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

IT Relation A/S

ISAE 3402 Type 2

Uafhængig revisors erklæring angående generelle it-kontroller relateret til drifts- og hostingydelser for 01.11.2011 til 31.10.2012

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

IT Relation A/S
Industrivej Syd 11
7400 Herning

1. Uafhængig revisors erklæring

Til ledelsen hos IT Relation A/S, IT Relation A/S' kunder og deres revisorer.

Omfang

Vi har fået til opgave at erklære os vedrørende IT Relation A/S' udsagn i afsnit 2 samt de tilhørende beskrivelser af system- og kontrolmiljøet i afsnit 3 for IT Relation A/S' drifts- og hostingydelser, omfattende design, implementering og effektivitet af kontroller anført i beskrivelsen. IT Relation A/S' beskrivelse omhandler de kontroller, som er etableret til sikring af system-, data- og driftsikkerheden for applikationer og underliggende infrastruktur på de serviceydelser, som IT Relation A/S tilbyder drifts- og hostingkunder (generelle it-kontroller).

Denne erklæring er udarbejdet efter helhedsmetoden og omfatter således ledelsens beskrivelse af kontrolmål og de hertil hørende kontrolaktiviteter hos IT Relation A/S på alle områder inden for de generelle it-kontroller, som kan henføres til de leverede serviceydelser.

IT Relation A/S' ansvar

IT Relation A/S er ansvarlig for udarbejdelse af efterfølgende udsagn samt beskrivelse af system- og kontrolmiljøet, jf. afsnit 3. IT Relation A/S er endvidere ansvarlig for sikring af beskrivelsens fuldstændighed og nøjagtighed, herunder sikre en korrekt fremstilling og præsentationen af udsagn og beskrivelse i denne erklæring. Det er endvidere IT Relation A/S' ansvar at levere de ydelser, som beskrivelsen omfatter, at udforme og designe samt implementere effektive kontroller for at opnå de identificerede kontrolmål.

Revisors ansvar

Det er vores ansvar, baseret på vores procedurer, at udtrykke en konklusion om IT Relation A/S' beskrivelse samt om design, implementering og effektivitet af kontroller relateret til de kontrolmål, der

er anført i deres beskrivelse. Vi har udført vores arbejder i henhold til International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," udgivet af International Auditing and Assurance Standards Board. Denne standard kræver, at vi opfylder etiske krav samt planlægger og udfører vores procedurer med henblik på at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er dækkende, og kontrollerne er hensigtsmæssigt designet og fungerer effektivt.

En erklæringsopgave med sikkerhed for beskrivelsen, design og effektiviteten af kontroller hos IT Relation A/S omfatter udførelse af procedurer med henblik på at opnå bevis for IT Relation A/S' beskrivelse af sit system samt for kontrollernes design og effektivitet. De udvalgte procedurer afhænger af revisors vurdering, herunder vurdering af risikoen for, at beskrivelsen ikke fremstår dækkende, og at kontroller ikke er hensigtsmæssigt designet eller ikke fungerer effektivt. Vores procedurer omfatter en test af effektiviteten af de kontroller, som vi anser som nødvendige for at opnå en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen bliver nået. Vores procedure omfatter endvidere en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør

IT Relation A/S' beskrivelse er udarbejdet med henblik på at imødekomme kravene fra en bred vifte af kunder og disses revisorer og kan derfor ikke omfatte alle aspekter af kontrol i et system, som den enkelte kunde anser som værende vigtigt for eget kontrolmiljø. Kontroller i en servicevirksomhed kan heller ikke i sagens natur forhindre eller opdage alle fejl eller udeladelser i proces- eller rapporteringstransaktioner. Derudover er forskydningen af effektivitetsvurdering udsat for den risiko, at kontroller i en servicevirksomhed kan blive utilstrækkelige eller fejle.

Endvidere vil en anvendelse af vores konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller eller i virksomhedens overholdelse af de beskrevne politikker og procedurer, hvorved vor konklusion muligvis ikke længere vil være gældende.

Konklusion

Vores konklusion er udformet på basis af de forhold, der er beskrevet i denne erklæring. De kriterier, som vi har anvendt i forbindelse med vores konklusion er beskrevet i afsnit 4. På grundlag af den udførte revision er det vores vurdering, at:

a) beskrivelsen af de generelle it-kontroller med relevans for system-, data- og driftssikkerheden for IT relation A/S' kunder, således som de var udformet og implementeret i perioden 01.11.2011 -31.10. 2012, i alle væsentlige henseender er dækkende, og
b) kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 01.11. 2011 -31.10. 2012, og
c) de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 01.11. 2011 – 31.10. 2012

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet samt arten, den tidsmæssige placering og resultatet af disse tests fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring, beskrivelse af system- og kontrolmiljø i afsnit 3 samt vores test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt IT Relation A/S' ydelser og disses revisorer, og som har tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risici for væsentlige fejlinformationer i deres regnskaber.

København, den 29. november 2012

Deloitte

Statsautoriseret Revisionspartnerselskab

Steen Gellert-Kristensen
statsautoriseret revisor

Henrik Roed Svendsen
director, CISA, CGEIT

2. Udsagn fra IT Relation A/S

Denne redegørelse omfatter en beskrivelse af system- og kontrolmiljøet, herunder de kontroller, som IT Relation A/S udfører for vores kunder i relation til de indgåede aftaler. Beskrivelse af arbejdsprocesser og udførte kontroller er nærmere anført i afsnit 3 – Systembeskrivelse fra IT Relation A/S. Redegørelsen har til formål at beskrive de arbejdsprocesser og udførte kontroller, som IT Relation A/S varetager for vores kunder.

Beskrivelsen omfatter perioden 01.11.2011 til 31.10.2012 og er udelukkende beregnet for IT Relation A/S' kunder og deres revisorer.

IT Relation A/S bekræfter, at:

- beskrivelserne giver en dækkende redegørelse for vores arbejdsprocesser og udførte kontroller til sikring af betryggende sikringsforanstaltninger omkring drifts- og hostingydelserne, herunder:
  - at der er defineret en risikovurderingsproces til identifikation af risici i hostingydelserne
  - at der med udgangspunkt i risici er fastsat kontrolmål og kontroller til imødegåelser af de identificerede risici
  - at de beskrevne arbejdsprocesser og kontroller er implementeret
  - at der er etableret ledelsesmæssige overvågningskontroller til sikring af, at kontrollerne er effektive
- beskrivelserne indeholder relevante oplysninger om væsentlige ændringer i de outsourcede ydelser i perioden 01.11.2011 til 31.10.2012
- beskrivelserne er udarbejdet under hensyntagen til, at de skal opfylde almindelige behov for information til brug for aflæggelse af IT Relation A/S' kunders regnskab

- beskrivelsen af de udførte kontroller er hensigtsmæssigt designet, er implementeret hos IT Relation A/S og har fungeret effektivt i hele perioden 01.11.2011 til 31.10.2012, herunder:
  - at etablerede kontroller er designet til at imødegå de identificerede risici
  - at etablerede kontroller vil – hvis de udføres som beskrevet – give høj grad af sikkerhed for at de identificerede risici forhindres eller minimeres til et acceptabelt niveau
  - at manuelle kontroller udføres af personer med tilstrækkelige kompetencer og beføjelser hertil

Herning, den 29. November 2012
IT Relation A/S

Niels Kamp
Underdirektør

3. Systembeskrivelse fra IT Relation A/S

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for IT Relations kunder og disses revisorer i overensstemmelse med kravene i den danske revisionsstandard ISAE3402 for erklæringsopgaver om kontroller hos serviceleverandør. Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret ifm. IT Relations leverance af serviceydelser på drifts- og hosting.

Beskrivelsen indeholder beskrivelser af de anvendte procedurer til sikring af en betryggende afvikling af systemer. Formålet er at give tilstrækkelige informationer til, at hosting-kunders revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet i det omfang, det kan medføre en risiko for væsentlige fejl i hosting-kunders it-drift for perioden 01.11.2011 til 31.10.2012.

3.2 Beskrivelse af IT Relation A/S' ydelser

IT Relation har siden etableringen i 2003 været en del af hosting-branchen og har leveret generationer af it-løsninger til flere forskellige brancher i markedet. IT Relation leverer udover hosting tillige en bred vifte af øvrige it-relaterede ydelser.

IT Relation tilbyder følgende serviceydelser til hosting-markedet:

- Hosting og Housing
- Remote backup
- ServiceDesk

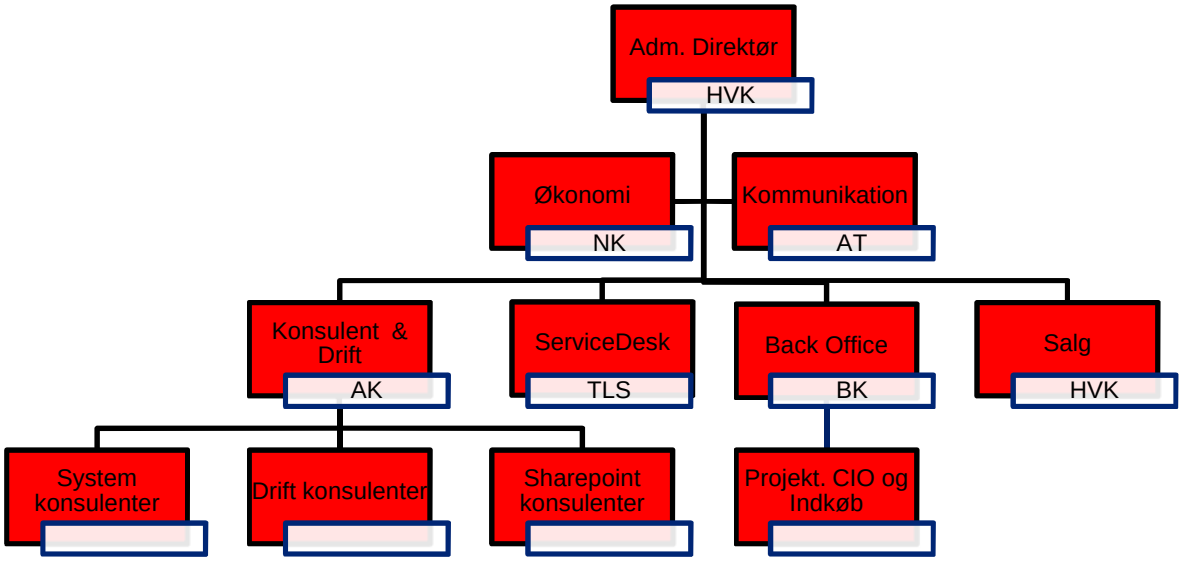
Nærværende systembeskrivelse indeholder en beskrivelse af anvendte arbejdsprocedurer og udførte kontroller på ovenstående serviceydelser.

Ud over ovenstående tilbyder IT Relation endvidere assistance på følgende områder:

- Rådgivning på CIO niveau
- Projektledelse

3.3 IT Relation A/S' organisation og sikkerhed

Ansvar og organisering i IT Relation A/S fremgår af nedenstående organisationsdiagram:



3.4 Risikostyring ved IT Relation A/S

Risikostyring gennemføres i IT Relation på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering, der sigter mod interne systemer generelt. Input til denne vurdering indhentes i hele organisationen. Processen faciliteters af Konsulent- og Driftschef, der udarbejder udkast til IT Relations ledelse. Efter intern bearbejdning godkendes vurderingen af IT Relations ledelse.

I projektindstillingsfasen udarbejdes der, afhængig af projektets karakter dels en sikkerhedsvurdering samt en vurdering af særlige risici og usikkerheder. Dette sker efter en foruddefineret proces.

På operationelt projektniveau gennemføres løbende risikostyring. Der arbejdes efter en fast projektstyringsmodel, hvor ansvaret for projektrelateret risikostyring gennemføres af projektlederen, som ofte vælger at inddrage projektdeltagere, eksterne partnere og eventuelle styregruppemedlemmer i processen.

3.5 Kontrol rammer, kontrolstruktur og kriterier for kontrolimplementering

IT Relations it-sikkerhedspolitik, etablerede processer og kontroller omfatter alle systemer og ydelser, der tilbydes kunderne. Det fortsatte arbejde med tilpasning og forbedring af IT Relations sikringsforanstaltninger sker løbende i samarbejde med højt kvalificerede specialister.

IT Relation er som medlem af BFIH endvidere underlagt en årlig system-/it revision, som bl.a. resulterer i en årlig revisionserklæring udarbejdet efter ISAE3402 standarden.

Fastsættelse af kriterier for kontrolimplementering hos IT Relation tager udgangspunkt i ISO 27001/27002. På basis af dette kontrol-framework er relevante kontrolområder og kontrolaktiviteter implementeret ud fra best practice for minimering af risici på de serviceydelser, som leveres af IT Relation. Med udgangspunkt i den valgte kontrolmodel indgår følgende kontrolområder i det samlede kontolmiljø:

- Informationssikkerhed
- Intern organisering af it-sikkerhed
- Fysisk sikkerhed
- Styring af kommunikation med kunder
- Backup
- Drift og overvågning
- Adgangskontrol
- Anskaffelse og vedligeholdelse af netværk

3.6 Etableret kontrolmiljø

Hvert enkelt område er detaljebeskrevet i de efterfølgende afsnit.

3.6.1 Informationssikkerhed

Formål
En ledelsesgodkendt It-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse, og kommunikeret ud til relevante medarbejdere i virksomheden.

Anvendte procedurer og kontroller
IT Relation afdækker relevante it risici på de etablerede serviceydelser. Dette varetages gennem en løbende trussels- og risikovurdering hos IT Relation, dels i forbindelse med alle udviklingsprojekter og ændringer i systemmiljøer og dels ved en årlig revurdering af risikoanalysen. Resultatet af den årlige gennemgang forelægges ledelsen. IT Relation stiller endvidere en række informationer til rådighed for hosting-kundernes revisorer til brug for deres vurdering af IT Relation som serviceleverandør. Ud over drifts-relaterede forhold kan IT Relation også informere om sikkerhedsmæssige forhold, i det omfang de tilsluttede kunder efterspørger dette.

Tidspunkt for udførsel af kontrollen
It-sikkerhedspolitikken revurderes mindst en gang årlig forinden udførelse af it-revision og udarbejdelse af erklæring.

Hvem udfører kontrollen
Den årlige gennemgang udføres af sikkerhedsgruppen.

Kontrol dokumentation
Der er versionsstyring af it-sikkerhedspolitikken.

3.6.2 Intern organisering af it-sikkerhed

Direktionen i IT Relation, som er den øverst ansvarlige for it-sikkerheden søger for, at der til stadighed er etableret procedurer og systemer, der understøtter overholdelsen af den til enhver tid gældende it-sikkerhedspolitik. It-sikkerhedsgruppen beskriver de overordnede målsætninger, og den Driftsansvarlige er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollabelt, hvor dette overhovedet er muligt, og være udtryk for best practice inden for de enkelte kontrolaktiviteter på de serviceområder, som tilbydes kunderne. It-sikkerhedsgruppen består pt. af følgende medlemmer:

- Underdirektør Niels Kamp
- Konsulent- og Driftschef Anders Kaag
- Driftsansvarlig Henning Kruse

Gruppen mødes 1gang årligt for at fastsætte og følge op på målsætninger i relation til it- sikkerheden.

3.6.3 Fysisk sikkerhed

It-Relation har indgået en aftale med BO Data ApS omkring Housing af IT Relations servermiljøer. IT Relation har fuld adgang til kundernes udstyr hos BO Data.

Fysisk adgangskontrol og sikring

Formål
Den fysiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med Hosting leverandør.

Anvendte procedurer og kontroller
Adgang til bygning er kontrolleret via nøgler, som er udleveret til IT Relation. Derudover kræves der en særlig nøgle ved adgang til Housing-centerets serverrum. Kun personer med behov for adgang til serverrummet i Housing-centeret har adgang til de udleverede nøgler. Endelig skal der anvendes nøgle til de rackskabe, som anvendes af IT Relation. Listen over udleverede nøgler opbevares og ajourføres af hosting-udbyder.

Serverrum er beliggende på 1. sal, og lokalet er beskyttet med fastmonteret gitter, som er SKAFOR BLÅ godkendt på alle vinduer. Endvidere er alle døre i data centeret sikret med Rukos nøgle/cylinder system, som er SKAFOR RØD godkendt. Endelig er der etableret et alarmsystem, som er godkendt til SKAFOR BLÅ sikringsklasse.

Tidspunkt for udførsel af kontrollen
Nøglelog hos IT Relation gennemgås ugentlig.

Hvem udfører kontrollen
Driftsafdelingen og Housing-leverandør udfører kontrollen. Kontroller omkring tildeling af nøgler generelt til data centeret er ikke en del af nærværende erklæring og Deloitte har ikke udført test på disse kontroller.

Kontrol dokumentation
Den enkelte bruger af nøglen fra IT Relation til Housing-centeret noterer i loggen ved afhentning og aflevering.

Sikring mod miljømæssige hændelser

Formål
It-udstyr er beskyttet mod miljømæssige hændelser som strømsvigt og brand.

Anvendte procedurer og kontroller
Data centerets serverrum er beskyttet mod følgende miljømæssige hændelser:

- Strømsikring
- Brandsikring
- Klima

På alt vitalt it udstyr er stabil strøm sikret med en UPS-installation, som kan holde systemerne med strøm indtil generatoren automatisk er startet og klar. I teknik- og serverrummet er der etableret røg-

og temperaturfølere, der er koblet sammen med det centrale brandovervågningssystem. Serverrummet er endvidere forsynet med automatisk brandbekæmpelsesudstyr (der aktiveres ved for høje værdier på enten røg eller varme). Der udføres løbende service på disse anlæg.

Varmeudviklingen i serverrummet reguleres gennem det fuldautomatiske kølesystem, som sikrer den korrekte temperatur for sikring af stabil drift og lang holdbarhed på det anvendte it-udstyr. Der udføres løbende service på anlægget.

Tidspunkt for udførsel af kontrollen
Der udføres daglig visuel kontrol af systemerne i Housing af leverandøren (BoData)
Der udføres 2 årlige kontroller af alarmsystemet fra alarmselskabet (Lund og Erichesen A/S)
Der udføres 1 årlig kontrol af ABA (Brand) af AGIS Fire & Security A/S
Der udføres 1 årlig kontrol af UPS af Eaton Power Quality Danmark
Der udføres service på generator og UPS hver 3 mdr. af Power-rent.dk

Hvem udfører kontrollen
Kontrollen udføres af Housing-leverandøren (BoData) + leverandøre af de øvrige systemer.

Kontrol dokumentation
Alle kontrolskemaer forefindes hos Housing-leverandør (BoData), og Deloitte har haft adgang til disse.

3.6.4 Styring af kommunikation med kunder

ServiceDesk og kundesupport
Formål
Der udføres betryggende brugersupport for bruger, der kontakter ServiceDesk, herunder at der ydes den aftalte support indenfor det aftalte område og tidsrum.

Anvendte procedurer og kontroller
IT Relation har etableret et sæt af skriftlige ServiceDesk-procedurer på de områder, der er aftalt i aftalen med kunden. ServiceDesk-procedurerne udarbejdes af ServiceDesk i et tæt samarbejde med kunden samt 3. parts leverandøre. Support til bruger sker via fjernovertagelsessoftwaren TeamViewer, samt via terminalserverens platformsværktøjer.

Svartider er aftalt i kundens SLA, og prioriteringer sker i sagssystemet ”Efecte”.

Tidspunkt for udførsel af kontrollen
ServiceDesk gennemgår dagligt sager, der afventer løsning.

Hvem udfører kontrollen
Kontroller udføres af ServiceDesk, og uden for normal arbejdstid udføres den af ServiceDesk-bagvagten.

Kontrol dokumentation
Alle hændelser logges i Efecte eller ITR-TID.

Incident håndtering

Formål
Der gennemføres en betryggende incident håndtering ud fra de indgåede aftaler med kunder, herunder at IT Relation kontrollerer, at dette sker til normal fuldførelse og med forventet resultat.

Anvendte procedurer og kontroller
IT Relation anvender ITR-TID til registrering og håndtering af incidents, der noteres følgende i sagen:

- Fejl (kommer fra mail – "Efecte" (ServiceDesk) eller fra manuel oprettelse)
- Hvad der er gjort for afhjælpning af fejl
- Hvem der har udført opgaven
- Tidsstempling for, hvad tid der er noteret i sagen
- Tidsregistrering (om det er ifølge driftsaftale, eller om det skal faktureres)

Ledelsen af driftsafdelingen er ansvarlig for overvågning af, at indkomne henvendelser i ServiceDesk prioriteres og tildeles ressourcer, samt at incidenthåndtering gennemføres i overensstemmelse med de indgåede kundeaftaler.

Tidspunkt for udførsel af kontrollen
Incidentshåndtering sker kontinuerligt gennem hele dagen.

Hvem udfører kontrollen
Håndteringerne af incidents udføres af IT Relations Driftsafdeling, og uden for normal arbejdstid udføres den af en konsulent (bagvagten).

Kontrol dokumentation
Alle hændelser logges i ITR-TID. Der er ikke opsat automatisk eskalering eller andet i IT-TID for kontrol af overholdelse af SLA-aftaler. Kunden har selv adgang til at følge sager i kundens ”SelfServiceportal”.

3.6.5 Backup

Formål
Data sikkerhedskopieres og opbevares, så de kan reetableres. IT Relation kontrollerer, om backup udføres fejlfrit, og ved fejl i backup at der udføres en vurdering af fejl og opfølgning på evt. fejlretning.

Anvendte procedurer og kontroller
Der er udarbejdet udførlig beskrivelse af backupprocedure. Backupproceduren er en del af den daglige kørsel og er således automatiseret i systemet. Manuelle rutiner i forbindelse med backup er beskrevet i driftsprocedurerne. Skift af backupmedie varetages af driftsafdelingen. Medierne er mærket med et unikt nummer / stregkode. Den interne opbevaring af backupmedier sker i databrandskab.
Backupsystemet er fysik placeret på anden lokalitet end Hosting-centeret (20 km afstand).

Backup testes løbende, idet backups anvendes til at reetablere kundedata, ligesom der ved den årlige afprøvning af recovery-procedurer sker en efterprøvning af restore i forbindelse med en fuld reetablering af **én** enkelt kundes miljø, dvs. både systemopsætning og brugerdata.

Tidspunkt for udførsel af kontrollen
Der udføres tjek af backuplogs i normal arbejdstid.

Hvem udfører kontrollen
Driftsafdelingen forestår den daglige kontrol af backuplogs.

Kontrol dokumentation
Daglig driftstjek af skema samt af det årlige tjekskema.
Der logges, hvilke medier der kommer ind og ud af databrandskab.

3.6.6 Drift og overvågning

Formål
Der udføres proaktiv overvågning af, at aftalte services er tilgængelig, at tilgængelige ressourcer er i overensstemmelse med de aftalte normer/tærskelværdier, og at nødvendige jobs og kørsler, såvel on-

line som batch, afvikles rettidigt og korrekt. IT Relation kontrollerer, at dette sker til normal fuldførelse og med forventet resultat.

Anvendte procedurer og kontroller
IT Relation har etableret et sæt af skriftlige driftsprocedurer på alle væsentlige drifts aktiviteter, som understøtter de generelle forventninger til betryggende drift som anført i IT Relations it-sikkerhedspolitik. Driftsprocedurerne udarbejdes af Driftsafdelingen i et tæt samarbejde med kunden, 3. parts leverandøre samt Driftsafdelingen.

Driftsafvikling sker via Terminalserverens platformsværktøjer. Der foreligger en række jobbeskrivelser for driftsafdelingen, hvor der er fastsat, hvilke overvågninger og kontroller der udføres dagligt – ugentlig - årligt. Konstaterede fejl i udførte kontroller og eventuelle fejl fra det systemtekniske overvågningssystem korrigeres hurtigst muligt ved hjælp af procedurer eller "Best practice"; kunden informeres løbende om omfanget og konsekvenserne af de konstaterede fejl.

Følgende funktionsområder har adgang til kundernes it-systemer: ServiceDesk-medarbejdere, Driftsmedarbejdere og konsulenter.

Tidspunkt for udførsel af kontrollen
Kontrollen udføres 24/7 eller i primær driftstid ifølge SLA-aftalen med den enkelte kunde.

Hvem udfører kontrollen
Kontroller udføres af IT Relations Driftsafdeling, og uden for normal arbejdstid udføres den af en konsulent (bagvagten).

Kontrol dokumentation
Alle hændelser logges i ITR-TID eller "Efecte".

3.6.7 Adgangskontrol

Formål
Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med de tilsluttede kunders behov.
Adgangen deles op i 3 områder:

- Kundens medarbejder
- IT Relations medarbejder
- 3. parts konsulenter

Anvendte procedurer og kontroller
Der er som standard anvendt fælles systemadgang for IT Relation og kundens interne it-medarbejdere (fælles administratorpassword). 3. parts konsulenter bliver oprettet som lokaladministrator på de systemer, som dækker kundens krav/behov. 3. parts konsulenters adgang og rettigheder til kundesystemer sker alene efter en formel godkendelse fra kunden.

Generelt oprettes brugere på baggrund af skriftlige henvendelser/mail sendt til IT Relations Driftsafdeling. Det er IT Relation, der fastsætter, hvilken af de foruddefinerede roller som brugerne skal tildeles på baggrund af kundens godkendelse.

Rettigheder til interne brugere hos IT Relation oprettes efter de samme principper og godkendes af Konsulent- og Driftschefen. For interne medarbejdere er der udarbejdet formelle retningslinjer vedrørende sletning af brugere. Disse sikrer bl.a., at en fratrådt medarbejder ved arbejdsophør hos IT Relation afleverer nøgler og adgangskort, således at der ikke kan opnås fysisk adgang til bygningen og vedkommendes bruger-id spærres for login.

Tidspunkt for udførsel af kontrollen
For kunder sker det i forbindelse med anmodning fra kunden, og når 3. part tilgår kundens system.
Internt sker der kontrol i forbindelse med personaleændringer.

Hvem udfører kontrollen
For kunder er det Driftsafdelingen ved IT Relation, der har ansvaret for, at proceduren for 3. parts adgang til kundens miljø bliver overholdt ifølge aftale med kunden. For medarbejdere ved IT Relation er det Konsulent- og Driftschefen, der har ansvaret for, hvem der har adgang til hvad (kunde miljø – interne systemer).

Kontrol dokumentation
Ved behov for adgang fra en 3. part til kundens it-miljø er det kundens it-ansvarlig, der fremsender en godkendelsesmail til Driftsafdelingen, denne lagres herefter på kundedrevet i kundens Driftsmappe.
For IT Relations medarbejder gemmes brugerskemaer i den enkeltes personalemappe på Direktionsdrevet.

3.6.8 Anskaffelse og vedligeholdelse af infrastruktur

Netværks og kommunikationssoftware

Formål
Netværks- og kommunikationssoftware vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.

Anvendte procedurer og kontroller
IT Relation har fuld dokumentation for netværk og kommunikationslinjer frem til de tilsluttede kunder, hvor der foreligger en aftale omkring drift af kundens netværksudstyr.

IT Relation vurderer løbende behov for opdatering af firmware på netværks- og kommunikations software. For at sikre en stabil drift vil der alene ske opdateringer, såfremt det er nødvendigt, for at sikre kommunikationen. Inden ændringer foretages, tages backup af konfigurationsfilerne til netværks komponenter, ligesom udskiftet udstyr beholdes i en karensperiode i tilfælde af, at nyt udstyr ikke fungerer korrekt eller optimalt. Væsentlige ændringer til netværkskonfigurationer foretages indenfor de med kunderne aftalte servicevinduer.

Tidspunkt for udførsel af kontrollen
Kontrollen udføres i forbindelse med opdatering og ændring.

Hvem udfører kontrollen
Netværksafdelingen har ansvaret for udførsel af opdateringer samt kontrol af funktionalitet.

Kontrol dokumentation
Der laves dokumentation i ITR-TID omkring opgaver, der er udført på kundens system.

Systemsoftware

Formål
Systemsoftware 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.

Anvendte procedurer og kontroller
For Windows-servere indhentes fyldestgørende systemdokumentation efter behov. IT Relation har fastsat procedurer for anskaffelse og opdatering af system software Windows-platformene. På Windows-platformen hentes opdateringer fra Microsoft og rulles automatisk på serverne via Lumension

Patchmanagement-system. Der sker således ikke manuel vurdering af disse opdateringer, idet leverandøren (Lumension) har testet og vurderet de enkelte opdateringer.

Tidspunkt for udførsel af kontrollen
Kontrollen for opdateringer sker via Lumension Patchmanagement-system, som indeholder logs for opdateringer.

Hvem udfører kontrollen
Driftsafdelingen er ansvarlig for udførsel af opdateringer og kontrol heraf.

Kontrol dokumentation
Ud over dokumentation i Lumension føres der ikke logs.

3.7 Supplerende information omkring det etablerede kontrolmiljø

3.7.1 Forhold, som skal iagtages af kundernes revisorer

Levering af serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på IT Relations standard betingelser. Det bevirker at kundernes afvigelser fra IT Relations standard betingelserne ikke er omfattet af nærværende erklæring. Kundernes egne revisorer bør derfor vurdere, om denne erklæring kan anvendes på den konkrete kunde og selv afdække eventulle andre risici, der vurderes som væsentlige for aflæggelse af kundernes årsregnskaber.

Brugeradministration

IT Relation giver adgang og tildeler rettigheder i overensstemmelse med kunderne instrukser i takt med, at disse bliver indmeldt i ServiceDesk. IT Relation er ikke ansvarlig for, at disse informationer er korrekte, og det er således kundernes ansvar at sikre, at de tildelte adgange og rettigheder til systemer og applikationer sker betryggende og i overensstemmelse med best practice omkring funktionsadskillelse.

IT Relation tildeler endvidere adgang til 3. parts konsulenter; primært udviklere, som skal vedligeholde applikationer, som indgår i hosting aftalen. Dette sker efter instruks fra IT Relations kunder.

Kundernes egne revisorer bør derfor selvstændigt vurdere, om tildelte adgange og rettigheder til applikationer, servere og databaser – såvel til kundens egne medarbejdere som til 3. parts konsulenter - er betryggende ud fra en vurdering af risici for fejl i regnskabsaflæggelsen.

Beredskabsplanlægning

I de generelle betingelser for hosting hos IT Relation er der ikke defineret krav til beredskabsstyring og reetablering af kundernes systemmiljø i tilfælde af en katastrofe. IT Relation sikrer, at der generelt tages backup af kundemiljøer, men garanti for reetablering af hele systemmiljøet efter en katastrofe er ikke omfattet af hostingaftalerne. Kundernes egne revisorer bør derfor selvstændigt vurdere risici ved manglende beredskabsplanlægning og regelmæssig test heraf i relation til en risiko for fejl i regnskabsaflæggelsen.

Internt har IT Relation defineret en beredskabsplan således, at selskabets it-anvendelse kan videreføres i tilfælde af en katastrofe.

Efterlevelse af relevant lovgivning

IT Relation har tilrettelagt procedurer og kontroller, således at de områder, som er IT Relations ansvar efterleves betryggende. IT Relation er ikke ansvarlig for applikationer, som afvikles på det hostede udstyr, og som følge af dette omfatter denne erklæring ikke sikkerhed for, at der er etableret betryggende kontroller i brugerapplikationerne, herunder at applikationerne efterlever bogføringsloven, persondataloven eller anden relevant lovgivning.

4. Information distribueret af Deloitte

4.1 Introduktion

Denne oversigt er udformet med henblik på at informere kunder om de kontroller hos IT Relation A/S, som kan påvirke behandling af regnskabsmæssige transaktioner og samtidig informere om effektiviteten af de kontroller, vi har efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i kundernes forretningsprocesser, har til hensigt at hjælpe kundernes revisorer med dels at planlægge revisionen af årsregnskabet og dels at vurdere risici for fejl i kundernes regnskaber, som muligvis påvirkes af kontroller hos IT Relation A/S.

Vores test af IT Relation A/S' kontroller er begrænset til de kontrolmål og relaterede kontroller, som vi har nævnt i nedenstående testskema i denne del af rapporten og er ikke udvidet til at omfatte alle de kontroller, som måtte fremgå af ledelsens systembeskrivelse, ligesom kontroller udført hos IT Relation A/S' kunder ikke er omfattet af vores erklæring. Sidstnævnte forudsættes gennemgået og vurderet af kundernes egne revisorer.

Endelig kan der hos kunderne være etableret kompenserende kontroller, som bevirker, at kontrolsvagheder nævnt i denne rapport minimeres til et revisionsmæssigt acceptabelt niveau. Denne vurdering kan alene foretages af kundernes revisorer.

4.2 Kontrolmiljøelementer

Vores test af kontrolmiljøet inkluderede forespørgsler hos relevant ledelse, tilsynsførende og personale samt inspektion af IT Relation A/S' dokumenter og registreringer. Kontrolmiljøet er vurderet mht. at bestemme karakteren, timingen og omfanget af kontrollers effektivitet.

4.3 Test af effektivitet

Vores test af kontrollers effektivitet inkluderer de tests, som vi betragter som nødvendige for at evaluere, hvorvidt de udførte kontroller og overholdelsen af disse er tilstrækkelige til at give en høj, men ikke absolut, overbevisning om, at de specificerede kontrolmål blev opnået i løbet af perioden 01.11.2011 til 31.10.2012. Vores test af kontrollernes effektivitet er udformet til at dække et repræsentativt antal af transaktioner i løbet af perioden 01.11.2011 til 31.10.2012 for hver kontrol, jf. nedenfor, som er designet til at opnå de specifikke kontrolmål. I udvælgelsen af specifikke tests har vi overvejet (a) karakteren af de testede områder, (b) typerne af tilgængelig dokumentation, (c) karakteren af revisionsmålene, der skal opnås, (d) det vurderede kontrolrisikoniveau og (e) testens forventede effektivitet.

4.4 Kontrolmål og kontrolaktiviteter

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
4.4.1 Kontrolområde - Driftsafvikling			
Batch og driftsafvikling – Skriftlige procedurer Kontrollen skal sikre, at skriftlige driftsprocedurer udarbejdes og opdateres for alle relevante og væsentlige områder.	IT Relation anvender faste procedurer i den daglige drift og udarbejder kontrollister med henblik på at dokumentere udførte driftskontroller.	Deloitte har vurderet de anvendte driftsprocedurer og planlagte kontroller. Vi har stikprøvevis gennemgået kontrollister og undersøgt, om der er signeret for udført kontrol, og at eventuelle konstaterede fejl er håndteret.	Ingen bemærkninger.
Driftsovervågning -generelt Kontrollen skal sikre, at der udføres løbende overvågning af driftsmiljøet i overensstemmelse med de generelle aftalebestemmelser, og at der følges op på alle fejl.	Der er etableret automatisk overvågning af alle servere og services, og der gives alarmer til driftspersonalet ved fejl.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har gennemgået stikprøve over alarmer fra driftsmiljøet og kontrolleret, at der på alarmer er gennemført en dokumenteret opfølgning.	Ingen bemærkninger.
Incidenthåndtering Kontrollen skal sikre, at der følges op på alle indkomne henvendelser fra kunder.	Alle kundehenvendelser registreres som en sag i enten Efecte eller ITR-TID. Henvendelserne prioriteres og tildeles de personer, som skal behandle sagen. Forløbet af sagen og løsningen dokumenteres i "Efecte" eller ITR-TID. Der følges løbende op på sagerne for at sikre, at alle sager bliver behandlet korrekt.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har stikprøvevis gennemgået indkomne incidents og observeret, at der løbende følges op på disse, og at dette dokumenteres i Efecte og ITR-TID.	Ingen bemærkninger.
Kapacitetsovervågning Kontrollen skal sikre, at der udføres løbende overvågning af systemer, hardware etc.	Der er opsat alarmering på hardware og alle væsentlige services (både interne og kundevendte). Der følges op på alle alarmer, og der anvendes realtime overvågning på skærme i driften.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har stikprøvevis gennemgået overvågning af driftsmiljøet og kontrolleret, at der for kunders systemer er opsat kapacitetsstyring.	Ingen bemærkninger.

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
4.4.2 Kontrolområde – Backup / Restore			
Backup – Strategi Kontrollen skal sikre, at grundlaget for valg og konfiguration af sikkerhedskopiering for relevante systemer og data er tilstrækkeligt til at dække såvel lovgivningens som ledelsens krav.	Der bliver udarbejdet backupstrategier ud fra den indgåede SLA for de enkelte kunder. Der tages backup af alt kundedata og alle servere, med mindre andet er aftalt med kunden.	Deloitte har gennemgået backupbeskrivelsen og vurderet, om den i tilstrækkelig grad afdækker backupkrav for kritiske systemer og data, som er anført i outsourcingsaftalerne med de tilsluttede virksomheder.	Ingen bemærkninger.
Backup – Konfiguration Kontrollen skal sikre, at konfiguration af backup gennemføres korrekt for alle relevante systemer og data.	IT Relation anvender en default backupkonfiguration, som anvendes til at tage backup af alle kundedata.	Deloitte har gennemgået procedurer for konfiguration af backup og vurderet kontrollens design. Deloitte har foretaget stikprøver på backupkonfigurationen og sammenholdt disse med den udarbejdede backupbeskrivelse.	Ingen bemærkninger.
Backup – Ekstern opbevaring Kontrollen skal sikre, at der periodisk bringes datamedier til ekstern opbevaring, således at selv større uheld ikke kan medføre tab af alle data.	Der fortages ekstern backup på IT Relations lokation. Disse data overføres fra det primære datacenter, BoData, som er placeret ca. 20km fra lokationen. Backupdata flyttes til brandskab.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har påset, at den eksterne arkivering af backupmedier bliver udført.	Ingen bemærkninger.
Backup – Test Kontrollen skal sikre, at der gennemføres test/vurdering af, at sikkerhedskopier kan anvendes til retablering af systemer og data som forudsat af ledelsen.	Der testes løbende for, at backupdata kan anvendes til reetablering. En gang om året tests backupen for, om det er muligt at kunne genskabe en kundes miljø.	Deloitte har gennemgået procedurer for reetablering af filer og fuld reetableringstest ud fra backup. Deloitte har gennemgået seneste backuptest for at en kundes miljø kunne genskabes ud fra backup.	Ingen bemærkninger.
4.4.3 Kontrolområde – Fysisk adgang og sikkerhed			
Fysisk adgang – Adgang til kritiske lokationer Kontrollen skal sikre, at adgang til f.eks. serverrum er tilstrækkeligt begrænset via adgangskontrolfaciliteter, at adgange kun tildeles på baggrund af konkrete godkendelser, og at adgange tildeles i overensstemmelse med de arbejdsbetingede behov herfor.	IT Relation anvender to lokationer: et primært datacenter hos BoData og et backupcenter på IT Relations lokation. Adgangen til BoData sikres med en nøgle, som kun udleveres til relevante personer, og der føres log for udleveringen. Adgangen til backuprummet er sikret med kode på døren, som kun er kendt af relevante personer.	Deloitte har påset sikkerhedsforanstaltninger og vurderet, om adgangen til kritiske lokationer er begrænset betryggende, herunder at evt. adgang til kritiske lokationer som serverrummet er godkendt i form af en nøglelog.	Ingen bemærkninger.

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
4.4.4 Kontrolområde – Sikring mod miljømæssige hændelser			
Fysisk sikkerhed – Strømsikring Kontrollen skal sikre, at der er etableret tilstrækkelig og hensigtsmæssig sikring imod kortere og længerevarende svigt i strømforsyningen for relevant it-udstyr.	Serverrummet er forsynet med stabil strøm via UPS-anlæg og strømgenerator. Der er yderligere indgået kontrakt om et periodisk syn af UPS-anlægget og generator.	Deloitte har påset, at der er opsat nødstrøm til kritiske maskiner, og at der er dokumentation for periodisk syn af løsningen.	Ingen bemærkninger.
Fysisk sikkerhed – Brandsikring Kontrollen skal sikre, at der er etableret tilstrækkelig og hensigtsmæssig sikring imod brand for relevant it-udstyr.	Serverrummet er forsynet med røg- og temperaturføler, der er koblet sammen med det centrale brandovervågningssystem. Serverrummet er yderligere forsynet med brandslukning og detektion (både røg og temperatur). Der er yderligere indgået kontrakt om en periodisk vedligeholdelse af brandslukningsanlægget.	Deloitte har påset, at der er opsat brandovervågning, at der i serverrummet er opsat brandslukningsanlæg, og at der er dokumentation for periodisk syn af løsningen.	Ingen bemærkninger.
Fysisk sikkerhed – Klimaovervågning og køling Kontrollen skal sikre, at der er etableret tilstrækkelig og hensigtsmæssig styring og overvågning af klimaforhold for relevant it-udstyr.	Serverrummet er forsynet med automatisk regulerende køling for at sikre en stabil drift. Der er yderligere indgået kontrakt om en periodisk vedligeholdelse af kølesystemet.	Deloitte har påset, at der er opsat køling i serverrummet, og at der er dokumentation for periodisk syn af løsningen.	Ingen bemærkninger.
Fysisk sikkerhed – Indretning Kontrollen skal sikre, at faciliteter for relevant it-udstyr indrettes hensigtsmæssigt under hensyntagen til relevante eksterne faktorer (f.eks. identificeret i it-risikoanalysen).	Serverrummet er indrettet således, at der ikke forefindes faldstammer, vandrør mv., som vil kunne forårsage skader på maskiner, der anvendes til kritiske systemer og data.	Deloitte har gennemgået indretningen af kritiske lokationer og vurderet, om der er forhold, som udgør en risiko.	Ingen bemærkninger.
4.4.6 Kontrolområde – It Governance			
It-sikkerhedspolitik Kontrollen skal sikre, at der udarbejdes en ledelsesgodkendt it-sikkerhedspolitik, som virksomheden implementerer og løbende følger op på.	Der er udarbejdet en it-sikkerhedspolitik, som bliver gennemgået mindst en gang om året.	Deloitte har gennemgået seneste ajourførte it-sikkerhedspolitik og vurderet, om denne er betryggende.	Ingen bemærkninger.
It-risikoanalyse Kontrollen skal sikre, at der periodisk foretages en formel analyse af de risici, som er forbundet med it-anvendelsen.	IT Relation har udarbejdet it-risikoanalyse for kritiske systemer, der anvendes i den daglige drift. Der gennemføres en årlig vurdering af, om forhold til risiko og trusler fortsat er gældende, eller der er behov for ændring til risikoanalysen.	Deloitte har vurderet seneste ajourførte it-risikoanalyse og vurderet, om denne er betryggende.	Ingen bemærkninger.

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
4.4.7 Kontrolområde – It-sikkerhedsadministration			
Brugerrettigheder – Oprettelser og ændringer Kontrollen skal sikre, at brugeradgange alene oprettes og ændres på netværk, operativsystemer, applikationer og databaser af autoriserede administratorer på baggrund af formelle godkendelser fra autorisationsansvarlige.	Brugere oprettes kun på baggrund af udfyldte blanketter, som sendes til ServiceDesken. Alle oprettelser dokumenteres i Efecte. Brugerne tildeles rettigheder i forhold til kundernes ønsker anført i oprettelsesblanketten.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har stikprøvevis gennemgået dokumentation for oprettede brugere og vurderet, om der er et gyldigt grundlag for tildelte adgange og rettigheder.	Ingen bemærkninger.
Brugerrettigheder – Udvidede rettigheder Kontrollen skal sikre, at tildeling af udvidede rettigheder (typisk administratorprivilegier) til brugere kun sker på baggrund af et arbejdsmæssigt behov.	Interne medarbejderes adgang til systemer følger samme processer som for øvrige brugere. Kun et begrænset antal nøglemedarbejdere er tildelt udvidede rettigheder på systemerne. Adgang til kunders systemer fortaget af IT Relations personale logges.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har gennemgået brugere med udvidede rettigheder på IT Relations centrale infrastruktur og verificeret, at disse er godkendt til de tildelte rettigheder.	Ingen bemærkninger.
Brugerrettigheder – Nedlæggelser Kontrollen skal sikre, at brugeradgange nedlægges eller inaktiveres i forbindelse med fratrædelser.	Brugere nedlægges kun på baggrund af udfyldte blanketter, som sendes til ServiceDesken. Alle nedlæggelser dokumenteres i Efecte. Det er kundernes eget ansvar at oplyse om nedlæggelse af brugere.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har foretaget en stikprøve på nedlagte brugere.	Ingen bemærkninger.
Brugerrettigheder – Periodisk revurdering af rettigheder og inaktivitet Kontrollen skal sikre, at der periodisk tages stilling til tildelte rettigheder til brugere på alle niveauer, omfattende normale brugere, administrative brugere samt service- og systemprofiler på både applikations-, database, netværks- og operativsystemniveau.	Der udføres løbende review af interne brugere på IT Relations management systemer.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har gennemgået brugere på det interne managementsystem.	Ingen bemærkninger.
It-sikkerhedslogning Kontrollen skal sikre, at der på alle relevante platforme og systemer er taget stilling til behovet for gennemførelse af sikkerhedsmæssig logning, at den specificerede logning implementeres, at logs periodisk kontrolleres, og at der følges op på evt. hændelser. Logning og periodisk gennemgang heraf bør derfor principielt omfatte log fra både OS, Firewall, applikationer og andre kritiske systemer.	Der er opsat logning af sikkerhedsmæssige hændelser på IT Relations infrastruktur. Der sker dog ingen periodisk gennemgang af disse logs.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har verificeret, om logning af kritiske systemer og netværk følger godkendte logningskrav.	Vi har konstateret, at der ikke formelt er dokumenteret en proaktiv gennemgang og overvågning af logs med sikkerhedsmæssige hændelser. Vi har fået oplyst, at gennemgang af logs alene sker på ad hoc basis, såfremt der er behov for at undersøge konkrete forhold.

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
It-sikkerhedsorganisation Kontrollen skal sikre, at it-sikkerhedsrelevante opgaver er defineret, og at ansvaret for opgaverne er placeret hos medarbejdere, som er bekendte med deres ansvar.	It-sikkerhedsmæssige roller og ansvarsområder er fordelt, og medarbejderne er bekendt med deres arbejdsopgaver og funktioner.	Deloitte har ved interview gennemgået funktionerne i organisationen og verificeret, at disse stemmer overens med de faktiske roller og ansvarsområder ved interview af medarbejdere.	Ingen bemærkninger.
4.4.8 Kontrolområde – Logisk sikkerhed			
Anvendelse af passwords Kontrollen skal sikre, at alle brugere autentificeres, og at kravene til passwords er fastlagte og implementerede på alle relevante platforme.	Autentificering af brugere sker via Windows AD og herfra yderligere adgangsstyring for at administrere den øvrige infrastruktur.	Deloitte har gennemgået konfigurationen af password settings på kritiske interne systemer og verificeret, at relevante brugere anvender disse.	Ingen bemærkninger.
Anvendelse af brugerprofiler Kontrollen skal sikre, at personlige brugere anvender personlige brugerprofiler, samt at anvendelsen af serviceprofiler og eventuelle fællesbrugerprofiler dokumenteres og godkendes.	Brugere er oprettet i Windows AD og alle anvender individuelle brugerprofiler på det interne netværk.	Deloitte har gennemgået anvendelsen af brugerprofiler på alle relevante systemer og platforme og verificeret, at disse er personlige og identificerbare.	Ingen bemærkninger.
4.4.9 Kontrolområde – Netværk og kommunikationssoftware			
Netværk og kommunikation – Patch management Kontrollen skal sikre, at relevante opgraderinger, patches og fixes fra leverandører til kritiske netværkskomponenter vurderes, godkendes og implementeres.	Relevante firmware-opdateringer vurderes løbende og implementeres efter behov. Der ændres ikke på firmware for netværkskomponenter, med mindre der er konstateret sikkerhedshuller.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Vi har vurderet designet af kontroller og vurderet, at disse er betryggende. Men i om med der ikke i den revideret periode har været ændringer til netværkets firmware, er det ikke muligt at teste de etablerede procedurer.	N/A
Netværk og kommunikation – Test Kontrollen skal sikre, at implementering af nye eller ændringer af eksisterende kritiske komponenter i netværket testes i tilstrækkeligt omfang.	Test af ændringer sker på redundant udstyr eller mindre kritiske komponenter inden ændringer anvendes i produktion.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Der har i den reviderede periode ikke været ændringer til netværkets firmware, og det er derfor ikke muligt at teste de etablerede procedurer.	N/A

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
Netværk og kommunikation – Fallback Kontrollen skal sikre, at der er etableret tilstrækkelige foranstaltninger til at kunne retablere det oprindelige miljø, såfremt der skulle opstå større fejl i forbindelse med ændringer til kritiske netværkskomponenter.	Der anvendes versioneringsværktøj til kritiske netværkskomponenters konfigurationsfiler. Kritiske ændringer til netværkskomponenter gemmes automatisk i flere versioner, så det er muligt at rulle tilbage til en tidligere konfiguration.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Der har i den reviderede periode ikke været ændringer til netværkets firmware, og det er derfor ikke muligt at teste de etablerede procedurer.	N/A
Netværk og kommunikation – Timing Kontrollen skal sikre, at ændringer implementeres på tidspunkter, hvor dette ikke forstyrrer den daglige drift, f.eks. på kritiske tidspunkter omkring større kørsler og tilsvarende.	Ændringer i netværksstrukturer foretages som udgangspunkt i definerede servicevinduer, som er aftalt med kunderne.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Der har i den reviderede periode ikke været ændringer til netværkets firmware, og det er derfor ikke muligt at teste de etablerede procedurer.	N/A
Netværk og kommunikation – Dokumentation af netværk Kontrollen skal sikre, at anvendelsen af netværk er dokumenteret med overblik over den samlede netværkstopologi, herunder etablerede adgangskontroller imellem interne og eksterne netværk.	Netværket dokumenteres i forskellige topologitegninger samt dokumenter med oplysninger om IP-adresser VLANs konfigurationer mv. Ændringer til dokumentationen sker i forbindelse med nye kunder, der skal oprettes i det hosted miljø.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har gennemgået seneste netværksdokumentation og verificeret, at disse løbende opdateres.	Ingen bemærkninger.
4.4.10 Kontrolområde – System software			
System software – Patch management Kontrollen skal sikre, at relevante patches og fixes fra leverandører til systemprogrammel vurderes, godkendes og implementeres.	Der sker en løbende opdatering af Windows platforme hvor opdateringerne hentes fra Microsoft og styres igennem Lumension Endpoint Management.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har foretaget en stikprøve på, at der løbende sker patching af servere.	Ingen bemærkninger.
System software – Test Kontrollen skal sikre, at ændringer til systemprogrammel, herunder ændringer fra leverandører, testes og godkendes forinden implementering i produktionsmiljøet.	Test udføres af Lumension, som af IT Relation vurderes at være kompetente til at teste og tage stilling til ændringer til system software.	Deloitte har vurderet anvendte procedurer og udførte kontroller. Deloitte har vurderet dokumentation for gennemførte test af ændringer til systemsoftware, som varetages af Lumension.	IT Relation gennemfører ikke test af ændringer til systemsoftware direkte op mod kundernes systemmiljøer. IT Relation har en aftale med Lumension, om at de gennemfører en generel test, og på baggrund af anbefalinger fra Lumension vurdere IT Relation, hvilke ændringer som skal implementeres.

Kontrolaktivitet	Etableret kontrol hos IT Relation A/S	Testplan	Testresultat
System software – Fallback Kontrollen skal sikre, at der er etableret tilstrækkelige foranstaltninger til at kunne retablere det oprindelige miljø, såfremt der skulle opstå større fejl i forbindelse med ændringer til systemprogrammel.	Fallback for patchning er at afinstallere patches i det omfang, det er muligt. Såfremt der er behov for det, er det muligt at reetablere ud fra backup.	Deloitte har foretaget en stikprøve på, at der i forbindelse med patching har været behov for fall-back, og om disse kunne foretages.	Ingen bemærkninger.
System software – Timing Kontrollen skal sikre, at ændringer implementeres på tidspunkter, hvor dette ikke forstyrrer den daglige drift, f.eks. på kritiske tidspunkter omkring større kørsler og tilsvarende.	Nye opdateringer installeres normalt indenfor de forud-definerede servicevinduer. Ved ekstraordinære servicevinduer advares kunderne.	Deloitte har foretaget en stikprøve på, at der i forbindelse med patching af systemsoftware er taget stilling til timing for implemente-ringen i produktion.	Ingen bemærkninger.
System software – Dokumentation af systemer Kontrollen skal sikre, at tilstrækkelig dokumentation for anvendt systemprogrammel og konfiguration af denne foreligger.	Der er etableret omfattende systemdokumentation af både interne servere og de hostede miljøer.	Deloitte har vurderet, om dokumen-tationen for anvendte systemer er betryggende.	Ingen bemærkninger.

5. Yderligere information fra IT Relation A/S

5.1 Beredskabsplanlægning i fremtiden

IT Relation har igangsat aktiviteter med henblik på at styrke procedurer og kontroller omkring beredskabsstyring i tilfælde af en katastrofe, således at disse også vil omfatte kundernes systemmiljøer. Disse aktiviteter forventes afsluttet i løbet at kalenderåret 2013.