B4Restore A/S

ISAE 3000 DK erklæring om generelle IT-kontroller relateret til B4Restore A/S' Hybrid Storage Solution og Hybrid Backup Solution

Statsautoriseret Revisionsvirksomhed
Annebergvej 10 – Tel: 35 36 33 56
9000 Aalborg – www.verifica.dk
CVR nr 33 68 40 96

Indholdsfortegnelse

Beskrivelse af generelle IT-kontroller i tilknytning til drift, overvågning, vedligeholdelse, support m.v. af B4Restore A/S' Hybrid Storage Solution og Hybrid Backup Solution.

B4Restore A/S (herefter B4Restore) stiller gennem drift, overvågning, support og vedligeholdelse Hybrid Storage Solution og Hybrid Backup Solution til rådighed for sine kunder placeret hos B4Restore eller hos kunden selv, hvilket denne beskrivelse med tilhørende erklæring vedrører.

B4Restores arbejde i relation til de generelle IT-kontroller, er tilrettelagt med udgangspunkt i risikovurdering og ISO27001:2013 certificerede informationssikkerhedsledelsessystem samt aftale mellem B4Restore og kunden, som beskrevet i driftskontrakt med tilhørende bilag.

Beskrivelsen og erklæringen dækker perioden 1. januar – 31. december 2015 og er beregnet for B4Restore, B4Restores Hybrid Storage Solution og Hybrid Backup Solution kunder samt deres revisorer.

Beskrivelsen, udtalelsen og erklæringen dækker vores Storage og Backup ydelser leveret til kunderne på deres egne dedikerede storage og backup samt -miljøer eller på B4Restores Hybrid Storage Solution og Hybrid Backup Solution placeret i Viby og Skanderborg.

B4Restore varetager overordnet set følgende IT-opgaver for sine Storage og Backup kunder:

- Sikkerhedskopiering af den enkelte kundes IT-løsninger i IBM Spectrum Protect (tidligere TSM) baseret på Hybrid eller dedikerede storage og backup-ydelser samt -miljøer. Sikkerhedskopiering af den enkelte kundes IT-miljøer foregår fra IT-datacenter i Viby, Skanderborg eller hos kunden selv. Backup-udstyret er enten ejet af B4Restore eller af kunden selv.
- Overvågning af sikkerhedskopiering.
- Support af kundernes Spectrum Protect-brugere. Herunder diverse fejlretning.

B4Restore er ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med det sigte at overholde de i driftskontrakten stillede krav.

Denne erklæring er udarbejdet efter helhedsmetoden og omfatter således både kontrolmål og tilknyttede kontroller hos B4Restore og hos vores underleverandører. B4Restore har regelmæssige møder med centrale underleverandører og indhenter en årlig revisionserklæring om udvalgte kontroller hos disse, hvor det er relevant.

Storage- og Backup miljøer placeret hos kunden er ikke omfattet af denne erklæring.

Risikostyring

B4Restore styrer egne IT-miljøer, herunder Storage og Backup-miljøerne, med udgangspunkt i en risikostyringsproces. Risikostyringen omfatter følgende:

- Identifikation af potentielle risici, der kan få indflydelse på IT-miljøerne både ud fra en teknisk og forretningsmæssig synsvinkel
- Vurdering af de identificerede potentielle risici, væsentlighed, sandsynlighed og konsekvenser på IT-miljøerne
- At tiltag til reduktion af sandsynligheden for, at risici indtræder, implementeres på en kost-effektiv måde.

Risikovurderingen foretages en gang om året, samt ved større organisatoriske og/eller tekniske ændringer. Dette skal være med til at sikre, at B4Restore lever op til høj standard, risikovurdering af samarbejdspartnere og review af Service Level Agreements, med særlig fokus på at sikre, at IT-miljøerne understøtter en høj tilgængelighed, fortrolighed og integritet af Storage og Backup-miljøerne.

Baseret på risikovurderingen er der udarbejdet og implementeret en informationssikkerhedspolitik med tilhørende informationssikkerhedshåndbog.

Risici klassificeres og dokumenteres.

Der gennemføres løbende accept eller iværksættelse af løsningstiltag af risici. Disse forhold rapporteres løbende til direktionen. Bestyrelsen modtager en årlig redegørelse om risikostyringen og informationssikkerhedsarbejdet.

Informationssikkerhedsarbejdet

B4Restore har valgt at organisere informationssikkerheden efter ISO/IEC 27002:2013 (herefter ISO27002) og med udgangspunkt i denne standard valgt at implementere relevante sikringsforanstaltninger for følgende områder:

5. Informationssikkerhedspolitikker
6. Organisering af informationssikkerhed
7. Personalesikkerhed
8. Styring af aktiver
9. Adgangsstyring
11. Fysisk sikring og miljømæssig sikring
12. Driftssikkerhed
13. Kommunikationssikkerhed
14. Anskaffelse, udvikling og vedligeholdelse af informationssystemer
15. Leverandørforhold
16. Styring af informationssikkerhedshændelser
17. Beredskabsstyring
18. Overensstemmelse

Områderne er udvalgt med udgangspunkt i de opgaver, B4Restore har ansvaret for og varetager på vegne af den enkelte kunde, og som er beskrevet i driftskontrakten med tilhørende bilag, samt i informationssikkerhedspolitikken.

De implementerede foranstaltninger hos B4Restore fremgår af afsnittet "Styringsmål og implementerede foranstaltninger fra ISO/IEC 27002:2013" på side 7-10 til denne beskrivelse.

En mere detaljeret beskrivelse af implementerede foranstaltninger fremgår af B4Restores Informationssikkerhedshåndbog version 2.4, samt i afsnittet om beskrivelse af vores kontrolmål og tilknyttede kontroller samt revisors beskrivelse af test af kontroller til denne erklæring.

B4Restore har i 2015 fortsat arbejdet med at få formaliseret informationssikkerhedsarbejdet. Dette har blandt andet medført at få defineret og beskrevet en række essentielle processer og forretningsgange efter ISO27001 og/eller ITIL. Dette arbejde er synliggjort ved, at alle medarbejdere løbende i 2015 er blevet informeret om arbejdet med ISO27001 og ITIL. B4Restore fik den 8. juli 2015 ISO/IES 27001:2013 certifikat for informationsledelsessystemet i relation til Managed Service for de i beskrivelsen omtalte ydelser. B4Restore fortsætter arbejdet med kontinuerlige forbedringer i informationssikkerhedsledelsessystemet og –arbejdet.

Baseret på risikovurderingen har B4Restore taget stilling til:

- Kontrolformål, der er relevante for styring af sikkerheden
- Risici, der truer opnåelse af kontrolformål
- Kontroller, der kan imødegå risiciene.

Kontrolformål og kontroller, der imødegår risiciene, er udvalgt fra ISO 27002 og tilpasset i fornødent omfang. Tilpasningen har primært været en præcisering af kontrollerne, der i standarden præsenteres som retningslinjer og ikke egentlige kontroller, hvor effektiviteten kan vurderes. Beskrivelse af kontrolformål fremgår af afsnittet revisors resultater af test af kontroller på side 16-28. Der anvendes samme nummerering som i ISO 27002 for de enkelte kontroller.

Udvælgelse af kontrolformål og tilhørende kontroller til imødegåelse af risici, er sket med udgangspunkt i anbefalinger fra FSR Informatikudvalg og vores revisor.

Afsnittet "Revisors beskrivelse af test af kontroller" på side 16-33 er udarbejdet til brug for vores kunder og deres revisorer, som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den enkelte kunde selv har anvendt ved vurdering af risiciene ved backup-løsningen.

Væsentlige ændringer i IT-miljøerne

B4Restore iværksatte i 2011 et projekt med henblik på at forbedre og formalisere processer og forretningsgange. Dette arbejde har blandt andet resulteret i udarbejdelsen af informationssikkerhedshåndbogen samt i en række procedurebeskrivelser. Den 8. Juli opnåede B4Restore som en af de få leverandører af Storage og Backup ydelser i Danmark ISO27001:2013 certifikat af vores Informationssikkerhedsledelsessystem. Arbejdet med løbende forbedringer af processer og kontroller fortsætter i henhold til ISO27001.

B4Restore har i 2015 udskiftet UPS-anlæg placeret i Datacenter 1&2. Endvidere er der implementeret et elektronisk gæsteregistreringssystem, der dækker såvel kontorfaciliteter som Datacenter 1, 2 og 4.

Derudover har der ikke været væsentlige ændringer i relation til ydelser udover almindelig opdatering og vedligeholdelse.

Komplementerende kontroller hos den enkelte kunde

Den enkelte kunde er selv ansvarlig for datatransmission mellem B4Restore og de enkelte Spectrum Protect klienter hos kunden. Det er således den enkelte kundens ansvar at sikre kontrollerne i forbindelse hermed.

Al brugeradministration, herunder tildeling af rettigheder samt beskyttelse af tilgang via servere og udstyr placeret på kundernes lokationer, er kundernes eget ansvar. Dette gælder også Spectrum Protect-Backup klienter. Kunderne skal således kontrollere alt omkring brugeradministrationen.

Anskaffelse, udvikling og implementering af systemer på Spectrum Protect-Backup klienterne hos kunderne er kundernes eget ansvar. Kontrollerne omkring systemudvikling, anskaffelse og ændringshåndtering er ligeledes kundernes ansvar.

Storage og Backup udstyr placeret andre steder end hos B4Restore backupcenter i Skanderborg eller Viby er kunderne selv ansvarlige for den fysiske og miljømæssige sikkerhed.

Kundespecifikke og/eller aftalebestemte service eller krav på dedikerede og Hybride løsninger.

B4Restores Spectrum Protect løsning understøtter IBMs krypteringsfacilitet i et Spectrum Protect-miljø. Kunderne er selv ansvarlig for opsætning af kryptering på de enkelte Spectrum Protect klienter.

Kontroller omkring nødplaner og beredskabsplaner af kundernes backup-ydelser, herunder Spectrum Protect-Backup klienter og tilhørende server samt restore og regelmæssige test af sikkerhedskopier er kundernes ansvar.

Den enkelte kunde skal som registeransvarlig indgå en kontrakt med B4Restore som registerfører, der skal sikre, at B4Restore alene handler efter instruks fra den enkelte kunde, og at B4Restore træffer alle nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger til behandling af persondata samt forretningskritiske informationer.

Styringsmål og implementerede foranstaltninger fra ISO/IEC 27002:2013

De kontroller, der er markeret med kursiv indgår i oversigt over kontrolmål og tilknyttede kontroller på side 16-33. Den uafhængige revisor har testet disse kontroller.

5 Informationssikkerhedspolitikker
5.1 Retningslinjer for styring af informationssikkerhed
5.1.1 Politikker for informationssikkerhed
5.1.2 Gennemgang af politikker for informationssikkerhed

6 Organisering af informationssikkerhed
6.1 Intern organisering
6.1.1 Roller og ansvarsområder for informationssikkerhed
6.1.2 Funktionsadskillelse
6.1.3 Kontakt med myndigheder
6.1.5 Informationssikkerhed ved projektstyring
6.2 Mobilt udstyr og fjernarbejdspladser
6.2.1 Politik for mobilt udstyr

7 Medarbejdersikkerhed
7.1 Før ansættelse
7.1.1 Screening
7.1.2 Ansættelsesvilkår og -betingelser
7.2 Under ansættelsen
7.2.1 Ledelsesansvar
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed
7.2.3 Sanktioner
7.3 Ansættelsesforholdets ophør eller ændring
7.3.1 Ansættelsesforholdets ophør eller ændring

8 Styring af aktiver
8.1 Ansvar for aktiver
8.1.1 Fortegnelse over aktiver
8.1.2 Ejerskab af aktiver
8.1.3 Accepteret brug af aktiver
8.1.4 Tilbagelevering af aktiver
8.2 Klassifikation af information
8.2.1 Klassifikation af information
8.2.2 Mærkning af information
8.2.3 Håndtering af aktiver
8.3 Mediehåndtering
8.3.1 Styring af bærbare medier
8.3.2 Bortskaffelse af medier
8.3.3 Fysiske medier under transport

9 Adgangsstyring
9.1 Forretningsmæssige krav til adgangsstyring
9.1.1 Politik for adgangsstyring

16.1.5 Håndtering af informations-sikkerhedsbrud
16.1.6 Erfaring fra informationssikkerhedsbrud
16.1.7 Indsamling af beviser

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
17.1 Informationssikkerhedskontinuitet
17.1.1 Planlægning af informationssikkerhedskontinuitet
17.1.2 Implementering af informationssikkerhedskontinuitet
17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten
17.2 Redundans
17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter

18 Overensstemmelse
18.1 Overensstemmelse med lov- og kontraktkrav
18.1.1 Identifikation af gældende lovgivning og kontraktkrav
18.1.2 Immaterielle rettigheder
18.1.3 Beskyttelse af registreringer
18.1.4 Privatlivets fred og beskyttelse af personoplysninger
18.2 Gennemgang af informationssikkerhed
18.2.1 Uafhængig gennemgang af informationssikkerhed
18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder
18.2.3 Undersøgelse af teknisk overensstemmelse

Egne kontroller

EK 1 Dispensationer fra ISMS

Udtalelse fra ledelsen vedrørende generelle IT-kontroller for Hybrid Storage Solution og Hybrid Backup Solution hos B4Restore A/S

Beskrivelsen på side 3-10 er udarbejdet til brug for B4Restores kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller som kunderne selv har anvendt, ved vurdering af risiciene.

B4Restore bekræfter, at:

a) Den medfølgende beskrivelse, side 3-10 giver en retvisende beskrivelse af de generelle IT-kontroller med relevans for de generelle IT kontroller for B4Restores Hybrid Storage Solution og Hybrid Backup Solution, der anvendes af B4Restores kunder i hele perioden 1. januar - 31. december 2015.

b) Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

i. redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:

- de typer af ydelser, der er leveret, når det er relevant
- de processer i både IT- og manuelle systemer, der er anvendt til styring af de generelle IT-kontroller
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementeret hos kunderne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle IT-kontroller

ii. indeholder relevante oplysninger om ændringer i de generelle IT-kontroller foretaget i perioden fra 1. januar - 31. december 2015

iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og

derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold

iv. medtager kontrolmål og tilknyttede kontroller hos vores underleverandører og vores kontrolaktiviteter med disse underleverandører

c) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i perioden 1. januar - 31. december 2015.

d) Kriterierne for denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

ii. de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden 1. januar - 31. december 2015.

Med baggrund i ovenstående vurderer B4Restore A/S, at vi i alle væsentlige forhold i overensstemmelse med driftsaftale og IT Sikkerhedspolitikken med tilhørende informationssikkerhedshåndbog har etableret effektive kontroller og en betryggende system-, drift- og datasikkerhed for Hybrid Storage Solution og Hybrid Backup Solution placeret på Åhave Parkvej 31, 8260 Viby J samt Skanderborg i perioden 1. januar – 31. december 2015.

Aarhus, den 2. marts 2016

B4Restore A/S

Henrik Lind
Administrerende direktør

Bent Andersen
Strategi direktør

Uafhængig revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet vedrørende generelle IT-kontroller for Hybrid Storage Solution og Hybrid Backup Solution hos B4Restore A/S

Til ledelsen hos B4Restore A/S, deres kunder og kundernes revisorer

Omfang

Vi har fået som opgave at afgive erklæring om B4Restore A/S' beskrivelse på side 3-10 af generelle IT-kontroller for Hybrid Storage Solution og Hybrid Backup Solution for perioden 1. januar til 31. december 2015 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

B4Restore A/S ansvar

B4Restore A/S er ansvarlig for udarbejdelsen af beskrivelsen på side 3-10 og tilhørende udtalelse på side 11-12, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Firmaet anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om B4Restore A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3000 DK, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte

handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet på side 3-10.

Ledelsens beskrivelse af generelle IT-kontroller omfatter kontrolmål og tilknyttede kontroller hos serviceunderleverandører. Denne erklæring er udarbejdet efter helhedsmetoden og vores test af kontroller omfatter kontroller hos serviceunderleverandører.

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

B4Restore A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet på side 11-12. Det er vores opfattelse,

a) at beskrivelsen af de generelle IT-kontroller med relevans for B4Restores kunder, således som det var udformet og implementeret i perioden 1. januar - 31. december 2015, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden 1. januar til 31. december 2015, og

c) at 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 perioden 1. januar til 31. december 2015.

Som tillæg til ovenstående skal vi i henhold til systemrevisionsbekendtgørelsen § 7 stk. 3, og baseret på a, b og c erklære, at de generelle IT-kontroller med relevans for B4Restores tilsluttede finansielle virksomheders system-, data- og driftssikkerhed efter vores opfattelse er betryggende og har fungeret betryggende i perioden 1. januar – 31. december 2015.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår på side 16-33.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 16-33 er udelukkende tiltænkt B4Restore kunder af Hybrid Storage Solution og Hybrid Backup Solution, samt deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber eller fejl i anden relevant rapportering.

Aalborg, den 2. marts 2016

Venlig hilsen

Verifica

Statsautoriseret Revisionsvirksomhed

Hans Henrik Berthing

Statsaut. revisor, CISA, CRISC, CGEIT

Tests af kontroller udført af den uafhængige revisor

Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med International Auditing and Assurance Standards Board's International Standard on Assurance Engagements (ISAE) 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Arbejdet er udført og erklæringen er udformet efter vejledning fra ISAE 3402 og efterlever alle krav, der er i ISAE3402. Erklæring med sikkerhed om kontroller hos en serviceleverandør.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen og som fremgår af side 17 - 33. Erklæringen er afgivet efter helhedsmetoden, således indgår relevante kontroller hos serviceunderleverandører.

Evt. andre kontrolmål, tilknyttede kontroller og kontroller hos den enkelte kunde er ikke omfattet af vores gennemgang / revision.

Vores test af funktionaliteten har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden fra 1. januar – 31. december 2015.

Udførte test

De udførte tests i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er implementeret og har fungeret i perioden 1. januar – 31. december 2015. Dette omfatter bl.a. vurdering af patchningsniveau, tilladte services, segmentering, passwordkompleksitet m.v. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af passende personale hos B4Restore. Forespørgsler har omfattet om hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentag den relevante kontrol. Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Resultater af test af kontroller

I nedenstående oversigt opsummeres tests udført af Verifica som grundlag for at vurdere det interne kontrolmiljø hos B4Restore A/S.

1. Sikkerhedspolitik (ISO27002 Afsnit 5)			
***Kontrolmål**: Der er etableret en informationssikkerhedspolitik som sikrer at:* • *der er udarbejdet en ajourført og af ledelsen godkendt informationssikkerhedspolitik* • *der er udarbejdet en informationssikkerhedshåndbog* • *ledelsen er involveret i informationssikkerhedsarbejdet*			
Ref	**Kontrol**	**Revisors test af kontroller**	**Bemærkninger**
5.1.1	Ledelsen godkender en skriftlig informations-sikkerhedspolitik, som offentliggøres og kommuni-keres til virksomhedens med-arbejdere og relevante eksterne parter.	Vi har observeret, at bestyrelsen har godkendt informations-sikkerhedspolitikken. Vi har forespurgt udvalgte medarbejdere. om informations-sikkerhedspolitik. Vi har inspiceret, at udvalgte medarbejdere har læst sikkerhedspolitikken.	Ingen væsentlige bemærkninger
5.1.2	Ledelsen har udviklet og udarbejdet en sikkerhedshåndbog, der indeholder relevante sikringsforanstaltninger fra ISO 27002, som nævnt i ovennævnte beskrivelse.	Vi har inspiceret, at sikkerheds-håndbogen indeholder relevante områder fra ISO27002, som nævnt i ovenstående beskrivelse.	Ingen væsentlige bemærkninger
5.1.2	Informationssikkerheds-politikken revurderes med planlagte intervaller eller ved væsentlige ændringer for at sikre dens fortsatte relevans og effektivitet.	Vi har observeret, at informationssikkerhedspolitikken er opdateret.	Ingen væsentlige bemærkninger

2. Organisering af informationssikkerhed (ISO27002 Afsnit 6)

***Kontrolmål**: Der er etableret betryggende kontroller som sikrer:*

- *at styre informationssikkerhed i virksomheden*
- *at sikkerhedsmæssige krav afspejles i kontraktlige bindinger og forventninger med kunderne*
- *at der er udfærdiget skriftlige samarbejdsaftaler med relevante leverandører*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
6.1.1	Ledelsen understøtter aktivt sikkerhed i virksomheden ved at vise retning, engagement, præcis opgavefordeling og anerkendelse af ansvar for informationssikkerhed.	Vi har forespurgt ledelsen, hvordan de aktivt understøtter sikkerheden, herunder ved at vise retning, engagement, fordele opgave og tage ansvar for informationssikkerhed. Vi har observeret information udsendt om informations-sikkerhed.	Ingen væsentlige bemærkninger
6.1.1	Sikkerhedsopgaver og -ansvar er fastlagt i overensstemmelse med virksomhedens retningslinjer og informa-tionssikkerhedspolitik.	Vi har for udvalgte medarbejdere involveret i opgaver relateret til B4Restores Backup ydelser forespurgt om deres opgaver og ansvar.	Ingen væsentlige bemærkninger
6.1.1	Informationssikkerhedsaktivit eter koordineres på tværs i virksomheden.	Vi har forespurgt forskellige medarbejdere på tværs i virksomheden om, hvordan informationssikkerhedsaktivitet er koordineres.	Ingen væsentlige be-mærkninger
6.1.1	Ansvaret for alle informationssikkerhedsaktivit eter, herunder beskyttelse af virksomhedens informations-aktiver og udførelsen af særlige sikkerhedsprocedurer er defineret og placeret.	Vi har forespurgt forskellige medarbejdere om, hvordan ansvaret for informations-sikkerhedsaktiviteter defineres og placeres.	Ingen væsentlige bemærkninger
6.1.2	Funktionsadskillelse er en organisatorisk sikringsforanstaltning til minimering af risikoen for fejlagtig eller bevidst misbrug af systemer. Der etableres funktionsadskillelse for at minimere risikoen for uautoriserede eller utilsigtede ændringer eller misbrug af virksomhedens informationsaktiver.	Vi har inspiceret organisationsdiagram med beskrivelse af ansvarsområder. Vi har forespurgt udvalgte medarbejdere om deres arbejdsopgaver i relation til B4Restores Backup ydelser.	Ingen væsentlige bemærkninger

2. Organisering af informationssikkerhed (ISO27002 Afsnit 6)

***Kontrolmål**: Der er etableret betryggende kontroller som sikrer:*

- *at styre informationssikkerhed i virksomheden*
- *at sikkerhedsmæssige krav afspejles i kontraktlige bindinger og forventninger med kunderne*
- *at der er udfærdiget skriftlige samarbejdsaftaler med relevante leverandører*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
6.1.2	Funktionsadskillelse er en organisatorisk sikringsforanstaltning til minimering af risikoen for fejlagtig eller bevidst misbrug af systemer. Der etableres funktionsadskillelse for at minimere risikoen for uautoriserede eller utilsigtede ændringer eller misbrug af virksomhedens informations-aktiver. B4Restore har en størrelse, der ikke kan sikre en komplet funktions-adskillelse af alle kritiske funktioner.	Vi har inspiceret organisationsdiagram med beskrivelse af ansvarsområder. Vi har forespurgt udvalgte medarbejdere om deres arbejdsopgaver i relation til B4Restores Backup ydelser.	Ingen væsentlige bemærkninger
6.1.3	B4Restore har en procedure i tilfælde af brud på person-datasikkerheden. Anmeldelse sker til tilsynsmyndigheden. Bruddets art, karakteren af bruddet på persondata-sikkerheden, konsekvenser og afhjælpende foranstaltninger skal beskrives. Ved brud vil relevant bevismateriale blive indsamlet	Vi har forespurgt udvalgte medarbejdere om deres hvorledes kontakt til myndigheder foretages.	Ingen væsentlige bemærkninger
6.2.1	Mobiltelefoner beskyttes alene med adgangskode. IT-udstyr registreres i B4Restore A/S' CMDB og de beskrevne processer for Configuration Management og Change Management følges. CMDB er at opfatte som inventarlisten for it-udstyr.	Vi har forespurgt udvalgte medarbejdere om, hvordan sikkerheden er for mobilt udstyr.	Ingen væsentlige bemærkninger

3. Personalesikkerhed (ISO27002 Afsnit 7)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af, at alle medarbejdere er opmærksomme på deres særlige ansvar i forhold til virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, svindel og misbrug af informationsaktiver.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
7.1.1	Før ansættelse af medarbejdere foretages der følgende baggrundscheck: • En personlig reference • Ansøgerens CV • Uddannelser og faglige kvalifikationer • Identitetskontrol. Hvor det er relevant skal kandidaten vise ren straffeattest.	Vi har for udvalgte medarbejdere inspiceret baggrundscheck og indhentelse af straffeattest.	Ingen væsentlige bemærkninger
7.1.2	Som en del af aftaleindgåelsen med såvel faste som midlertidige medarbejdere underskrives en aftale/kontrakt, der beskriver virksomhedens og medarbejderens ansvar og forpligtelser vedrørende informationssikkerhed.	Vi har drøftet forretningsgangen for afgivelse af tavshedserklæring med den HR ansvarlige. Vi har inspiceret, at der i medarbejdernes ansættelsesaftaler fremgår, at medarbejdere har tavshedspligt.	Ingen væsentlige bemærkninger
7.2.1	Ledelsen sikrer sig, at alle medarbejdere implementerer og fastholder informations-sikkerhed i overensstemmelse med virksomhedens sikkerhedspolitik, retningslinjer og procedurer.	Vi har drøftet hvorledes Direktionen og den sikkerheds-ansvarlige sikrer sig, at medarbejderne overholder sikkerhedspolitikken.	Ingen væsentlige bemærkninger
7.2.2	Alle virksomhedens medarbejdere gøres løbende opmærksomme på og uddannes i virksomhedens sikkerhedspolitik og -procedurer.	Vi har for udvalgte medarbejdere involveret i opgaver relateret til B4Restores Backup ydelser fore-spurgt om deres opmærksomhed og uddannelse om sikkerheds-politik.	Ingen væsentlige bemærkninger
7.2.3	Ledelsen skal sikre, at sanktioner for brud på Selskabets politikker, regler eller retningslinier håndhæves konsekvent og i overensstemmelse med gældende lovgivning.	Vi har forespurgt ledelse om processen for sanktioner. Vi har forespurgt ledelsen om, der er i 2015 har været behov for at sanktionere medarbejdere for brud på B4Restore politikker.	Ingen væsentlige bemærkninger
7.3.1	I forbindelse med ansættel-sesforholdets ophør sikres det, at fortrolighed opretholdes, aktiver returneres og rettigheder fjernes.	Vi har forespurgt ledelse om processen for ansættelses-forholdets ophør. Vi har inspiceret kontroller vor medarbejder fratrådt i 2015.	Ingen væsentlige bemærkninger

4. Styring af aktiver (ISO27002 Afsnit 8)			
***Kontrolmål**: Der er etableret betryggende kontroller for at opnå og opretholde passende beskyttelse af virksomhedens aktiver.*			
Ref	**Kontrol**	**Revisors test af kontroller**	**Bemærkninger**
8.1.1	Alle kritiske informationsaktiver identificeres, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver.	Vi har inspiceret virksomhedens asset management system. Vi har for et udvalg af aktiver inspiceret registreringer for de udvalgte aktiver.	Ingen væsentlige bemærkninger
8.3.1	Hemmelige og fortrolige informationer skal sikres med adgangskode, når de opbevares eller transporteres på bærbare medier, der er afgrænset til pc'er og mobiltelefon.	Vi har forespurgt udvalgte medarbejdere om processen for opbevaring og transport af bærbare medier .	Ingen væsentlige bemærkninger
8.3.2	Alle datamedier, skal sikkerhedsslettes eller fysisk destrueres inden bortskaffelse, hvis de indeholder informationer, der er klassificeret hemmelige og/eller fortrolig.	Vi har forespurgt udvalgte medarbejdere om processen for sletning/ destruktion af bærbare medier .	Ingen væsentlige bemærkninger
8.3.3	Fysiske datamedier beskyttes mod tab, forvanskning og misbrug under transport.	Vi har forespurgt om proceduren for transport af fysiske medier.	Ingen væsentlige bemærkninger
8.3.3	Transport af fysiske medier af eksterne foretages af autoriseret transportør for de pågældende medier. Transportøren skal være forsikret for de aktuelle fysiske medier.	Vi har forespurgt udvalgte medarbejdere om processen for transport af bærbare medier	Ingen væsentlige bemærkninger

5. Adgangsstyring (ISO27002 Afsnit 9)

Kontrolmål: *Der er etableret betryggende kontroller til sikring af, at adgang til systemer, data og netværk styres i overensstemmelse med forretningsmæssige og lovgivningsbetingede krav.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
9.1.1	Der foreligger retningslinjer for virksomhedens adgangsstyring.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af adgangsrettigheder sker.	Ingen væsentlige bemærkninger
9.2.1	Der er en forretningsgang for tildeling og afbrydelse af brugeradgang.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af adgangsrettigheder sker.	Ingen væsentlige bemærkninger
9.2.2	Tildeling af adgangskoder styres ved en formaliseret proces.	Vi har inspiceret, hvorledes adgangskoder tildeles.	Ingen væsentlige bemærkninger
9.2.3	Tildeling og anvendelse af udvidede adgangsrettigheder begrænses og overvåges.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af adgangsrettigheder sker. Vi har inspiceret adgangsrettigheder til Spectrum Protect, Unix, Omnitracker.	Ingen væsentlige bemærkninger
9.2.5	Brugernes adgangsrettigheder gennemgås regelmæssigt.	Vi har inspiceret proceduren for gennemgang af adgangs-rettigheder. Vi har for et udvalg af medarbejdere inspiceret om adgangsrettigheder svarer til deres arbejdsområder.	Ingen væsentlige bemærkninger
9.2.6	Alle medarbejderens adgangsrettigheder inddrages ved samarbejdets ophør.	Vi har fået en oversigt over fratrådte medarbejdere i 2015. Ifølge det oplyste er adgangsrettigheder for fratrådte medarbejdere i 2015 inddraget.	Ingen væsentlige bemærkninger
9.3.1	Virksomhedens retningslinjer for brugernes valg og anvendelse af adgangskoder er i overensstemmelse med god skik og brug.	Vi har inspiceret kravene til brug af adgangskoder på udvalgte servere.	Ingen væsentlige bemærkninger
9.3.1	Alle brugere skal har en unik identitet til personlig brug, og der skal vælges en passende autentifikationsteknik til verifikation af brugernes identitet.	Vi har for et udvalg af servere inspiceret oprettede brugere og vurderet om der er en unik identitet.	Ingen væsentlige bemærkninger
9.4.2	Systemadgang beskyttes af en sikker log-on-procedure.	Vi har genudført proceduren for log-on.	Ingen væsentlige bemærkninger
9.4.3	Systemer til styring af adgangskoder er interaktive og sikrer, at der kun benyttes adgangskoder med den fastlagte kvalitet.	Vi har forespurgt, hvordan reglerne er for administration af adgangskoder.	Ingen væsentlige bemærkninger

6. Fysisk og miljømæssig sikkerhed Viby (ISO27002 Afsnit 11)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af,*

- *at væsentlige informationsaktiver er beskyttet mod uautoriseret fysisk adgang, fysisk skade og forstyrrelser.*
- *at kritisk informationsbehandlingsudstyr og lagringsmedier huses i sikre områder beskyttet af nødvendige barrierer og adgangskontroller.*
- *at undgå tab af, skader på eller kompromittering af informationsaktiver.*
- *at udstyr beskyttes mod fysiske trusler.*
- *at nødvendige forsyninger af el og ventilation samt kabelinstallationer er tilstrækkelige.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
11.1.1	Virksomheden etablerer en sikker fysisk afgrænsning for at beskytte områder med informationsbehandlingsudstyr og lagringsmedier.	Vi har inspiceret områder, hvor backup udstyr er placeret hos B4Restore.	Ingen væsentlige bemærkninger
11.1.2	Sikre områder beskyttes af adgangskontrol, så kun autoriserede personer kan få adgang.	Vi har inspiceret, at der kræves adgangsbrik og personlig kode for at få adgang til driftslokale.	Ingen væsentlige bemærkninger
11.1.4	Virksomheden har tilrettelagt den fysiske sikkerhed, så skadevirkninger fra brand, oversvømmelser, jordskælv, eksplosioner, civile optøjer, terrorisme og andre former for natur- eller menneskeskabte trusler minimeres.	Vi har inspiceret områder, hvor backup udstyr er placeret hos B4Restore, for at påse, at der er implementeret brandalarm og -slukning, samt køling og UPS-anlæg.	Ingen væsentlige bemærkninger
11.1.6	Af- og pålæsningsområder samt andre områder, hvor offentligheden kan få adgang, er overvåget.	Vi har inspiceret, at der ikke er offentlig adgang til områder, hvor backup udstyr er placeret, samt at der er overvågning.	Ingen væsentlige bemærkninger
11.2.1	Udstyr er placeret og beskyttet, så risikoen for skader og uautoriseret adgang minimeres.	Vi har inspiceret områder, hvor backup udstyr er placeret hos B4Restore, for at påse, at der er implementeret adgangskontrol.	Ingen væsentlige bemærkninger
11.2.1	Lokale hvor backup udstyr er placeret er beskyttet mod statisk elektricitet ved at installere kobbertråde i gulvet og jorde dem.	Vi har forespurgt om områder, hvor backup udstyr er placeret hos B4Restore er beskyttet mod statisk elektricitet.	Ingen væsentlige bemærkninger
11.2.2	Udstyr er sikret mod forsyningssvigt i overensstemmelse med udstyrets betydning for kritiske forretningssystemer.	Vi har inspiceret områder, hvor backup udstyr er placeret hos B4Restore, for at påse, at der er installeret UPS. Vi har endvidere inspiceret, at der er årlig service på UPS.	Test af UPS sker uformelt ved midlertidige strøm-afbrydelser.
11.2.3	Kabler til elektricitetsforsyning og datakommunikation er sikret mod skader og uautoriserede indgreb.	Vi har inspiceret områder, hvor backup udstyr er placeret hos B4Restore for at påse, at kabler til EL og datakommunikation er sikret mod skader.	Ingen væsentlige bemærkninger

6. Fysisk og miljømæssig sikkerhed Viby (ISO27002 Afsnit 11)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af,*

- *at væsentlige informationsaktiver er beskyttet mod uautoriseret fysisk adgang, fysisk skade og forstyrrelser.*
- *at kritisk informationsbehandlingsudstyr og lagringsmedier huses i sikre områder beskyttet af nødvendige barrierer og adgangskontroller.*
- *at undgå tab af, skader på eller kompromittering af informationsaktiver.*
- *at udstyr beskyttes mod fysiske trusler.*
- *at nødvendige forsyninger af el og ventilation samt kabelinstallationer er tilstrækkelige.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
11.2.4	Udstyr vedligeholdes efter forskrifterne for at sikre dets tilgængelighed og pålidelighed.	Vi har forespurgt om procedurer for vedligeholdelse af udstyr. Vi har inspiceret, at der er serviceaftaler på kølingsudstyr, UPS-anlæg, servere, Tape-station og SAN-udstyr.	Ingen væsentlige bemærkninger
11.2.5	Virksomhedens informationsaktiver må ikke fjernes fra virksomheden uden fornøden autorisation.	Vi har forespurgt udvalgte medarbejdere om proceduren for fjernelse af informationsaktiver fra virksomheden.	Ingen væsentlige bemærkninger
11.2.7	Alt udstyr med lagringsmedier kontrolleres for at sikre, at kritiske/følsomme informationer og licensbelagte systemer er fjernet eller overskrevet, i forbindelse med at udstyret bortskaffes eller genbruges.	Vi har forespurgt om procedurer for bortskaffelse af Tapes. Vi har forespurgt om procedurer for genbrug af diske.	Ingen væsentlige bemærkninger

8. Fysisk og miljømæssig sikkerhed Global Connect (ISO27002 Afsnit 11)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af,*

- *at væsentlige informationsaktiver er beskyttet mod uautoriseret fysisk adgang, fysisk skade og forstyrrelser.*
- *at kritisk informationsbehandlingsudstyr og lagringsmedier huses i sikre områder beskyttet af nødvendige barrierer og adgangskontroller.*
- *at undgå tab af, skader på eller kompromittering af informationsaktiver.*
- *at udstyr beskyttes mod fysiske trusler.*
- *at nødvendige forsyninger af el og ventilation er tilstrækkelige.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
11.1.1	Virksomheden etablerer en sikker fysisk afgrænsning for at beskytte områder med informationsbehandlings-udstyr og lagringsmedier.	Vi har inspiceret B4Restore primære driftslokation.	Ingen væsentlige bemærkninger
11.1.2	Sikre områder beskyttes af adgangskontrol, så kun autoriserede personer kan få adgang.	Vi har inspiceret, at der kræves adgangsbrik for at få adgang til den primære lokation. Vi har forespurgt, hvem fra B4Restore der har adgang til den sekundære lokation.	Ingen væsentlige bemærkninger
11.1.4	Fysisk sikkerhed er tilrette-lagt, så skader fra brand, oversvømmelser, jordskælv, eksplosioner, optøjer, terrorisme og andre former for natur- eller menneskeskabte trusler minimeres.	Vi har inspiceret B4Restores primære lokation, for at påse, at der er implementeret brandalarm og -slukning, samt køling.	Ingen væsentlige bemærkninger
11.1.6	Af- og pålæsningsområder samt andre områder, hvor offentligheden kan få adgang, er overvåget.	Vi har inspiceret, at der ikke er offentlig adgang til den primære lokation, samt at der er overvågning.	Ingen væsentlige bemærkninger
11.2.1	Udstyr er placeret og beskyttet, så risikoen for skader og uautoriseret adgang minimeres.	Vi har inspiceret B4Restores primære lokation, for at påse, at der er implementeret adgangskontrol.	Ingen væsentlige bemærkninger
11.2.5	Virksomhedens informationsaktiver må ikke fjernes fra virksomheden uden fornøden autorisation.	Vi har forespurgt udvalgte medarbejdere om proceduren for fjernelse af informationsaktiver fra virksomheden.	Ingen væsentlige bemærkninger
11.2.6	Udstyr uden for B4Restore sikres på behørig vis	Vi har inspiceret B4Restores primære lokation, for at påse, at udstyr er sikret på behørig vis.	Ingen væsentlige bemærkninger
11.2.7	Udstyr med lagringsmedier kontrolleres for at sikre, at følsomme informationer og licensbelagte systemer er fjernet eller overskrevet, i forbindelse med at udstyret bortskaffes eller genbruges.	Vi har forespurgt om procedurer for bortskaffelse af Tapes. Vi har forespurgt om procedurer for genbrug af diske.	Ingen væsentlige bemærkninger

9. Driftssikkerhed (ISO27002 Afsnit 12)

Kontrolmål: *Der er etableret betryggende kontroller til sikring af*

- *en korrekt og betryggende driftsafvikling.*
- *at systemer og data sikkerhedskopieres, at sikkerhedskopier opbevares betryggende og at sikkerhedskopier er læsbare.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
12.1.1	Driftsafviklingsprocedurer for forretningskritiske systemer er dokumenterede, ajourførte og tilgængelige for drifts-afviklingspersonalet og andre med et arbejdsbetinget behov.	Vi har inspiceret B4Restores operationsprocedures.	Ingen væsentlige bemærkninger
12.1.2	Ændringer til forretnings-kritisk informationsbehand-lingsudstyr, -systemer og -procedurer styres gennem en formaliseret procedure.	Vi har observeret change management procedurer. Vi har forespurgt udvalgte medarbejdere om hvordan ændringshåndtering udføres.	Ingen væsentlige bemærkninger.
12.1.3	Ressourceforbruget overvåges og tilpasses	Vi har inspiceret driftsprocesser for verificering af passende ressourcekapacitet mod anvendt ressourceforbrug. Vi har forespurgt udvalgte medarbejdere, hvad de gør når der stor belastning på systemkraft, diske eller tapes.	Ingen væsentlige bemærkninger
12.2.1	B4Restore har installeret antivirus- på relevante enheder. De opdateres løbende efter leverandørens opdateringer.	Vi har inspiceret, at der er installeret opdateret antivirus software på et udvalg af servere	Ingen væsentlige bemærkninger
12.3.1	Der tages sikkerhedskopier af virksomhedens væsentlige informationsaktiver, herunder parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har inspiceret processen for sikkerhedskopiering af nye versioner/releases af Spectrum Protect og AIX.	Ingen væsentlige bemærkninger
12.4.1	Brugen af virksomhedens informationsbehandlingssyste mer overvåges og følges op løbende.	Vi har observeret, hvorledes der foretages overvågning af sikkerhedskopiering.	Ingen væsentlige bemærkninger
12.4.1	Fejl logges og analyseres, og nødvendige udbedringer og modforholdsregler gennemføres.	Vi har observeret, hvorledes fejl eller manglende backup jobs bliver fulgt op på med udgangs-punkt i registreringer i Wizard/Spectrum Protect eller Zendesk.	Ingen væsentlige bemærkninger

9. Driftssikkerhed (ISO27002 Afsnit 12)

Kontrolmål: *Der er etableret betryggende kontroller til sikring af*

- *en korrekt og betryggende driftsafvikling.*
- *at systemer og data sikkerhedskopieres, at sikkerhedskopier opbevares betryggende og at sikkerhedskopier er læsbare.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
12.4.2	Log-faciliteter og log-oplysninger beskyttes mod manipulation og tekniske fejl. Dette sker ved anvendelse af adgangskontrolsystemer, fysisk adskillelse eller netværkssegmentering.	Vi har forespurgt, hvordan log oplysninger beskyttes mod ændring og sletning. Vi har forespurgt, hvem der har adgang til log.oplysninger	Ingen væsentlige bemærkninger
12.4.3	Aktiviteter udført af systemadministratorer og -operatører samt andre med særlige rettigheder skal logges.	Vi har inspiceret om administratorer og operatører aktiviteter logges.	Ingen væsentlige bemærkninger
12.5.1	Browsere skal opsættes jævnfør sikkerhedspolitikken. Brugere må installere programmer på B4Restore, når COO har godkendt programmet og leverandøren. Operativsystemer og applikationer må kun installeres og ændres af COO.	Vi har forespurgt COO, proceduren for installation af systemsoftware på servere.	Ingen væsentlige bemærkninger
12.6.1	Virksomheden indhenter løbende informationer om eventuelle sårbarheder i de anvendte systemer. Sårbarhederne evalueres, og passende foranstaltninger skal implementeres for at modvirke de nye risici.	Vi har forespurgt udvalgte medarbejdere om, hvordan sårbarheder for Backupmiljøet indsamles, evalueres og tilhørende foranstaltninger implementeres. Vi har observeret, at Spectrum Protect kører mindst version 6.2 og AIX version 6.1.6.3.	Ingen væsentlige bemærkninger
12.6.1	B4Restore udfører regelmæssige scanninger og gennemgang af malwarebeskytelse..	Vi har forespurgt udvalgte medarbejdere om, hvordan sårbarheder for backup-miljøet indsamles, evalueres og tilhørende foranstaltninger implementeres. Vi har forespurgt COO om gennemgang af malware beskyttelse.	Ingen væsentlige bemærkninger
12.6.1	Windows opdateringer udføres via Microsofts værktøj Windows Update. Windows sikkerhedsrelaterede opdateringer udrulles seneste 30 dage efter offentliggørelse.	Vi har forespurgt COO om opdatering af sikkerheds-relaterede windows opdateringer.	Ingen væsentlige bemærkninger

9. Driftssikkerhed (ISO27002 Afsnit 12)

Kontrolmål: *Der er etableret betryggende kontroller til sikring af*

- *en korrekt og betryggende driftsafvikling.*
- *at systemer og data sikkerhedskopieres, at sikkerhedskopier opbevares betryggende og at sikkerhedskopier er læsbare.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
12.6.2	Generelt må administrative adgangskoder ikke gives til de arbejdsstationer, der anvendes i Selskabet. Dispensation gives kun af direktionen.	Vi har forespurgt om, administrative adgangsrettigheder begrænses.	Alle teknikere har administrative rettigheder til deres PC. Dette er begrundet i et arbejdsmæssigt behov, der er godkendt af direktionen.

10. Kommunikationssikkerhed (ISO27002 Afsnit 13)			
***Kontrolmål**: Der er etableret betryggende kontroller til sikring af beskyttelse af informationer i netværk og af understøttende informationsbehandlingssystemer.*			
Ref.	**Kontrol**	**Udførte test af kontroller**	**Bemærkninger**
13.1.1	Alle servere og netværk skal beskyttes mod trusler ved hjælp af firewall. COO skal sikre, at der er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder logning og overvågning.	Vi har inspiceret, netværksstegning og påset, at der er installeret firewall.	Ingen væsentlige bemærkninger
13.1.1	Fysisk og logisk adgang til diagnose- og konfigurationsporte kontrolleres.	Vi har forespurgt udvalgte medarbejdere om der på firewalls er portregler, der skal sikre kun tilladt trafik får adgang til netværket.	Ingen væsentlige bemærkninger
13.1.2	B4Restore har procedurer for anvendelse af netværks-tjenester.	Vi har inspiceret proceduren for netværkstjenester.	Ingen væsentlige bemærkninger
13.1.3	B4Restore har segmenteret netværket for at etablere en passende adskillelse imellem forskellige tjenester, brugergrupper eller systemer.	Vi har forespurgt, hvordan netværket er segmenteret.	Ingen væsentlige bemærkninger
13.2.1	B4Restore har procedure for håndtering af opbevaringstiden for data.	Vi har inspiceret proceduren B4R-ISO-PR2013017 - Data Retention Backup".	Ingen væsentlige bemærkninger
13.2.2	Fortrolig information må ikke videregives til tredjepart i nogen form, uden godkendelse af dette fra System- og Dataejer. Dette gælder især for følsom information, samt personhenførbare oplysninger givet til Selskabet.	Vi har forespurgt udvalgte medarbejdere om videregivelse af fortrolig information.	Ingen væsentlige bemærkninger
13.2.3	B4Restore har procedurer for elektroniske meddelelser.	Vi har inspiceret proceduren for brug af elektroniske meddelelser.	Ingen væsentlige bemærkninger
13.2.4	Der er en forretningsgang for afgivelse af tavshedserklæring, som afspejler virksomhedens krav til behandling af følsomme/fortrolige informationer.	Vi har forespurgt om forretningsgangen for afgivelse af tavsheds-erklæring med den HR ansvarlige. Vi har inspiceret, at der i et udvalg af medarbejderes ansættelsesaftaler fremgår, at medarbejdere har tavshedspligt.	Ingen væsentlige bemærkninger

11. Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer (ISO27002 Afsnit 14)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af,*

- *at sikkerhed indgår som en integreret del af styresystemer, infrastruktur og tjenesteydelser.*
- *at kravene til sikkerhed skal være identificeret og aftalt før implementering af informationsbehandlingssystemer.*
- *at sikre de systemtekniske filer i driftsmiljøet.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
14.1.1	Anskaffelse og installation af nyt informationsbehandlings-udstyr og -systemer følger en formel godkendelses-procedure.	Vi har inspiceret proceduren "B4R-ISO-PR2013025 - System Update and Patch Management".	Ingen væsentlige bemærkninger
14.1.2	Der benyttes sikre autentifikations- og autorisationsprocesser for at sikre service-transaktioner over offentlige netværk.	Vi har forespurgt om auten-tifikations- og autorisations-processer ved service-transaktioner over offentlige netværk.	Ingen væsentlige bemærkninger
14.2.2	Kontrollerne er beskrevet ovenfor i punkt 12.1.2 ændringsstyring	Ikke relevant	Ikke relevant se 12.1.2
14.2.3	Større og kritiske ændringer til forretningssystemer gennemgås og testes. Ændringer i produktions-miljøerne annonceres i god tid således, at beredskabs-planerne tilrettes i overensstemmelse med ændringerne.	Vi har forespurgt, hvordan større og kritiske ændringer til forretningssystemer udføres.	Ingen væsentlige bemærkninger
14.2.4	Ændringer i standard-systemer skal begrænses til nødvendige ændringer, og sådanne ændringer skal styres omhyggeligt.	Vi har forespurgt, hvordan ændring til standardsystemer udføres.	Ingen væsentlige bemærkninger
14.2.8	Der foreligger generelle god-kendelseskriterier for nye systemer og nye versioner eller opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, før de kan godkendes og sættes i drift.	Vi har inspiceret processen for opdatering af nye versioner/ releases af Spectrum Protect og AIX.	Ingen væsentlige bemærkninger

12. Leverandørforhold (ISO27002 Afsnit 15)

***Kontrolmål**: Der er etableret betryggende kontroller som sikrer,*

- *at der er udfærdiget skriftlige samarbejdsaftaler med relevante leverandører med angivelse af aftalt niveau for informationssikkerhed*
- *at sikre beskyttelse af virksomhedens aktiver, underleverandører har adgang til*

Ref	Kontrol	Udførte test af kontroller	Bemærkninger
15.1.1	Ved samarbejde med andre parter, der har adgang til virksomhedens informations-aktiver gennemføres en risiko-vurdering, og relevante sikringsforanstaltninger identificeres og implementeres.	Vi har forespurgt, hvorledes andre parter risikovurderes inden de få adgang til Backup miljø.	Ingen væsentlige bemærkninger
15.1.2 15.2.1	Ethvert væsentligt eksternt samarbejde er baseret på en samarbejdsaftale, som sikrer, at B4Restores sikkerheds-målsætning ikke kompromitteres.	Vi har inspiceret udvalgte samarbejdsaftaler med eksterne parter. Vi har forespurgt, hvordan B4Restore sikrer sig, at Global Connect efterlever B4Restores sikkerhedspolitik.	Ingen væsentlige bemærkninger
15.2.1	Ved serviceleverance, bliver der udarbejdet en gensidig aftale omkring det ønskede serviceniveau, eksempelvis gennem formelle SLA (Service Level Agreements) som en del af den indgåede driftsaftale. B4Restore sikrer sig, at aftalte sikrings- og kontrolforan-staltninger, serviceydelser og servicemål bliver etableret, leveret og opretholdt	Vi har observeret, at der er indgået housing aftale med Global Connect. Vi inspiceret forholdene hos Global Connect og testet relevante kontroller, som Global Connect udfører på vegne af B4Restore.	Ingen væsentlige bemærkninger
15.2.1	B4Restore overvåger regelmæssigt serviceleverandøren. Dette sker ved gennemgang af aftalte rapporter samt udføre egentlige revisioner, for at sikre at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres betryggende.	Vi har observeret, at der er indgået housing aftale med Global Connect. Vi har inspiceret housing lokaliteter hos Global Connect med henblik på at indhente tilstrækkelig information og bevis om implementering og funktionalitet om kontroller hos Global Connect. Vi har forespurgt om ledelsen hos B4Restore er i dialog med Global Connect om IT sikkerhed.	Ingen væsentlige bemærkninger
15.2.2	COO sikre, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinier som B4Restore	Vi har forespurgt, hvordan procesen for håndtering af ændringer hos serviceunderleverandører.	Ingen væsentlige bemærkninger

13. Styring af informationssikkerhedshændelser (ISO27002 Afsnit 16)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af, at informationssikkerhedshændelser og svagheder i forbindelse med informationssikkerhedssystemer kommunikeres på en sådan måde, at der iværksættes korrigerende handling rettidigt.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
16.1.1	Ledelsens ansvar og de nødvendige forretningsgange er fastlagt for at sikre en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.	Vi har forespurgt ledelsen, om dets ansvar til at sikre håndtering af sikkerhedsbrud.	Ingen væsentlige bemærkninger
16.1.2	Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt.	Vi har forespurgt udvalgte medarbejdere om, hvordan de rapporterer sikkerhedshændelser. Vi har forespurgt ledelsen, hvordan information om sikkerhedshændelser indsamles.	Ingen væsentlige bemærkninger
16.1.3	Alle medarbejdere, samarbejdspartnere og andre brugere af systemer og tjenester skal have pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i systemer og tjenester.	Vi har forespurgt udvalgte medarbejdere om, hvordan de rapporterer sikkerheds-svagheder. Vi har forespurgt ledelsen, hvordan de indsamler information om sikkerhedssvagheder.	Ingen væsentlige bemærkninger
16.1.6	B4Restore har et system, der kan kvantificere og overvåge typer, omfang og omkost-ninger ved håndteringen af sikkerhedsbrud samt undgå gentagelser	Vi har forespurgt, hvorledes systemet for overvågning af sikkerhedsbrud styres.	Ingen væsentlige bemærkninger

14. Beredskabsstyring (ISO27002 Afsnit 17)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af, at modvirke afbrydelser af forretningsaktiviteter og at beskytte kritiske forretningsprocesser mod virkningerne af større nedbrud af informationssystemer eller katastrofer og at sikre rettidig retablering.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
17.1.1	Der udarbejdes og vedligeholdes en tværorganisatorisk beredskabsstyringsproces, som behandler de krav til informationssikkerhed, der er nødvendige for virksomhedens fortsatte drift.	Vi har forespurgt udvalgte medarbejdere om beredskabsstyring. Vi har inspiceret, at der er en beredskabsplan og vagtplan.	Ingen væsentlige bemærkninger
17.1.2	Der udarbejdes planer for vedligeholdelse og retablering af virksomhedens forretnings-aktiviteter inden for den fastsatte tidsramme efter en afbrydelse af eller fejl i virksomhedens kritiske forretningsprocesser.	Vi har forespurgt udvalgte medarbejdere, hvad de gør i tilfælde af en afbrydelse eller en fejl for at retablere driften.	Ingen væsentlige bemærkninger
17.1.3	Beredskabsplaner afprøves og opdateres for at sikre, at de er tidssvarende og effektive, herunder, at informations-sikkerhed er tænkt ind.	Vi har forespurgt udvalgte medarbejdere, hvordan beredskabsplaner afprøves.	Ingen væsentlige bemærkninger

15. Overensstemmelse (ISO27002 Afsnit 18)

***Kontrolmål**: Der er etableret betryggende kontroller til sikring af, at brud på love, lovbestemte, forskriftsmæssige elle kontraktlige forpligtelser og på sikkerhedskrav.*

Ref	Kontrol	Revisors test af kontroller	Bemærkninger
18.1.1	B4Restore foretager en gang om året en vurdering om, hvilke lov-, myndigheds- og kontraktkrav, der er gældende for backup ydelser. Disse krav bliver identificeret og dokumenteret.	Vi har forespurgt ledelsen, om hvilke relevante hvilke lov-, myndigheds- og kontraktkrav, der er for B4Restore.	Ingen væsentlige bemærkninger
18.1.4	Anmeldelse til datatilsynet som edb-servicevirksomhed i henhold til lov om behandling af personoplysninger § 53	Vi har inspiceret anmeldelse til datatilsynet som edb-servicebureau.	Ingen væsentlige bemærkninger
18.2.1	Hver enkelt leder sikrer informationssikkerheden inden for eget ansvarsområde.	Vi har forespurgt til procedurer, for, at ledere sikrer informations-sikkerheden overholdes inden for deres ansvarsområde.	Ingen væsentlige bemærkninger