Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med hostingydelser i perioden 01-02-2018 til 31-01-2019

ISAE 3402-II

Sotea A/S

CVR-nr.: 10 08 52 25

Juni 2019

Indholdsfortegnelse

Afsnit 1: Sotea A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Sotea A/S' hostingydelser, 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 kundernes regnskaber. Sotea A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Sotea A/S' hostingydelser til kunder i hele perioden fra 01-02-2018 til 31-01-2019. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan systemet 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 at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- Relevante kontrolmål og kontroller, udformet til at nå disse mål
- Kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificerede 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 behandlingen og rapporteringen af kunders transaktioner.

(ii) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 01-02-2018 til 31-01-2019

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra 01-02-2018 til 31-01-2019. Kriterierne for denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificerede

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 01-02-2018 til 31-01-2019.

Silkeborg, 21. juni 2019
Sotea A/S

Jess Teilmann
Adm. direktør

Afsnit 2: Sotea A/S' beskrivelse af kontroller i forbindelse med drift af deres hostingydelser

SOTEA har det totale ansvar for drift af IT systemer for både danske og udenlandske virksomheder, og vores sikkerhed er derfor vedvarende i fokus. "SOTEA sikkerhedspolitik" beskriver de krav vi stiller til vores driftsmiljø, herunder de fysiske forhold, organisationen og diverse procedurer. Nærværende beskriver SOTEA's generelle forhold, og ikke specifikt på vores enkelte kunder.

1 Virksomheden og vores ydelser

1.1 Virksomheden

SOTEA blev etableret i 2000, af Bo Jensen og Jess Munch Teilmann, hvor vores primære forretning var udvikling af ERP systemer til hvidevarer- og tekstilbranchen. I 2005 begyndte vi at hoste IT, og hosting er i dag vores kerneforretning. I 2009 byggede vi vores eget datacenter, placeret ved Ferskvandscentret i Silkeborg.

Vi beskæftiger pt. 22 medarbejdere, og har præsteret løbende vækst på mere end 25% årligt de sidste 6 år. Vi er, som medlemmer af Microsoft Hosting Community, blandt de førende hostere i Danmark, af Microsoft produkter og services. Vi er Microsoft Silver Partner, hvilket er garanti for at vi har nødvendige kompetencer i drift af Microsoft produkter. Vi er som medlemmer af BFIH, underlagt krav om at levere en høj kvalitet af hosting.

SOTEA har fokus på at levere Overskuelig IT til danske og internationale virksomheder. Vores DNA er, IT i øjenhøjde, vores mål er at gøre det komplekse enkelt for vores kunder. Vi har en simpel gennemskuelig afregningsmodel, som består af 4 elementer:

- Antal Virtuelle Servere
- Antal Brugere
- Antal Licenser
- Datamængder

Ovenstående enkle model danner grundlag for hvad kunden skal betale pr. måned alt inklusive, og uden ekstraregninger.

Derudover er vi unikke i markedet med vores 3 garantier:

PRIS GARANTI: SOTEA garanterer en fast månedlig pris uden ekstraregninger, og uforudsete udgifter. Tværtimod optimerer vi løbende din IT drift med henblik på besparelser, og forbedringer.

LEVERINGS GARANTI: SOTEA's tilbud på implementering er en fast pris på den endelige levering – uanset det aktuelle timeforbrug.

KVALITETS GARANTI: Kunden betaler ikke en øre, før kunden har gennemtestet vores løsning i et parallelt miljø, og er fuldt tilfreds med kvaliteten. Hvis vi mod forventning ikke lever op til kundens krav, kan aftalen annulleres inden endelig flytning, og uden omkostninger for kunden.

Vi udvikler forsat vores virksomhed, men én ting ændrer sig aldrig: At SOTEA altid vil levere løsninger der er brugbare, overskuelige og udviklet på brugernes præmisser.

1.2 Ydelser:

Vi har som udgangspunkt et produkt, og det er en fuldt hostet løsning hvor SOTEA ejer hardware og software, og kunder lejer sig ind på vores platform på abonnementsbasis. Derudover udbyder vi Microsoft cloud services, herunder Office 365 og Azure.

Vores primære ydelser, som er omfattet af nærværende erklæringer:

1.2.1 *IT Hosting*

Med en hosting aftale hos SOTEA betaler kunden et fast månedligt abonnement. Vores hosting aftale er fuldt dynamisk, og kan ændres efter behov med måneds varsel. Der er altid adgang til sidste nye version af softwaren, som en del af aftalen. Derudover sørger SOTEA for at servere er sikkerhedsopdaterede, samt varetager den løbende drift, også som en fast del af aftalen.

1.2.2 *Kompromisløs Support*

Alle vores aftaler er inklusive Kompromisløs Support, hvor alle slutbrugere må ringe/maile direkte til vores support – uden at det koster ekstra. Lige fra printproblemer, over nulstilling af password, til oprettelse af SQL-databaser. Selv support af tredje parts programmer håndterer vores supportere, og hvis nødvendigt kontakter vi leverandøren for kunden, og får løst problemerne hurtigt.

1.2.3 *Løbende Optimering*

SOTEA giver dig et komplet overblik over din aftale hvert kvartal, sammen med din faktura, hvor kunden kan se hvad der betales for.

2 Organisation og ansvar

Direktionen: Direktionen har det overordnede ansvar for IT sikkerheden i SOTEA, og gennemgår denne 1 gang om året, i november måned.

Ledergruppe: SOTEA's ledelse har det strategiske ansvar for SOTEA's vækst og videre udvikling, samt ansvaret for den daglige ledelse.

Presales: Presales har ansvaret for at flytte nye kunder ind i vores hosting miljø. De har ansvaret fra kontrakten er underskrevet, og til kunden er i produktion. Refererer til vores Adm. Direktør.

Aftersales: Når kunden er implementeret, og gået i produktion, overtages kunden af aftersales, som er vores support funktion. Alle sager registreres i vores ticket system, og håndteres af vores first level support, og eskaleres til second level support/driftsafdelingen, hvis first level support ikke kan løse opgaven. Derudover bidrager supporten i presales ved implementering af nye kunder, alt efter behov. Refererer til vores Adm. Direktør.

Drift: Har det overordnede ansvar for overvågning og drift af vores hosting miljø/Datacenter, Driftsafdelingen fungerer også som second level og third level support, samt bistår med implementering af nye kunder. Referere til vores Tekniske Chef.

Sikkerhedsgruppe: Der er nedsat en sikkerhedsgruppe. Dette udvalg har ansvaret for at udarbejde SOTEA's IT sikkerhed, i forhold til dokumentation og implementering af procedurer.

3 Generelt om vores kontrolmål og implementering

Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om, at levere stabil, overskuelig, og sikker it-drift til vores kunder. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartet og gennemsigtig.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer nævnt under afsnit 1.2. Ydelser.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 (Regelsæt for styring af informationssikkerhed).

4 Risikovurdering og –håndtering

4.1 It-risikoanalyse (bevis)

4.1.1. Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores IT Hosting – Kompromisløs Support – Løbende Optimering. Dermed kan vi sikre, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau.

4.1.2. Der holdes et årligt review møde, hvor der foretages en risikovurdering jf. nedenstående punkt 4.2. Håndtering af sikkerhedsrisici. Efter dette møde foreligger der et skriftligt referat, som indeholder eventuelle ændringer i risikovurderingen, samt en handlingsplan for yderligere aktivitet.

Derudover holdes der ½ årlige møde i sikkerhedsgruppen, hvor aktuelle og nye risici drøftes.

4.2 Procedure for risikohåndtering

Vi har udarbejdet faste procedurer for behandling af risici, hvor der årligt afholdes en generel risikovurdering.

Derudover er der en procedure for risikohåndtering/håndtering af sikkerhedshændelser, hvor risici kommunikeres til vores Tekniske Chef, eller Adm. Direktør, der indledningsvis tager stilling til risikoens omfang, og vurderer om der skal reageres øjeblikkelig, eller om det noteres til behandling på kommende ½ årlige møde i sikkerhedsgruppen.

5 Sikkerhedspolitik

5.1 Målsætning/formål

5.1.2 **TILGÆNGELIGHED**
Opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab.

5.1.3 **INTEGRITET**
Opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer.

5.1.4 **FORTROLIGHED**
Opnå fortrolig behandling, transmission og opbevaring af data.

5.1.5 **AUTENTICITET**
Opnå en gensidig sikkerhed omkring de involverede parter.

5.1.6 **UAFVISELIGHED**
Opnå en sikkerhed for gensidig og dokumenterbar kontakt.

5.2 Omfang

5.2.1. En informationssikkerhedspolitik, der godkendes af ledelsen.
5.2.2. En driftshåndbog, der uddyber informationssikkerhedspolitikken.
5.2.3. Sikkerhedsinstrukser og –procedurer, som formuleres af respektive ejere ud fra krav og retningslinjer i driftshåndbogen
5.2.4. ISAE 3402 erklæring fra REVI-IT.

5.3 Gyldighedsområde

5.3.1. Politikken er gældende for alle SOTEA's it relaterede aktiviteter, nævnt under punkt 1.2. Ydelser.
5.3.2. Data, programmer og informationer

5.4 Organisation og ansvar:

Der er nedsat en sikkerhedsgruppe, som har ansvaret for at udarbejde SOTEA's IT sikkerhed, i forhold til dokumentation og implementering af procedurer.

5.5 Beredskabsplanlægning:

5.3.3. Skadebegrænsende tiltag
5.3.4. Etablering af temporære nødløsninger
5.3.5. Genetablering af permanent løsning
Se Kapitel 14. Beredskabsstyring

5.6 Sanktioner:

Medarbejdere, der bryder de gældende informationssikkerhedsbestemmelser i SOTEA, kan straffes disciplinært. De nærmere regler om dette fastsættes i overensstemmelse med den gældende personalepolitik under afsnittet "Misligholdelse".

6 Organisering af informationssikkerhed

6.1 Intern organisering

6.1.1. Delegering af ansvar for informationssikkerhed

Det er SOTEA's Adm. Direktør der har det overordnede ansvar for sikkerhedspolitikken, og herunder politikker og procedurer, og den Adm. Direktør der godkender opdateringer og tilføjelser hertil.

Der foretages årligt review af sikkerhedspolitikken, og herunder politikker og procedurer.

6.1.2. Funktionsadskillelse
Vores dokumentationer og processer generelt sikrer, at vi udelukker eller minimere nøgleperson-afhængighed.

Funktionsadskillelse er en vigtig del af vores organisation og drift, hvorfor vi, via adgangskontroller og rettighedsstyring, sikrer, at kun autoriseret personale kan udføre de nødvendige handlinger på systemer og data.

6.1.3. Informationssikkerhed som en del af projektstyring

Vi tager stilling til it-sikkerhed i vores It projekter, både i forhold til kunde projekter og interne projekter. Alle projekter/projektforløb findes i SharePoint under "Project".

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1. Politik for mobile enheder

Vi sikrer, i bedst muligt omfang, vores medarbejderes bærbare udstyr såsom bærbare pc, PDA, mobiltelefon og lign. Dog er ingen medarbejderes udstyr koblet i domæne, så alt adgang foregår via Fjern Skrivebord/RDP, så der vil aldrig ligge vitale data på deres PC'ere, PDA eller mobiltelefoner, udover mail.

Vi har åbnet adgang til, at vi og vores kunder kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Ud over kode, har vi ikke implementeret andre sikkerhedsforanstaltninger til sikring af disse enheder og disses brugeradgange.

6.2.2. Fjernarbejdsplads

Adgang til vores netværk og dermed potentielt til systemer og data, sker kun for autoriserede personer.

Hjemmearbejdsplads for vores medarbejdere er sikret via krypteret TSG-forbindelse, hvor bruger skal have bruger-id og password for at logge på.

7 Sikkerhed i forhold til HR

Alle ansatte, uanset funktion, er i det følgende benævnt medarbejder, og er sammen med SOTEA's ydelser og service, SOTEA's største aktiver.

De gældende regler for SOTEA's medarbejdere er angivet i Personalehåndbogen.

For at bevare og udbygge sikkerheden omkring SOTEA's informationsaktiver er det vigtigt, at der er fokus på informationssikkerhed under alle ansættelsesforløbets faser.

7.1 Inden ansættelsen

7.1.1. Screening

7.1.1.1. Der skal, i ansættelseskontrakten, tydeligt angives Stillings- og funktionsbeskrivelse, samt eventuelle særlige sikkerhedsmæssige opgaver og ansvar.

7.1.1.2. Under ansættelsesinterview skal ansøgeren informeres om hvilke sikkerhedsmæssige krav ansættelsesforholdet indebærer.

7.1.1.3. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.

7.1.1.4. Der indhentes ren straffeattest.

7.1.2. Ansættelsesforhold

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.

7.2 Under ansættelse

7.2.1. Ledelsens ansvar

I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. Ligeledes er det klart defineret som en del af kontraktmaterialet, hvad den ansattes ansvar og rolle er.

I forbindelse med anvendelse af eksterne leverandører, som har adgang til vores systemer, sikrer vi at der indgås fortrolighedsaftaler.

7.2.2. Bevidsthed om, uddannelse og træning i informationssikkerhed

Vores aktiver er i høj grad vores medarbejdere, og vi sikrer at vores medarbejdere løbende uddan-

nes. Dette foregår ved intern vidensdeling, samt relevante eksterne uddannelser og certificeringer.

Der afholdes årligt, gennemgang af vores sikkerhedspolitik, hvor sikkerhedspolitik fremsendes til relevante medarbejdere, hvorefter denne gennemgås, og medarbejder fremsender efterfølgende mail på bekræftelse af at sikkerhedspolitik er læst og forstået.

Derudover sendes der løbende information omkring trusler, ændringer i vores sikkerhedspolitik, ændringer i vores driftshåndbog, eller sikkerhedsinformationer generelt, på mail, hvor det findes relevant.

7.2.3. Sanktioner

Generelle vilkår for ansættelse er beskrevet i hver medarbejders ansættelseskontrakt. Der er i ansættelseskontrakten henvisning til Personalehåndbogen, hvorunder forhold omkring sanktioner ved evt. sikkerhedsbrud er beskrevet.

7.3 Ophør og ændring i ansættelse

7.3.1. Ophør eller ændringer i ansvarsforhold

Generelle vilkår for ansættelse, herunder forhold omkring ophør, er beskrevet i Soteas driftshåndbog. Ledelsen er ansvarlig for, at medarbejderen er informeret om de gældende regler ved og efter ansættelsesophør.

8 Styring af aktiver

8.1 Ansvar for aktiver

8.1.1 *Fortegnelse over aktiver*

Vores netværk og miljø er komplekst med mange systemer og kunder, og for at sikre mod uvedkommende adgang, og for at sikre gennemskuelighed af opbygningen, har vi udformet en række dokumentation, der beskriver det interne netværk, med enheder, navngivning af enheder, logisk opdeling mv.

8.1.2 *Ejerskab af aktiver*

Vi arbejder i SOTEA med ejerskab over aktiver for at sikre, at ingen enheder, systemer eller data bliver glemt i forhold til sikkerhedsopdateringer, backup, drift og vedligehold.

8.1.3 *Tilbagelevering af aktiver*

Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm., og at den ansattes adgange lukkes og inddrages rettidigt.

Det skal sikres at alle medarbejderens adgangsrettigheder inddrages. Det skal afgøres, om det er nødvendigt at slette disse rettigheder, eller om det blot er tilstrækkeligt at spærre disse. De rettigheder, der skal spærres eller slettes, inkludere fysisk adgang, samt adgang til systemer.

8.2 Dataklassifikation

8.2.1 *Klassifikation af data*

For at kunne prioritere data – f.eks. ved genskabelse, er data klassificeret i typer, vigtigheden samt tilhørsforhold til kunderne eller internt. Klassifikation er beskrevet i driftshåndbogen.

8.2.2 *Mærkning af data*

Der udarbejdes en liste hvor kunder generelt er prioriteret, hvor der kan sættes lighedstegn mellem kundens prioritet og datas prioritet. Denne liste opdateres minimum 1 gang årligt. Systemdata for netværk, dokumentation er prioriteret højst, herunder sikret betryggende. Processen er dokumenteret.

8.2.3 *Håndtering af aktiver*

Vi skal sikre, at vores og vores kunders systemer og data beskyttes. Vi håndterer derfor ikke kunders data på håndbårne medier (USB, CD/DVD, flytbare diske) uden forudgående aftale med kunderne.

8.3 Mediehåndtering

8.3.1 *Styring af bærbare medier*

Vi sikrer, i bedst muligt omfang, vores medarbejderes bærbare udstyr såsom bærbare pc, PDA, mobiltelefon og lign. Dog er ingen medarbejderes udstyr koblet i domæne, så alt adgang foregår via Fjern Skrivebord/RDP, så der vil aldrig ligge vitale data på deres PC'ere, PDA eller mobiltelefoner, udover mail.

Vi anbefaler at der etableres et login på vores bærbare udstyr, samt at der installeres antivirus.

8.3.2 *Bortskaffelse af medier*

Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt. Der er udarbejdet vejledninger som sikrer, at data på medierne ikke kan genskabes.

8.3.3 *Fysiske medier under transport*

Forsendelse af fysiske medier (bånd, diske, CD, DVD og lignende) skal ske med pålidelig og troværdig transportør (herunder UPS, GLS, Budstikken, Post Danmark m.m.). Fortrolige og følsomme data på medierne skal være sikret på bedst mulig måde, ligesom der skal foreligge en sikret backup til beskyttelse imod tab og bortkomst.

9 Adgangskontrol

9.1 Politikker for adgangsstyring

Vi har politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik.

Fysisk adgang:

Adgang til SOTEA kontorlokaler og informationsaktiver, herunder datacentre, kontrolleres og reguleres primært på 2 måder, og det er:

a. **Pinkode:** Alle medarbejdere får udleveret en pinkode til kontoret. Medarbejdere og kunder som skal have adgang til Datacenter, får udleveret pinkode til Datacenter. Pinkode sendes pr. mail personligt til vedkommende der skal bruge den. Pinkoden, der udleveres sammen med en nøgle, er personlig og fortrolig, på samme måde som alle andre passwords, og skal håndteres derefter.
b. **Nøglesystem:** Udlevering og administration af nøgler varetages af den Tekniske Chef. Der udfyldes nøglekvittering ved udlevering.
c. **Logisk adgang:** Logisk adgang til SOTEA systemer sker ved at tilknytte rettigheder til den enkelte konto, der entydigt er udpeget af kombinationen bruger-id og password. Adgang tildeles og administreres af SOTEA support.

Medarbejdere og konti med udvidede adgangsrettigheder, herunder kunder som skal have udvidede rettigheder, oftest systemkonti, skal til stadighed være nøje overvåget, og antallet begrænses til det absolut nødvendige.

Tildeling af udvidede adgangsrettigheder må alene ske ud fra en arbejdsmæssig begrundelse, efter at den nødvendige autorisation foreligger, og der skal til stadighed findes en ajourført fortegnelse over de tildelte rettigheder.

9.1.1 *Adgang til netværk og netværksservices*

Fysisk:
Alle netværksenheder er installeret i aflåste rum i datacenteret, hvor der kun er adgang for SOTEA personale.

Logisk:
Adgang til netværksenheder og administration heraf, kan kun ske fra management netværket. Det er et ikke-routningsnetværk, og der er kun adgang til netværket fra vores overvågningsserver.

9.2 Administration af brugeradgang

9.2.1 *Brugeroprettelses- og nedlæggelsesprocedure*

Vores kunders brugere oprettes/nedlægges alene på baggrund af vores kunders ønsker, og oprettes/nedlægges af vores support. Der skal foreligge mail som dokumentation for oprettelse/nedlæggelse af en bruger for en kunde.

Vores egne brugere oprettes/nedlægges alene på baggrund af autorisation fra vores Tekniske Chef eller Adm. Direktør.

Ved fratrædelse sikrer vores procedurer aflevering af materiel og lukning af medarbejderens konti.

Adgang til systemer og data fjernes alene på baggrund af skriftligt ønske fra kunde, system- eller dataejer.

Alle brugere skal være personhenførbare, dvs. have tydeligt mærke med personnavn. Er der tale om servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon inaktiveret, så vidt det er muligt. Der er dog tilfælde hvor kunder har oprettet konti til deres tredjeparts leverandører, hvor disse brugere har adgang til kundens server, men hvor brugernavn er en generel betegnelse, eller leverandørens navn, da der kan være flere personer fra leverandøren der bruger samme konto, dette grundet kunden afregnes pr. bruger pr. måned.

9.2.2 *Rettighedstildeling*

Tildeling af privilegier, og rettigheder, er kontrolleret i forbindelse med vores normale brugeradministrations proces.

9.2.3 *Kontrol med privilegerede adgangsrettigheder*

Anvendelse af password er kontrolleret via regler implementeret automatisk ved hjælp af GPO og lignende.

9.2.4 *Håndtering af fortrolige logon informationer*

Vores it-sikkerhedspolitik foreskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.

Medarbejdere skriver årligt under på, at de har læst og forstået seneste version af vores sikkerhedspolitik.

Da vi har en del brugere, såsom service accounts og lign., som ikke kan bruges til at logge på med, og af systemmæssige årsager ikke skifter passwords, har vi et system til opbevaring af disse passwords. Kun auto-

riseret personale har adgang til systemet. Krav til disse passwords er højere end vores almindelige password-politik.

9.2.5 *Evaluering af brugeradgangsrettigheder*

Vi har en årlig kontrol af vores AD, hvor interne brugere kontrolleres for privileger m.m.

9.2.6 *Nedlæggelse eller tilpasning af adgangsrettigheder*

Vi har procedurer for nedlæggelse og tilpasning af adgangsrettigheder. Det er kun udvalgte personer hos vores kunder, der kan bede om adgangsrettigheder.

9.3 Brugeransvar

9.3.1 *Brug af fortrolige logon informationer*

Vores it-sikkerhedspolitik foreskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.

Medarbejdere bekræfter en gang årligt, at de har læst og forstået seneste version af vores sikkerhedspolitik.

Da vi har en del brugere, såsom service accounts og lign., som ikke kan bruges til at logge på med, og af systemmæssige årsager ikke skifter passwords, har vi et system til opbevaring af disse passwords. Kun autoriseret personale har adgang til systemet. Krav til disse passwords er højere end vores almindelige password-politik.

9.4 Kontrol af adgang til systemer og data

9.4.1 *Begrænset adgang til data*

Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen.

9.4.2 *Procedurer for sikker logon*

Al adgang til vores systemer foregår via Fjernskrivebord, hvor bruger logger på med personlig brugerkonto og password. Interne password skiftes som minimum hvert ½ år, og vores anbefaling til vores kunder er hver tredje måned.

Interne medarbejdere har alle en administrativ bruger med begrænsede rettigheder, som anvendes i det daglige arbejde. Hvis medarbejder har behov for yderligere rettigheder, er dette på en anden brugerkonto som betegnes admin konto.

9.4.3 *System for administration af adgangskoder*

Alle brugere på tværs af både kundesystemer og egne systemer, har restriktioner omkring adgangskode. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger ift. udformningen af kodeordet.

Koder skal skiftes regelmæssigt, være komplekse, og brugeradgange inaktiveres automatisk hvis brugeren ikke har skiftet kodeordet inden for det definerede tidsrum. Som udgangspunkt skifter vores kunders brugere adgangskode hver tredje måned, dog er der kunder som har ønsket anden frekvens. Interne medarbejdere skal som minimum skifte password hvert ½ år.

Passwords på domænet er kontrolleret via regler defineret i GPO'er.

10 Kryptografi

10.1 Kontrol med anvendelsen af kryptografi

10.1.1 *Politik for anvendelse af kryptografi*

Vi anvender kun standard kryptering, hvor krypteringsnøgler ligger dokumenteret i firewalls og klienter. Vi vurdere der ikke er behov for yderligere dokumentation i forhold til kryptografi.

10.1.2 *Administration af krypteringsnøgler*

Vi anvender kun standard kryptering, hvor krypteringsnøgler ligger dokumenteret i firewalls og klienter. Vi vurdere der ikke er behov for yderligere dokumentation i forhold til kryptografi.

11 Fysisk sikkerhed

11.1 Sikre områder

Datacenteret (DC) ligger i IT-Huset ved Ferskvandscentret (FVC) på adressen Vejlsøvej 51, 8600 Silkeborg. DC ligger i kælderen af IT-Huset og for at få adgang skal der dels bruges dør-kode samt en chip baseret nøgle, der er programmeret specielt til den enkelte bruger. Ved hovedindgangen til IT-huset kræves der adgang kun via førnævnte nøgle. Hovedindgangen er åben på hverdage 07:00-19:00, dørene låses automatisk kl. 19:00 og åbnes igen kl. 7:00. I kælderen er der en dør, der giver adgang til DC yderområder herunder lagerrum/administrationslokale og sanitet samt selve DC. Adgang hertil sker også kun via nøglen. For at komme ind i selve DC indsættes nøglen og hvis den lyser grøn, indtaster man sin personlige kode og låser sig ind.

Alene autoriserede personer får adgang til lokaler via den etablerede procedure.

Skal eksterne personer have adgang til lokalet, er det i følgeskab med en af vores autoriserede medarbejdere, medmindre der er indgået særskilt aftale om selvstændig adgang via nøgle og kode. Eksterne service tekniker vil efter aftale blive låst ind af SOTEA, der også sørger for at der bliver aflåst igen.

Adgang til DC kan kun ske vha. elektronisk kodet nøgle og PIN-kode der er udleveret efter aftale og som kræver underskrift af de enkelte personer. I DC er der monteret tyverialarm, i tilfælde af indbrud alarmeres den private vagtcentral, og vagtcentral ringer til SOTEA medarbejder jf. prioriteret liste udleveret til vagtcentral - der sendes vagt så snart alarm går. Der er ligeledes monteret brandslukningsudstyr/Inergen anlæg, som tilsvarende vores tyverialarm er koblet op på vagtcentral.

Der er andre alarmer i form af fejl på UPS, Køleanlæg og temperatur, hvor der ved fejl sendes SMS til den Tekniske Chef, Direktøren og Driftschefen, samt mail til support@sotea.dk, hvor der automatisk bliver oprettet en ticket på alarmen, som så håndteres af SOTEA support.

Vi anvender til sikring af driftsfaciliteterne køle- og brandanlæg. Disse anlæg testes og serviceres periodisk. Som med tyveri er den private vagtcentral også her tilkoblet og i tilfælde af alarm vil relevante personer hos SOTEA blive notificeret.

11.2 Sikring af udstyr

Vores centrale netværksudstyr samt kundernes servere, som har etableret aftale om placering af udstyr hos os, og andet udstyr er, fysisk placeret i aflåst lokale, som har monteret køling og brandslukning mv.

Til sikring af forsyning af elektricitet til DC i forbindelse med strømudfald er der monteret UPS og diesel generator. Dette setup er anslået til at kunne køre i 6 timer på en fuld tank. En gang i måneden tester vi UPS og generator og en gang årligt udføres der service af ekstern service tekniker.

12 Sikkerhed i forbindelse med drift

12.1 Operationelle procedurer og ansvarsområder

12.1.1 *Dokumenterede driftsprocedurer*

Det er i vores organisation ikke muligt at have 100% overlap på alle opgaver, systemer og kompetencer. Vi sikrer, så vidt det er muligt, at alle medarbejdere, nye som gamle, kan arbejde på vores systemer, uden stor operationel og historisk erfaring. Dette via dokumentationer og procesbeskrivelser, af de mest vitale opgaver, systemer og kompetencer.

Det vil dog altid være opgaver, systemer og kompetencer, som kræver en vis ekspertise og historisk erfaring, hvor opgave kun kan foretages af enkelte nøglemedarbejdere, eller eksterne kompetencer. Vi forsøger dog at sikre denne personafhængighed, så vidt det er muligt, med dobbeltroller på udvalgte systemer. Dobbeltroller kan både være i forhold til intern medarbejder, og ekstern partner/kompetence.

12.1.2 *Ændringsstyring*

Vi har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder, tilrettelægges hensigtsmæssigt i forhold til interne forhold, håndteres så de er til mindst mulig gene for kunden og vores drift generelt.

Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten, og vurdering af påvirkning af kunder, og andre systemer.

Vi har en standard projektmodel, til styring/håndtering af ændringer, som er inddelt i en række faser, der som minimum indeholder en foranalyse/beskrivelse fra kunde, løsning, test og implementering.

Opgaver af en vis størrelse, som er væsentlige ændringer i vores generelle driftssystemer som påvirker flere kunder, kræver godkendelse af vores Tekniske Chef, Driftschef eller alternativt Adm. Direktør.

12.1.3 *Kapacitetsstyring*

Det påhviler Driftschefen at overvåge ressourceforbruget indenfor vedkommendes ansvarsområde, og løbende at udarbejde udviklingsprognoser således at de nødvendige og tilstrækkelige ressourcer er til rådighed. Dette primært i forhold til om vores kunders, og egne systemer performer som de skal, samt at der er de nødvendige ressourcer til rådighed.

12.1.4 *Adskillelse af udviklings-, test- og driftsfaciliteter*

Vi har adskilte miljøer til test/udviklingsmiljø og produktion. Miljøerne er adskilte logisk, med et test-/udviklingsmiljø og et produktionsmiljø.

Vi har med ovenstående Funktionsadskillelse etableret de nødvendige adgangskontroller for at sikre, at kun autoriseret personale kan tilgå vores produktionsmiljø.

Vores test-/udviklingsmiljø er ikke vitalt, og der ligger ikke vitale data, så dette kan alle der har et behov tilgå, og dette uden risiko for at forstyrre vores produktionsmiljø og driften af vores kunder.

12.2 Beskyttelse mod malware

12.2.1 *Foranstaltninger mod Malware*

Alle servere i SOTEA driftsmiljø, skal være udstyret med opdateret og aktivt antivirusprogram.

Alt elektronisk trafik (e-mail, downloads o.l.) skal scannes for at sikre imod malware.

Til sikring imod smitte og angreb fra de ydre net, skal alle net være beskyttet af vedligeholdt og overvåget firewall.

Opdatering af firewall er dokumenteret via vores normale change procedure.

Herudover er vores kundesystemer sikret mod at de selv kan installere programmer. Dog kan der gives tilladelse til at kunder kan have lokale administratorret, dette skal dog skriftligt aftales, hvor SOTEA gør opmærksom på risikoen herved, samt ansvarsfraskrivelse fra SOTEA's side.

Vi har etableret foranstaltninger til sikring mod cyberkriminalitet, herunder DDoS og ransomware. Skulle uheldet på trods af foranstaltningerne være ude, har vi endvidere procedurer til håndtering af hændelserne.

12.3 Backup

12.3.1 *Sikkerhedskopiering af informationer*

Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, og efter de aftaler, vi har med vores kunder.

Omfanget af backup er formelt beskrevet i vores aftale med kunderne.

Vi har etableret en testplan for verificering af hvorvidt sikkerhedskopieringen fungere samt en test af hvordan systemer og data praktisk kan reetableres. Der føres log over disse tests således at vi kan følge op på om vi kan ændre på procedurer og processer for at højne vores løsning.

Med mindre andet er aftalt med vores kunder, foretager vi sikkerhedskopiering af hele deres miljø hos os. Vi foretager sikkerhedskopiering af vores egne systemer og data på samme vis, som vores kunders systemer og data.

Vi har udarbejdet faste procedurer og beskrivelser for opsætning og vedligehold af backup.

Hver nat føres en fuld kopi af data fra SOTEA Datacenter I til SOTEA Backuplokation (co-location) ved hjælp af vores backup-system. Dermed er data fysisk separeret fra vores driftssystemer.

En ansvarlig medarbejder sikrer herefter, at sikkerhedskopieringen er sket, foretager det fornødne, hvis jobbet er fejlet, og herefter logger dette.

12.4 Logning og overvågning

12.4.1 *Hændelseslogning*

Vi har opsat overvågning og logning af netværkstrafik, og vores driftsafdeling følger dette. Vi foretager ikke proaktiv overvågning af logførte hændelser, men vi følger op såfremt vi mistænker at en hændelse kan relatere til forhold afdækket i log.

Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident og problem management procedurer til sikring af, at hændelser registreres, prioriteres, styres, eskaleres og at der foretages de nødvendige handlinger.

12.4.2 *Beskyttelse af logoplysninger*

Logs må kun kunne tilgås af autoriseret personale.

Der skal for hver log være procedurer for håndteringen af loggen, og oplysningerne i denne.

Rettelse i logs må ikke foretages.

12.4.3 *Administrator- og operatørlog*

Logning af administratorer sker i forbindelse med den almindelige logning.

12.4.4 *Tidssynkronisering*

Alle servere bliver løbende synkroniseret med tiden på en fælles tids server.

12.5 Styring af software på driftssystemer

12.5.1 *Installation af programmer på driftssystemer*

Vi sikrer at der alene installeres godkendte og testede opdateringer på vores systemer. Ydermere sikrer vi at kritiske opdateringer ikke bliver mere end 2 måneder gamle, før de installeres.

Vores politik i forhold til opdatering af software, gælder kun software som er lejet/ejet af SOTEA, og software som SOTEA har det fulde ansvar for, og dermed ikke kundens eget software.

Vores driftssystem består af en kompleks konfiguration, og når vi planlægger ændringer heri – selv når disse er af mindre karakter, men som kan have en væsentlig påvirkning – drøftes det internt på supportmøder. Først herefter foretages ændringen, og hvis det er major change, skal disse godkendes af ledelsen. Ændringen sker i vores fastsatte, eller udmeldte, servicevinduer. Vi planlægger samtidig et fallback scenarie hvor det er muligt, og vi beskriver dels ændringen og opdaterer vores dokumentation. Vi anvender samme procedure for ændringer, om de er bestilt af vores kunder eller interne ændringer. Patches og andre opdateringer til systemer og databaser styres ligeledes efter samme procedure.

12.6 Styring af tekniske sårbarheder

12.6.1 *Styring af tekniske sårbarheder*

Den Tekniske Chef eller Driftschefen godkender idriftsættelsen af nye it-systemer og nye versioner og opdateringer af eksisterende it-systemer, samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

Medarbejdere opfordres aktivt til, at søge informationer omkring sikkerhedssvagheder på forskellige fora, eller generelt være opmærksomme på hvad man hører og ser – gennem vores personalehåndbog.

Den Tekniske Chef eller Driftschefen skal sikre, at det løbende vurderes, om der er behov for at installere rettelser til operativsystemer i SOTEA's driftsmiljø. Opdateringer kategoriseret som kritiske af software leverandører, skal installeres inden for 2 måneder fra frigivelses dato. Herunder kun software som SOTEA har det fulde ansvar for, og som er en del af SOTEA ydelse.

Den Tekniske Chef eller Driftschefen skal sikre, at det løbende vurderes, om større operativsystemopdateringer og programpakkeopdateringer (service packs) skal installeres i SOTEA driftsmiljø.

12.6.2 *Begrænsning af programinstallering*

Vi installere kun kritiske sikkerhedsopdateringer, der er godkendt af leverandører. Hvis der skal installeres yderligere opdateringer, vil dette være på opfordring fra de enkelte kunder, eller hvis vi internt har opdateringer der kræves installeret.

12.7 Overvejelser i forbindelse med revision af informationssystemer

12.7.1 *Foranstaltninger i forbindelse med revision af informationssystemer*

Foranstaltninger i forbindelse med revision af informationssystemer

En gang årligt lader vi os undergå uvildig it-revision, med henblik på afgivelse af en 3402 erklæring for overholdelse af kontroller nævnt i denne kontrolbeskrivelse.

13 Kommunikationssikkerhed

13.1 Håndtering af netværkssikkerhed

13.1.1 *Netværksforanstaltninger*

SOTEA anvender elektroniske netværk, både kablede og trådløse, dog er det trådløse netværk ikke logisk forbundet med vores driftsnet, og det trådløse netværk er ikke vitalt for vores drift. Vi er yderst afhængige af et velfungerende og sikkert kablede netværk, i forhold til alle vores systemer.

Beskyttelse af netværket skal afstemmes efter de resultater vores årlige risikovurdering giver, således at der er den nødvendige og tilstrækkelige sikkerhed ved anvendelsen af nettet.

It-sikkerheden omkring systemers og datas ydre rammer, er netværket mod internettet. Vi mener at have sikret data og systemer, både på det interne netværk, såvel som det ydre værn mod uvedkommende adgang, hvilket er af højeste prioritet hos os. Det ydre værn er primært beskyttet af en firewall, som løbende bliver opdateret og vedligeholdt.

Ansvaret for netværk og netværkssikkerhed ligger hos vores Driftschef, og der er udarbejdet procedurer, vejledninger og dokumentation til anvendelse i forbindelse med drift og vedligehold af netværk.

13.1.2 *Sikring af netværkstjenester*

Adgang til vores systemer fra vores kunder, sker enten via en offentlig internet forbindelse, hvor adgang sker via krypteret TSG adgang eller via konfigureret VPN tunnel til kundens lokation/firewall, eller adgang via MPLS/Punkt til punkt forbindelse.

Adgang mellem SOTEA Datacenter I og SOTEA Backuplokation sker via SOTEA's egen sorte fiber, hvor der er SOTEA udstyr i begge ender.

Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall.

Vi er ansvarlige for driften og sikkerheden hos os, dvs. fra og med systemerne hos os og ud til internettet (eller MPLS/Punkt til punkt). Vores kunder er selv ansvarlige for at kunne tilgå internettet fra egen lokation.

13.1.3 *Opdeling af netværk*

Alle netværk har deres eget VLAN og der routes kun mellem de 2 produktionsnetværk, 10.254.251.0/24. Alle netværk styres direkte, eller indirekte af firewallen.

14 Anskaffelse, udvikling og vedligeholdelse

14.1 Sikkerhedskrav til informationssystemer

14.1.1 *Analyse og specifikation af sikkerhedskrav*

SOTEA's anskaffelse, udvikling og afvikling af informationsbehandlingssystemer, følger regler og procedurer jf. punkt 12.1.2. Ændringsstyring.

Informationsbehandlingssystemer omfatter styresystemer, infrastruktur, forretningssystemer (såvel egen-udviklede som færdige standard-systemer), brugerudviklede systemer og tjenesteydelser.

14.1.2 *Procedure for styring af ændringer*

Vi har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder, tilrettelægges hensigtsmæssigt i forhold til interne forhold, håndteres så de er til mindst mulig gene for kunden og vores drift generelt.

Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten, og vurdering af påvirkning af kunder, og andre systemer.

Vi har en standard projektmodel, til styring/håndtering af ændringer, som er inddelt i en række faser, der som minimum indeholder en foranalyse/beskrivelse fra kunde, løsning, test og implementering.

Opgaver af en vis størrelse, som er væsentlige ændringer i vores generelle driftssystemer som påvirker flere kunder, kræver godkendelse af vores Tekniske Chef, Driftschef og alternativt Adm. Direktør.

14.1.3 *Begrænsning af ændringer af softwarepakker*

Vi installere kun kritiske sikkerhedsopdateringer, der er godkendt af leverandører. Hvis der skal installeres yderligere opdateringer, vil dette være på opfordring fra de enkelte kunder, eller hvis vi internt har opdateringer der kræves installeret.

14.1.4 *Sikkerhedstestning af systemer*

Vi har procedure for sikkerhedstestning af systemer inden implementering. Kunder tester altid, hvis muligt, inden systemer flyttes i produktion.

14.1.5 *Test af systemaccept*

Når vi opsætter nye systemer foretages test af funktionalitet og herunder kapacitet- og performancetest. Først efter godkendelse fra de berørte parter godkendes systemer til drift.

Godkendelse af idriftsættelse er dokumenteret via vores normale changeprocedurer.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

15.1.1 *IT-sikkerhedspolitik i forhold til leverandørforhold*

Der er etableret fortrolighed med de primære eksterne partnere, gennem indgåelse af samarbejdsaftale, hvor SOTEA eller leverandøren gør opmærksom på at fortrolighed og tavshedspligt skal overholdes.

15.1.2 *Sikkerhedsforhold i leverandøraftaler*

Der er etableret fortrolighed med de primære eksterne partnere, gennem indgåelse af samarbejdsaftale, hvor SOTEA eller leverandøren gør opmærksom på at fortrolighed og tavshedspligt skal overholdes.

15.2 Styring af serviceydelser fra tredjepart

15.2.1 *Overvågning og evaluering af serviceydelser fra tredjepart*

Vi har procedurer der sikrer at aftalte leverancer fra tredjepart gennemføres jf. aftale, her tænkes specielt på årlige service eftersyn, samt hvis der skal indhentes revisorerklæringer hos tredjepart.

15.2.2 *Styring af ændringer af serviceydelser*

Når der sker ændringer til vores ydelser fra vores eksterne samarbejdspartnere, ved fremsendelse af ny partneraftale, eller andre forhold som kan have indflydelse på vores aftale med kunderne, er der procedu-

rer for at sikre at vi forholder os aktivt til disse ændringer, og deres konsekvens for vores generelle forretningsbetingelser.

16 Styring af sikkerhedshændelser

16.1 Styring af informationssikkerhedsbrud og forbedringer

16.1.1 *Ansvar og procedurer*

Alle medarbejdere er forpligtet til at holde sig opdateret vha. producenters supporthjemmesider, debatfora, reagere på alarmer fra vores systemer, leverandører, samarbejdspartnere mv. for at konstatere svagheder

De skal informeres om, og skal følge de gældende regler og forretningsgange for rapportering af sikkerhedshændelser.

Der er formelt udpeget systemansvarlige, og kravene til de systemansvarlige er klart og formelt defineret. Det er den systemansvarliges ansvar at udarbejde og vedligeholde procedurer, som sikrer rettidig og korrekt indgriben i forbindelse med sikkerhedsbrud.

Systemansvarlige er Teknisk Chef og Adm. Direktør, som har det overordnede ansvar for at procedurer, til håndtering af sikkerhedshændelser, udarbejdes og vedligeholdes løbende. Alle sikkerhedshændelser skal som minimum gennemgås og evalueres (i forhold til vores generelle risikovurderingsmodel), på de ½ årlige møder i sikkerhedsgruppen, og hvis der er alvorlige trusler skal disse evalueres med det samme.

16.1.2 *Rapportering af informationssikkerhedshændelser*

Vores support system, hvori vi håndterer langt de fleste sager for kunder og interne forhold, er samtidig vores system til håndtering af sikkerhedshændelser. Heri kan vi eskalere forhold således, at opgaver får højere prioritet end andre. Herudover vil sikkerhedshændelser afstedkomme fra hhv. egne observationer, alarmering ud fra log- og overvågningssystemer, telefonisk henvendelse fra kunder, underleverandører eller samarbejdspartnere, blive eskaleret fra vores support til driftsafdelingen med samtidig orientering til ledelsen.

16.1.3 *Rapportering af sikkerhedssvagheder*

Vores medarbejdere er forpligtet til at anmelde enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelser, og nødvendige tiltag kan udføres jf. de etablerede procedurer.

16.1.4 *Vurdering af informationssikkerhedsbrud*

Vi har en formel procedure for vurdering af sikkerhedshændelser. Alle sikkerhedshændelser oprettes i Driftsloggen, hvorefter ledelsen informeres automatisk pr. mail, og vurdere hændelse straks derefter.

16.1.5 *Reaktion på informationshændelser*

Vi har en formel procedure for reaktion på sikkerhedshændelser. Alle sikkerhedshændelser oprettes i Driftsloggen, hvorefter ledelsen straks informeres automatisk pr. mail, hvorefter der reageres på hændelse straks.

16.1.6 *At lære af informationssikkerhedsbrud*

Alle sikkerhedshændelser gennemgås til den årlige risikovurdering, og på baggrund af konklusionen på vores analyse og evaluering, opdatere vi vores it-sikkerhedspolitik, og andre relevante dokumenter.

16.1.7 *Indsamling af beviser*

Indsamling af beviser, er en del af vores rapportering, og efterfølgende evaluering.

17 Informationssikkerhedsaspekter ved beredskabsstyring

17.1 Beredskab

17.1.1 *Beredskabsplanlægning*

Vi skal på 3 dage kunne retablere primære enheder i vores datacenter. Dette sikrer vi ved, at afveje risici, klassificere enheder i vores datacenter, og har procedurer der sikrer, at vi i vores beredskabsplanlægning kan foretage udskiftning af vores driftsplatform, så de leverede ydelser vil blive retableret rettidigt.

17.1.2 *Implementering af nødplaner og procedurer*

Sikkerhedsgruppen er ansvarlig for at SOTEA's informationssikkerhedspolitik, og at de givne retningslinjer og vejledninger efterleves. Desuden skal sikkerhedsgruppen sikre den løbende vedligeholdelse af risikovurderinger, samt udarbejde og vedligeholde beredskabsplaner for alle væsentlige informationsaktiver i SOTEA.

Sikkerhedsgruppen varetager også håndteringen af alle lokale sikkerhedshændelser, altså alle hændelser, hvor der er sket brud på informationssikkerheden, samt indberetning og evaluering af disse i overensstemmelse med de regler der er udarbejdet på området.

Beredskabsplanen gennemgås, ved den årlige beredskabstest.

17.1.3 *Prøvning, vedligeholdelse og revurdering af beredskabsplaner*

Planen testes som en del af vores beredskab, så vi sikrer, at kunderne i mindst muligt omfang, vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation. Efter endt test analyseres resultatet, og på den baggrund opdateres de relevante elementer, procedurer og beredskabsplaner.

17.2 Redundans

17.2.1 *Tilgængelighed af driftssystemer*

Vi har etableret tilstrækkelig redundans for at imødegå krav til tilgængelighed. Herunder redundans på:

- Strøm
- Køl
- Internet/fiber
- Vitale switche og netværk

18 Overensstemmelse

18.1 Overensstemmelse med love og kontraktmæssige krav

18.1.1 *Identifikation af gældende lovgivning og kontraktmæssige krav*

Vi overholder lovgivning i forhold til behandling af persondata.

18.1.2 *Ophavsrettigheder*

Alle licenser som SOTEA har ansvaret for, og som SOTEA fakturerer videre til kunder, er SPLA licenser som opgøres pr. måned. Vi har systemer til at registrere hvilke brugere der er på vores systemer, samt hvilke applikationer de har adgang til, og dermed hvilke licenser vi skal rapportere og afregne med vores leverandører af software.

Vi har ikke andre forhold i relation til ophavsrettigheder vi er underlagt.

18.1.3 *Beskyttelse af registreringer*

Adgang er forbeholdt nøglepersoner, herunder diverse passwords, dokumentation af netværk m.m.

18.1.4 *Beskyttelse af personoplysninger*

Alle personoplysninger ligger i ledelsesmappen, herunder ansættelseskontrakter, hvor kun ledelsen har adgang. Der findes ikke kritiske personhenførbare oplysninger andre steder.

18.1.5 *Regulering af kryptografi*

Vi anvender kun standard kryptering, hvor krypteringsnøgler ligger dokumenteret i firewalls og klienter. Vi vurderer der ikke er behov for yderligere dokumentation i forhold til kryptografi.

18.2 **Review** af **informationssikkerheden**

18.2.1 *Uafhængig evaluering af informationssikkerhed*

En gang årligt lader vi os undergå uvildig it-revision, med henblik på afgivelse af en 3402 erklæring for overholdelse af kontroller nævnt i denne kontrolbeskrivelse.

18.2.2 *Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder*

SOTEA sikrer forankring af it-sikkerhedspolitikken, ved at alle medarbejdere årligt skal gennemlæse vores it-sikkerhedspolitik, og underskrive at de forstår og efterlever den.

18.2.3 *Kontrol af teknisk overensstemmelse*

Der udsendes jævnligt orienterende mails til alle medarbejdere, omkring vores it-sikkerhedspolitik samt regler og procedurer. Derudover er der uddannelsesforløb, hvor it-sikkerhedspolitikken gennemgås, og hvor vi sikrer at der er forståelse og efterlevelse af regler og procedurer.

Der bliver minimum hvert ½ år foretaget stikprøve kontroller af om sager er registreret jf. vores regler og procedurer.

19 Ændringer i perioden

19.1.1 *Væsentlige ændringer i revisionsperioden*

Der er indført faste servicevinduer hver mandag, onsdag og fredag fra kl. 01:00 til kl. 05:00, hvor alle kundeservere opdateres med kritiske sikkerhedspatches.

Der er sket ændring af kontrolbeskrivelse og sikkerhedspolitik, som er opdateret fra ISO 27002:2005 til ISO 27002:2013.

20 Komplementerende kontroller

20.1 Forhold kunderne selv antages af være ansvarlige for

Som udgangspunkt har SOTEA det fulde ansvar for hardware og software, som er ejet eller administreret af SOTEA, og som kunden lejer jf. indholdet i underskrevet kontrakt.

Hardware og software som ikke er ejet eller administreret af SOTEA, og dermed ikke er en del af vores kontraktlige forpligtelser, er kundens eget ansvar. Det er eksempelvis drift, vedligehold og support af:

- Udstyr ejet af kunden selv. Herunder:
  - PC/Bærbar
  - Printere
  - Netværk
  - Servere
  - m.m.

- Software ejet af kunden selv, eller af tredjepart:
  - ERP Systemer
  - Licenser til lokale desktops
  - Software installeret på kundens server hos SOTEA, som er ejet af kunden selv, eller tredjepart
  - m.m.

Afsnit 3: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

Til ledelsen hos Sotea A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om Sotea A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af Sotea A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hostingydelser i perioden 01-02-2018 til 31-01-2019, samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Sotea A/S' ansvar

Sotea A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. Sotea A/S er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål og for udformningen, implementeringen og effektiviteten af fungerende kontroller for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

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

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

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Sotea A/S' beskrivelse (afsnit 2) og om udformningen og funktionaliteten af de kontroller, der knytter sig til de 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 planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede og fungerer effektivt.

Opgaven med afgivelse af en erklæring med sikkerhed om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og 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 udformede eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere en vurdering af den samlede præ-

sentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2.

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

Begrænsninger i kontroller hos en serviceleverandør

Sotea A/S' beskrivelse i afsnit 2 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 vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Sotea A/S' beskrivelse i afsnit 2 og det er på den baggrund vores vurdering,

(a) at beskrivelsen af kontroller, således som de var udformet og implementeret i hele perioden 01-02-2018 til 31-01-2019, i alle væsentlige henseender er retvisende
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 01-02-2018 til 31-01-2019
(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 01-02-2018 til 31-01-2019.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i det efterfølgende hovedafsnit (afsnit 4).

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt Sotea A/S' hostingydelser, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 21. juni 2019

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CIPP/E, CRISC, adm. direktør

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Sotea A/S har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 01-02-2018 til 31-01-2019.

Vi har således ikke nødvendigvis testet alle de kontroller, som Sotea A/S har nævnt i sin beskrivelse i afsnit 2.

Kontroller, udført hos Sotea A/S' kunder, er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos Sotea A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført – eller har observeret – en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Risikovurdering og -håndtering

Risikovurdering

Kontrolmål: Formålet er at sikre, at virksomheden periodisk foretager en analyse og vurdering af it-risikobilledet.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
4.1	Vi har procedurer for løbende risikovurdering af vores forretning. Vi sikrer, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Der holdes et årligt review møde, hvor der foretages en risikovurdering.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af it-risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået. Vi har desuden inspiceret dokumentation for periodisk kontrol. Vi har forespurgt til ledelsesgodkendelse af it-risikoanalysen, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Ingen væsentlige afvigelser konstateret.

Informationssikkerhedspolitikker

Retningslinjer for styring af informationssikkerhed

Kontrolmål: Formålet er at sikre, at der gives retningslinjer for og understøttelse af informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
5.1	Det er SOTEA's Adm. Direktør der har det overordnede ansvar for sikkerhedspolitikken, og herunder politikker og procedurer, og den Adm. Direktør der godkender opdateringer og tilføjelser hertil. Der foretages årligt review af sikkerhedspolitikken, og herunder politikker og procedurer	Vi har forespurgt til udarbejdelsen af en informationssikkerhedspolitik, og vi har inspiceret dokumentet. Vi har forespurgt til periodisk gennemgang af informationssikkerhedspolitikken, og vi har inspiceret, at dokumentet er gennemgået i revisionsperioden. Vi har desuden inspiceret kontrol for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Ingen væsentlige afvigelser konstateret.

Organisering af informationssikkerhed

Intern organisering

Kontrolmål: Formålet er at sikre, at der etableres et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
6.1	Det er SOTEA's Adm. Direktør der har det overordnede ansvar for sikkerhedspolitikken, og herunder politikker og procedurer, og den Adm. Direktør der godkender opdateringer og tilføjelser hertil. Der foretages årligt review af sikkerhedspolitikken, og herunder politikker og procedurer. Vores dokumentationer og processer generelt sikrer, at vi udelukker eller minimere nøglepersonafhængighed. Funktionsadskillelse er en vigtig del af vores organisation og drift, hvorfor vi, via adgangskontroller og rettighedsstyring, sikrer, at kun autoriseret personale kan udføre de nødvendige handlinger på systemer og data. Vi tager stilling til it-sikkerhed i vores It projekter, både i forhold til kunde projekter og interne projekter. Alle projekter/projektforløb findes i SharePoint under "Project".	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen og vedligeholdelsen af ansvarsbeskrivelser. Vi har forespurgt til adskillelse af adgang i forhold til funktion, og vi har inspiceret dokumentation for differentieret adgang. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter. Vi har stikprøvevis inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser **Kontrolmål: Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
6.2	Vi sikrer, i bedst muligt omfang, vores medarbejderes bærbare udstyr såsom bærbare pc, PDA, mobiltelefon og lign. Dog er ingen medarbejderes udstyr koblet i domæne, så alt adgang foregår via Fjern Skrivebord/RDP, så der vil aldrig ligge vitale data på deres PC'ere, PDA eller mobiltelefoner, udover mail. Vi har åbnet adgang til, at vi og vores kunder kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Ud over kode, har vi ikke implementeret andre sikkerhedsforanstaltninger til sikring af disse enheder og disses brugeradgange. Adgang til vores netværk og dermed potentielt til systemer og data, sker kun for autoriserede personer. Hjemmearbejdsplads for vores medarbejdere er sikret via krypteret TSG-forbindelse, hvor bruger skal have bruger-id og password for at logge på.	Vi har forespurgt til styring af mobile enheder, og vi har inspiceret løsningen. Vi har forespurgt til sikring af fjernarbejdspladser, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Medarbejdersikkerhed

Før ansættelsen

Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
7.1	Der skal, i ansættelseskontrakten, tydeligt angives Stillings- og funktionsbeskrivelse, samt eventuelle særlige sikkerhedsmæssige opgaver og ansvar. Under ansættelsesinterview skal ansøgeren informeres om hvilke sikkerhedsmæssige krav ansættelsesforholdet indebærer. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt. Der indhentes ren straffeattest. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har endvidere stikprøvevis inspiceret dokumentation for, at proceduren er fulgt. Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevis inspiceret indholdet af kontrakter.	Ingen væsentlige afvigelser konstateret.

Under ansættelsen **Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
7.2	I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. Ligeledes er det klart defineret som en del af kontraktmaterialet, hvad den ansattes ansvar og rolle er. I forbindelse med anvendelse af eksterne leverandører, som har adgang til vores systemer, sikrer vi at der indgås fortrolighedsaftaler. Vores aktiver er i høj grad vores medarbejdere, og vi sikrer at vores medarbejdere løbende uddannes. Dette foregår ved intern vidensdeling, samt relevante eksterne uddannelser og certificeringer. Der afholdes årligt, gennemgang af vores sikkerhedspolitik, hvor sikkerhedspolitik fremsendes til relevante medarbejdere, hvorefter denne gennemgås, og medarbejder fremsender efterfølgende mail på bekræftelse af at sikkerhedspolitik er læst og forstået. Derudover sendes der løbende information omkring trusler, ændringer i vores sikkerhedspolitik, ændringer i vores driftshåndbog, eller sikkerhedsinformationer generelt, på mail, hvor det findes relevant.	Vi har forespurgt til ledelsens ansvar for videreformidling af politikker og procedurer, og vi har inspiceret dokumentation for tildeling af ansvar. Vi har forespurgt til videreuddannelse af personale, og vi har stikprøvevis inspiceret dokumentation for videreuddannelse. Vi har forespurgt til retningslinjer for sanktionering, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring **Kontrolmål: Formålet er at beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
7.3	Generelle vilkår for ansættelse, herunder forhold omkring ophør, er beskrevet i Soteas driftshåndbog. Ledelsen er ansvarlig for, at medarbejderen er informeret om de gældende regler ved og efter ansættelsesophør.	Vi har forespurgt til medarbejderes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør i ansættelse, og vi har inspiceret dokumentation for medarbejdernes forpligtelser.	Ingen væsentlige afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver

Kontrolmål: Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
8.1	Vores netværk og miljø er komplekst med mange systemer og kunder, og for at sikre mod uvedkommende adgang, og for at sikre gennemskuelighed af opbygningen, har vi udformet en række dokumentation, der beskriver det interne netværk, med enheder, navngivning af enheder, logisk opdeling mv. Vi arbejder i SOTEA med ejerskab over aktiver for at sikre, at ingen enheder, systemer eller data bliver glemt i forhold til sikkerhedsopdateringer, backup, drift og vedligehold. Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm., og at den ansattes adgange lukkes og inddrages rettidigt. Det skal sikres at alle medarbejderens adgangsrettigheder inddrages. Det skal afgøres, om det er nødvendigt at slette disse rettigheder, eller om det blot er tilstrækkeligt at spærre disse. De rettigheder, der skal spærres eller slettes, inkludere fysisk adgang, samt adgang til systemer.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har forespurgt til oversigt over ejerskab for aktiver, og vi har inspiceret oversigten. Vi har forespurgt til retningslinjer for brugen af aktiver, og vi har inspiceret retningslinjerne. Vi har forespurgt til procedure til sikring af tilbagelevering af udleverede aktiver, og vi har inspiceret proceduren.	Ingen væsentlige afvigelser konstateret.

Klassifikation af information **Kontrolmål: Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
8.2	For at kunne prioritere data – f.eks. ved genskabelse, er data klassificeret i typer, vigtigheden samt tilhørsforhold til kunderne eller internt. Klassifikation er beskrevet i driftshåndbogen. Der udarbejdes en liste hvor kunder generelt er prioriteret, hvor der kan sættes lighedstegn mellem kundens prioritet og datas prioritet. Denne liste opdateres minimum 1 gang årligt. Systemdata for netværk, dokumentation er prioriteret højst, herunder sikret betryggende. Processen er dokumenteret. Vi skal sikre, at vores og vores kunders systemer og data beskyttes. Vi håndterer derfor ikke kunders data på håndbårne medier (USB, CD/DVD, flytbare diske) uden forudgående aftale med kunderne.	Vi har forespurgt til politik for klassificering af data, og vi har inspiceret politikken. Vi har forespurgt til mærkning af data, og vi har inspiceret retningslinjerne for mærkning af data. Vi har forespurgt til retningslinjer for håndtering af aktiver, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Mediehåndtering

Kontrolmål: Formålet er at sikre hindring af uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
8.3	Vi sikrer, i bedst muligt omfang, vores medarbejderes bærbare udstyr såsom bærbare pc, PDA, mobiltelefon og lign. Dog er ingen medarbejderes udstyr koblet i domæne, så alt adgang foregår via Fjern Skrivebord/RDP, så der vil aldrig ligge vitale data på deres PC'ere, PDA eller mobiltelefoner, udover mail. Vi anbefaler at der etableres et login på vores bærbare udstyr, samt at der installeres antivirus. Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt. Der er udarbejdet vejledninger som sikrer, at data på medierne ikke kan genskabes. Forsendelse af fysiske medier (bånd, diske, CD, DVD og lignende) skal ske med pålidelig og troværdig transportør (herunder UPS, GLS, Budstikken, Post Danmark m.m.). Fortrolige og følsomme data på medierne skal være sikret på bedst mulig måde, ligesom der skal foreligge en sikret backup til beskyttelse imod tab og bortkomst.	Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen. Vi har forespurgt til retningslinjer for bortskaffelse af medier, og vi har inspiceret dokumentation for bortskaffelse. Vi har forespurgt til politik for transport af medier, og vi har inspiceret politikken.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring

Kontrolmål: Formålet er at begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.1	Vi har politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik. Adgang til netværksenheder og administration heraf, kan kun ske fra management netværket	Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken. Vi har forespurgt til håndtering af adgang til netværk og netværksservices, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Administration af brugeradgange **Kontrolmål: Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.2	Vi har procedurer for nedlæggelse og tilpasning af adgangsrettigheder. Det er kun udvalgte personer hos vores kunder, der kan bede om adgangsrettigheder. Tildeling af privilegier, og rettigheder, er kontrolleret i forbindelse med vores normale brugeradministrations proces. Da vi har en del brugere, såsom service accounts og lign., som ikke kan bruges til at logge på med, og af systemmæssige årsager ikke skifter passwords, har vi et system til opbevaring af disse passwords. Kun autoriseret personale har adgang til systemet. Krav til disse passwords er højere end vores almindelige passwordpolitik.	Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret dokumentation for oprettelse og nedlæggelse af brugere. Vi har forespurgt til proces for tildeling af rettigheder, og vi har inspiceret processen. Vi har forespurgt til overvågning af anvendelsen af privilegerede adgangsrettigheder, og vi har stikprøvevis inspiceret dokumentation for overvågning. Vi har forespurgt til proces for periodisk gennemgang af brugere, og vi har inspiceret dokumentation for seneste gennemgang. Vi har forespurgt til procedure for inddragelse af rettigheder, og vi har inspiceret proceduren. Vi har forespurgt til opdeling af mapper og adgange, og vi inspiceret løsningen.	Vi har observeret i vores stikprøvegrundlag, at virksomheden ikke har oprettet tickets for lukning af 2 ud af 2 af virksomhedens medarbejdere i forbindelse med fratrædelse. Vi har dog observeret, at medarbejdernes adgange til systemerne har været lukket. Vi har endvidere observeret at virksomheden ikke har oprettet tickets for oprettelse af 2 ud af 2 medarbejdere i forbindelse med ansættelse. Ingen væsentlige afvigelser konstateret i øvrigt.
Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.3	Vores it-sikkerhedspolitik foreskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Styring af system- og applikationsadgang **Kontrolmål: Formålet er at forhindre uautoriseret adgang til systemer og applikationer.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.4	Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen. Al adgang til vores systemer foregår via Fjernskrivebord, hvor bruger logger på med personlig brugerkonto og password. Interne medarbejdere har alle en administrativ bruger med begrænsede rettigheder, som anvendes i det daglige arbejde. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger ift. udformningen af kodeordet. Passwords på domænet er kontrolleret via regler defineret i GPO'er.	Vi har forespurgt til begrænsning af adgang til data, og vi har inspiceret dokumentation for begrænsning. Vi har forespurgt til procedure for sikker logon, og vi har inspiceret løsningen. Vi har forespurgt til system til styring af adgangskoder. Vi har inspiceret løsningen og udvalgte konfigurationer.	Ingen væsentlige afvigelser konstateret.

Kryptografi

Kryptografiske kontroller **Kontrolmål: Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
10.1	Vi anvender kun standard kryptering, hvor krypteringsnøgler ligger dokumenteret i firewalls og klienter. Vi vurderer der ikke er behov for yderligere dokumentation i forhold til kryptografi.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	Vi har observeret, at virksomheden ikke har defineret kontroller eller politikker til sikring af effektiviteten af kryptering vedrørende services, som er eksponeret på offentlige netværk. Ingen væsentlige afvigelser konstateret i øvrigt.

Fysisk sikring og miljøsikring

Sikre områder

Kontrolmål: Formålet er at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
11.1	Datacenteret (DC) ligger i IT-Huset ved Ferskvandscentret (FVC/DTU Aqua). DC ligger i kælderen af IT-Huset og for at få adgang skal der dels bruges dør-kode samt en chip baseret nøgle, der er programmeret specielt til den enkelte bruger. Ved hovedindgangen til IT-huset kræves der adgang kun via førnævnte nøgle. Adgang til DC kan kun ske vha. elektronisk kodet nøgle og PIN-kode der er udleveret efter aftale og som kræver underskrift af de enkelte personer. I DC er der monteret tyverialarm, i tilfælde af indbrud alarmeres den private vagtcentral. Alene autoriserede personer får adgang til lokaler via den etablerede procedure.	Vi har inspiceret de fysiske rammer for betryggende sikring, herunder sikring af adgang til driftsfaciliteter og kontorområder. Vi har forespurgt til procedure for tildeling og nedlukning af adgang til driftsfaciliteter, og vi har inspiceret proceduren. Vi har forespurgt til kontrol med adgang til driftsfaciliteter, og vi har inspiceret kontrol for gennemgang af adgange til driftsfaciliteter. Vi har forespurgt til sikring mod miljømæssige trusler ved driftscenteret, og vi har inspiceret tiltag til sikring mod miljømæssige trusler.	Ingen væsentlige afvigelser konstateret.

Udstyr

Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
11.2	Vores centrale netværksudstyr samt kundernes servere, som har etableret aftale om placering af udstyr hos os, og andet udstyr er, fysisk placeret i aflåst lokale, som har monteret køling og brandslukning mv. Til sikring af forsyning af elektricitet til DC i forbindelse med strømudfald er der monteret UPS og diesel generator. Dette setup er anslået til at kunne køre i 6 timer på en fuld tank. En gang i måneden tester vi UPS og generator og en gang årligt udføres der service af ekstern service tekniker.	Vi har forespurgt til erklæring fra underleverandør af understøttende forsyninger, og vi har inspiceret erklæringen for betryggende sikring for relevante forhold. Vi har forespurgt til håndtering af hændelser i DC, og vi har inspiceret politik for dette. Vi har forespurgt til hændelser i DC, og vi har inspiceret dokumentation for hændelser. Vi har forespurgt til løbende kontrol af generator, diske, køleanlæg og inergen, og vi har inspiceret løsningen. Vi har forespurgt til politik for ryddeligt skrivebord, og vi har inspiceret politikken.	I forbindelse med understøttende forsyninger har der i underleverandørens erklæring været en afvigelse i forhold til fysiske forhold. I underleverandørens erklæring er der følgende observation: "OMC modtog ikke alarm på åben dør i repeaterstationen i Viborg på grund af fejl i konfigurationen i overvågningsværktøjet." Det fremgår af rapporten, at fejlen er blevet udbedret. Ingen væsentlige afvigelser konstateret i øvrigt.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

Kontrolmål: Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.1	Vi sikrer, så vidt det er muligt, at alle medarbejdere, nye som gamle, kan arbejde på vores systemer, uden stor operationel og historisk erfaring. Dette via dokumentationer og procesbeskrivelser, af de mest vitale opgaver, systemer og kompetencer. Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten, og vurdering af påvirkning af kunder, og andre systemer. Det påhviler Driftschefen at overvåge ressourceforbruget indenfor vedkommendes ansvarsområde, og løbende at udarbejde udviklingsprognoser således at de nødvendige og tilstrækkelige ressourcer er til rådighed. Dette primært i forhold til om vores kunders, og egne systemer performer som de skal, samt at der er de nødvendige ressourcer til rådighed. Vi har adskilte miljøer til test/udviklingsmiljø og produktion.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til ændringsstyring, og vi har stikprøvevis inspiceret dokumentation for håndtering af ændringer i perioden. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Vi har forespurgt til anvendelsen af testmiljø, og vi har inspiceret dokumentation for eksistensen af testmiljø.	Ingen væsentlige afvigelser konstateret.

Malwarebeskyttelse

Kontrolmål: Formålet er at sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.2	Alle servere i SOTEA driftsmiljø, skal være udstyret med opdateret og aktivt antivirusprogram. Alt elektronisk trafik (e-mail, downloads o.l.) skal scannes for at sikre imod malware. Til sikring imod smitte og angreb fra de ydre net, skal alle net være beskyttet af vedligeholdt og overvåget firewall.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen væsentlige afvigelser konstateret.

Backup **Kontrolmål: Formålet er at beskytte mod tab af data.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.3	Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, og efter de aftaler, vi har med vores kunder. Vi har etableret en testplan for verificering af hvorvidt sikkerhedskopieringen fungere samt en test af hvordan systemer og data praktisk kan reetableres. Der føres log over disse tests således at vi kan følge op på om vi kan ændre på procedurer og processer for at højne vores løsning. Vi har udarbejdet faste procedurer og beskrivelser for opsætning og vedligehold af backup. En ansvarlig medarbejder sikrer herefter, at sikkerhedskopieringen er sket, foretager det fornødne, hvis jobbet er fejlet, og herefter logger dette.	Vi har forespurgt til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for opsætningen. Vi har forespurgt til test af genopprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse. Vi har forespurgt til dokumentation for, at fejlede backups er blevet gennemført, og vi har inspiceret dokumentation for dette.	Ingen væsentlige afvigelser konstateret.

Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.4	Vi har opsat overvågning og logning af netværkstrafik, og vores driftsafdeling følger dette. Vi foretager ikke proaktiv overvågning af logførte hændelser, men vi følger op såfremt vi mistænker at en hændelse kan relatere til forhold afdækket i log. Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident og problem management procedurer til sikring af, at hændelser registreres, prioriteres, styres, eskaleres og at der foretages de nødvendige handlinger. Logs må kun kunne tilgås af autoriseret personale. Alle servere bliver løbende synkroniseret med tiden på en fælles tidsserver.	Vi har forespurgt til logning af brugeraktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger, og vi har inspiceret løsningen. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Styring af driftssoftware **Kontrolmål: Formålet er at sikre integriteten af driftssystemer.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.5	Vi sikrer at der alene installeres godkendte og testede opdateringer på vores systemer. Ydermere sikrer vi at kritiske opdateringer ikke bliver mere end 2 måneder gamle, før de installeres.	Vi har forespurgt til retningslinjer for installation af software på driftssystemer, og vi har inspiceret retningslinjerne. Vi har forespurgt til rettidig opdatering af driftssystemer, og vi har inspiceret dokumentation for opdatering af driftssystemerne.	Ingen væsentlige afvigelser konstateret.

Sårbarhedsstyring **Kontrolmål: Formålet er at forhindre, at tekniske sårbarheder udnyttes.**			
Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.6	Den Tekniske Chef eller Driftschefen godkender idriftsættelsen af nye it-systemer og nye versioner og opdateringer af eksisterende it-systemer, samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift. Den Tekniske Chef eller Driftschefen skal sikre, at det løbende vurderes, om der er behov for at installere rettelser til operativsystemer i SOTEA's driftsmiljø. Vi installere kun kritiske sikkerhedsopdateringer, der er godkendt af leverandører. Hvis der skal installeres yderligere opdateringer, vil dette være på opfordring fra de enkelte kunder, eller hvis vi internt har opdateringer der kræves installeret	Vi har forespurgt til styring af tekniske sårbarheder, og vi har inspiceret dokumentation for styringen. Vi har forespurgt til styring af adgang til programinstallation, og vi har inspiceret dokumentation for begrænsningen af brugere med rettighed til programinstallation.	Vi har observeret, at virksomheden ikke har konfigureret krypteringsprotokoller på services, der er eksponeret på internettet. Der henvises i øvrigt til resultat af test jf. punkt 10.1. Ingen væsentlige afvigelser konstateret i øvrigt.

Kommunikationssikkerhed

Styring af netværkssikkerhed

Kontrolmål: Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
13.1	Beskyttelse af netværket skal afstemmes efter de resultater vores årlige risikovurdering giver, således at der er den nødvendige og tilstrækkelige sikkerhed ved anvendelsen af nettet. Ansvaret for netværk og netværkssikkerhed ligger hos vores Driftschef, og der er udarbejdet procedurer, vejledninger og dokumentation til anvendelse i forbindelse med drift og vedligehold af netværk. Adgang til vores systemer fra vores kunder, sker enten via en offentlig internet forbindelse, hvor adgang sker via krypteret TSG adgang eller via konfigureret VPN tunnel til kundens lokation/firewall, eller adgang via MPLS/Punkt til punkt forbindelse. Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall. Alle netværk har deres eget VLAN og der routes kun mellem de 2 produktionsnetværk. Alle netværk styres direkte, eller indirekte af firewallen.	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall og patching af firewall. Vi har forespurgt til sikring af netværkstjenester, og vi har inspiceret dokumentation for betryggende sikring.	Ingen væsentlige afvigelser konstateret.

Informationsoverførsel

Kontrolmål: Formålet er at opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
13.2	Der er etableret fortrolighed med de primære eksterne partnere, gennem indgåelse af samarbejdsaftale, hvor SOTEA eller leverandøren gør opmærksom på at fortrolighed og tavshedspligt skal overholdes.	Vi har forespurgt til politikker og procedurer for dataoverførsel. Vi har forespurgt til aftaler om dataoverførsel. Vi har forespurgt til retningslinjer for afsendelse af fortrolig information. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen væsentlige afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold

Kontrolmål: Formålet er at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
15.1	Når der sker ændringer til vores ydelser fra vores eksterne samarbejdspartnere, ved fremsendelse af ny partneraftale, eller andre forhold som kan have indflydelse på vores aftale med kunderne, er der procedurer for at sikre at vi forholder os aktivt til disse ændringer, og deres konsekvens for vores generelle forretningsbetingelser.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret aftalen med henblik på at efterse hensyntagen til informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Styring af leverandørydelser

Kontrolmål: Formålet er at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
15.2	Når der sker ændringer til vores ydelser fra vores eksterne samarbejdspartnere, ved fremsendelse af ny partneraftale, eller andre forhold som kan have indflydelse på vores aftale med kunderne, er der procedurer for at sikre at vi forholder os aktivt til disse ændringer, og deres konsekvens for vores generelle forretningsbetingelser.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører.	Der henvises til resultat af test jf. punkt 11.1. Ingen væsentlige afvigelser konstateret i øvrigt.

Styring af informationssikkerhedsbrud

Styring af informationssikkerhedsbrud og forbedringer

Kontrolmål: Formålet er at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
16.1	Det er den systemansvarliges ansvar at udarbejde og vedligeholde procedurer, som sikrer rettidig og korrekt indgriben i forbindelse med sikkerhedsbrud. Systemansvarlige er Teknisk Chef og Adm. Direktør, som har det overordnede ansvar for at procedurer, til håndtering af sikkerhedshændelser, udarbejdes og vedligeholdes løbende. Alle sikkerhedshændelser skal som minimum gennemgås og evalueres (i forhold til vores generelle risikovurderingsmodel), på de ½ årlige møder i sikkerhedsgruppen, og hvis der er alvorlige trusler skal disse evalueres med det samme. Vores medarbejdere er forpligtet til at anmelde enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelser, og nødvendige tiltag kan udføres jf. de etablerede procedurer. Vi har en formel procedure for vurdering af sikkerhedshændelser. Alle sikkerhedshændelser oprettes i Driftsloggen, hvorefter ledelsen informeres automatisk pr. mail, og vurdere hændelse straks derefter. Vi har en formel procedure for reaktion på sikkerhedshændelser. Alle sikkerhedshændelser oprettes i Driftsloggen, hvorefter ledelsen straks informeres automatisk pr. mail, hvorefter der reageres på hændelse straks. Indsamling af beviser, er en del af vores rapportering, og efterfølgende evaluering.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden inspiceret procedure til håndtering af informationssikkerhedshændelser. Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne. Vi har forespurgt til informationssikkerhedshændelser i perioden. Vi har forespurgt til procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren. Vi har forespurgt til løbende nyhedsorientering, og vi har inspiceret dokumentation for nyhedsbreve.	Ingen væsentlige afvigelser konstateret.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Informationssikkerhedskontinuitet

Kontrolmål: Formålet er at sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
17.1	Vi skal på 3 dage kunne retablere primære enheder i vores datacenter. Dette sikrer vi ved, at afveje risici, klassificere enheder i vores datacenter, og har procedurer der sikrer, at vi i vores beredskabsplanlægning kan foretage udskiftning af vores driftsplatform, så de leverede ydelser vil blive retableret rettidigt. Planen testes som en del af vores beredskab, så vi sikrer, at kunderne i mindst muligt omfang, vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation. Efter endt test analyseres resultatet, og på den baggrund opdateres de relevante elementer, procedurer og beredskabsplaner.	Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen. Vi har forespurgt til implementering af kompenserende tiltag i forbindelse med test af beredskabsplan, og vi har inspiceret dokumentation for implementeringen. Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurdering.	Ingen væsentlige afvigelser konstateret.

Redundans

Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
17.2	Vi har etableret tilstrækkelig redundans for at imødegå krav til tilgængelighed.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Overensstemmelse

Gennemgang af informationssikkerheden

Kontrolmål: Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
18.2	En gang årligt lader vi os undergå uvildig it-revision, med henblik på afgivelse af en 3402 erklæring for overholdelse af kontroller nævnt i denne kontrolbeskrivelse. Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder SOTEA sikrer forankring af it-sikkerhedspolitikken, ved at alle medarbejdere årligt skal gennemlæse vores it-sikkerhedspolitik, og underskrive at de forstår og efterlever den. Der udsendes jævnligt orienterende mails til alle medarbejdere, omkring vores it-sikkerhedspolitik samt regler og procedurer. Derudover er der uddannelsesforløb, hvor it-sikkerhedspolitikken gennemgås, og hvor vi sikrer at der er forståelse og efterlevelse af regler og procedurer. Der bliver minimum hvert ½ år foretaget stikprøve kontroller af om sager er registreret jf. vores regler og procedurer.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer, og vi har inspiceret dokumentation for interne kontroller. Vi har forespurgt til egenkontrol af teknisk overensstemmelse, og vi har inspiceret de opsatte kontroller.	Ingen væsentlige afvigelser konstateret.