OKTOBER 2018

FRONTSAFE A/S

CVR-nummer 29631123

ISAE 3402 TYPE 2 ERKLÆRING

Revisors erklæring vedrørende afdækning af de tekniske og organisatoriske sikringsforanstaltninger i tilknytning til driften af Cloud backup-ydelser.

Herudover er der tilført en kontrolbeskrivelse vedrørende databeskyt-elsesforordningen og Frontsafe A/S' rolle som databehandler.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR-nr. 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af de tekniske og organisatoriske sikringsforanstaltninger for driften af Cloud backup-ydelser.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af de tekniske og organisatoriske sikringsforanstaltninger, deres udformning og funktionalitet.

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

KAPITEL 1:

Ledelseserklæring

Beskrivelsen af Frontsafe A/S' tekniske og organisatoriske sikringsforanstaltninger samt rollen som databehandler i kapitel 2 er udarbejdet til brug for kunder, der har anvendt eller påtænker at anvende Frontsafe A/S' 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 A/S' Cloud backup-ydelsers tekniske og organisatoriske sikringsforanstaltninger i hele perioden 1. oktober 2017 - 30. september 2018. 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 tekniske og organisatoriske sikringsforanstaltninger
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, 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 tekniske og organisatoriske sikringsforanstaltninger

(ii) indeholder relevante oplysninger om ændringer i Frontsafe A/S' tekniske og organisatoriske sikringsforanstaltninger foretaget i perioden 1. oktober 2017 - 30. september 2018

(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. oktober 2017 - 30. september 2018. 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. oktober 2017 - 30. september 2018

(C) Den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af Frontsafe A/S' standardaftale, grundlaget for Cloud backup-ydelser og ydelser omkring de tekniske og organisatoriske sikringsforanstaltninger. 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

Høje Taastrup, den 26. oktober 2018

Einar Boije, General Manager

Reda Al Karabalaie, Technical Partner Manager

KAPITEL 2:

Beskrivelse af de tekniske og organisatoriske sikringsforanstaltninger 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 hos serviceleverandører.

Beskrivelsen giver derudover en afdækning af de tekniske og organisatoriske sikringsforanstaltninger, som er impliceret i forbindelse af driften af Cloud backup-ydelser.

Som supplement til nedenstående beskrivelse er der tilføjet et selvstændigt afsnit (Overensstemmelse med rollen som databehandler) med beskrivelse af centrale krav i forbindelse med rollen som databehandler, kombineret med generelle krav fra databehandleraftaler.

Beskrivelsen giver herudover information om de kontroller, der er anvendt for driften i Frontsafe A/S' Cloud backup-ydelser backup i perioden 1. oktober 2017 - 30. september 2018.

Beskrivelse af Frontsafe A/S og omfang af ydelser

Frontsafe A/S er en del af j2 Global, som er en af verdens største serviceleverandører indenfor Cloud backup. Der er fortsat dansk support, drift og salg med fokus på opbygning af en velfungerende partner strategi.

Frontsafe A/S har hovedsæde i Taastrup og datacentre placeret i Viby J.

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 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 backup-relaterede services, herunder 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 7 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%
2016: 10,08%
2017: 16,80%

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 virksomheder til en optimal 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 sikringssikringsforanstaltninger hos Frontsafe A/S fremgår af bilag 1 til denne beskrivelse.

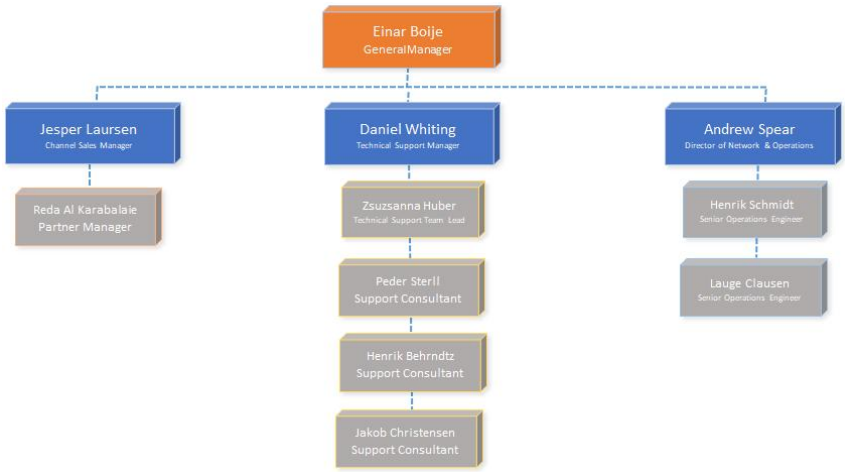
Frontsafe A/S' organisation og organisering af it-sikkerheden

j2 Global er børsnoteret på den amerikanske NASDAQ børs og blev etableret i 1995 med fokus på forretningskritisk teknologi og beskæftiger mere end 2.000 medarbejdere.
j2 Global servicerer +11 millioner tilfredse kunder over 6 kontinenter.

Frontsafe A/S beskæftiger 9 medarbejdere og har en flad organisationsstruktur.

It-sikkerhedsansvarlig: Network & Operations Director

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. Tilgangen hertil er meget uformel. Den uformelle 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 håndteringen ligger hos General Manager 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

Det er Network & Operations Director, der har det daglige ansvar for it-sikkerhed, med opbakning fra ledelsen, 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.

HR, medarbejdere og uddannelse

Alle medarbejdere skal ved ansættelsens start sikkerhedsgodkendes og bliver baggrundschecket i forhold til bl.a. ren straffeattest. De skal underskrive j2 Global's sikkerhedspolitikker og "Business code of ethics", derudover bliver Frontsafe's lokale informationssikkerhed gennemgået, herunder fortrolighed omkring kunder og partnere.

Alle medarbejdere skal kende deres ansvar og rolle i forbindelse med IT-sikkerhed for at minimere risikoen for menneskelige fejl som tyveri, svindel og misbrug af informationsaktiver.

Frontsafe A/S er Certificeret IBM Partner med kompetencer på IBM Spectrum Protect og er derudover 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' backup-anlæg er placeret i et sikkert og ISAE 3402-revisorerklæret datacenter med følgende sikringsforanstaltninger baseret på ISO 27002-2013 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

For nuværende tilbyder Frontsafe A/S følgende backup-services:

1. Cloud backup
   Data sendes direkte til Frontsafe's IBM Spectrum Protect backup servere og storage. Derefter bliver kundens data kopieret til Frontsafe's secondary datastore, som har en anden fysisk lokation.
   Med Cloud backup-løsning har kunden 2 offsite-kopier af sine data.

2. Hybrid backup
   Ved at vælge denne løsning, har kunden en lokal kopi og en offsite kopi af sine backup-data.
   a. Kunden har en lokal IBM Spectrum Protect server, som er en Front-Server. Denne Front-Server synkroniserer sin backup-storage med datalagret på Frontsafe's backup-servere.
   b. Kunden har en lokal Veeam backup-løsning, som sender en offsite-kopi af sit backup lager til Frontsafe's storage-lager.

3. Veeam Cloud Connect (Repository backup)
   Ydelsen omfatter muligheden for at gemme ekstra kopier af sin Veeam backup i Frontsafe's datacenter, hvor man til enhver tid kan genskabe data.

Backup hos Frontsafe A/S opbevares i danske datacentre, som er sikret fysisk og elektronisk (beskrevet i kontrolmål 9-13).

Formålet med backup er at sikre, at kundens data i Frontsafe A/S' datacenter kan genskabes, nøjagtigt og hurtigt.

Alle data sikres dagligt i andet geografisk placeret datacenter.

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 "Frontsafe outage". 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, samt en uddybende fejlbeskrivelse.

Ved totalskade på et af serverrummene er der udarbejdet en plan for, hvad der skal ske, herunder re-etablering af hardware. Herefter vil systemerne kunne gendannes fra backup-server.

Hver 12. måned gennemføres skrivebordstest af Frontsafe katastrofeplan.

Overensstemmelse med rollen som databehandler

Det er ledelsen hos Frontsafe A/S' der er ansvarlig for at sikre, at alle relevante juridiske og kontraktuelle krav er identificeret og korrekt overholdt. Relevante krav kan fx være:

- EU's Persondataforordning
- Dansk lov om Databeskyttelse
- Databehandleraftaler
- Frontsafe A/S Service Level Agreement
- Frontsafe A/S standardkontrakt eller andre relevante kilder

Tilstedeværelsen af alle nødvendige aftaler samt andre relevante dokumenter sikrer overholdelsen af relevante juridiske og kontraktuelle krav.

Frontsafe A/S er forpligtet til at inddrage juridiske eksperter efter behov for at sikre et passende niveau i forhold til overholdelsen af lovgivningen.

Desuden gennemgår Frontsafe A/S' Compliance Manager regelmæssigt alle Frontsafe A/S' sikkerheds-politikker, evt. med inddragelse af relevante interessenter. Frontsafe A/S' sikkerhedspolitikker revideres regelmæssigt af en uvildig, ekstern part, og revisionsrapporten deles ved efterspørgsel med alle Frontsafe A/S' kunder.

EU Databeskyttelsesforordningen (GDPR)

Frontsafe A/S' backup-services understøtter kundernes arbejdsprocesser. Frontsafe A/S ejer ikke de data, kunderne indsamler, men udvikler og driver de it-services, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er Frontsafe A/S databehandler, og kunden er dataansvarlig.

Frontsafe A/S samarbejder med juridiske eksperter med henblik på at sikre, at alle relevante juridiske krav er identificeret og imødekommet. Frontsafe A/S har også sørget for at have relevante kontrakter med alle nøgleinteressenter (herunder kunder, samarbejdspartnere, nøgleleverandører osv.) med henblik på at sikre overholdelse af loven. Desuden samarbejder Frontsafe A/S med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.

Ifølge GDPR sikrer arbejdsrammen fra ISO 27001-standarden et passende informationssikkerheds-niveau. Udover at overholde de relevante ISO-krav, sikrer Frontsafe A/S data privacy og –sikkerhed på et kontraktuelt niveau.

Privatliv og beskyttelse af personoplysninger

Som nævnt er Frontsafe A/S databehandler for sine kunder, i og med, at kunderne tilbydes en backup-service, hvortil de kan overføres data. Frontsafe A/S er ikke ansvarlig for nogen af de data, som kunderne uploader til deres backup-service. Med udgangspunkt i kategorier af fortrolighed af de data, kunden overlader til databehandlingen, skal Frontsafe A/S iværksætte alle nødvendige sikringsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Nedenfor beskrives Frontsafe A/S' procedurer for, hvordan Frontsafe A/S som databehandler opererer under instrukser fra de dataansvarlige.

Databehandleraftaler

Frontsafe A/S indgår databehandleraftaler med alle sine kunder. Databehandleraftalen er en fastlagt procedure ved kontraktindgåelse, og der benyttes enten Frontsafe A/S' egen skabelon eller kundens skabelon. Disse aftaler beskriver Frontsafe A/S' rolle og ansvar som databehandler.

Som databehandler pålægges Frontsafe A/S' et særligt ansvar defineret i Persondataforordningen, udmøntet som krav i en databehandleraftale. Frontsafe A/S skal blandt andet:

- Føre fortegnelse over, hvilke kategorier af persondata der behandles i de respektive it-services.
- Beskrive de tekniske og organisatoriske sikringsforanstaltninger, som er iværksat med henblik på at værne om persondata.
- Bidrage til at opfylde kundens forpligtelser vedr. den registreredes rettigheder (jf. kapitel 3 i EU Persondataforordningen).
- Stille ekspertise til rådighed for kunden for at sikre efterlevelse af Artikel 32 – 34.
    - Artikel 32 – behandlingssikkerhed
    - Artikel 33 – Anmeldelse af brud på persondatasikkerheden

- Artikel 34 – Underretning om brud på persondatasikkerheden for de registrerede
- Iagttage kundens krav vedr. overførsel af persondata uden for EEA.
- Navn og kontaktinformation på leverandører, der er underdatabehandlere.
- Sikre, at krav vedr. persondatabehandling fra kunden matcher krav til en underdatabehandler.

Efter anmodning fra kunden skal Frontsafe A/S til enhver tid formidle denne liste til kunden eller til Datatilsynet.

Formålsbestemthed og hjemmel

Som databehandler arbejder Frontsafe A/S med persondata på baggrund af instrukser fra kunderne, der beskriver en formålsafgrænsning for, hvad data må benyttes til. Frontsafe A/S er således ansvarlig for, at data indsamlet med ét formål ikke behandles i strid med dette.

Hjemmelen for behandling af persondata i Frontsafe A/S' udbudte Cloud backup-ydelser, skal søges i den dataansvarliges overholdelse af retlig forpligtigelse eller opfyldelse af kontraktligt forhold. (GDPR Art. 6 L b og c).

Adgang til kundedata

Frontsafe A/S tilbyder løsninger som Cloud backup-ydelser, der driftes af Frontsafe A/S's driftsafdeling. Frontsafe påtager dermed det fulde ansvar for behandling af kunders data. Generelt har medarbejdere i Frontsafe A/S ikke adgang til kundedata, medmindre specifikke arbejdsopgaver taler herfor.

Frontsafe A/S har indført principper for medarbejderes adgang til og arbejde med kunders data:

- Det er kun betroede medarbejdere, der har adgang til kundedata, ud fra et arbejdsbetinget behov.
- Omfattende introduktionsforløb med fokus på regler for omgang med kundedata og opfølgning via awarenes-kampagner.
- Procedure for tildeling og revision og kontrol af adgange til kundedata.
- Regler for behandling af kundedata i Frontsafe A/S' ISMS.

Frontsafe A/S logger og overvåger adgangen til kundernes data for at sikre, at ingen uautoriserede personer får adgang, eller tildelte adgange misbruges.

Væsentlige ændringer i forhold til it-sikkerhed

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

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver den generelle ramme for Frontsafe A/S' Cloud backup-ydelser, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Frontsafe A/S 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-ydelser. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål. I forbindelse med håndteringen af password-sikkerheden er revisionen udført ud fra et generelt perspektiv.

For nogle virksomheder kan sikkerheden omkring password-opbygningen ligge under rammen, såfremt ledelsen hos kunden har ønsket det. Ansvaret for afstemning af kontrolmiljøet for password-sikkerheden ligger hos den enkelte brugervirksomhed, og hos dem som anvender denne erklæring.

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

BILAG 1:

Frontsafe A/S har arbejdet med følgende kontrolmål og sikringsforanstaltninger fra ISO27002:2013

5. Informationssikkerhedspolitik
- 5.1. Retningslinjer for styring af informationssikkerhed

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

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

8. Styring af aktiver
- 8.1. Ansvar for aktiver
- 8.3. Mediehåndtering

9. Adgangsstyring
- 9.1. Forretningsmæssige krav til adgangsstyring
- 9.2. Administration af brugeradgang
- 9.3. Brugernes ansvar

11. Fysisk sikkerhed og miljøsikring

(Ikke omfattet af revisionserklæringen)
- 11.1. Sikre områder
- 11.2. Udstyr

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

13. Kommunikationssikkerhed
- 13.1. Styring af netværkssikkerhed

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

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

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

18. Overensstemmelse
- 18.1. Overensstemmelse med lov- og kontraktkrav

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af de tekniske og organisatoriske sikringsforanstaltninger, deres udformning og funktionalitet

Til kunder af Frontsafe A/S' Cloud backup-ydelser og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Frontsafe A/S' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af de tekniske og organisatoriske sikringsforanstaltninger, som udføres i forbindelse med driften af Frontsafe A/S' Cloud backup-ydelser til behandling af kunders transaktioner i perioden 1. oktober 2017 - 30. september 2018, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. Frontsafe A/S anvender eksterne samarbejdspartnere på følgende områder:

- Co-location/ datacenter – den fysiske sikkerhed omkring produktionsudstyr.

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.

Beierholms uafhængighed og kvalitetsstyring

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

Vi 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.

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 væsentlige 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 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 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 Beierholm' 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 Frontsafe A/S' tekniske og organisatoriske sikringsforanstaltninger til Cloud backup-ydelser, således som de var udformet og implementeret i hele perioden 1. oktober 2017 - 30. september 2018, 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. oktober 2017 - 30. september 2018, 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. oktober 2017 - 30. september 2018.

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.

Søborg, den 26. oktober 2018

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 ISAE 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.

Hvad angår periode har vi i vores test forholdt os til, om Frontsafe A/S har levet op til kontrolmålene i perioden 1. oktober 2017 - 30. september 2018.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som Frontsafe A/S jf. sin dokumentation har iværksat for at leve op til kravene
- Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet
- Tredje kolonne viser resultatet af vores test.

De udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne 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.
Forespørgsler	Forespørgsel til passende personale hos Frontsafe A/S. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

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 iht. 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 at 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.

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 organisationen 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 håndteringen af sikkerhedsforholdene er passende.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevist 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 sikringsforanstaltninger, således at området er afdækket i forhold til risikovurderingen for området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Det 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 bekendt 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 backupydelser 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 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 A/S' 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 hosting-center 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 A/S' drift af Cloud backup-ydelser. Vi har kontrolleret, at kontrakter og SLA anvendes som et centralt værktøj til at sikre definition, adskillelse og afgrænsning mellem Frontsafe A/S' ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data. Derved påhviler der typisk kunden et eget ansvar med 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 A/S' 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 af brugeradgang er implementeret i Frontsafe A/S' 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 standardpassword.	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. • at standardpassword ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standardpassword.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 12:

Driftsikkerhed

Kontrolmål: Driftsprocedurer 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 driftsafviklingsprocedurer 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 stikprøvevist 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 sikringsforanstaltninger 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 kontrolsikringsforanstaltninger, 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. • stikprøvevist gennemgået backuplog, til bekræftelse af, at backup er gennemført succesfuldt, og at tilfælde af mislykket 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. • stikprøvevist 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 procedurer/ 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, at 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 change 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 styresystemer 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 patch 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 sikre beskyttelse 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. Produktionsmiljøet skal være sikret mod forsyningssvigt i forhold til redundans til netværksforbindelse til internettet. Netværkstrafikken/ adgange fra produktionsmiljøet ud til omverdenen kan opnås ved hjælp af flere forsyningsindgange eller adgang fra mere end ét forsyningsselskab.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • Der er etableret passende procedurer for styring af netværksudstyr. • Der er funktionsadskillelse mellem brugerfunktioner. • Der er etableret passende procedurer og løbende opfølgning på logs og overvågning. • Styring af virksomhedens netværk er koordineret for at sikre en optimal udnyttelse af ressourcer og et sammenhængende sikkerhedsniveau. • Påset, at der er etableret forbindelser for datakommunikation mod internettet via mere end én ISP-leverandør. • Stikprøvevist gennemgået dokumentationen fra leverandøren i forhold til skriftligt aftalegrundlag samt løbende afregning af ydelser hos ISP-leverandøren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal være etableret passende forretningsgange for håndtering af trusler i form af angreb fra internettet (cyber-angreb). I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.	Det er kontrolleret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for håndtering af cyber-angreb. • at der er udarbejdet og implementeret planer for håndtering af truslen. • at planerne har et tværorganisatorisk samarbejde mellem interne grupper.	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.
Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende anerkendte leverandører.	Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere. Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører. Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal udføres regelmæssig overvågning, herunder føres tilsyn med eksterne samarbejdspartnere.	Vi har påset, at findes passende processer og procedurer for løbende overvågning af eksterne leverandører. Vi har kontrolleret, at der udføres løbende tilsyn gennem uafhængig revisors rapporter.	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 brud på sikkerheden.	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

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Principper for behandling af personoplysninger:

Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme i form af standardkontrakter, Service Level Agreement samt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, der indeholder krav til lovlig behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Databehandler:

Der efterleves procedurer og kontroller, som sikrer, at databehandlerens tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Den foreligger instruks for behandling og beskyttelse af personoplysninger hos databehandleren, herunder behandling hos andre anvendte databehandlere.	Vi har kontrolleret, at der forligger dokumentation for, at den dataansvarlige har givet databehandleren instruks for behandling og beskyttelse af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Fortegnelse over behandlingsaktiviteter:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over den behandling af personoplysninger, som er under databehandlerens ansvar.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der skal foreligge en fortegnelse over behandlingsaktiviteterne for den enkelte backup løsning kombineret med en tilhørende dataansvarlig.	Vi har kontrolleret dokumentationen for, at der foreligger en fortegnelse over behandlingsaktiviteterne for den enkelte backup-løsning sammenstillet med en dataansvarlig.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der foretages løbende – og mindst en gang årligt – vurdering af, hvorvidt fortegnelsen er opdateret og korrekt.	Vi har kontrolleret dokumentationen for, at fortegnelsen over behandlingsaktiviteterne for den enkelte dataansvarlige er opdateret og korrekt.	Ikke relevant på nuværende tidspunkt.

Databehandlers ansvar:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retlig bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af en databehandler, som er godkendt af den dataansvarlige.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Den dataansvarlige har givet instruks for behandling og beskyttelse af personoplysninger hos databehandleren, herunder behandling hos andre anvendte databehandlere.	Vi har kontrolleret dokumentationen for, at den dataansvarlige har givet databehandleren instruks for behandling og beskyttelse af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Den dataansvarlige har godkendt de af databehandler givne garantier for, at procedurer, tekniske foranstaltninger og kontroller opfylder kravene i forordningen.	Vi har kontrolleret dokumentationen for, at den dataansvarlige har godkendt de af databehandleren godkendte garantier for, at procedurer, tekniske foranstaltninger og kontroller opfylder kravene i forordningen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Den dataansvarlige har godkendt databehandlers anvendelse af andre databehandlere, der er anvendt som underleverandører. Der gennemføres kontrol af behandling hos databehandlere, der er anvendt som underleverandører.	Vi har kontrolleret dokumentationen for, at den dataansvarlige har godkendt anvendelsen af andre databehandlere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden:

Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden, samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.

Frontsafe A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som opdateres mindst en gang årligt, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for håndtering af brud på persondatasikkerheden, herunder at rettidig kommunikation til den dataansvarlige er beskrevet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandler sikrer registrering af alle brud på persondatasikkerheden.	Vi har kontrolleret dokumentationen for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har kontrolleret dokumentationen for, at ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har ikke ved vores test konstateret væsentlige afvigelser.