekampsgade 6
Postboks 1600
0900 København C
Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

IT RELATION A/S
Att.: Henning Kruse
Industrivej Syd 11
7400 Herning A/S

Erklæring fra uafhængig revisor vedrørende design og implementering af generelle it-kontroller til efterlevelse af sikkerhedspolitik pr. 31. august 2011

Indledning

IT Relation A/S tilbyder sine kunder en række forskellige ydelser inden for outsourcing af hostede applikationer/services, housing etc. og fungerer som totalleverandør af it i forhold til disse kunder i form af single-point-of-contact konceptet.

Vi har indgået en aftale med IT Relation A/S om at påse, at virksomheden har implementeret den udarbejdede it-sikkerhedspolitik i relation til kundeaktiviteterne. Revisionen tager udgangspunkt i it-sikkerhedspolitik version 7 af 29. august 2011, og de kontroller som selskabet har implementeret til at efterleve it-sikkerhedspolitikken.

Det er ledelsens ansvar at etablere og sikre betryggende kontroller til efterlevelse af it-sikkerhedspolitikken. Vores ansvar er, baseret på vores arbejde, at udtrykke en konklusion om, hvorvidt vi enige i, at selskabet har designet og implementeret betryggende kontroller, som sikrer, at it-sikkerhedspolitikken efterleves.

Vores erklæring er udarbejdet til brug for IT Relation A/S og de af IT Relation A/S' kunder, som enten har eller ønsker at indgå aftale med IT Relation A/S om varetagelse af it-drift og it-serviceydelser, samt disses revisorer.

Den udførte revision

Vores arbejde er udført i overensstemmelse med den danske revisionsstandard om andre erklæringsopgaver med sikkerhed (RS3000) med henblik på at opnå høj, men ikke fuldstændig, grad af sikkerhed for vores konklusion omkring, at selskabet har tilrettelagt og implementeret betryggende it-kontroller. Den udførte revision er tilrettelagt ud fra følgende kriterier:

- Erklæringen omfatter en vurdering af kontrollernes design og implementering på erklæringsdatoen, og udtrykker således ingen konklusion om kontrollernes effektivitet over en længere periode.
- De udførte revisionshandlinger er udvalgt fra Deloittes kontrolmål for gennemgang af it-kontroller på relevante områder i forhold til den gældende sikkerhedspolitik, jf. bilag 1.
- Det faktiske sikkerhedsniveau måles op mod Deloittes "baseline" for god it-sikkerhed i det omfang, andet ikke er konkret defineret i it-sikkerhedspolitikken eller underliggende bilag.

Revisionen omfatter forespørgsler, observationer, samt vurdering og stikprøvevis efterprøvelse af den information, vi har modtaget. Det er vores opfattelse, at det udførte arbejde giver et tilstrækkeligt grundlag for vor konklusion.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdækkes af vores arbejde. Endvidere vil en anvendelse af vores konklusion omkring betryggende tilrettelæggelse og implementering på efterfølgende perioder være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, ændring i kravene til behandling af oplysninger eller IT Relation A/S' overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

I vedlagte bilag 1 har vi anført de kontrolområder, som er omfattet af erklæringen, samt vores bemærkninger til de enkelte kontrolområder.

Konklusion

Det er vores opfattelse, at de generelle it-kontroller hos IT Relation A/S, til efterlevelse af it-sikkerhedspolitik version 7, af 29. august 2011, er hensigtsmæssigt designet og implementeret.

Århus, den 31. august 2011

Deloitte
Statsautoriseret Revisionsaktieselskab

Mikkel Schøning
statsautoriseret revisor, CISA

Henrik Roed Svendsen
director, CISA, CGEIT

Bilag 1: Kontrolområder

Nedenfor vises Deloittes kontrolområder og –aktiviteter for generelle it-kontroller, som omfattes af revisionen i relation til den gældende sikkerhedspolitik.

Kontrolområder
IT-sikkerhedshedsorganisation
Dataejer • Dataejer, som har det grundlæggende ansvar for tilstrækkelig sikkerhed på virksomhedens og kundernes data, defineres.
Sikkerhedsorganisation • Retningslinjer for sikkerhedsorganisation
Systemejer • Retningslinjer for systemejer.
Revision • Retningslinjer for regelmæssig revision/revurdering af it-sikkerhedspolitikken.
It-driftsorganisationen hos IT Relations Housing partner • Retningslinjer for IT Relations Housing partner
Opgaver og ansvar • Definering af opgaver og ansvar.
Regelsæt
It-strategi • Retningslinjer for udarbejdelse og ændring af it-strategi
Regler for it-brugere • Retningslinjer og krav til medarbejdere hos IT Relation.
Persondatalov
Ansvar og kompetence • Retningslinjer for efterlevelse af lovgivningsmæssige forhold
Fysisk sikkerhed
Bygningsindretning • Krav til indretning af særlige it-lokaler
Adgangskontrol • Krav til at kun autoriserede medarbejdere tildeles adgang.
Alarmsystemer • Retningslinjer og krav til sikring og overvågning af adgang til fysiske lokationer.
Registrering af aktiver/forsikring • Retningslinjer for sikring af aktiver

Kontrolområder
Datasikkerhed
Adgang • Retningslinjer for adgang til data, herunder adgang til kundedata.
Anvendelse • Retningslinjer for logning af hændelser
Tab, herunder backup
Data • Retningslinjer for sikkerhedskopiering.
Datakvalitet • Retningslinjer for test af systemer.
Dokumentation • Retningslinjer for krav til dokumentation af systemer
Intern kontrol • Retningslinjer for krav til etablering af intern kontrol
Virus • Retningslinjer og krav til sikring mod virusangreb
Datakommunikation
Firewall • Retningslinjer og krav til etablering af Firewall.
Netværk • Retningslinjer og krav til opbygning og sikkerhed omkring netværk.
Hjemmearbejdspladser • Retningslinjer og krav til opbygning og sikkerhed omkring hjemmearbejdspladser.
Mobile arbejdspladser • Retningslinjer og krav til opbygning og sikkerhed omkring mobile arbejdspladser.
Internet, herunder e-mail • Krav og formelle procedurer på alle kritiske driftsoperationer, herunder nødprocedurer for uplanlagte systemnedbrud.
Udvikling og anskaffelse af it-systemer
Anskaffelse af systemer • Retningslinjer for anskaffelse af systemer
Egenudvikling af systemer • Retningslinjer for egenudvikling af systemer.
Nødberedskab
• Procedurer og krav til betryggende nødberedskab