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

# A/S ScanNet

# ISAE 3402 Type 2

# Uafhængig revisors erklæring angående generelle it-kontroller relateret til drifts- og hostingydelser for 1. januar 2014 til 31. december 2014

# Indholdsfortegnelse

# 1. Uafhængig revisors erklæring

**Til ledelsen hos A/S ScanNet, A/S ScanNets kunder og deres revisorer.**

## Omfang

Vi har fået til opgave at erklære os vedrørende A/S ScanNets udsagn i afsnit 2 samt de tilhørende beskrivelser af system- og kontrolmiljøet i afsnit 3 for A/S ScanNets drifts- og hostingydelser, omfattende design, implementering og effektivitet af kontroller anført i beskrivelsen. A/S ScanNets beskrivelse omhandler de kontroller, som er etableret til sikring af system-, data- og driftssikkerheden for applikationer og underliggende infrastruktur på de serviceydelser, som A/S ScanNet 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 A/S ScanNet på alle områder inden for de generelle it-kontroller, som kan henføres til de leverede serviceydelser.

## A/S ScanNets ansvar

A/S ScanNet er ansvarlig for udarbejdelse af efterfølgende udsagn samt beskrivelse af system- og kontrolmiljøet, jf. afsnit 3. A/S ScanNet 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 A/S ScanNets ansvar at levere de ydelser, som beskrivelsen omfatter og 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 A/S ScanNets 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 A/S ScanNet omfatter udførelse af procedurer med henblik på at opnå bevis for A/S ScanNets 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

A/S ScanNets 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 vigtig 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 A/S ScanNets kunder, således som de var udformet og implementeret i perioden 01.01.2014 - 31.12.2014, i alle væsentlige henseender er dækkende
b) kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 01.01.2014 - 31.12.2014

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 01.01.2014 - 31.12.2014.

## 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 A/S ScanNets 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, d. 23. januar 2015

**Deloitte**

Statsautoriseret Revisionspartnerselskab

Steen Gellert-Kristensen
statsautoriseret revisor

Henrik Roed Svendsen
director, CISA, CEGIT

# 2. Udsagn fra A/S ScanNet

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

Beskrivelsen omfatter perioden 01.01.2014 til 31.12.2014 og er udelukkende beregnet for A/S ScanNets kunder og deres revisorer.

A/S ScanNet 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 01.01.2014 til 31.12.2014
- beskrivelserne er udarbejdet under hensyntagen til, at de skal opfylde almindelige behov for information til brug for aflæggelse af A/S ScanNets kunders regnskab

- beskrivelsen af de udførte kontroller er hensigtsmæssigt designet, er implementeret hos A/S ScanNet og har fungeret effektivt i hele perioden 01.01.2014 til 31.12.2014, 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.

Kolding, den 23. januar 2015

A/S ScanNet

Jens Peter Andersen
Teknisk Direktør

# 3. Systembeskrivelse fra A/S ScanNet

## 3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for A/S ScanNets kunder og disses revisorer i overensstemmelse med kravene i den danske revisionsstandard ISAE 3402 for erklæringsopgaver om kontroller hos serviceleverandør. Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret ifm. A/S ScanNets 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 hostingkunders revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet i det omfang, det kan medføre en risiko for væsentlige fejl i hostingkunders it-drift for perioden 01.01.2014 til 31.12.2014.

## 3.2 Beskrivelse af A/S ScanNets ydelser

A/S ScanNet er en dansk it-servicevirksomhed med fokus på internettet. A/S ScanNet har siden 1995 beskæftiget sig med internet, drift og udvikling

Produktområderne omfatter i dag bl.a. kommerciel webhosting, serverhosting, domæneregistrering, shopping-systemer, betalingsløsninger, CMS-systemer, ERP-integration, databaseløsninger samt it-outsourcing. Serverdriften foregår i Danmark i specialindrettede serverrum, som er tyverisikrede og udstyret med brandhæmmende inergén-anlæg samt øvrige sikringsforanstaltninger til tidssvarende serverrum. A/S ScanNet har endvidere aftaler med store leverandører på WAN, som sikrer en høj tilgængelighed til og fra A/S ScanNets lokationer.

A/S ScanNet har siden starten været i rivende udvikling og er i dag et af Danmarks største kommercielle webhoteller og domæneudbyder med mere end 60.000 domæner registreret og hostet. I takt med udviklingen har A/S ScanNet løbende haft fokus på at optimere kvaliteten og servicegraden samt tilpasning af produktudvalg.

A/S ScanNet prioriterer kundeservice, driftsstabilitet og effektiv, personlig support meget højt. Supportteamet er nøje sammensat, hvilket sikrer den kvalitet, som A/S ScanNet er kendte for.

### 3.3 A/S ScanNets organisation og sikkerhed

A/S ScanNet har ca. 57 medarbejdere og er organiseret i salgs-, drifts-, udviklings- og support og administrative funktioner. Supportfunktionen varetager de daglige support, drifts- og udviklingsfunktioner og understøtter som specialister driftscenteret, herunder håndterer større og komplekse ændringer i kundernes driftsmiljøer.

AS/ ScanNet har indgået aftale med Global Connect A/S udelukkende til housing-faciliteter til selskabet sekundære lokation. Den sekundære lokation anvendes ikke til drift af kundernes systemmiljøer men alene til opbevaring af ekstern backup samt som nødlokation i tilfælde af en katastrofesituation. A/S ScanNet har aftale med Global Connect A/S om årligt at modtage en 3402 revisionserklæring på de serviceydelser, som leveres af Global Connect A/S.

### 3.4 Risikostyring ved A/S ScanNet

A/S ScanNet har fastsat processer for risikovurdering af deres forretning. Formålet med it-risikovurderingen er at sikre, at de risici, som er forbundet med de services og ydelser, som A/S ScanNet stiller til rådighed, er reduceret til et acceptabelt niveau.

It-risikovurderingen revurderes med fastsatte intervaller og som minimum i forbindelse med, at der indføres nye services. It-risikovurderingen gennemføres af projektkoordinator, øvrige relevante medarbejdere og godkendes af A/S ScanNets tekniske direktør eller administrerende direktør.

### 3.5 Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering

A/S ScanNets it-sikkerhedspolitik er gældende for alle medarbejdere og er etableret med henblik på at skabe et styringsværktøj for hensigtsmæssig og pålidelig drift af de kerneydelser, som A/S ScanNet tilbyder kunderne. Der arbejdes løbende med forbedring af såvel fysisk som logisk sikkerhed, driftsafvikling, nød-/beredskabsplanlægning og support af it-infrastrukturen samt udførelse og dokumentation af de etablerede kontroller.

Fastsættelse af kriterier og omfang for kontrolimplementering hos A/S ScanNet sker ud fra ISO 27001/27002 standarderne. Med udgangspunkt i dette kontrol-framework er relevante kontrolområder og kontrolaktiviteter implementeret på de serviceydelser, som leveres af A/S ScanNet. Med udgangspunkt i den valgte kontrolmodel indgår følgende kontrolområder i det samlede kontrolmiljø:

- Informationssikkerhed
- Intern organisering af it-sikkerhed
- Fysisk sikkerhed
- Styring af kommunikation og drift
  - Backup
  - Netværks- og kommunikationssoftware
  - Systemsoftware
  - Overvågning
  - Incidenthåndtering
- Adgangskontrol
  - Logisk sikring
  - Brugeradministration
- Business Continuity Management

## 3.6 Etableret kontrolmiljø

Nedenfor er de enkelte kontrolområder nærmere beskrevet.

### 3.6.1 Informationssikkerhed

**It-risikoanalyse**

**Formål med it-risikoanalyse**

Formålet med it-risikoanalysen er at sikre, at de risici, som er forbundet med de services, som A/S ScanNet stiller til rådighed er afdækket. Det giver mulighed for at vurdere, hvis der skal laves tiltag for at minimere risici.

**It-risikoanalyse**

It-risikoanalysen gennemgås med fastsatte intervaller, og når der indføres nye services. Det vurderes, om der skal laves tiltag for at minimere risici. It-risikoanalysen gennemgås af projektkoordinator og de relevante medarbejdere. Risikoanalysen godkendes af den tekniske direktør eller den administrerende direktør

**It-sikkerhedspolitik**

**Formål med it-sikkerhedspolitik**

Formålet med it-sikkerhedspolitikken er at sikre, at A/S ScanNet har beskrevet såvel fysisk som logisk sikkerhed.

It-sikkerhedspolitikken gennemgås med fastsatte intervaller, og når der indføres nye services, som kan have indflydelse på enten den fysiske eller logiske sikkerhed. It-sikkerhedspolitikken gennemgås af

projektkoordinator og de relevante medarbejdere. It-sikkerhedspolitikken godkendes af den tekniske direktør eller administrerende direktør

### 3.6.2 Intern organisering af it-sikkerhed

Den administrerende direktør er som medlem af direktionen øverst ansvarlige for it-sikkerheden over for bestyrelsen og A/S ScanNets kunder. Den tekniske direktør er ansvarlig for, at der til stadighed er etableret procedurer og systemer, der understøtter overholdelsen af den til enhver tid gældende it-sikkerhedspolitik, herunder etablering og gennemførelse af kontroller med henblik på at sikre, at de etablerede procedurer efterleves i A/S ScanNet.
Det daglige sikkerhedsarbejde udføres af alle ansatte hos A/S ScanNet. Sikkerhedsarbejdet overvåges af teknisk direktør og udvalgte personer fra øvrige funktioner.

Sikkerhedsniveauet skal være målbart og kontrollabelt ud fra en ressourcemæssig vurdering af omkostninger og risiko samt være udtryk for best practice inden for de enkelte kontrolaktiviteter på de serviceområder, som tilbydes A/S ScanNets kunder.

### 3.6.3 Fysisk sikkerhed

**Adgang til kritiske lokationer**
Adgang til co-location og A/S ScanNets primære og sekundære serverrum er begrænset til autoriseret personale. Der er kun adgang til rummene inde fra selve A/S ScanNets bygning. Adgangsdøre til rummene er sikringsdøre, og der er opsat elektroniske kortlæsere ved dørene. Alle kort, der giver adgang til co-location eller serverrum er forsynet med billede. Der skal altid anvendes kode sammen med kortet for at få adgang til co-location og serverrum. Til co-location skal kunder desuden benytte en fingeraftrykslæser for at få adgang. Uden for normal arbejdstid er der ikke adgang til området omkring bygningen med køretøj uden anvendelse af adgangskort.

Der er tegnet servicekontrakt på alarmanlægget med en anerkendt leverandør. Alarmanlægget serviceres med de anbefalede intervaller.

Kun udvalgte driftsmedarbejdere kan tildele adgang til serverrum og co-location. Adgangsanmodning skal altid foregå fra nærmeste chef via change request i ITSM. Den tekniske direktør skal orienteres, inden adgangen kan tildeles. Der foreligger et underskrevet dokument for hver af kundens medarbejdere, som har adgang til co-location.

For A/S ScanNet personales adgang gælder, at det med faste mellemrum kontrolleres, at det kun er godkendte personer, som har adgang.

For kundeadgang gælder, at det med faste mellemrum kontrolleres, at det kun er de af kunden godkendte personer, som har adgang.

**Overvågning af kritiske lokationer**
Alle registreringer, som foretages med de elektroniske kortlæsere til serverrum og co-location bliver logget.

A/S ScanNets bygninger og adgangsveje er overvåget med videokameraer. Dette gælder også hall og døre ind til serverrummene. Der er desuden videoovervågning i både serverrum og co-location.
Ved forsøg på at tiltvinge sig adgang til A/S ScanNets bygninger, serverrum og co-location udløses alarm, som automatisk tilkalder sikkerhedsvagter og A/S ScanNets driftspersonale.

**Test af anlæg**
Alarmanlægget bliver testet af driftspersonalet med faste intervaller. Testene bliver dokumenteret.

**Strømsikring**
A/S ScanNet har etableret sikringsforanstaltninger til at imødegå risici omkring udfald af strøm. Dette er etableret dels gennem UPS-anlæg og dels via nødstrømsgenerator. Formålet med strømsikring er at sikre, at et eventuelt strømsvigt eller spændingsskift i strømforsyningen ikke får indflydelse på driften af de systemer, som A/S ScanNet hoster for kunden.

<u>UPS-anlæg</u>
For A/S ScanNets primære og sekundære lokationer samt co-location gælder, at de er sikret med UPS. UPS-enhederne er dimensioneret ud fra princippet n+1 for at sikre, at en fejl på en enkelt UPS-enhed ikke får indflydelse i tilfælde af strømsvigt. I tilfælde hvor UPS-enhederne overtager strømforsyningen af serverrummene, starter nødstrømsgeneratoren automatisk og overtager efter kort tid strømforsyningen af serverrummene. Der er tegnet servicekontrakt på UPS-enhederne med en anerkendt leverandør. De bliver serviceret med de anbefalede intervaller. Leverandøren udfylder og afleverer en servicerapport.

UPS-enhederne bliver testet af driftspersonalet med faste intervaller. Testene bliver dokumenteret.

For UPS-enhederne gælder, at der er opsat overvågning, så driftspersonalet bliver alarmeret i tilfælde af, at UPS-enhederne bliver aktiveret, eller hvis der opstår fejl på UPS-enhederne.

Nødstrømsgenerator

For A/S ScanNets primære og sekundære lokationer samt co-location gælder, at de er sikret med nødstrømsgenerator.

Der er tegnet servicekontrakt på nødstrømsgeneratorerne med en anerkendt leverandør. De bliver serviceret med de anbefalede intervaller. Leverandøren udfylder og afleverer en servicerapport.

Nødstrømsgeneratorerne bliver testet af driftspersonalet med faste intervaller, og testene bliver dokumenteret.
For nødstrømsgeneratorerne gælder, at der er opsat overvågning, så driftspersonalet bliver alarmeret i tilfælde af, at nødstrømsgeneratorerne bliver aktiveret, eller hvis der opstår fejl på nødstrømsgeneratorerne.

**Brandsikring**

Formålet med brandsikring er at minimere risikoen for brandskader i A/S ScanNets primære og sekundære lokationer samt co-location.

Der er opsat røgdetektorer i A/S ScanNets bygninger. Røgdetektorerne er tilkoblet alarmcentralen, så brandvæsenet og A/S ScanNets driftspersonale automatisk bliver tilkaldt.

I A/S ScanNets primære og sekundære lokationer samt co-location er der installeret automatisk brandslukningsanlæg. Brandslukningsanlægget er designet til anvendelse i serverrum.

Der er tegnet servicekontrakt på brandsikringsanlæggene med en anerkendt leverandør. De bliver serviceret med de anbefalede intervaller. Leverandøren udfylder og afleverer en servicerapport.

Brandalarmeringen bliver testet af driftspersonalet med faste intervaller. Testene bliver dokumenteret.
For brandalarmeringsanlægget gælder, at der er opsat overvågning, så brandvæsen og driftspersonalet bliver alarmeret i tilfælde af, at der opstår fejl på anlægget.

**Køling**

Formålet med køling er at sikre, at udstyr placeret i A/S ScanNets primære og sekundære lokationer samt co-location er sikret mod overophedning.

For A/S ScanNets primære og sekundære lokationer samt co-location gælder, at der er opsat køleanlæg. Køleanlæggene er dimensioneret ud fra princippet n+1 for at sikre, at en fejl på en enkelt køleenhed ikke påvirker temperaturen i rummene.

Der er tegnet servicekontrakt på køleanlæggene med en anerkendt leverandør. De bliver serviceret med de anbefalede intervaller. Leverandøren udfylder og afleverer en servicerapport. For køleanlæggene gælder, at der er opsat overvågning, så driftspersonalet bliver alarmeret i tilfælde af, at der opstår fejl på anlægget.

**Indretning**

Formålet med indretningen af A/S ScanNets primære og sekundære lokationer samt co-location er at sikre udstyr, som er placeret i rummene.

Indretning af serverrum og co-location

For A/S ScanNets primære, sekundære lokationer og co-location gælder, at rummene er designet og indrettet til it-drift. Indretningen af serverrummene er sket i samarbejde med en anerkendt leverandør. Rummene anvendes kun til it-drift. Der er lagerfaciliteter i lokaler i umiddelbar nærhed af rummene, her opbevares udstyr, som ikke er i drift. Udpakning af udstyr foregår ligeledes i disse lokaler.

A/S ScanNets primære lokation er placeret 40 meter over havets overflade i et område med minimal risiko for oversvømmelse. Serverrummene er placeret i bygningens kælderetage i en betonskal, som er sikret mod vandgennemtrængning.

I serverrummene er der hævet gulv (60 cm), og der er fugtfølere på gulvet. Der er overvågning af vandstand i den lavest liggende samlebrønd.

For fugtfølere og vandstand i samlebrønd gælder, at der er opsat overvågning, så driftspersonalet bliver tilkaldt i tilfælde af, at der er alarm.

### 3.6.4 Styring af kommunikation og drift

#### 3.6.4.1 Backup

**Formålet med backup**

Formålet med A/S ScanNets backup-produkter er at sikre, at data kan genskabes nøjagtigt og rettidigt. Backup-data er placeret på en anden fysisk lokation i forhold til de data, der bliver taget backup af.

**A/S ScanNets backupprodukter**

A/S ScanNet tilbyder to backup-produkter, som benævnes som "*Backup*" og "*Online Backup*". Det valgte backup-software dækker de krav, A/S ScanNet har til en backup-løsning. Softwaren dækker de systemer, som A/S ScanNet har behov for at tage backup af, og sikres med løbende support og opdatering af softwaren.

”*Backup*”

Alle backup-data placeres på et disksystem i A/S ScanNets sekundære server-lokation. A/S ScanNet installerer og schedulerer backup-klienten. A/S ScanNet monitorerer backuppen. Backup-aftalen kan indgås, således at det enten er A/S ScanNet eller kunden, der udbedrer de fejl, der måtte opstå i forbindelse med backup af data. Backup af kundeservere følger de til enhver tid gældende kontrakter.

”*Online Backup*”

Data er placeret på et disksystem i A/S ScanNets primære lokation og bliver replikeret til A/S ScanNets sekundære lokation. Kunden installerer backup-softwaren på klienten, schedulerer og monitorerer backuppen.

**Backup-konfiguration**

For både ”*Backup*” og ”*Online Backup*” gælder det, at A/S ScanNet konfigurerer, monitorerer og vedligeholder backend-delen af backup-softwaren. Backend-delen består af den hardware, som backup-data bliver lagret på, den installerede backup software og tilhørende servere. Backend-delen monitoreres, så kritiske fejl automatisk tilgår driftspersonalet. Ikke-kritiske fejl og daglig vedligehold bliver varetaget af driftspersonalet.

”*Backup*”-klienten konfigureres og installeres af A/S ScanNet på det system, hvor der skal foretages data-backup. Driftspersonalet gennemgår dagligt de gennemførte data-backup for fejl. Hvis kunden selv varetager fejlretning, bliver kunden kontaktet pr. e-mail eller telefon. De øvrige fejl bliver håndteret af driftspersonalet hos A/S ScanNet.

”*Online Backup*”-klienten stilles til rådighed for kunden, som selv har ansvaret for installation, konfiguration og tilgængelighed af denne. Kunden har ansvaret for, at backup-klienten kan tilgå kundes PC og data, og at klienten på kundens PC kan afsende data til backup-serveren hos A/S ScanNet.

**Identifikation af backup-data**

Backup data fra ”*Backup*” bliver lagret i en entydig struktur. Dette sikrer, at det altid er muligt at genfinde og genskabe de ønskede data.

Det er kundens ansvar at sikre den struktur, som kunden ønsker for deres ”*Online Backup*”-data.

**Opbevaring af backup-data**

For ”*Backup*” gælder det, at alle data lagres på A/S ScanNets sekundære lokation. Dette er for at sikre, at backup-data aldrig befinder sig på samme lokation som de aktive data. Data bliver overført fra

den primære lokation til den sekundære via fiberforbindelse. Det er kun driftspersonale, som har logisk adgang til backup-data.

For *"Online Backup "* gælder det, at backup-data lagres på A/S ScanNets primære lokation, og at data efterfølgende replikeres til A/S ScanNets sekundære lokation. Data bliver overført fra den primære lokation til den sekundære via A/S ScanNets dedikerede fiberforbindelse. Det er kun driftspersonale og kunden, som har logisk adgang til backup-data.

A/S ScanNet har indgået aftale med en underleverandør omkring opbevaring af den eksterne kopi af backup'en på den sekundære lokation. Der henvises i øvrigt til afsnittet " Fysisk sikring og adgangssikkerhed" for en nærmere beskrivelse af de fysiske sikringsforanstaltninger.

**Restore-test**
For at sikre at der kan foretages gendannelse af data, udføres der med fastsatte mellemrum restore-test. Testene består altid af en fuld genskabelse af et system. Det vurderes, at det ikke er nødvendigt at udføre restore-tests af enkelte filer, da dette implicit er dækket af en fuld systemgendannelse. Restore-testen foretages af driftspersonalet. Resultatet af restore-testen dokumenteres.

#### 3.6.4.2 Netværks- og kommunikationssoftware

**Ændringskontrol – patch management**
Formålet med patch management er at sikre, at relevante opgraderinger, patches og fixes implementeres for at sikre, at systemerne er opdateret med disse, og at implementeringen foregår på en kontrolleret måde.

De relevante opgraderinger, patches og fixes vurderes af de af driftspersonalet, som er ansvarlig for systemerne. De relevante opdateringer udvælges og implementeres i servicevinduerne. I tilfælde af kritiske opdateringer vurderes det af medarbejderen og den tekniske direktør, om opdateringen kan vente til de planlagte opdateringer, eller om implementeringen skal foretages uden for servicevinduet.

**Ændringskontrol – timing**
Formålet med timing af patch management er at minimere nedetid og driftsforstyrrelser uden for servicevinduerne. Patching af systemer foregår i A/S ScanNets servicevinduer, hvis ikke andet er aftalt med brugerne af systemet. I tilfælde af kritiske opdateringer vurderes det af medarbejderen og den tekniske direktør, om opdateringen skal foretages uden for servicevinduet.

**Ændringskontrol – fallback**
Formålet med en fallback-plan i forbindelse med patch management er at sikre, at systemet kan bringes tilbage til normal drift, hvis en opdatering har uhensigtsmæssig virkning.

Opdateringer testes på test- eller ikke driftskritiske systemer inden implementering. Hvis dette ikke er muligt planlægges fallback eller andre alternativer for at kunne retablere normal drift, hvis en opdatering har uhensigtsmæssig virkning. Planen godkendes af de medarbejdere, som er ansvarlige for systemerne samt af den tekniske direktør inden implementeringen.

**Dokumentation af netværk**
A/S ScanNets netværkstopologi er dokumenteret i oversigtstegninger og detaljerede tegninger. Vedligeholdelse af dokumentationen sker med fastsatte intervaller, og når der indføres nye services. Dokumentationen gennemgås af den tekniske direktør og de relevante medarbejdere.

**Ændringskontrol af kritiske komponenter i netværket – test**
Formålet med test ved ændringer af kritiske komponenter i netværket er at sikre, at ændringerne fungerer som ønsket og uden uønsket påvirkning af de øvrige systemer.

Ændringer på netværkskomponenter sker ved gradvis udrulning af ændringer på mindre kritisk udstyr først, og med fallback-plan hvis ændringen har utilsigtet virkning. Hvis ændringen ikke viser utilsigtet virkning, implementeres ændringen på resten af netværkselementerne. Dette dokumenteres dog ikke.

#### 3.6.4.3 Systemsoftware

**Nyudvikling/anskaffelse af systemsoftware**
Inden nyudvikling/anskaffelse af system-software skal der foreligge en projektbeskrivelse og tilhørende forretningsvurdering. Beskrivelserne godkendes overordnet af den administrerende direktør eller den tekniske direktør, som derved bliver sponsor for projektet. Til godkendte system-softwareprojekter tilknyttes en projektleder, der rapporterer til sponsor under projektforløbet.

Prioritering af projekter

Projektleder gennemgår projektprioriteringen, når nye system-software-projekter er godkendt. System-software-projekter, som i nogen grad afviger fra projektplanen bliver revurderet og genprioriteret, og sponsor orienteres om ændringerne.

**Ændringskontrol – patch management**

Formålet med patch management er at sikre, at relevante opgraderinger, patches & fixes fra leverandøren implementeres for at sikre, at systemerne er opdateret med disse, og at implementeringen foregår på en kontrolleret måde. De relevante opgraderinger om patches og fixes vurderes af de af driftspersonalet, som er ansvarlige for systemerne. De relevante opdateringer udvælges og implementeres i servicevinduerne. I tilfælde af kritiske opdateringer vurderes det af driftsmedarbejderen og den tekniske direktør, om opdateringen kan vente til de planlagte opdateringer, eller om implementeringen skal foretages uden for servicevinduet.

**Ændringskontrol – timing**

Formålet med timing af patch management er at minimere nedetid og driftsforstyrrelser uden for servicevinduerne.

Patching af systemer foregår i A/S ScanNets servicevinduer, hvis ikke andet er aftalt med brugerne af systemet. I tilfælde af kritiske opdateringer vurderes det af driftsmedarbejderen og den tekniske direktør, om opdateringen skal foretages uden for servicevinduet.

**Ændringskontrol – fallback**

Formålet med en fallback-plan i forbindelse med patch management er at sikre, at systemet kan bringes tilbage til normal drift, hvis en opdatering har uhensigtsmæssig virkning.

Opdateringer testes på test- eller ikke driftskritiske systemer inden implementering. Hvis dette ikke er muligt, planlægges fallback eller andre alternativer for at kunne reetablere normal drift, hvis en opdatering har uhensigtsmæssig virkning. Planen godkendes af de medarbejdere, som er ansvarlige for systemerne samt af den tekniske direktør inden implementeringen.

**Dokumentation af systemprogrammel**

A/S ScanNets systemprogrammel er dokumenteret i oversigtstegninger og detaljerede dokumenter.

Vedligeholdelse af dokumentationen sker med fastsatte intervaller, og når der indføres nye services. Dokumentationen gennemgås af teknisk direktør og relevante medarbejdere.

**Ændringskontrol af kritisk systemprogrammel – test**
Formålet med test ved ændringer af kritisk systemprogrammel er at sikre, at ændringerne fungerer som ønsket og uden uønsket påvirkning af de øvrige systemer.

Ændringer på kritisk systemprogrammel sker ved udrulning på testsystemer eller ikke-kritiske systemer. Først med en fallback-plan hvis ændringen har utilsigtet virkning, og hvis ændringen ikke har utilsigtet virkning, udrulles ændringen på de kritiske systemer. Dette dokumenteres dog ikke.

#### 3.6.4.4 Overvågning

**Formål med overvågning**
Formålet med driftsovervågning af udvalgte centrale services er at minimere nedetiden og sikre den bedst mulige tilgængelighed for kunden.

**Overvågning**
Der er konfigureret overvågning af udvalgte centrale services. Overvågningen af disse services er aktiv 24 timer i døgnet på alle årets dage. Hvis en service fejler, bliver de relevante medarbejdere alarmeret. Medarbejderne påbegynder fejlretningen inden for 30 minutter. Alle alarmer registreres, og fejlretningen dokumenteres.

**Formål med produktet *"Døgnovervågning"***
Formålet med driftsovervågning af services (f.eks. ASP, PHP, HTTP, SQL, SMTP og POP3) er at minimere nedetiden og sikre den bedst mulige tilgængelighed for kunden.

**Produktet *"Døgnovervågning"***
Der konfigureres driftsovervågning af de services, som kunden ønsker overvåget. For nogle ydelser er der foruddefineret, hvilke services, der overvåges. Overvågningen af de udvalgte services er aktiv 24 timer i døgnet på alle årets dage. Døgnovervågningsaftalen kan indgås, så alarmen enten tilgår A/S ScanNet eller kunden.

Hvis en service fejler, og alarmen tilgår A/S ScanNet, bliver de relevante medarbejdere alarmeret. Medarbejderne påbegynder fejlretningen inden for 30 minutter. Alle alarmer registreres, og fejlretningen dokumenteres.

Hvis alarmer tilgår kunden, afventer A/S ScanNet kundens instrukser på, hvad der skal iværksættes for at afhjælpe eventuelle fejl.

**It-sikkerhedslogning**

Der foretages sikkerhedslogning af udvalgte platforme og systemer. De platforme og systemer, for hvilke der foretages it-sikkerhedslogningen, gennemgås med fastsatte intervaller, og når der indføres nye services. Omfanget af it-sikkerhedslogningen fastsættes af teknisk direktør, de relevante medarbejdere og godkendes af teknisk direktør.

Sikkerhedslogningen overvåges løbende. Overvågningen er konfigureret forskelligt, så overvågning af logningen er afstemt i forhold til de systemer, som overvåges.

#### 3.6.4.5 Incidenthåndtering

**Formål med incidenthåndtering**

Formålet med incident management er at sikre, at alle kundehenvendelser dokumenteres og behandles i overensstemmelse med de til enhver tid gældende kontrakter.

Alle kundehenvendelser registreres med et sagsnummer i A/S ScanNets IT Service Management System (ITSM). Henvendelserne prioriteres og tildeles de personer, som skal behandle sagen. Forløbet af sagen og løsningen dokumenteres i IT Service Management Systemet (ITSM). Der følges løbende op på sagerne for at sikre, at alle sager bliver behandlet korrekt.

### 3.6.5 Adgangskontrol

#### 3.6.5.1 Logisk sikring

**Anvendelse af passwords**

Formålet med bruger-authentication i form af passwords er at sikre, at kun autoriseret personale har adgang til systemerne.

**Krav til passwords**

Alle passwords skal som minimum opfylde best practice-kravene til kompleksitet. Passwords er personlige og skal skiftes med fastsatte intervaller. For de systemer hvor det er muligt gælder, at systemerne skal konfigureres således, at kravene til passwords er fastlagt i systemet (f.eks. Windows Group Policy). For de systemer hvor det ikke er muligt at have personlige passwords gælder, at de skal skiftes i forbindelse med fratrædelse af medarbejdere, som har haft kendskab til disse passwords.

**Ændring af standardpasswords**

Formålet med ændring af standardpasswords er at forhindre uautoriseret adgang til systemer.

For de systemer hvor der er standardpasswords gælder, at passwords skal ændres i henhold til dokumentationen, så de overholder kravene til passwords.

**Anvendelse af screensavere**
Formålet med anvendelse af screensaver er at forhindre uautoriseret adgang til systemer. Password-beskyttet screensaver skal altid aktiveres, når systemet ikke er under brugerens direkte opsyn.

**Anvendelse af åbne netværk**
Formålet med at beskytte datatransmission over åbne netværker er at forhindre uautoriseret adgang til data. Adgang til kritiske data er kun tilgængelig via udvalgte segmenter på A/S ScanNets LAN. Adgang til kritiske data/systemer via internet er begrænset til udvalgte A/S ScanNet-medarbejdere. Ved adgang via internet anvendes kryptering og brug af jumphosts.

#### 3.6.5.2 Brugeradministration

**It-sikkerhedsadministration**
A/S ScanNet har defineret formelle procedurer for administration af brugeradgange og tildeling af rettigheder dels hos kunderne og dels til egne medarbejdere. A/S ScanNet har opdelt forretningen i et ScanNet-domain, som omfatter den administrative del af forretningen, og i kundedomains, som giver adgang til kundernes systemer. Generelt tildeles adgang og rettigheder efter ”need to know”-princippet, hvilket bevirker, at der kun tildeles adgang, såfremt en medarbejder har et dokumenteret behov for adgangen.

Adgang til kundernes systemer er kundens eget ansvar. A/S ScanNet opretter adgange og tildeler rettigheder efter kundernes anvisninger og foretager som udgangspunkt ikke nogen sikkerhedsvurdering af de tildelte adgang og rettigheder på kundemiljøer.

**ScanNet-domain – A/S ScanNet-medarbejdere**
*Ikke-administrative rettigheder*
Oprettelses- og ændringsanmodninger af brugeradgang oprettes af nærmeste chef. Udvalgte drifts-medarbejdere udfører anmodningen. Hvis der anmodes om adgang til områder uden for chefens ansvarsområde, skal systemejeren via mail godkende adgangen.

*Tildeling af administrative rettigheder*
Medarbejdere i driftsafdelingen har pr. default administratorrettigheder. Derudover vil tildelingen af administrative rettigheder kunne foretages, hvis der er et specifikt arbejdsmæssigt behov derfor.

Anmodning om administrative rettigheder oprettes af nærmeste chef. Udvalgte driftsmedarbejdere udfører anmodningen. Hvis der anmodes om adgang til områder uden for chefens ansvarsområde, skal systemejeren via change request i ITSM godkende adgangen. Denne proces anvendes også, såfremt en A/S ScanNet-medarbejder tildeles administrativ adgang til kundedomain.

*Nedlæggelse af brugeradgang*
Nedlæggelsesanmodninger af brugeradgang oprettes af nærmeste chef. Udvalgte driftsmedarbejdere udfører anmodningen.

*Revurdering af brugerrettigheder*
For at sikre at brugerrettighederne er korrekte, udføres der med fastsatte mellemrum et review af alle tildelte administratorrettigheder. Reviewet udføres af udvalgte driftsmedarbejdere og godkendes af de systemansvarlige.

**Kundedomains – kundens medarbejdere**
Alle henvendelser omkring oprettelse af adgang til kundemiljøer skal ske gennem support-afdelingen, som sikrer sporbarhed, og at kundeaftalerne omkring autoriserede oprettelser sikres.

*Oprettelse af normale og udvidede rettigheder*
Oprettelses- og ændringsanmodninger af brugeradgang sker på anmodning fra kunden. Kun den, der er oprettet som den primære kontaktperson hos kunden kan anmode om oprettelse og ændringer, hvis ikke andet er aftalt. Udvalgte A/S ScanNet-medarbejdere udfører anmodningen.

*Nedlæggelse af brugeradgang*
Nedlæggelsesanmodninger af brugeradgang sker på anmodning fra kunden. Kun den, der er oprettet som den primære kontaktperson hos kunden kan anmode om nedlæggelse af brugeradgang, hvis ikke andet er aftalt. Udvalgte A/S ScanNet-medarbejdere udfører anmodningen.

*Revurdering af brugerrettigheder*
Revurdering af brugerrettigheder sker på anmodning fra kunden. Kun den, der er oprettet som den primære kontaktperson hos kunden kan anmode om revurdering af brugerrettigheder, hvis ikke andet er aftalt. Udvalgte A/S ScanNet-medarbejdere udfører anmodningen.

**It-sikkerhedsorganisation**
A/S ScanNet har placeret det udførende ansvar for it-sikkerheden hos den tekniske direktør og medarbejdere fra driftsorganisationen.

### 3.6.6 Business Continuity Management

**Formål med Business Continuity**

Formålet med Business Continuity er at sikre, at udvalgte services kan retableres i forhold til de krav, A/S ScanNet skal overholde. A/S ScanNet har ikke etableret en Business Continuity-plan på kundernes systemer og data. Reetablering af kundernes systemer og data omfatter alene en reetablering på baggrund af de gennemførte backups, som beskrevet ovenfor.

**Business Continuity-elementer**

Der er lavet aftaler med leverandører af forretningskritiske elementer i A/S ScanNets infrastruktur for at sikre vigtige elementers redundans, så redundansen hurtigt kan genetableres i forbindelse med fejl på et element. Påbegyndelsen af reetablering er beskrevet i kontrakten med leverandører.

A/S ScanNet har ligeledes et hardware-lager, der er med til at sikre en genetablering af udvalgte elementers redundans. Påbegyndelse af fejlretning tilstræbes igangsat, så snart A/S ScanNet er bekendt med fejlen.

**Business Continuity-test**

Formålet med test af Business Continuity er at sikre, at både elementer og processer fungere, hvis de skal bringes i brug. I forbindelse med gennemgangen af Business Continuity-elementer foretages en vurdering af, om der er områder, som ikke allerede er omfattet af test i anden forbindelse (f.eks. nødstrømsgenerator test). Hvis dette er tilfældet, vil en testprocedure blive udfærdiget og testen efterfølgende gennemført.

## 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 A/S ScanNets standardbetingelser for hosting. Det bevirker, at indgåede kundeaftaler, som på de leverede serviceydelser er forskellige fra standardbetingelserne ikke er omfattet af nærværende erklæring. Kundernes egne revisorer bør vurdere, om denne erklæring kan anvendes på den konkrete kundeaftale og selv afdække eventulle andre risici, der vurderes som væsentlige for aflæggelse af kundernes årsregnskaber.

**Brugeradministration**

A/S ScanNet giver adgang og tildeler rettigheder i overensstemmelse med kundernes instrukser i takt med, at disse bliver indmeldt. A/S ScanNet er ikke ansvarlig for, at disse informationer er korrekte, og

det er således kundernes eget ansvar at sikre, at de tildelte adgange og rettigheder til systemer og applikationer sker i overensstemmelse med kundernes egne forventninger til en betryggende funktionsadskillelse i de hostede systemmiljøer.

**Online backup**

Kunder, som anvender A/S ScanNets online backup-løsning er selv ansvarlige for installation, konfiguration og overvågning af backup-klienter, og at backupdata afsendes til A/S ScanNets centrale miljøer. Kundernes egne revisorer bør vurdere dette i relation til afdækning af risici for utilstrækkelig backups af kundens it-miljøer.

**Efterlevelse af relevant lovgivning**

A/S ScanNet tilrettelægger procedurer og kontroller således, at de områder, som er A/S ScanNets ansvar efterleves betryggende. A/S ScanNet 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 A/S ScanNet, 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 revisor med dels at planlægge revisionen af årsregnskabet og dels at vurdere risici for fejl i kundernes regnskaber, som muligvis påvirkes af kontroller hos A/S ScanNet.

Vores test af A/S ScanNets 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 A/S ScanNets 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 A/S ScanNet 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 01.01.2014 til 31.12.2014. Vores test af kontrollernes effektivitet er udformet til at dække et repræsentativt antal af transaktioner i løbet af perioden 01.01.2014 til 31.12.2014 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 Sikkerhed: 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.

### 4.4.1 Sikkerhedspolitik

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Ledelsen har gennem godkendt it-sikkerhedspolitik fastlagt niveauet for virksomhedens anvendelse, herunder hvorledes ledelsen ønsker it-sikkerhed implementeret og kontrolleret. It-sikkerhedspolitikken er udarbejdet med udgangspunkt i en it-risikoanalyse.** | | | |
| *4.4.1.1 It-sikkerhedspolitik* | Den eksisterende it-sikkerhedspolitik bliver løbende opdateret, såfremt der er behov for dette. Efter væsentlige opdateringer bliver politikkerne godkendt af bestyrelsen. | Deloitte har gennemgået seneste ajourførte it-sikkerhedspolitik og vurderet, om denne er betryggende. | Ingen bemærkninger. |
| *4.4.1.2 It-risikoanalyse* | Trussels- og risikovurderinger bliver løbende opdateret, såfremt der er behov for dette. Analysen afspejler ScanNets vurdering af sandsynlighed og konsekvens for en række forretningsrisici samt hvilke tiltag, der allerede er eller skal implementeres. Risikovurderingen er godkendt af ledelsen. | Deloitte har gennemgået seneste ajourførte it-risikoanalyse og vurderet, om denne er betryggende. | Ingen bemærkninger. |

### 4.4.2 Fysisk sikkerhed

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: It-faciliteterne administreres hensigtsmæssigt for at sikre, at integriteten af finansielle informationer, således som denne, håndteres af de relevante komponenter af it-infrastrukturen.** | | | |
| *4.4.2.1 Adgang til kritiske lokationer* | Adgang til co-location og A/S ScanNets primære og sekundære serverrum er begrænset til autoriseret personale. Der er kun adgang til rummene inde fra selve A/S ScanNets bygning. Adgangsdøre til rummene er sikringsdøre, og der er opsat elektroniske kortlæsere ved dørene. Alle kort, der giver adgang til co-location eller serverrum er forsynet med billede. Der skal altid anvendes kode sammen med kortet for at få adgang til co-location og serverrummene. Til co-location skal kunder desuden benytte en fingeraftrykslæser for at få adgang. Uden for normal arbejdstid er der ikke adgang til området omkring bygningen i bil uden anvendelse af adgangskort. | Deloitte har vurderet, om adgangen til kritiske lokationer er begrænset betryggende, og at evt. adgang til kritiske lokationer, som serverrummet, er godkendt. | Ingen bemærkninger. |
| *4.4.2.2 Strømsikring* | Der er i serverrummet forbundet UPS-anlæg på alle kritiske maskiner. Der er yderligere indgået kontrakt om en periodisk vedligeholdelse af UPS-anlægget. Endvidere er der etableret nødstrømsgenerator, som også regelmæssigt testes og serviceres. | Deloitte har påset, at der er opsat nødstrøm til kritiske maskiner, og at der er dokumentation for periodisk gennemgang af løsningen. | Ingen bemærkninger. |
| *4.4.2.3 Brandsikring* | Serverrum er forsynet med røg- og temperaturføler, der er koblet sammen med det centrale brandovervågningssystem.<br><br>Serverrum er yderligere forsynet med brandslukning og detektion (både røg og temperatur).<br><br>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 gennemgang af løsningen. | Ingen bemærkninger. |
| *4.4.2.4 Klimaovervågning* | Serverrummet er forsynet med køling, så maskinerne ikke bliver overophedet.<br><br>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 gennemgang af løsningen. | Ingen bemærkninger. |
| *4.4.2.5 Indretning* | Serverrummet er indrettet således, at der ikke forefindes faldstammer, vandrør mv., som vil kunne forsage skader på maskiner, der anvendes til kritiske systemer og data. Yderligere er der placeret videoovervågning i alle væsentlige lokaler, således at ophold i gangarealer detekteres. | Deloitte har gennemgået indretningen af kritiske lokationer og vurderet, om der er forhold, som udgør en risiko. | Ingen bemærkninger. |

### 4.4.3 Backup

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Data administreres hensigtsmæssigt for at skabe rimelig overbevisning for, at finansielle data forbliver nøjagtige, fuldstændige og gyldige gennem opdaterings- og arkiveringsprocessen.** | | | |
| *4.4.3.1*<br>*Strategi* | Der er udarbejdet backupbeskrivelser for hele det hostede miljø. Der tages backup af alle relevante data og alle relevante servere. | 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. |
| *4.4.3.2*<br>*Konfiguration* | Ændringer til backupkonfigurationen sker i takt med ændringer til den generelle backupbeskrivelse. Ændringer til konfigurationen udføres i et samarbejde mellem evt. systemejere og driftsafdelingen. | Deloitte har foretaget stikprøve på, at backupkonfigurationen stemmer overens med den udarbejdede backupbeskrivelse. | Ingen bemærkninger. |
| *4.4.3.3*<br>*Ekstern opbevaring* | *Backup:* Der laves backup til egen dedikerede backupservere på sekundær lokation.<br><br>*Online Backup:* Der laves backup til dedikerede backupservere i det primære datacenter, og data replikeres dagligt til dedikerede backupservere på sekundær lokation, som forefindes hos en ekstern samarbejdspartner. | Deloitte har påset dokumentation for, at den eksterne arkivering af backup bliver udført.<br><br>Vi har endvidere gennemgået seneste offentliggjorte 3402 erklæring fra den underleverandør, som er ansvarlig for den fysiske opbevaring af den eksterne backupkopi. | Ingen bemærkninger.<br><br>Vi skal dog bemærke, at ekstern opbevaring af backup sker hos en underleverandør af Housing faciliteter, hvor der på nuværende tidspunkt foreligger en 3402 erklæring omkring etablerede kontroller frem til 31. maj 2014. |
| *4.4.3.4*<br>*Test* | For at sikre, at der kan foretages gendannelse af data, udføres der med fastsatte mellemrum restoretest. Disse test består altid af en fuld genskabelse af et system. Det vurderes, at det ikke er nødvendigt at udføre restoretests af enkelte filer, da dette implicit er dækket af en fuld systemgendannelse. Restoretesten foretages af driftspersonalet. Resultatet af restoretesten dokumenteres. | Deloitte har påset, at der har været udført test af backuppen for kritiske systemer, og at reetablering af disse er blevet godkendt. | Ingen bemærkninger. |

### 4.4.4 Netværks- og kommunikationssoftware

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Ny netværkssoftware samt modifikationer til eksisterende netværkssoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.** | | | |
| *4.4.4.1*<br>*Patch management* | Relevante firmware-opdateringer skal løbende vurderes og implementeres efter behov. Dette sker i praksis ved løbende review af hele netværket. | Deloitte har foretaget en stikprøve på, at patching sker, bliver dokumenteret og godkendt. | Ingen bemærkninger. |
| *4.4.4.2*<br>*Test* | Hvis det er muligt, skal udskiftning af netværkskomponenter testes før implementering.<br><br>Mindste sikkerhedsforanstaltning er backup af konfigurationsfilerne, inden ændringer gennemføres. | Deloitte har gennemgået forhold omkring test i forbindelse med opdatering og idriftsættelse af netværkskomponenter. | Ingen bemærkninger. |
| *4.4.4.3*<br>*Fallback* | Inden ændringer foretages, skal der, om muligt, tages backup af konfigurationsfilerne til netværkskomponenter. | Deloitte har foretaget en stikprøve på, at der for udvalgte netværkskomponenter findes gemte konfigurationer. | Ingen bemærkninger. |
| *4.4.4.4*<br>*Timing* | Væsentlige ændringer til netværkskonfigurationer skal, om muligt, ske i de faste servicevinduer, således at driften ikke forstyrres unødigt. | Deloitte har foretaget en stikprøve på, at der i forbindelse med patching af netværkskomponenter er taget stilling til timing for implementeringen. | Ingen bemærkninger. |
| *4.4.4.5*<br>*Dokumentation* | Netværket dokumenteres via forskellige topologitegninger. Der skal, om muligt, tages backup af netværkskomponenternes konfigurationsfiler. | Deloitte har indhentet seneste dokumentation for netværket og verificeret ved interview, at denne stemmer overens med det faktiske setup. | Ingen bemærkninger. |

### 4.4.5 Systemsoftware

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Ny systemsoftware samt modifikationer til eksisterende software implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.** | | | |
| *4.4.5.1*<br>*Patch management* | Implementering af patches sker i forud planlagte service-vinduer. Opdatering af Windows-servere sker via WSUS, og opdatering af Linux-servere sker manuelt. | Deloitte har foretaget en stikprøve på, at der løbende sker patching af servere. | Ingen bemærkninger. |
| *4.4.5.2*<br>*Test* | Om muligt skal der gennemføres test før opdatering af produktionsmiljøet.<br><br>Opdateringerne installeres som kontrol først på en enkelt server. Først når der er relativ sikkerhed for problemfri udrulning, implementeres øvrige servere. | Deloitte har gennemgået forhold omkring test i forbindelse med opdatering og idriftsættelse af ændringer til servere. | Ingen bemærkninger. |
| *4.4.5.3*<br>*Fallback* | Om muligt afinstalleres patchen – alternativt reetableres ud fra backup. | Deloitte har foretaget en stikprøve på, at der i forbindelse med patching af systemsoftware er taget stilling til fallback inden implementering i produktion. | Ingen bemærkninger. |
| *4.4.5.4*<br>*Timing* | Nye opdateringer installeres normalt inden for de forud definerede servicevinduer. | Deloitte har foretaget en stikprøve på, at der i forbindelse med patching af systemsoftware er taget stilling til timing for implementeringen i produktion. | Ingen bemærkninger. |
| *4.4.5.5*<br>*Dokumentation* | Der er etableret omfattende systemdokumentation af både interne servere og hele det hostede miljø. | Deloitte har vurderet, om dokumentationen for anvendte systemer er betryggende. | Ingen bemærkninger. |

### 4.4.6 Overvågning

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Der udføres løbende overvågning af systemer og services, og der følges op på eventuelle konstaterede fejl.** | | | |
| *4.4.6.1 Overvågning* | Der er etableret automatisk overvågning af alle relevante servere og services, og der gives alarmer til driftspersonalet ved fejl. | Deloitte har gennemgået stikprøve over alarmer fra driftsmiljøet og kontrolleret, at der for disse er lavet dokumenteret opfølgning. | Ingen bemærkninger. |

### 4.4.7 Incidenthåndtering

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Alle henvendelser fra kunder besvares og behandles rettidigt i forhold til de indgåede aftaler.** | | | |
| *4.4.7.1 Incidenthåndtering* | Alle kundehenvendelser registreres som en sag i A/S ScanNets service management system. Henvendelserne prioriteres og tildeles de personer, som skal behandle sagen. Forløbet af sagen og løsningen dokumenteres i service management systemet.<br><br>Der følges løbende op på sagerne for at sikre, at alle sager bliver behandlet korrekt. | Deloitte har gennemgået stikprøve af indkomne service requests og observeret, at der løbende følges op, og at dette dokumenteres. | Ingen bemærkninger. |

### 4.4.8 Logisk sikring

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Systemsikkerhed er hensigtsmæssigt implementeret og administreres 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 finansiel information.** | | | |
| *4.4.8.1 Anvendelse af passwords* | 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 systemer og verificeret, at relevante brugere anvender disse. | Ingen bemærkninger. |
| *4.4.8.2 Anvendelse af brugerprofiler* | Brugere er oprettet i Windows AD og på individuelle Linux-servere, og alle anvender individuelle brugerprofiler. | Deloitte har gennemgået anvendelsen af brugerprofiler på alle relevante systemer og platforme og verificeret, at disse er personlige og identificerbare. | Ingen bemærkninger. |
| *4.4.8.3 Ændring af standardpasswords* | Der er procedure til sikring af, at standardbrugeres password skiftes i forbindelse med implementering af centrale applikationer og hardware komponenter. | Deloitte har gennemgået kritiske systemer og platforme for at verificere, at kendte standardbrugeres default password er ændret. | Ingen bemærkninger. |
| *4.4.8.4 Anvendelse af åbne netværk* | Der anvendes kun lukkede forbindelser til ScanNets sekundære lokationer, og kunder opnår adgang via Citrix og RDP. | Deloitte har gennemgået dokumentation for netværket og vurderet dette passende. | Ingen bemærkninger. |

### 4.4.9 Brugeradministration

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Adgangstildeling til systemer og programmer administreres hensigtsmæssigt for at sikre mod uautoriserede og utilsigtede handlinger, som kan resultere i ufuldstændig, unøjagtig eller ugyldig behandling eller registrering af finansiel information.** | | | |
| *4.4.9.1 Oprettelser og ændringer* | Brugere oprettes kun på baggrund af skriftlige henvendelser (mails) modtaget i fælles mailboks til brugeradministration. Brugerne tildeles rettigheder i forhold til ønsket i mail. | Deloitte har foretaget en stikprøve på oprettede brugere og vurderet, om der er et gyldigt grundlag for tildelte adgange og rettigheder. | Ingen bemærkninger. |
| *4.4.9.2 Udvidede rettigheder* | Interne medarbejderes adgang til systemer følger samme processer som for øvrige brugere. Kun et begrænset antal nøglemedarbejdere er tildelt udvidede rettigheder på systemerne. Der laves regelmæssig gennemgang af brugere. | Deloitte har gennemgået brugere med udvidede rettigheder på ScanNets centrale infrastruktur og verificeret, at disse er godkendt til de tildelte rettigheder. | Ingen bemærkninger. |
| *4.4.9.3 Nedlæggelser* | Nedlæggelse af brugere sker på baggrund af skriftlig henvendelse (mail) fra medarbejderens nærmeste chef. | Deloitte har foretaget en stikprøve på nedlagte brugere.<br><br>Vi har endvidere verificeret for udvalgte medarbejdere, som er fratrådt eller opsagt, at deres adgang er blevet inddraget. | Ingen bemærkninger. |
| *4.4.9.4 Periodisk review af rettigheder* | Der udføres regelmæssigt review af brugere med udvidede rettigheder på ScanNets systemer, og dette godkendes af de systemansvarlige. | Deloitte har gennemgået dokumentation for seneste review af brugerrettigheder. | Ingen bemærkninger. |
| *4.4.9.5 It-sikkerhedslogning* | Der er opsat logning af sikkerhedsmæssige hændelser på ScanNets infrastruktur samt logning af adgang til kundedata. Der laves daglig gennemgang af logs. | Deloitte har verificeret, om logning af kritiske systemer og netværk følger godkendte logningskrav, og om der udføres review af logs. | Ingen bemærkninger. |
| *4.4.9.6 It-sikkerhedsorganisationen* | 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. |

### 4.4.10 Business Continuity Management

| Kontrolaktivitet | Etableret kontrol hos A/S ScanNet | Testplan | Testresultat |
|---|---|---|---|
| **Kontrolmål: Retningslinjer for genetablering af driften er udarbejdet og godkendt af ledelsen.** | | | |
| *4.4.10.1 Retningslinjer* | ScanNet tilbyder ikke beredskabsstyring i relation til kundernes systemmiljøet ud over eventuelt aftalt backup.<br><br>I relation til genetablering af datacenterets infrastruktur er der etableret et eget hardware-lager, ligesom der er indgået aftaler med centrale leverandører om support på væsentligt udstyr. | Deloitte har gennemgået A/S ScanNets etablerede foranstaltninger for videreførelse af datacenterets infrastruktur. | Ingen bemærkninger. |