JUNI 2016

FRONTSAFE A/S

ISAE 3402 TYPE 2 ERKLÆRING

Revisors erklæring vedrørende de generelle it-kontroller i tilknytning til driften af Frontsafe Cloud backup ydelser.

Beierholm
Statsautoriseret Revisionspartnerselskab
Ellebjergvej 52, 2.
2450 København SV
CVR-nr. 32 89 54 68
Tlf +45 33 38 98 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Erklæringsopbygning

Kapitel 1:
Frontsafe A/S' ledelseserklæring

Kapitel 2:
Frontsafe A/S' beskrivelse af de generelle it-kontroller for driften af Cloud backup ydelser.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om de generelle it-kontroller, deres udformning og funktionalitet.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf.

KAPITEL 1:

Frontsafe A/S' ledelseserklæring

Beskrivelsen af Frontsafe A/S' generelle it-kontroller i kapitel 2 er udarbejdet til brug for kunder, der har anvendt eller påtænker at anvende Frontsafe Cloud backup ydelser, 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 for væsentlig fejlinformation i deres regnskaber. Frontsafe A/S bekræfter hermed, at

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af Frontsafe Cloud backup ydelsers generelle it-kontroller i hele perioden 1. maj 2015 - 30. april 2016. Kriterierne for dette udsagn er, 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 systemets udformning har forudsat ville være implementeret af Frontsafe A/S, 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 Frontsafe A/S' generelle it-kontroller foretaget i perioden 1. maj 2015 - 30. april 2016.

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller 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 kontroller, som den enkelte kunde måtte anse som vigtig efter deres særlige forhold.

(B) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. maj 2015 - 30. april 2016. Kriterierne for dette udsagn er, 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 forhindrer opnåelsen af de anførte kontrolmål, og

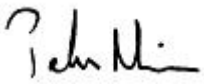
(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. maj 2015 - 30. april 2016.

(C) den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af Frontsafe standardaftale, grundlaget for Cloud backup ydelser og ydelser omkring de generelle it-kontroller. Kriterierne for dette grundlag var:

(i) Service Level Agreement for Cloud backup ydelser Vrs. 7 – 2016

(ii) Almindelige betingelser for Cloud backup ydelser Vrs. 7 - 2016

Viby J., den 15. juni 2016
Peter M. Nielsen



Direktør
Frontsafe A/S, Søndervangs Alle 20, DK-8260 Viby J, Tel (+45) 8743 4090, CVR: 29631123

KAPITEL 2:

Frontsafe A/S' beskrivelse af de generelle it-kontroller for driften af Cloud backup ydelser

Indledning

Formålet med nærværende beskrivelse er at levere information til Frontsafe A/S' kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller for serviceleverandører.

Beskrivelsen giver herudover information om de kontroller, der er anvendt for driften i Frontsafe Cloud backup ydelser backup i perioden 1. maj 2015 - 30. april 2016.

Beskrivelse af Frontsafe A/S og omfang af ydelser

Frontsafe A/S er en del af en dansk velkonsolideret IT-koncern, JS Holding, som opererer i flere forskellige IT-selskaber med over 125 medarbejdere fordelt mellem Jylland og København.

Frontsafe A/S har hovedsæde og datacenter placeret i Viby J, hvor den primære organisation har sin dagligdag. Derudover har Frontsafe A/S egen udviklingsafdeling placeret i København. Denne afdeling udvikler Frontsafe Cloud Portal Software primært til IBM Spectum Protect suiten. Cloud Portal Softwaren er udviklet i arkitekturen REST API, som benyttes af danske og udenlandske kunder døgnet rundt.

Frontsafe A/S er specialiseret og fokuseret leverandør af Cloud Backup ydelser til virksomheder på det danske marked. Frontsafe A/S leverer Cloud Backup løsninger til tusindvis af kunder, som dagligt får sikret mere end 13.000 servere i døgnet gennem en solid service og support med +10 års erfaring i drift af storage og backup.

Frontsafe A/S har gennem de seneste år udviklet viden og kompetencer og tilbyder i dag markedet nye backup-relaterede produkter, herunder CommVault, VEEAM Cloud Repository, som sammen med IBM Spectrum Protect er ledende på verdensmarkedet for backup både som en service og On-Premise løsninger.

Forretningsstrategi/ it-sikkerhedsstrategi

Hos Frontsafe A/S har vi et mål om kontinuerligt at nedbringe den belastning, som driften af vores services har på miljøet. Vi har opstillet et konkret mål om at nedbringe energiforbruget pr. lagret GB med minimum 5 procent hvert år. Det er således et krav i Frontsafe indkøbsafdelingen, at tilsikre at indkøb af hardware og software til driften påvirker målopfyldelsen i positiv retning. De følgende tal er de procentvise besparelser fra år til år i KW strømforbrug pr. lagret GB i Frontsafe produktionen gennem de seneste 5 års drift:

KW/GB besparelse i procent i forhold til året før

2011: 34,66%
2012: 24,63%
2013: 5,79%
2014: 22,86%
2015: 30,57%

Som det fremgår, har Frontsafe A/S levet op til målet om en årlig nedbringelse af strømforbruget pr. lagret GB med minimum 5 procent.

Det er en vigtig del af Frontsafe A/S' strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet ikke påføres uacceptable risici.

Frontsafe A/S har tre overordnede strategiske pejlepunkter:

- Frontsafe hjælper danske virksomheder til en optimalt brug af moderne informationsteknologi
- Frontsafe arbejder primært med administrative systemer til sikring af data
- Frontsafe er en god arbejdsplads for en stabil og veluddannet medarbejderstyrke

Frontsafe A/S arbejder med it-sikkerhed på et forretningsstrategisk niveau og arbejder derfor løbende med at sikre et højt service- og kvalitetsniveau. Ledelsen prioriterer gennem selskabets sikkerhedspolitik, at it-sikkerhed skal være og er en vigtig del af selskabets virksomhedskultur. Frontsafe A/S har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27002:2013, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

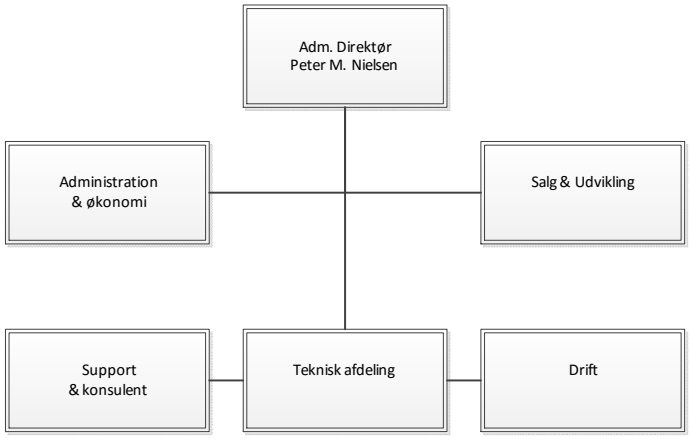
- Informationssikkerhedspolitik
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Leverandørforhold
- Styring af informationssikkerhed
- Informationssikkerhedsaspekter ved nød-, beredskabs – og reetableringsstyring

De implementerede sikringsforanstaltninger hos Frontsafe A/S fremgår af bilag 1 til denne beskrivelse.

Frontsafe A/S organisation og organisering af it-sikkerheden

Frontsafe A/S beskæftiger 15 medarbejdere og har en flad organisationsstruktur.

It-sikkerhedsansvarlig: Den tekniske chef.
Ved brug af eksterne samarbejdspartnere udarbejdes samarbejdsaftale inden arbejde påbegyndes.



Risikostyring i Frontsafe A/S

Det er Frontsafe A/S' politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift. Frontsafe A/S gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering.

Frontsafe A/S har indarbejdet faste procedurer for risikovurdering af forretningen og herunder Cloud backup ydelsen. Vi sikrer dermed, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er

minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderer relevante i forbindelse med at revurdere vores generelle risikovurdering. Ansvaret for risikovurderingen ligger hos direktør Peter Nielsen og skal efterfølgende forankres og godkendes hos virksomhedens ledelse.

Som led i ovenstående it-sikkerhedsstrategi arbejder Frontsafe A/S med den internationale standard for it-sikkerhed - ISO27002:2013 – som primær referenceramme for it-sikkerheden. Arbejdsprocessen omkring it-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at Frontsafe A/S til hver en tid er i overensstemmelse med sine kunders krav og behov.

Håndtering af IT-sikkerhed

Ledelsen hos Frontsafe A/S har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet Frontsafe A/S' struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

Frontsafe A/S' kvalitetsstyringssystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker it-drift til kunderne. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

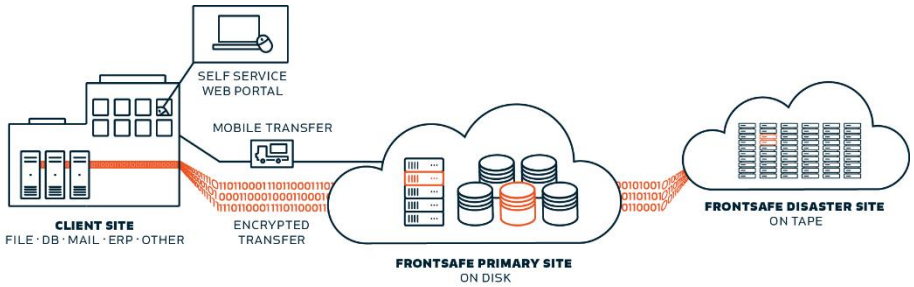
Frontsafe A/S' it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedshullet omgående.

Alle servere og netværksenheder er dokumenteret i Frontsafe dokumentationssystem. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) ligger gemt i vores dokumentationssystem.

Sikkerhedspolitikken sætter de grundlæggende politikker for Frontsafe A/S' infrastruktur og omhandler ikke forhold vedrørende specifikke produkter, ydelser eller brugere.

Sikkerhedspolitikken er udarbejdet, så Frontsafe A/S har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

Frontsafe A/S' aktuelle tekniske setup er beskrevet i Service Level Agreement version 7.



Frontsafe A/S kan som led i den it-sikkerhedsstrategiske udvikling tilbyde partnere og Cloud backup kunder en ydelse til automatisk test af deres backupgrundlag. På baggrund af de data, som en kunde har i sit backupgrundlag for en given server, genskabes hele serveren inklusive operativsystem, programmer og data til en virtuel platform i Frontsafe A/S' datacenter. Herefter gennemføres som tilvalg forespørgsler ned i serverens data, og hele resultatet sendes automatiseret til partneren og/eller kunden, som herefter har dokumenteret, om backupgrundlaget er som forventet, og hvor lang tid restore af den samlede server tager.

HR, medarbejdere og uddannelse

Frontsafe A/S er Certificeret IBM Partner med kompetencer på IBM Spectrum Protect. Desuden er Frontsafe A/S certificeret Veeam Partner.

Alle udførende konsulenter har kompetencer inden for de områder, de beskæftiger sig med. Det dokumenteres ved hjælp af relevante certificeringer.

Frontsafe A/S skal leve op til en række krav fra IBM og Veeam, herunder specifikke krav om at et bestemt antal konsulenter har bestået bestemte produktcertificeringer, som løbende skal fornyes. Frontsafe A/S sikrer via løbende produkttræning og kursusdeltagelse at denne høje certificeringsstatus opretholdes.

Fysisk sikkerhed

Frontsafe A/S' backupanlæg er placeret i et sikkert og ISAE 3402-revisorerklæret datacenter med følgende sikringsforanstaltninger baseret på ISO 27002-standarden:

- Nødstrømsanlæg opstartes automatisk ved eventuelt udfald eller fejl på den primære strømforsyning. Alt udstyr er endvidere forsynet med UPS, så normal drift fortsættes uden driftsstop.
- Køl sikrer optimal temperatur i driftsmiljøet.
- For at undgå katastrofer ved eventuel røgudvikling og brand er der installeret et fintfølende brandalarmeringsanlæg, der består af et røgsnifferanlæg og ion-meldere, som indsuger og analyserer luften i serverrummet og udløser brandbekæmpelse ved den mindste røgudvikling.
- Til brandbekæmpelse er installeret Inergen-anlæg, der benytter en gasart, der fjerner ilt fra luften, således at ild øjeblikkeligt bekæmpes. Serverrummet er udformet som selvstændig brandcelle. Brandbekæmpelsessystemet har alarmoverførsel direkte til brandvæsenet.
- Krydsfelter og netværksudstyr er placeret i aflåste serverrum.
- Der anvendes personlige adgangskort med kode.
- Alarmanlæg anvendes til alle alarmovervågninger. Der føres log over alarmer. Alle alarmer overføres til vagtcentral og/eller driftsvagt, som iværksætter og træffer de nødvendige aktioner.
- Primære datalinjer er etableret som redundante linjer. Disse linjer er fremført som uafhængige fibre til 2 forskellige TDC centraler.

Overvågning

Frontsafe A/S har etableret automatisk overvågning af servere, storagesystemer, netværk, m.v. og har uddannet personale på vagt i en turnusordning således, at nødvendig kompetence er til rådighed 24/7/365.

Hvis en fejl konstateres, afsendes alarm både visuelt på en overvågningsskærm og på SMS/Mail. Opstår en situation, hvor der konstateres en fejl på en komponent, der ikke er en del af den automatiske overvågning, tages der skridt til, at den fremover registreres i systemet.

Datacentret overvåges med hensyn til strømafbrydelser, temperatur, brand, vand, luftfugtighed, og hele datacenteret er i øvrigt kameraovervåget.

Hvis der sker hændelser, som kan påvirke driften, vil overvågningssystemet automatisk alarmere vagtberedskabet, og der forefindes en indarbejdet procedure for eskalation sluttende med, at den adm. direktør involveres.

Listen over personer med adgang til datacenteret revideres løbende jvf. procedure herfor.

Backup

Formålet med backup er at sikre, at kundens data i Frontsafe A/S' datacenter kan genskabes, nøjagtigt og hurtigt. Al data sikres dagligt i andet geografisk placeret serverrum.

Frontsafe A/S udfører restore-test jævnligt på udvalgte systemer.

Patch management / ændringshåndtering

Formålet med patch management er at sikre, at alle relevante opdateringer som patches, fixes og service packs fra leverandører implementeres for at sikre systemerne mod nedetid og uautoriseret adgang, og at implementeringen sker på en kontrolleret måde.

Alle produktionsservere opdateres med kritiske og vigtige opdateringer i det månedlige driftsvindue. Det sikrer, at alle produktionsservere IKKE har kritiske og vigtige opdateringer ældre end 30 dage.

Frontsafe A/S har udarbejdet en fall-back plan i forbindelse med patch management. Formålet med fall-back planen er at sikre, at systemerne kan komme tilbage i normal drift, hvis opdateringen ikke virker efter hensigten.

Styring af it-sikkerhedshændelser

Sikkerhedshændelser og svagheder i Frontsafe A/S' systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Alle medarbejdere i Frontsafe A/S er bekendt med procedure-rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af Frontsafe drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til ledelsen.

Ledelsen har ansvaret for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Brugerstyring/ adgangssikkerhed

Den logiske sikkerhed omfatter logisk beskyttelse af elektroniske systemer og information, der vedrører serviceydelsen. Fx fastlægger den, at kun autoriserede personer har elektronisk adgang hertil.

- Krav til password - alle brugere med adgang til Frontsafe A/S' systemer, anvender password med mindst 7 karakterer, hvor både tal og bogstaver indgår.
- Krav om pauseskærm - pauseskærm er aktiveret på alle vores brugere, for at beskytte dem mod uautoriseret adgang.

Beredskabsstyring

Ved alvorlige fejl sendes en mail til mailgruppen "Alle Frontsafe Sikkerhedsgruppe". Mailen indeholder en kort fejlbeskrivelse og en tidshorisont på nedetiden. Som afslutning på fejlretning sendes en ny mail til mailgruppen om, at fejlen er løst og en uddybende fejlbeskrivelse.

Ved totalskade på et af serverrummene er der udarbejdet en plan for, hvad der skal ske, herunder reetablering af hardware. Herefter vil systemerne kunne gendannes fra backupserver.

Hver 6. måned gennemføres skrivebordstest af Frontsafe katastrofeplan.

Væsentlige ændringer i forhold til it-sikkerhed

For erklæringsperioden har der ikke været væsentlige it-sikkerhedsmæssige ændringer.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Ovenstående beskrivelse er baseret på ovennævnte ramme, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvaret for de forretningssystemer og brugersystemer, som drives via Frontsafe A/S' Cloud backup, er kundernes eget ansvar. Kunderne har ansvaret for at sikre de nødvendige kontroller i forbindelse med systemudvikling, anskaffelse og ændringshåndtering.

Frontsafe er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til Frontsafe A/S' Cloud backup. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Kunderne er ansvarlige for datatransmission til Frontsafe A/S' Cloud backup løsning, og det er kundernes ansvar at skabe den nødvendige datatransmission til Frontsafe datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Frontsafe beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af Frontsafe A/S' Cloud backup. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

BILAG 1:

Frontsafe har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27002:2013

5. Informationssikkerhedspolitikker
- 5.1. Retningslinjer for styring af informationssikkerhed

6. Organisering af informationssikkerhed
- 6.1. Intern organisering
- 6.2. Mobilt udstyr og fjernarbejdspladser

7. Medarbejdersikkerhed
- 7.1. Før ansættelse
- 7.2. Under ansættelsen
- 7.3. Ansættelsesforholds ophør eller ændring

8. Styring af aktiver
- 8.1. Ansvar for aktiver
- 8.2. Klassifikation af informationer
- 8.3. Mediehåndtering

9. Adgangsstyring
- 9.1. Forretningsmæssige krav til adgangsstyring
- 9.2. Administration af brugeradgang
- 9.3. Brugernes ansvar
- 9.4. Styring af system- og applikationsadgange

11. Fysisk sikkerhed og miljøsikring
- 11.1. Sikre områder
- 11.2. Udstyr

12. Driftssikkerhed
- 12.1. Driftsprocedurer og ansvarsområder
- 12.2. Malwarebeskyttelse
- 12.3. Backup
- 12.4. Logning og overvågning
- 12.5. Styring af driftssoftware
- 12.6. Sårbarhedsstyring

13. Kommunikationssikkerhed
- 13.1. Styring af netværkssikkerhed

15. Leverandørsikkerhed
- 15.1. Informationssikkerhed i leverandørforhold
- 15.2. Styring af leverandørydelser

16. Styring af informationssikkerhedsbrud
- 16.1. Styring af informationssikkerhedsbrud og forbedringer

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- 17.1. Informationssikkerhedskontinuitet
- 17.2. Redundans

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om de generelle it-kontroller, deres udformning og funktionalitet

Til kunder af Frontsafe Cloud backup ydelser og deres revisorer

Omfang

Vi har fået til opgave at afgive erklæring om Frontsafe A/S' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af de generelle it-kontroller, som udføres i forbindelse med driften af Frontsafe Cloud backup ydelser til behandling af kunders transaktioner i perioden 1. maj 2015 - 30. april 2016, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Erklæringen er afgivet efter helhedsmetoden, hvilket betyder, at denne erklæring også omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere.

Frontsafe er medlem af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), hvilket medfører en række forhold, som virksomheden skal overholde for at opnå retten til at bruge BFIH's kvalitetsmærke – Certificeret IT-hosting.

Erklæringen dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. virksomhedsbeskrivelsen kapitel 2, afsnittet om komplementerende kontroller.

Frontsafe A/S' ansvar

Frontsafe A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i kapitel 2 (inkl. bilag 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet 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.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om Frontsafe A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB. Denne standard kræver, at vi overholder etiske krav samt 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 væsentlig henseender er hensigtsmæssigt udformet og fungerer effektivt. En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelse, udformning og funktionalitet 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 risicierne 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 i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som Frontsafe A/S har specificeret og beskrevet i kapitel 2 (inkl. bilag 1).

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

Begrænsninger i kontroller hos Frontsafe A/S

Frontsafe 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 vigtig efter deres særlige forhold. Endvidere vil kontroller hos Frontsafe A/S, 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 serviceleverandører 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 kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelsen af de af Frontsafe A/S' generelle it-kontroller til Cloud backup ydelser, således som de var udformet og implementeret i hele perioden 1. maj 2015 - 30. april 2016, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. maj 2015 - 30. april 2016, 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 hele perioden 1. maj 2015 - 30. april 2016, og

d) at kontrollerne i forhold til de særlige krav, som er tilknyttet Frontsafe A/S' medlemskab af BFIH jf. virksomhedsbeskrivelsen i kapitel 2, var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden 1. maj 2015 - 30. april 2016.

Vi skal bemærke, at der for de enkelte kunder kan være specifikke forhold, som gør, at den generelle konklusion ikke er dækkende. Hvis det er aftalt mellem kunden og Frontsafe A/S, at der udarbejdes en specifik erklæring vedrørende kundens kontrakt, vil forholdene fremgå heraf.

Beskrivelse af test kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt Frontsafe A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 15. juni 2016

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
It Auditor, Manager

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med IASE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27002:2013.

Derefter opremser vi i første kolonne de aktiviteter, som Frontsafe A/S jf. sin dokumentation har iværksat for at leve op til kontrolmålene, i anden kolonne hvordan vi har valgt at teste, om det forholder sig som beskrevet, og i tredje kolonne, hvad resultatet af vores test har været.

Hvad angår periode har vi i vores test forholdt os til, om Frontsafe har levet op til kontrolmålene i perioden 1. maj 2015 - 30. april 2016.

INDLEDENDE KONTROLMÅL:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i driften af Cloud backup ydelser. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Gennem en risikovurdering er der sket identificering og prioritering af risici. Udgangspunkt for vurderingen er de i beskrivelsen definerede Cloud backup ydelser. Resultatet bidrager til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for Cloud backup ydelser arbejdes med en løbende risikovurdering, som opstår som følge af de forretningsmæssige forhold og deres udvikling. Vi har kontrolleret, at risikovurderingen er forankret ned igennem de organisatoriske forhold. Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes efter planlagte intervaller.	Vi har indhentet og revideret Frontsafe A/S' seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrolleret, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen kontrolleret, at de underliggende støttepolitikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og den er gjort tilgængelig for medarbejderne via Frontsafe A/S' intranet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikringsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering. Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer. Der foreligger passende forretningsgange for medarbejdere omkring angivelse af tavshedserklæring.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisation i forhold til Cloud backup ydelser. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder. Gennem forespørgsler og stikprøve på ansættelsesaftale har vi kontrolleret, at medarbejdere i Frontsafe A/S er bekendte med deres tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til kunder er håndteret.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevis inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos Frontsafe A/S har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, således at området er afdækket i forhold til risikovurderingen for området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Der skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Via fastlagte arbejdsprocesser og procedurer er det sikret, at alle nye medarbejdere får oplyst deres særlige ansvar og rolle i forbindelse med ansættelse i Frontsafe A/S. Herunder de fastlagte rammer for deres arbejde og den omkringliggende it-sikkerhed. Eventuelle sikkerhedsansvar er fastlagt, og nærmere beskrevet gennem stillingsbeskrivelse og i form af vilkår i ansættelseskontrakten. Medarbejderne er bekendte med deres tavshedspligt via en underskrevet ansættelseskontrakt og via Frontsafe A/S' personalepolitik.	Vi har kontrolleret, at de af ledelsen udarbejdede forretningsgange og procedurer i forbindelse med ansættelse og ansættelsesophør er overholdt. Gennem stikprøver har vi testet, om ovenstående forretningsgange og procedurer er overholdt både i forhold til ansættelse og ansættelsesophør. Ved interview har vi kontrolleret, at væsentlige medarbejdere for Cloud backup ydelser er bekendt med deres tavshedspligt. Vi har gennemgået centrale medarbejderes stillingsbeskrivelser, og efterfølgende testet den enkelte medarbejders kendskab til arbejdsmæssige roller og tilhørende sikkerhedsansvar. Revisionen har påset, at Frontsafe A/S' personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos Frontsafe A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 8:

Styring af aktiver

Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig "ejer". Virksomheden skal sikre, at informationsaktiver i forhold til Cloud backup ydelser får et passende beskyttelsesniveau.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver. Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af Cloud backup ydelser.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af Frontsafe Cloud backup ydelser. Gennem observation og kontrol har vi kontrolleret relationer over til de centrale knowhow systemer for driften af Cloud backup ydelser. Vi har ved observationer og forespørgsler kontrolleret, at Frontsafe A/S overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationer og data i relation til Cloud backup ydelser og den efterfølgende drift af hostingcenter er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed.	Vi har kontrolleret, at der er passende opdeling og tilhørende procedurer/forretningsgange ifm. beskyttelse omkring ejerskab mellem applikationer og data samt øvrige enheder i forhold til Frontsafe drift af Cloud backup ydelser. Vi har kontrolleret, at kontrakter og SLA anvendes som et centralt værktøj til at sikre definitionen, adskillelse og afgrænsning mellem Frontsafe A/S' ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data. Derved påhviler det typisk kunden et eget ansvar at sikre, at der er et passende beskyttelsesniveau på egne informationer og data.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.	Vi har: • forespurgt ledelsen om hvilke procedurer/kontrolaktiviteter, der udføres. • stikprøvevist gennemgået procedurerne for destruktion af databærende medier, til bekræftelse af at de er formelt dokumenterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for Frontsafe adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i Frontsafe A/S. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. Frontsafe A/S' retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger Frontsafe A/S' retningslinjer, og at autorisationer tildeles i henhold til aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåges.	Vi har forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i Frontsafe A/S. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende autorisationssystemer i relation til adgangsstyring i Frontsafe A/S. • at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgang er implementeret i Frontsafe systemer, og at der foretages løbende opfølgning på registrerede brugere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Interne brugeres adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang.	Vi har ved stikprøvevis inspektion påset, at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne, herunder: • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med udvidede rettigheder hver 3. måned • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med almindelige rettigheder hver 6. måned.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Tildeling af adgangskoder styres gennem en formaliseret og kontrolleret proces, som bl.a. sikrer at der sker skift af standard password.	Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i Frontsafe A/S. Vi har ved stikprøvevis inspektion påset, • at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

	• at standard password ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standard password.	
Adgange til operativsystemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (7 tegn), med krav til kompleksitet. Dog er ingen krav omkring maksimal løbetid, lige som password-opsætninger medfører, at password kan genbruges. Endvidere bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i Frontsafe A/S. Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for: • minimum længde for password • Kompleksitet • lockout efter fejlede login forsøg	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 11:

Fysisk sikkerhed og miljøsikring

Der skal være beskyttelse af virksomhedens lokaler og informationsaktiver mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser. Der skal opbygges sikkerhedstiltag, som sikrer, at der undgås tab af, skader på eller kompromittering af virksomhedens informationsaktiver samt forstyrrelser af virksomhedens forretningsaktiviteter. Beskyttelsesforanstaltningerne skal også omfatte destruktion af forældet eller beskadiget udstyr samt nødvendige forsyninger som el, vand og ventilation samt kabelinstallationer.

Frontsafe A/S kontroller	Revisors test af kontroller	Resultat af test
Der er etableret en sikker fysisk afgrænsning, som beskytter de områder, hvorfra Cloud backup ydelser driftes. De sikre områder er beskyttet med adgangskontrol, så kun autoriserede personer kan få adgang. Der er etableret overvågning af områder til af- og pålæsning samt øvrige områder, hvortil offentligheden har adgang.	Jf. serviceleverandørens beskrivelse er den fysiske adgangssikkerhed bl.a. gennemgået og kontrolleret med udgangspunkt i de af ledelsen fastsatte krav. Vi har gennemgået og kontrolleret de fysiske adgange til begge datacentre, som bl.a. sikres via et nøglesystem kombineret med personlig kode, som sikrer begrænset adgang til Frontsafe A/S' datacenter. Via besøg, interview og observation er det kontrolleret, at adgangen til begge Frontsafe A/S' datacentre er i overensstemmelse med ovenstående forretningsgange omkring adgangsbegrænsning. Vi har stikprøvevist gennemgået procedurer for fysisk sikkerhed vedrørende sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt at personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse. Vi har stikprøvevis gennemgået medarbejdere med adgang til sikre områder og påset, at de er oprettet i henhold til de fastlagte procedurer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Udstyr som er placeret i datacenter beskyttes mod fysiske trusler såsom brand, vandskade, strømafbrydelse, tyveri eller hærværk. Datacenteret er sikret mod forsyningssvigt som elektricitet, vand, varme og ventilation. Der er installeret udstyr til overvågning af indeklima, såsom luftfugtighed. Kabler til brug for datakommunikation og elforsyning er beskyttet imod uautoriserede indgreb.	Vi har gennemgået og kontrolleret, at Frontsafe A/S' datacenter overholder de af ledelsen fastsatte krav. Revisionen har kontrolleret overholdelsen af de nødvendige sikringsforanstaltninger jf. ISO 27002 afsnit 11 i forholdene til beskyttelse mod skader, forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk. Konkret har vi: • påset tilstedeværelse af brandbekæmpelsessystemer og køling i datacenter. • gennemgået og kontrolleret dokumentation for vedligeholdelse til bekræftelse af, at UPS og dieselgenerator løbende vedligeholdes og testes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Udstyret til brug for Cloud backup ydelser vedligeholdes efter forskrifterne for at sikre dets tilgængelighed og pålidelighed. Det udstyr, der benyttes uden for datacenteret, beskyttes efter samme retningslinjer, som gælder for udstyr inden i datacenter, under hensyntagen til de særlige risici ved ekstern anvendelse. Alt udstyr med lagringsmedier kontrolleres for at sikre, at kritiske/følsomme informationer og licensbelagte systemer er fjernet eller overskrevet, når udstyret bortskaffes eller genbruges.	• observeret under besøg i datacenter, at der foretages monitering af UPS og dieselgenerator. • påset tilstedeværelse af udstyr til overvågning af indeklima i datacentre. • påset sikring af kabler for datakommunikation og elforsyning. • stikprøvevis gennemgået dokumentationen for at vedligeholdelse af udstyr til beskyttelse med fysiske trusler sker ved løbende vedligeholdelse. • gennemgået og kontrolleret de af ledelsen udarbejdede procedurer til bortskaffelse af udstyr tilknyttet driften af Cloud backup ydelser.	
I forbindelse med anvendelse af datacenter 2 skal sikkerhedstiltagene være ligestillet med kravene til Frontsafe A/S' eget datacenter.	Gennem revision har vi testet, at datacenter 2 indeholder og overholder de samme tiltag for Frontsafe A/S' eget datacenter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Driftsprocedure og ansvarsområder

En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er dokumenteret driftsafviklingsprocedure for forretningskritiske systemer, og de er tilgængelige for personale med et arbejdsbetinget behov. Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse.	Vi har: • forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret. • i forbindelse med revisionen af de enkelte driftsområder stikprøvevis kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. • foretaget inspektion af brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud. Der foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har: • forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. • stikprøvevist gennemgået, at ressourceforbruget i driftsmiljøet bliver overvåget og tilpasset i forhold til det forventede og nødvendige kapacitetsbehov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Malwarebeskyttelse

At beskytte mod skadevoldende programmer, som eksempelvis virus, orme, trojanske heste og logiske bomber.
Der skal træffes foranstaltninger til at forhindre og konstatere angreb af skadevoldende programmer.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret både forebyggende, opklarende og udbedrende sikrings- og kontrolforanstaltninger, herunder den nødvendige uddannelses- og oplysningsindsats for virksomhedens brugere af informationssystemer mod skadevoldende programmer.	Vi har: • forespurgt og inspiceret de procedurer/ kontrolaktiviteter, der udføres i tilfælde af virusangreb eller –udbrud. • forespurgt og inspiceret de aktiviteter, som skal gøre medarbejdere opmærksomme på forholdsregler ved virusangreb eller udbrud. • kontrolleret at servere har installeret antivirusprogrammer, inspiceret signaturfiler, der dokumenterer, at de er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Backup

At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foretages sikkerhedskopiering af alle virksomhedens væsentlige informationsaktiver, herunder eksempelvis parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede. • stikprøvevis gennemgået backup-log vedrørende backup, for bekræftelse af at backup er gennemført succesfuldt og at tilfælde af mislykkede backup håndteres rettidigt. • gennemgået fysisk sikkerhed (bl.a. adgangsbegrænsning) for intern opbevaringslokation, til bekræftelse af, at backup opbevares betryggende.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Logning og overvågning

At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. Frontsafe A/S logger, når brugerne logger af og på systemerne. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter der udføres, og gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder, bliver logget. • stikprøvevis kontrolleret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår. Om muligt overvåges for, om en fejl er ved at opstå, for at kunne handle proaktivt. Alarmer sker igennem en overvågningsskærm, der er monteret i projekt- og driftsafdelingen. Kritiske alarmer afgives også pr. mail og sms. Der indmeldes statusrapporter pr. mail fra forskellige systemer. Nogle dagligt – andre når der opstår en hændelse i systemet. Driftsvagten har til ansvar dagligt at kontrollere disse mails.	Vi har: • forespurgt ledelsen om de procederer/ kontrolaktiviteter, der udføres. • påset, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for samtlige medarbejdere. • påset, at der afgives alarmer pr. mail og sms ved opståede fejl. • gennemgået statusrapporter • påset, at der er etableret en driftsvagt, samt at denne tjekker rapporter dagligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Styring af driftssoftware samt Sårbarhedsstyring At sikre der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.		
Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i Frontsafe A/S. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til Frontsafe A/S' produktionsmiljøer • at ændringer til driftsmiljøer i Frontsafe A/S følger de gældende retningslinjer, herunder at registreringer og dokumentation af ændringsanmodninger foretages korrekt. Vi har stikprøvevist inspiceret, at styresystemerne er opdateret efter gældende procedurer samt at status herpå registreres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgange og processer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i Frontsafe A/S. Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til produktionsmiljøerne, herunder at krav til change management kontroller sikrer: • at der sker registrering og beskrivelse af ændringsanmodninger • at alle ændringer er underlagt formel godkendelse inden idriftsætning • at ændringer er underlagt formelle konsekvensvurderinger • at der beskrives fall-back planer • at der sker identifikation af systemer der påvirkes af ændringer • at der sker en dokumenteret test af ændringer inden idriftsætning • at dokumentationen opdateres så den i al væsentlighed afspejler de påførte ændringer • at procedurer er underlagt styring og koordination i et "change board".	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttelse af informationsbehandlingsfaciliteter.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • er etableret et ansvar for procedurer for styring af netværksudstyr • funktionsadskillelse • procedurer og ansvar for styring af netværksudstyr inkl. fjernarbejdspladser • de fornødne lognings- og overvågningsprocedurer skal være etableret • styringen af virksomhedens netværk skal koordineres for at sikre en optimal udnyttelse og et sammenhængende sikkerhedsniveau.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevist inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

At opnå at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.	Vi har forespurgt ledelsen, om der er etableret procedurer for rapportering af sikkerhedshændelser. Vi har kontrolleret, at der er udarbejdet procedurer og forretningsgange for rapportering og behandling af sikkerhedshændelser, samt at rapporteringen tilgår de rette steder i organisationen jf. retningslinjer. Vi har kontrolleret, at ansvaret for håndteringen af kritiske hændelser er klart placeret, og at de tilhørende forretningsgange sikrer, at der sker en hurtig, effektiv og metodisk håndtering af et brud på sikkerhed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse.	Vi har forespurgt ledelsen, om der er udarbejdet beredskabsstyring for Cloud backup ydelser i Frontsafe A/S. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring. • at der er udarbejdet og implementeret beredskabsplaner. • at planerne har et tværorganisatorisk beredskabsstyring. • at planerne indeholder passende strategi og procedurer for kommunikation med Frontsafe A/S' interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Vi har ikke ved vores test konstateret væsentlige afvigelser