et trygt samfund med it og data

v

Revisorerklæring

CVR nr.: 10 08 52 25

Sotea A/S

ISAE 3402 type 2 erklæring om generelle it-kontroller for
perioden 1. februar 2020 til 31. januar 2021 relateret til IT-hosting aktiviteter.

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Juni 2021

Indholdsfortegnelse

Afsnit 1: Beskrivelse af Sotea A/S' ydelser i forbindelse med drift af hosting-platform samt generelle it-kontroller relateret hertil.

I det følgende beskrives Sotea A/S' ydelser til kunder, som er omfattet af de generelle it-kontroller, som erklæringen omhandler. Erklæringen omfatter generelle processer og systemopsætninger m.v. hos Sotea A/S. Processer og systemopsætninger m.v., der er individuelt aftalt med Sotea A/S' kunder er ikke omfattet af erklæringen. Vurdering af eventuelle kundespecifikke processer og systemopsætninger m.v. vil fremgå af specifikke erklæringer til kunder, der har bestilt sådanne.

Kontroller i applikationssystemerne er ikke omfattet af denne erklæring.

Generelle it-kontroller hos Sotea A/S

Indledning

I det følgende beskrives de generelle it-kontroller relateret til Sotea A/S' ydelser til kunder, jf. beskrivelsen ovenfor.

Anvendelse af underleverandører

Sotea A/S anvender flere væsentlige leverandører: Front-safe A/S og GlobalConnect A/S.

Forord og introduktion

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. 30 medarbejdere, og har præsteret løbende vækst på mere end 20% 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.

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 Kundeservice chef.

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 Kundeservice chef.

Drift: Har det overordnede ansvar for overvågning og drift af vores hosting miljø/Datacenter, Driftsafdelingen fungerer også som second level og 3rd 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.

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:

5.5.1. Skadebegrænsende tiltag
5.5.2. Etablering af temporære nødløsninger
5.5.3. 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 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. Her opdeles medarbejdere i:

- Administrativ
- First level support
- Second level support
- Third level support

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.

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 RDG-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, som findes i SharePoint på Home fanen.

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. Der skal, i ansættelseskontrakten, tydeligt angives Stillings- og funktionsbeskrivelse, samt eventuelle særlige sikkerhedsmæssige opgaver og ansvar.
7.1.2. Under ansættelsesinterview skal ansøgeren informeres om hvilke sikkerhedsmæssige krav ansættelsesforholdet indebærer.
7.1.3. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.
7.1.4. Der indhentes ren straffeattest.

7.1.1. 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 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.

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 SOTEA's 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.

Den ansattes nærmeste leder har ansvaret for at den ansatte afleverer nedenstående, den sidste arbejdsdag:

- Nøgler
- Adgangskort
- Kreditkort
- Mobiltelefon
- Bærbar pc
- Evt. andet udleveret udstyr

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's 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 administrationen. Der udfyldes nøglekvittering ved udlevering.

Logisk adgang:
Logisk adgang til SOTEA's 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's personale.

Logisk:
Adgang til netværksenheder og administration heraf, kan kun ske fra management netværket. Det er et ikke-routingnetværk, 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 autoriseret personale har adgang til systemet. Krav til disse passwords er højere end vores almindelige passwordpolitik.

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 passwordpolitik.

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 vurderer 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 vurderer 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, og Direktøren, 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 sker 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. Der skelnes mellem om det er en "minor" eller "major" change, jf. nedenstående definition:

Major Change:

Opgaver med høj risiko, af en vis størrelse, som er væsentlige ændringer i vores generelle driftssystemer som påvirker flere kunder, kræver godkendelse af vores Tekniske Chef eller Driftschef (eks. ændring, afvikling eller anskaffelse af nyt SAN, VMM, netværk, SOTEA forretningsapplikation m.m.).

Minor Change:

Opgaver med lav risiko, som er opgaver vi udfører ofte, og som typisk kun vil berøre en enkelt kunde, kan udføres af alle support medarbejdere med respektive rettigheder til at udføre opgaven (eks. installation af program på kundeserver, genstart af kundeserver, ændring af rettighed på kundeserver m.m.).

Derudover skelnes mellem følgende opgaver, under ændringsstyring:

- **Ændringsanmodning/change:** Når en kunde beder om at få lavet en ændring på kundens server, kundens firewall, eller få genstartet en server, få installeret et program, eller andet system som dedikeret er kundens, eller kunden ønsker ændring i vores delte ressourcer, SAN, Exchange, Netværk, Filserver m.m.
- **Sikkerhedshændelse/incident:** En sikkerhedshændelse er en hændelse med negativ virkning på vores sikkerhedsniveau. En hændelse medfører ikke nødvendigvis skade i alle tilfælde (f.eks. en branddør i serverrum som står åben). Hændelsen kan ske forsætligt eller uforsætligt.
  Sikkerhedshændelser skal løbende vurderes, og skal som minimum gennemgås ved de ½ årlige møder i Sikkerhedsgruppen.
- **Internt projekt:** Dette er ændringer som ikke involverer kunder, men er rene interne projekter, så som installation af ny hardware i DC, nyt SAN, opgradering af Exchange, indsætte en ny host m.m.
- **Kunde implementering:** Ved implementering af ny kunde, eller eksisterende kunde der skal have flere ydelser, er der defineret projektforløb til gennemførelse af dette.

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

12.1.3. Kapacitetsstyring

Det påhviler Teknisk Chef 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 fungerer 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.

Medmindre 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 (colocation) 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 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 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's ydelse.

Den Tekniske Chef eller 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 installerer 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 Tekniske Chef, 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 internetforbindelse, hvor adgang sker via krypteret RDGw 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.

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 serviceeftersyn, 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 procedurer 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 er ikke underlagt særlig lovgivning i forhold til vores ydelser. Udover vi selvfølgelig er underlagt databeskyttelsesforordningen, herunder GDPR.

18.1.2. Ophavsrettigheder

Alle licenser som SOTEA har ansvaret for, og som SOTEA fakturerer videre til kunder, er SPLA og CSP 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. Følgende SharePoint lister er kategoriseret som fortrolige data:

- Driftshåndbog
- Intern Netværk
- Kontaktpersoner
- Kunde Netværk
- Licenskoder
- Offentlig IP Index
- Configurations manager
- kunde kontakt

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.

19. Ændringer i perioden

19.1. Væsentlige ændringer i revisionsperioden

19.1.1. Der er indført faste ugentlige servicevinduer pr. kunde fra kl. 01:00 til kl. 05:00, hvor alle kundeservere opdateres med kritiske sikkerhedspatches.

19.1.2. 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/bærbare
  - 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 2: Sotea A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Sotea A/S' hosting-platform, 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 anvender serviceunderleverandørerne Front-safe A/S og GlobalConnect A/S. Denne erklæring er udarbejdet efter partielmetoden, og Sotea A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Front-safe A/S og GlobalConnect A/S.

Sotea A/S bekræfter, at:

(a) Den medfølgende beskrivelse i Afsnit 1, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Sotea A/S' hosting-platform, der har behandlet kunders transaktioner i perioden fra 1. februar 2020 til 31. januar 2021.

Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været udformet og implementeret, herunder redegør for:
- De typer af ydelser, der er leveret.
- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål og kontroller udformet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå.
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

(ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget i perioden fra 1. februar 2020 til 31. januar 2021

(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 perioden fra 1. februar 2020 til 31. januar 2021. Kriterierne for denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. februar 2020 – 31. januar 2021

Silkeborg, den 15. juni 2021
Sotea A/S

Jess Munch Teilmann
Adm. direktør

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

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

Omfang

Vi har fået som opgave at afgive erklæring om Sotea A/S' beskrivelse i Afsnit 1 af generelle it-kontroller for drift af brugersystemer til behandling af Sotea A/S' kunders transaktioner i perioden 1. februar 2020 – 31. januar 2021 og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Sotea A/S anvender serviceunderleverandørerne Front-safe A/S og GlobalConnect A/S. Denne erklæring er udarbejdet efter partielmetoden, og Sotea A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Serviceunderleverandørerne Front-safe A/S og GlobalConnect A/S.

Enkelte af de kontrolmål, der er anført i Sotea A/S' beskrivelse i Afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne (eller den specifikke kunde) er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Sotea A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Sotea A/S' ansvar

Sotea A/S er ansvarlig for udarbejdelsen af beskrivelsen (Afsnit 1) og tilhørende udtalelse (Afsnit 2), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og 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.

REVI-IT anvender ISQC 1[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.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Sotea A/S' beskrivelse (Afsnit 1) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning.

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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system 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 udformet 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 desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet Sotea A/S' udtalelse 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 1 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 de generelle it-kontroller, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller 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. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Sotea A/S' udtalelse i Afsnit 2. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var udformet og implementeret i perioden fra 1. februar 2020 til 31. januar 2021, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra 1. februar 2020 til 31. januar 2021
(c) 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 perioden fra 1. februar 2020 til 31. januar 2021

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 Afsnit 4 om kontrolmål, udførte kontroller, test og resultater heraf.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i Afsnit 4 er udelukkende tiltænkt kunder, der har anvendt Sotea A/S' hosting-platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risicene for væsentlige fejlinformationer i deres regnskaber.

København, den 15. juni 2021

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Basel Obari
Partner, CISA, CISM

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

4.1. Formål og omfang

Beskrivelse og resultat af vores tests af kontroller fremgår af efterfølgende skema. I det omfang vi ved vores test har konstateret afvigelser i design, implementering eller operationel effektivitet af de testede kontroller, har vi anført disse under resultat af test.

Denne erklæring er udarbejdet efter partielmetoden og Sotea A/S' kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos Sotea A/S' underleverandører Front-safe A/S og GlobalConnect A/S.

Kontroller udført hos Sotea A/S' kunder, er ikke omfattet af vores erklæring.

4.2. Udførte test

Metoder anvendt til test af kontrollers funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Sotea A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3. Resultater af test

I nedenstående oversigt har vi opsummeret tests udført af REVI-IT som grundlag for vurdering af de generelle it-kontroller hos Sotea A/S.

A.4 Risikovurdering og -håndtering

Risikovurdering
Kontrolmål: At sikre, at virksomheden regelmæssigt foretager en analyse og vurdering af it-risikobilledet.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
4.1	*It-risikovurdering* Sotea A/S' sikkerhedsprogram er struktureret omkring 3 primære aktiviteter: Risikovurdering, risikohåndtering og løbende monitorering. Risikovurderinger er en gennemgående og kontinuerlig opgave. Der udføres årligt et antal risikoanalyser. Efter verifikation og klassifikation dokumenteres de fundne risici i Sotea A/S' risikoregister. Her dokumenteres også hvilke initiativer, der er igangsat for at reducere eller imødegå de enkelte risici.	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 og godkendt af ledelsen i perioden.	Ingen afvigelser konstateret.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed
Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
5.1.1	*Politikker for informationssikkerhed* Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.	Vi har observeret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.	Ingen afvigelser konstateret.
5.1.2	*Gennemgang af politikker for informationssikkerhed* Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken. Vi har inspiceret, at informationssikkerhedspolitikken er evalueret for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

A.6.1 Intern organisering

Kontrolmål: At etablere 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
6.1.1	*Roller og ansvarsområder for informationssikkerhed* Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret dokumentation, der viser, at ansvaret for informationssikkerhed er klart defineret og fordelt.	Ingen afvigelser konstateret.
6.1.2	*Funktionsadskillelse* Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har inspiceret procedurer vedrørende tildeling og opretholdelse af adskillelse af ansvarsområder og funktioner.	Ingen afvigelser konstateret.

A.6.2 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
6.2.1	Politik for mobilt udstyr Der vedtages en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.	Vi har inspiceret politik for sikring af mobile enheder. Vi har inspiceret, at der er defineret tekniske kontroller til sikring af mobile enheder. Vi har inspiceret, at tekniske kontroller er implementeret på mobile enheder.	Ingen afvigelser konstateret.
6.2.2	Fjernarbejdspladser Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.	Vi har inspiceret politik for sikring af fjernarbejdspladser, og vi har inspiceret underliggende sikkerhedsforanstaltninger til beskyttelse af fjernarbejdspladser.	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen

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

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
7.1.1	*Screening* Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.	Vi har inspiceret proceduren for ansættelse af nye medarbejdere og de sikkerhedsopgaver, der skal udføres i den forbindelse. Vi har inspiceret et udvalg af ansættelsesaftaler med henblik på at konstatere, om proceduren med hensyn til baggrundscheck efterleves for nye medarbejdere.	Ingen afvigelser konstateret.
7.1.2	*Ansættelsesvilkår og -betingelser* Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har inspiceret et udvalg af kontrakter med medarbejdere med henblik på at konstatere om medarbejderne havde underskrevet kontrakten.	Ingen afvigelser konstateret.

A.7.2 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
7.2.1	*Ledelsesansvar* Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har inspiceret proceduren vedrørende fastsættelse af krav til medarbejdere og kontrahenter. Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde it-sikkerhedspolitikken.	Ingen afvigelser konstateret.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
7.2.2	*Bevidsthed om, uddannelse og træning i informationssikkerhed* Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter vil ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, idet omfang det er relevant for deres jobfunktion.	Vi har inspiceret procedurer til sikring af tilstrækkelig uddannelse og træning (awarenesstræning). Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejdere.	Ingen afvigelser konstateret.
7.2.3	*Sanktioner* Der etableres en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.	Vi har inspiceret, at der er etableret en formel sanktionsproces, som er kommunikeret.	Ingen afvigelser konstateret.

A.7.3 Ansættelsesforholdets ophør eller ændring

Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
7.3.1	*Ansættelsesforholdets ophør eller ændring* Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.	Vi har forespurgt til medarbejderes og kontrahenters forpligtelser til opretholdelse af informationssikkerhed i forbindelse med ophør af ansættelse eller kontrakt. Vi har inspiceret dokumentation for at informationssikkerhedsansvar og -forpligtelser er defineret og kommunikeret.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

A.8.1 Ansvar for aktiver
Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
8.1.1	*Fortegnelse over aktiver* Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Vi har inspiceret fortegnelser over aktiver.	Ingen afvigelser konstateret.
8.1.2	*Ejerskab af aktiver* Der udpeges en ejer i organisationen for hvert aktiv.	Vi har inspiceret oversigt over ejerskab til aktiver.	Ingen afvigelser konstateret.
8.1.3	*Accepteret brug af aktiver* Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, dokumenteres og implementeres.	Vi har inspiceret reglerne for accepteret brug af aktiver.	Ingen afvigelser konstateret.
8.1.4	*Tilbagelevering af aktiver* Alle medarbejdere og eksterne brugere afleverer alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.	Vi har inspiceret proceduren til sikring af tilbagelevering af udleverede aktiver. Vi har forespurgt om, hvorvidt udleverede aktiver inddrages.	Ingen afvigelser konstateret.

A.8.2 Klassifikation af information Kontrolmål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.			
Nr.	**Sotea A/S' kontrol l**	**REVI-IT's test**	**Resultat af test**
8.2.1	*Klassifikation af information* Information klassificeres efter lovmæssige krav, værdi og efter hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.	Vi har inspiceret politik for klassificering af information.	Ingen afvigelser konstateret.
8.2.2	*Mærkning af information* Der udarbejdes og implementeres et passende sæt procedurer til mærkning af information i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.	Vi har forespurgt til procedurerne for mærkning af data, og vi har inspiceret, at information er mærket i overensstemmelse med klassifikationssystemet.	Ingen afvigelser konstateret.
8.2.3	*Håndtering af aktiver* Der udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.	Vi har forespurgt til procedurer for håndtering af aktiver, og vi har inspiceret procedurerne.	Ingen afvigelser konstateret.

A.8.3 Mediehåndtering Kontrolmål: at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
8.3.1	*Styring af bærbare medier* Der implementeres procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget.	Vi har forespurgt til procedurer for styring af bærbare medier, og vi har inspiceret dokumentation for løsningen.	Ingen afvigelser konstateret.
8.3.2	*Bortskaffelse af medier* Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.	Vi har inspiceret procedurer for bortskaffelse af medier. Vi har forespurgt til om medier bortskaffes i overensstemmelse med procedurerne.	Det har ikke været muligt at teste effektiviteten af kontrollen, da vi er blevet oplyst om, at der ikke er blevet bortskaffet medier i perioden. Ingen afvigelser konstateret.
8.3.3	*Fysiske medier under transport* Medier, der indeholder information, beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.	Vi har inspiceret procedurer for beskyttelse af medier under transport.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

A.9.1 Forretningsmæssige krav til adgangsstyring
Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.1.1	*Politik for adgangsstyring* En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.	Vi har inspiceret politikken for adgangsstyring med henblik på at konstatere, om den var opdateret og godkendt.	Ingen afvigelser konstateret.
9.1.2	*Adgang til netværk og netværkstjenester* Brugere har kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester. Vi har inspiceret et udvalg af brugere med henblik på at konstatere, at de kun har adgang til netværkstjenester, der er tildelt på baggrund af et arbejdsrelateret behov.	Ingen afvigelser konstateret.

A.9.2 Administration af brugeradgang
Kontrolmål: 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
9.2.1	*Brugerregistrering-og afmelding* Der implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.	Vi har forespurgt til procedurer for registrering og afmelding af brugere, og vi har inspiceret procedurerne. Vi har inspiceret et udvalg af registrering og afmelding af brugere med henblik på at konstatere om proceduren er fulgt.	Ingen afvigelser konstateret.
9.2.2	*Tildeling af brugeradgang* Der implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har inspiceret, at proceduren for brugeradministration er implementeret.	Ingen afvigelser konstateret.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.2.3	*Styring af privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder.	Ingen afvigelser konstateret.
9.2.4	*Styring af hemmelig autentifikationsinformation om brugere* Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces.	Vi har inspiceret proceduren vedrørende tildeling af passwords til platforme. Vi har, for et udvalg at tildelinger af passwords inspiceret, at proceduren overholdes.	Ingen afvigelser konstateret.
9.2.5	*Gennemgang af brugeradgangsrettigheder* Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har inspiceret proceduren for regelmæssig gennemgang og evaluering af adgangsrettigheder. Vi har inspiceret et udvalg af gennemgang og evalueringer af adgangsrettigheder.	Ingen afvigelser konstateret.
9.2.6	*Inddragelse eller justering af adgangsrettigheder* Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Vi har inspiceret procedurerne for inddragelse og justering af adgangsrettigheder. Vi har for et udvalg af fratrådte medarbejdere inspiceret, hvorvidt medarbejderne har fået deres adgangsrettigheder inddraget.	Ingen afvigelser konstateret.

A.9.3 Brugernes ansvar
Kontrolmål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
9.3.1	*Brug af hemmelig autentifikationsinformation* Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.	Vi har inspiceret retningslinjer for brug af fortrolige passwords.	Ingen afvigelser konstateret.

A.9.4 Styring af system- og applikationsadgang Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
9.4.1	*Begrænset adgang til informationer* Adgang til information og applikationssystemers funktioner begrænses i overensstemmelse med politikken for adgangsstyring.	Vi har inspiceret retningslinjer og procedurer til sikring af begrænsning af adgang til applikationssystemers funktioner.	Ingen afvigelser konstateret.
9.4.2	*Procedurer for sikker logon* Adgang til systemer og applikationer styres af en procedure for sikker logon.	Vi har forespurgt til procedure for sikkert login, og vi har inspiceret den implementerede løsning.	Ingen afvigelser konstateret.
9.4.3	*System for administration af passwords* Systemer til administration af passwords er interaktive og sikrer passwords med god kvalitet.	Vi har inspiceret, at der i politikker eller procedurer stilles krav til kvaliteten af passwords. Vi har inspiceret at systemer til administration af passwords er opsat i overensstemmelse med de stillede krav.	Ingen afvigelser konstateret.

A.10 Kryptografi

A.10.1 Kryptografiske kontroller Kontrolmål: 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**
10.1.1	*Politik for anvendelse af kryptografi* Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	Ingen afvigelser konstateret.
10.1.2	*Administration af nøgler* Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

A.11.1 Sikre områder
Kontrolmål: 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
11.1.1	*Fysisk perimetersikring* Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.	Vi har inspiceret proceduren for fysisk beskyttelse af faciliteter og perimetersikkerhed. Vi har inspiceret relevante lokationer og deres perimetersikring for at konstatere, hvorvidt der er sikringsforanstaltninger til at forhindre uautoriseret adgang.	Ingen afvigelser konstateret.
11.1.2	*Fysisk adgangskontrol* Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har inspiceret procedurerne for adgangskontrol til sikre områder. Vi har inspiceret udvalgte adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til produktionsfaciliteterne.	Ingen afvigelser konstateret.
11.1.3	*Sikring af kontorer, lokaler og faciliteter* Fysisk sikring af kontorer, lokaler og faciliteter er tilrettelagt og etableret.	Vi har inspiceret, at der er etableret fysisk sikring af kontorer, lokaler og faciliteter. Vi har inspiceret, at der foretages inspektion af brandslukningsudstyr og UPS-anlæg m.v. Vi har inspiceret, at der gennemføres test af generatorer, UPS-anlæg m.v.	Ingen afvigelser konstateret.
11.1.4	*Beskyttelse mod eksterne og miljømæssige trusler* Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret.	Vi har inspiceret proceduren vedrørende beskyttelse mod eksterne og miljømæssige trusler. Vi har forespurgt om implementering af sikkerhedsforanstaltninger til at forhindre trusler fra ild, varme og fugt og inspiceret relevante lokationer for at konstatere, om der er installeret brandslukningsudstyr, brand- og røgalarmer m.v.	Ingen afvigelser konstateret.

A.11.2 Udstyr Kontrolmål: 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**
11.2.1	*Placering og beskyttelse af udstyr* Udstyr er placeret og beskyttet, så risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes.	Vi har inspiceret proceduren vedrørende placering og beskyttelse af udstyr. Vi har inspiceret relevante lokationer for at vurdere, hvorvidt lokaler er sikkert aflåst og kontrolleret, og at kun medarbejdere med et arbejdsbetinget behov har adgang hertil.	Ingen afvigelser konstateret.
11.2.2	*Understøttende forsyninger (forsyningssikkerhed)* Udstyr er beskyttet mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.	Vi har inspiceret procedurer for beskyttelse af udstyr mod strømafbrydelser og andre afbrydelser som følge af svigt i understøttende forsyninger. Vi her inspiceret at backupstrøm, UPS-anlæg og dieselgeneratorer med tilstrækkelig kapacitet har været til rådighed. Vi har inspiceret servicerapporter, der viser, at serviceinspektioner er udført i overensstemmelse med leverandørers anbefalinger, og at udstyr testes regelmæssigt.	Ingen afvigelser konstateret.
11.2.3	*Sikring af kabler* Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, er beskyttet mod indgreb, interferens og skader.	Vi har inspiceret beskyttelsen af et udvalg af strøm- og datakabler med henblik på at konstatere om kablerne var beskyttet mod indgreb og skader.	Ingen afvigelser konstateret.
11.2.4	*Vedligeholdelse af udstyr* Udstyr vedligeholdes korrekt for at sikre dets fortsatte tilgængelig hed og integritet.	Vi har forespurgt til servicerapporter vedrørende vedligeholdelse af et udvalg af udstyr med henblik på at konstatere, om udstyret var vedligeholdt i overensstemmelse med leverandørernes anbefalinger. Vi har inspiceret servicerapporter, der viser, at serviceinspektioner er udført i overensstemmelse med leverandørers anbefalinger, og at udstyr testes regelmæssigt.	Ingen afvigelser konstateret.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
11.2.5	*Fjernelse af aktiver* Udstyr, information og software må ikke fjernes fra organisationen uden forudgående tilladelse.	Vi har inspiceret retningslinjer for fjernelse af udstyr, information og software fra virksomheden.	Ingen afvigelser konstateret.
11.2.6	*Sikring af udstyr og aktiver uden for organisationen* Der er etableret sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen.	Vi har inspiceret retningslinjer for sikring af udstyr og aktiver uden for organisationen.	Ingen afvigelser konstateret.
11.2.7	*Sikker bortskaffelse eller genbrug af udstyr* Alt udstyr med lagringsmedier verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.	Vi har inspiceret proceduren for sletning af data og software på lagringsmedier inden bortskaffelse af lagringsmediet. Vi har forespurgt til bortskaffelse af et udvalg af udstyr med henblik på at konstatere, om data og software blev slettet inden bortskaffelsen fandt sted.	Det har ikke været muligt at teste effektiviteten af kontrollen, da vi er blevet oplyst at udstyr ikke er blevet bortskaffet eller genbrugt i perioden. Ingen afvigelser konstateret.
11.2.8	*Brugerudstyr uden opsyn* Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.	Vi har inspiceret proceduren for sikring af beskyttelse af udstyr, som er uden opsyn.	Ingen afvigelser konstateret.
11.2.9	*Politik for ryddeligt skrivebord og blank skærm* Der er udarbejdet en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.	Vi har inspiceret politik for ryddeligt skrivebord og blank skærm.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

A.12.1 Driftsprocedurer og ansvarsområder
Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.1.1	*Dokumenterede driftsprocedurer* Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem.	Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret og vedligeholdt. Vi har stikprøvevis inspiceret, at driftsdokumentation er opdateret og tilgængelig for medarbejdere, som har behov for dem.	Ingen afvigelser konstateret.
12.1.2	*Ændringsstyring* Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret proceduren for ændringsstyring. Vi har stikprøvevis inspiceret hvorvidt ændringer foretaget på platforme er håndteret i overensstemmelse med proceduren for ændringsstyring.	Vi har via vores stikprøver observeret at proceduren for ændringsstyring ikke har været fulgt konsekvent i perioden. Ingen yderligere afvigelser konstateret.
12.1.3	*Kapacitetsstyring* Anvendelsen af ressourcer overvåges og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.	Vi har inspiceret proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav. Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring.	Ingen afvigelser konstateret.
12.1.4	*Adskillelse af udviklings-, test- og driftsmiljøer* Udviklings-, test- og driftsmiljøer adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.	Vi har forespurgt til sikring af adskillelse af udviklings-, test- og driftsmiljøer. Vi har stikprøvevis inspiceret, at der enten er logisk eller fysisk adskillelse mellem udvikling, test og produktion.	Ingen afvigelser konstateret.

A 12.2 Malwarebeskyttelse Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
12.2.1	*Kontroller mod malware* Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen afvigelser konstateret.

A.12.3 Backup Kontrolmål: At beskytte mod tab af data.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
12.3.1	*Backup af information* Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har forespurgt til krav til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for, at opsætningen var i overensstemmelse med kravene. Vi har forespurgt til test af gendannelse fra backupfiler, og vi har inspiceret dokumentation for test af gendannelse.	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning Kontrolmål: At registrere hændelser og tilvejebringe bevis.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
12.4.1	*Hændelseslogning* Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Vi har forespurgt til logning af brugeraktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne.	Ingen afvigelser konstateret.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
12.4.2	*Beskyttelse af log- oplysninger* Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har forespurgt til proceduren for sikring af logoplysninger. Vi har inspiceret et udvalg at logningskonfigurationer med henblik på at konstatere, om logningsinformationer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	*Administrator- og operatørlog* Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt.	Vi har inspiceret proceduren vedrørende logning af aktiviteter udført af systemadministratorer og -operatører. Vi har inspiceret logopsætninger med henblik på at konstatere, om systemadministratorers og -operatørers handlinger logges.	Ingen afvigelser konstateret.
12.4.4	*Tidssynkronisering* Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne er synkroniserede til en enkelt referencetidskilde.	Vi har forespurgt til proceduren for synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware Kontrolmål: At sikre integriteten af driftssystemer.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
12.5.1	*Softwareinstallation på driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret retningslinjer for installation af software på driftssystemer.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
12.6.1	Styring af tekniske sårbarheder Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder. Vi har stikprøvevis inspiceret servere, databasesystemer og netværkskomponenter for at konstatere, hvorvidt de er patchet rettidigt.	Ingen afvigelser konstateret.
12.6.2	Begrænsninger på softwareinstallation Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.	Vi har forespurgt til procedurer for begrænsning af softwareinstallation, som foretages af brugere. Vi har inspiceret, at regler for softwareinstallation efterleves.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

A.13.1 Styring af netværkssikkerhed
Kontrolmål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
13.1.1	*Netværksstyring* Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har inspiceret, at der er defineret krav om styring og kontrol af netværk, herunder krav og regler om kryptering, segmentering, firewalls og andre relevante sikkerhedsforanstaltninger.	Ingen afvigelser konstateret.
13.1.2	*Sikring af netværkstjenester* Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.	Vi har observeret, at der foreligger skriftlige krav til sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester.	Ingen afvigelser konstateret.
13.1.3	*Opdeling af netværk* Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.	Vi har inspiceret retningslinjerne for segmentering af netværk. Vi har inspiceret netværksoversigt.	Ingen afvigelser konstateret.

A.13.2 Informationsoverførsel
Kontrolmålet: 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
13.2.1	*Politikker og procedurer for informationsoverførsel* Der foreligger formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.	Vi har inspiceret politikker og procedurer for dataoverførsel.	Ingen afvigelser konstateret.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
13.2.2	*Aftaler om informationsoverførsel* Aftaler omhandler sikker overførsel af forretningsinformation mellem organisationen og eksterne parter.	Vi har forespurgt til aftaler om dataoverførsel. Vi har inspiceret, at der foreligger aftaler med kunder og andre eksterne parter, der beskriver krav til sikker udveksling af data.	Ingen afvigelser konstateret.
13.2.3	*Elektroniske meddelelser* Informationer i elektroniske meddelelser beskyttes på passende måde.	Vi har forespurgt til retningslinjer for afsendelse af fortrolig information.	Ingen afvigelser konstateret.
13.2.4	*Fortroligheds- og hemmeligholdelsesaftaler* Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, identificeres, gennemgås regelmæssigt og dokumenteres.	Vi har forespurgt til procedure for etablering af fortrolighedsaftaler. Vi har inspiceret et udvalg af underskrevne fortrolighedsaftaler med henblik på at konstatere, om proceduren efterleves ved ansættelse af nye medarbejdere.	Ingen afvigelser konstateret.

A.15 Leverandørforhold

A.15.1 Informationssikkerhed i leverandørforhold
Kontrolmål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
15.1.1	*Informationssikkerhedspolitik for leverandørforhold* Informationssikkerhedskravene til at minimere risicienе forbundet med leverandørers adgang til organisationens aktiver aftales med leverandøren og dokumenteres.	Vi har inspiceret proceduren for indgåelse af aftaler med leverandører. Vi har inspiceret proceduren vedrørende udvælgelse og beskyttelse af testdata.	Ingen afvigelser konstateret.
15.1.2	*Håndtering af sikkerhed i leverandøraftaler* Alle relevante informationssikkerhedskrav fastlægges og aftales med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information.	Vi har inspiceret proceduren for indgåelse af aftaler med leverandører. Vi har stikprøvevis inspiceret indgåede leverandøraftaler m.h.t. aftaler om informationssikkerhedskrav.	Ingen afvigelser konstateret.

15.2 Styring af leverandørydelser Kontrolmål: 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**
15.2.1	*Overvågning og gennemgang af leverandørydelser* Organisationer overvåger, gennemgår og auditerer leverandørydelser.	Vi har inspiceret at proceduren for overvågning og gennemgang af serviceydelser leveret af underleverandører er i overensstemmelse med det aftalte. Vi har Inspiceret et udvalg af statusmødereferater, driftsrapporteringer m.v. som anvendes til sikring af, at det der leveres, er i overensstemmelse med det aftalte. Vi har Inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører.	Ingen afvigelser konstateret.
15.2.2	*Styring af ændringer af leverandørydelser* Leverandørydelser overvåges, gennemgås og auditeres.	Vi har forespurgt til styring af ændringer hos leverandører og inspiceret dokumentation for håndteringen.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

A.16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: 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
16.1.1	*Ansvar og procedurer* Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har forespurgt til ansvar og procedurer i forbindelse med informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har endvidere inspiceret procedure til håndtering af informationssikkerhedshændelser.	Ingen afvigelser konstateret.
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne.	Ingen afvigelser konstateret.
16.1.3	*Rapportering af informationssikkerhedssvagheder* Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester.	Vi har forespurgt til informationssikkerhedshændelser i perioden, samt inspiceret disse.	Ingen afvigelser konstateret.
16.1.4	*Vurdering af og beslutning om informations- sikkerhedshændelser* Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	Vi har inspiceret proceduren for vurdering og evaluering af informationssikkerhedsbrud.	Ingen afvigelser konstateret.
16.1.5	*Håndtering af informationssikkerhedsbrud* Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer.	Vi har forespurgt hvorvidt informations sikkerhedsbrud har været håndteret i overensstemmelse med de dokumenterede procedurer.	Det har ikke været muligt at teste effektiviteten af kontrollen, da vi er blevet oplyst at der ikke har været informationssikkerhedsbrud i perioden. Ingen afvigelser konstateret.

Nr.	Sotea A/S' kontrol	REVI-IT's test	Resultat af test
16.1.6	*Erfaring fra informationssikkerhedsbrud* Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.	Vi har forespurgt vedrørende Problem Management-funktion, der analyserer informationssikkerhedsbrud med henblik på at reducere sandsynligheden for at de gentager sig.	Ingen afvigelser konstateret.

A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

A.17.1 Informationssikkerhedskontinuitet

Kontrolmål: 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
17.1.1	*Planlægning af informationssikkerhedskontinuitet* Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.	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.	Ingen afvigelser konstateret.
17.1.2	*Implementering af informationssikkerhedskontinuitet* Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.	Vi har forespurgt om der er procedurer der sikrer, at alle relevante systemer indgår i beredskabsplanlægningen. Vi har inspiceret om beredskabsplanen vedligeholdes.	Ingen afvigelser konstateret.
17.1.3	*Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten* Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til regelmæssig revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurderingen.	Ingen afvigelser konstateret.

A.17.2 Redundans Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.			
Nr.	**Sotea A/S' kontrol**	**REVI-IT's test**	**Resultat af test**
17.2.1	*Tilgængelighed af informationsbehandlingsfaciliteter* Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	Vi har forespurgt til etablering af redundans til sikring af tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen afvigelser konstateret.

A.18 Overensstemmelse

A.18.2 Gennemgang af informationssikkerheden Kontrolmål: 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**
18.2.1	*Uafhængig gennemgang af informationssikkerhed* Organisationens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.	Vi har observeret, at der er etableret krav om regelmæssig uafhængig revisionsmæssig gennemgang af informationssikkerheden.	Ingen afvigelser konstateret.
18.2.2	*Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder* Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.	Vi har forespurgt vedrørende lederes sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder.	Ingen afvigelser konstateret.

Afsnit 5: Ledelsens bemærkninger til revisionens testresultater

12.1.2 Ændringsstyring:

Revisors bemærkning tages til efterretning.

Vi har haft en periode hvor change er registret som almindelige tickets, og dermed har det været svært at få overblik over change generelt, for vores medarbejdere. Vi har igangsat nyt system og ny procedure omkring registrering af change, så disse er mere tilgængelige og mere synlige for hele organisationen.