

reviit

et trygt samfund med IT og data

v

Revisorerklæring

Softværket a.m.b.a

ISAE 3402 type 2 erklæring om generelle IT-kontroller for perioden 1. juni 2021 til 31. maj 2022 relateret til ydelser i forbindelse med drift af deres IT-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF

Juni 2022

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

Indholdsfortegnelse

Afsnit 1:	Beskrivelse af Softværket a.m.b.a's ydelser i forbindelse med drift af deres IT-hostingløsning Forsyning Hosting samt finans- og forbrugersystemet Forsyning FOF samt generelle IT-kontroller relateret hertil.	1
Afsnit 2:	Softværket a.m.b.a's udtalelse	6
Afsnit 3:	Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet.....	8
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf.....	11

Afsnit 1: Beskrivelse af Softværket a.m.b.a's ydelser i forbindelse med drift af deres IT-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF samt generelle IT-kontroller relateret hertil.

Formål

Hensigten med denne kontrolbeskrivelse er at tilkendegive over for alle, som har en relation til Softværket, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Softværket ønsker at opretholde og løbende udbygge et IT-sikkerhedsniveau på højde med de krav, som skitseres i ISO 27002. Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretlige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Softværket fremstår troværdig. For at fastholde Softværket troværdighed skal det sikres, at information behandles med fornøden fortrolighed, og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer og data betragtes, næst efter medarbejderne, som Softværket mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, sikkerhed, høj kvalitet, overholdelse af lovgivningskrav, og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at Softværket image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Alle personer betragtes som værende potentiel årsag til et muligt brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

På de efterfølgende sider behandles de enkelte punkter, der læner sig op ad rækkefølgen i ISO 27002.

Bemærk at dokumentation i ISO 27002 starter med punkt 4, da punkt 1 til 3 er indledende bemærkninger.

4 - Risikovurdering og -håndtering

Softværket har en procedure for løbende risikovurdering af udvikling og vedligeholdelse af hosting-miljøet og Forsyning|FOF. Dermed kan Softværket sikre, at de risici, som er forbundet med hosting-miljøet samt udvikling og vedligeholdelsen af Forsyning|FOF, er minimeret til et acceptabelt niveau.

Risikovurdering opdateres en gang årligt, samt når der foretages større ændringer i udviklingen eller vedligeholdelsen, som vurderes relevante i forhold til at revurdere den generelle risikovurdering. Alle risici bliver inddelt i kategorierne Grøn, Gul og Rød. Ledelsen i Softværket forholder sig til alle risici i alle kategorier.

IT-sikkerhedsudvalget og den samlede ledergruppe har det overordnede ansvar for implementering af korrigerende handlinger for at minimere de identificerede risici.

5 - Sikkerhedspolitik

IT-Sikkerhedspolitikken gennemgås en gang årligt. Denne gennemgang ligger som en fast opgave i årshjulet for IT-sikkerhedsudvalget.

6 - Organisering af informationssikkerhed

Der er skarp funktionsadskillelse, hvilket betyder, at det kun er udviklere, der kan tilgå og ændre i kildekode og programmets funktionalitet. Ligeledes er det kun ansatte hos vores hosting-partner, Teknisk Afdeling, GIS- og udviklingsafdelingen, der i samarbejde har adgang til at lave ændringer i Hosting-miljøet, der kan påvirke driftsstabiliteten.

Kunder har kun adgang til egne data. Brugere er oprettet som navngivne brugere og anvender personligt brugernavn og password. Adgang til produktionsdata, sker via en krypteret forbindelse.

Den enkelte medarbejder har ikke direkte adgang til produktionsserverne fra egen PC. Er det nødvendigt at tilgå produktionsdata for at yde support eller fejlfinde, sker dette igennem RDS eller TeamViewer, hvor der er sporbarhed af, hvem der logger på.

7 - Sikkerhed i forhold til HR

Eksterne konsulenter skal underskrive en fortrolighedserklæring inden de får adgang til Hosting- eller udviklingsmiljøet. Softværket anvender kun konsulenter, der har en høj standard, og hvor velbeskrevne IT-sikkerhedsprocedurer er en del af standardaftalen.

Alle medarbejdere i Softværket har underskrevet en fortrolighedserklæring, og er instrueret i håndtering af fortrolige oplysninger. Denne fortrolighed er også gældende ved ansættelses ophør. Brud på sikkerhedspolitikken kan medføre en opsigelse af ansættelsesforholdet.

8 - Styring af aktiver

Alle data i Hosting-miljøet er håndteret som fortrolige kundedata. Alle medier indeholdende kundedata skal behandles med største omhu. Det bliver registreret, hvilket databærende udstyr en medarbejder får udleveret, og ved ophør af ansættelsesforholdet bliver alt udstyr inddraget.

Ligesom med systemdata, opererer Softværket med systemejere, der er ansvarlig for forskellige aktiver. Herigennem sikrer vi individuel fokus på sikkerheden i alle delelementer.

Alt databærende udstyr destrueres og bortskaffes på ansvarlig vis.

Alt kildekode og programmer, der udvikles, er Softværkets ejendom, og må ikke kopieres eller overdrages til 3. part.

9 – Adgangskontrol

Det er kun Teknisk Afdeling, der har adgang til at oprette nye brugere, og alle medarbejderne her er instrueret i håndtering af kunders brugernavn og kodeord.

Det er kun Teknisk Afdeling, der har adgang til at oprette nye brugere og roller i databaserne samt ændre passwords.

Oprettelse og lukning af brugere sker udelukkende via skriftlig henvendelse, og efter at identitet er blevet bekræftet. Alle brugere oprettes med et stærkt kodeord, der for hosting-brugere skal skiftes mindst en gang årligt og for medarbejdere i Softværket 2 gange årligt.

Der er yderligere sikring af kunders data ved, at en konto automatisk bliver spærret ved 5 på hinanden følgende fejl i indtastning af kodeord. Dette er for at forhindre, at man kan gætte sig frem til et kodeord. Der er også sat flere interne kontroller op til at registrere eventuelt misbrug af rettigheder i Hosting-miljøet. Forsyning|Hosting benytter 2-faktor login.

Brugerrettigheder gennemgås en gang årligt. Denne gennemgang ligger som en fast opgave i årshjulet for IT-sikkerhedsudvalget.

10 - Kryptografi

Al adgang til Hosting-miljøet sker via en krypteret forbindelse.

Softværket anvender et krypteret system til opbevaring af administrative kodeord.

Kommunikation af følsomt og fortroligt data sker via sikker mail.

Softværket holder sig løbende opdateret på krypterings-teknologier/protokoller.

11 - Fysiske og miljømæssige sikringer

Fysisk adgang til bygningen via hovedindgang er overvåget af en reception. Alle andre indgange er låst med en elektronisk lås.

Adgang til serverrum er også sikret med elektronisk lås, og serverne er yderligt beskyttet af et metalgitter med elektronisk lås. Eksterne konsulenter har kun ledsaget adgang til serverrum. Alle lokaler er monteret med tyverialarm, og der er brandslukningsudstyr i serverrummet. Derudover er der UPS-anlæg i serverrummet, som sikrer mod kortvarigt strømudfald.

For Forsyning | Hostings vedkommende sikres den fysiske og organisatoriske sikkerhed via de indgåede aftaler med underleverandørerne.

Der tages daglig backup af alle data i Hosting miljøet, og hver nat føres en kopi af data fra Softværket Hosting til en sikret sekundær lokation. Samme procedure er gældende for Softværkets interne miljø.

12 - Sikkerhed i forbindelse med drift

Softværket opererer med dobbeltroller på udvalgte systemer, som sikrer personuafhængighed. Desuden er der en fyldestgørende systemdokumentation, som løbende opdateres.

Aktiv overvågning sikrer kapacitetsstyring i Hosting-miljøet, af både hosting-partner og Softværket.

Sikkerhed i Hosting-miljøet sker primært ved at brugerne har begrænsede rettigheder. Det er ikke muligt selv at installere programmer, ligesom download fra hjemmesider som udgangspunkt er spærret. Hele systemet er desuden sikret via firewall og ved begrundet mistanke overvåges netværkstrafik.

13 - Kommunikationssikkerhed

Sikkerhed af vores netværk er af højeste prioritet. Alt er sikret via firewall, og der er udarbejdet procedurer, vejledninger og dokumentation til anvendelse i forbindelse med drift og vedligehold af netværket. Disse opbevares sammen med systemdokumentationen.

Der er opsat overvågning og logning af netværkstrafik. Alene godkendt netværkstrafik kommer gennem vores firewall. Dette gælder både indgående og udgående trafik.

Der er en segmentering af netværket, afhængig af funktionsbehov.

Softværket overfører ikke, medmindre det konkret er aftalt, kunders data eller dele deraf til 3. part. Der er etableret fortrolighedsaftaler for alle involveret med kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.

14 - Anskaffelse, udvikling og vedligeholdelse

Der er fastsatte procedurer ifm. egen udvikling og indkøb/implementering af software. Disse dækker over procedure, før-, under og efter i idriftsættelse.

Udvikling af Forsyning|FOF forestås primært af Softværkets udviklingsafdeling.

Der foreligger en proces beskrivelse for brug af testdata, så data bliver anonymiseret og ikke er personhenførbare.

15 - Leverandørforhold

Der er fortrolighedserklæringer med alle konsulenter der får adgang til systemet. Som udgangspunkt arbejder de udelukkende med hard- og softwareproblemstillinger, stillet af Softværket.

Softværket anvender kun konsulenter, der har en høj standard, og hvor velbeskrevne IT-sikkerheds procedurer er en del af standardaftalen.

Softværket har delvist uddelegeret driften for Hosting-miljøet til hosting-partner. Softværket har selv driftsansvaret for eget servermiljø hos Softværket.

Softværket fører tilsyn med underleverandører ud fra en risikobaseret vurdering af de enkelte underleverandører. Tilsynet kan foretages ved gennemlæsning af revisionserklæringer, ISO-standard-certifikater, fysiske besøg eller i kombination.

16 - Styring af sikkerhedshændelser

Softværket har klare procedurer for alle sikkerhedshændelser.

Alle hændelser bliver registreret og løst uden ophold. Det er IT sikkerhedsudvalget, der har det overordnede ansvar for processen.

17 - Informationssikkerhedsaspekter ved beredskabsstyring

Katastrofer forsøges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttet ud fra en afvejning af risici holdt op imod sikringsomkostninger. Softværket har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer.

Softværket beredskabsplan omfatter:

- Skadebegrænsende tiltag
- Etablering af temporære nødløsninger
- Genetablering af permanent løsning

Softværket har implementeret formelle nødplaner, og procedurer til beredskab for alle punkter. Softværket har redundans i alle kritiske netværkskomponenter. Derudover refereres der til hosting-partnerens IT-revisi-
onserklæring.

18 - Overensstemmelse

Hverken Softværket eller vores kunder, er underlagt særlig lovgivning i forhold til vores ydelse. Softværket er dog opmærksom på, at lovændringer kan medføre behov for at revurdere nogle af selskabets procedurer og retningslinjer for opbevaring af data.

En gang årligt gennemgås den gældende sikkerhedspolitik af IT-sikkerhedsudvalget. Yderligere gennemganges foretages i forbindelse med større ændringer i organisationen eller hosting-miljøet.

Det er IT-sikkerhedsudvalget, der har det overordnede ansvar for IT-sikkerhedspolitikken.

Der foretages evalueringen af en ekstern IT-revisor samt i forbindelse med udarbejdelse af de årlige ISAE 3402 erklæringer.

Kvalitetssikring af Forsyning|FOF

Udgangspunktet for test og kvalitetssikring i Softværket er, at alle udviklingsopgaver bliver testet både manuelt og via. automatiske tests, inden de bliver frigivet i en ny release af Forsyning|FOF.

Der anvendes et testværktøj til udvikling af automatiserede tests, og de automatiserede tests udvikles og opdateres løbende. Der udgives ikke en nye release af Forsyning|FOF før alle tests, både manuelle og automatiske, udføres uden fejl.

Komplementerende kontroller

De forhold som Softværkets kunder antages at være ansvarlige for - både de indlysende og jf. Softværkets forretningsvilkår/SLA.

Softværkets kunder er, medmindre andet er aftalt, ansvarlige for selv at etablere forbindelse til Softværkets hostingmiljø. Herudover er Softværkets kunder, medmindre andet er aftalt, ansvarlige for:

At det aftalte niveau for backup dækker kundens behov

Eget sikkerhedsniveau, beredskab, backup, løbende opdateringer, drift osv., såfremt de ikke benytter Forsyning|Hosting

Ændringer i perioden

- Af organisatoriske ændringer er der i perioden ansat i alt 5 medarbejdere fordelt på henholdsvis GIS-, teknisk-, konsulent- og supportafdelingen samt administrationen. 3 medarbejdere er fratrådt.
- Ændring af produktansvarlig for Forsyning|FOF
- Navneændring fra DFF|EDB a.m.b.a til Softværket a.m.b.a
- Fået installeret Logningsudstyr i Forsyning|Hosting fra EnergiCert
- DKIM er tilføjet på mail
- Advanced Treat Protection (ATP) aktiveret i spam-filter
- 2 eksterne Business Central konsulenter samt 1 projektleder indlejet
- Efter 1. december 2021 forlanges der forevisning af straffeattest i forbindelse med ansættelser
- Fra 09.03.2022 er der indført yderligere tiltag således der tages offline backup for Softværkets eget miljø samt offline backup i Forsyning|Hosting.
- Ændring i vores produktansvarsorganisation (PAO) i foråret 2022. Ændringen omfatter, at stillingen som Product Manager nedlægges og de produktansvarlige vil i stedet have faglig reference til direktøren. I den forbindelse er der kommet ny produktansvarlig for Forsyning|Hosting.

Afsnit 2: Softværket a.m.b.a's udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Softværket a.m.b.a's ydelser i forbindelse med drift af deres IT-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, 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.

Softværket a.m.b.a anvender serviceunderleverandøren Curanet A/S. Denne erklæring er udarbejdet efter partielmetoden, og Softværket a.m.b.a's kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Curanet A/S. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Softværket a.m.b.a's beskrivelse i afsnit 1 af generelle IT-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Softværket a.m.b.a. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Softværket a.m.b.a bekræfter, at:

- (a) Den medfølgende beskrivelse i afsnit 1, giver en retvisende beskrivelse af de generelle IT-kontroller med relevans for Softværket a.m.b.a's ydelser i forbindelse med drift af deres IT-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, der har behandlet kunders transaktioner i perioden fra 1. juni 2021 til 31. maj 2022.

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. juni 2021 til 31. maj 2022.
- (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. juni 2021 til 31. maj 2022, hvis relevante kontroller hos underleverandør var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af Softværket a.m.b.a i hele perioden fra 1. juni 2021 til 31. maj 2022. 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. juni 2021 til 31. maj 2022.

Kolding, den 28. juni 2022
Softværket a.m.b.a



Jan Elmstrøm Blaabjerg
Adm. direktør

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

Til Softværket a.m.b.a, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om Softværket a.m.b.a's beskrivelse i afsnit 1 af generelle IT-kontroller for drift af brugersystemer til behandling af Softværket a.m.b.a's kunders transaktioner i perioden 1. juni 2021 til 31. maj 2022 og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Softværket a.m.b.a anvender serviceunderleverandøren Curanet A/S. Denne erklæring er udarbejdet efter partielmetoden, og Softværket a.m.b.a's kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Curanet A/S. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af Softværket a.m.b.a's kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Softværket a.m.b.a.

Enkelte af de kontrolmål, der er anført i Softværket a.m.b.a's beskrivelse i afsnit 1 af generelle IT-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Softværket a.m.b.a. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Softværket a.m.b.a's ansvar

Softværket a.m.b.a 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 International Ethics Standards Board for Accountants' internationale retningslinjer for revisorerets etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

REVI-IT anvender ISQC 1¹ 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 Softværket a.m.b.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 kontrollerens 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 Softværket a.m.b.a.'s udtalelse i afsnit 1.

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

Softværket a.m.b.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 Softværket a.m.b.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 1. juni 2021 til 31. maj 2022, 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. juni 2021 til 31. maj 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandøren var operationelt effektive, og hvis kunderne har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Softværket a.m.b.a.'s kontroller i perioden fra 1. juni 2021 til 31. maj 2022
- (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 1. juni 2021 til 31. maj 2022

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 Softværket a.m.b.a.'s ydelser i forbindelse med drift af deres IT-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, 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 risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 28. juni 2022

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Henrik Paaske

Statsautoriseret revisor



Basel Rimón 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 Softværket a.m.b.a.'s kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos Softværket a.m.b.a.' underleverandør Curanet A/S.

Kontroller, som er specifikke for de enkelte kundeløsninger, eller som er udført af Softværket a.m.b.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 Softværket a.m.b.a. 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 Softværket a.m.b.a.

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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
5.1.1	<p><i>Politikker for informationssikkerhed</i></p> <p>Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.</p> <p>Der er etableret faste procedurer for behandling af risici.</p>	<p>Vi har observeret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.</p> <p>Vi har inspiceret risikovurderingen for at vurdere, hvorvidt den fortsat er egnet, fyldestgørende og effektiv.</p>	Ingen afvigelser konstateret.
5.1.2	<p><i>Gennemgang af politikker for informationssikkerhed</i></p> <p>Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.</p> <p>Der gennemføres regelmæssigt en analyse og vurdering af IT-risikobilledet.</p>	<p>Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken.</p> <p>Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
6.1.1	<i>Roller og ansvarsområder for informationssikkerhed</i> Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret dokumentation for, at ansvaret for informationssikkerhed er klart defineret og fordelt.	Ingen afvigelser konstateret.
6.1.2	<i>Funktionsadskillelse</i> 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. Ved forespørgsel og inspektion af systemudtræk har vi undersøgt om driftspersonale kun har adgang til at administrere rettigheder på systemer, for hvilke de er ansvarlige, og om udviklere har adgang til produktionsmiljøet.	Ingen afvigelser konstateret.
6.1.3	<i>Kontakt med myndigheder</i> Der opretholdes passende kontakt med relevante myndigheder.	Vi har inspiceret dokumentation for, at der er retningslinjer for passende kontakt med myndigheder.	Ingen afvigelser konstateret.
6.1.4	<i>Kontakt med særlige interessegrupper</i> Der opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.	Vi har inspiceret proceduren vedrørende vedligeholdelse af reglerne for passende kontakt med særlige interessegrupper, faglige sikkerhedsfora og faglige organisationer.	Ingen afvigelser konstateret.

A.6.2 Mobilt udstyr og fjernarbejdspladser

Kontrolmål: Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
6.2.1	<p><i>Politik for mobilt udstyr</i></p> <p>Der er etableret en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.</p>	<p>Vi har inspiceret politik for sikring af mobile enheder.</p> <p>Vi har inspiceret, at der er defineret tekniske kontroller til sikring af mobile enheder.</p> <p>Vi har inspiceret, at tekniske kontroller er implementeret på mobile enheder.</p>	Ingen afvigelser konstateret.
6.2.2	<p><i>Fjernarbejdspladser</i></p> <p>Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
7.1.1	<p><i>Screening</i></p> <p>Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse se 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.</p>	<p>Vi har inspiceret procedure for ansættelse af nye medarbejdere og de sikkerhedsopgaver, der skal udføres i den forbindelse.</p> <p>Vi har inspiceret dokumentation for, at screening er gennemført i forbindelse med ansættelser.</p>	Ingen afvigelser konstateret.
7.1.2	<p><i>Ansættelsesvilkår og -betingelser</i></p> <p>Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.</p>	<p>Vi har inspiceret et udvalg af kontrakter med medarbejdere, med henblik på at konstatere om medarbejdere havde underskrevet kontrakten.</p> <p>Vi har inspiceret, at en standardansættelseskontrakt indeholder pågældende og organisationens ansvar for informationssikkerhed.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
7.2.1	<p><i>Ledelsesansvar</i></p> <p>Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.</p>	<p>Vi har inspiceret proceduren vedrørende fastsættelse af krav til medarbejdere og kontrahenter.</p> <p>Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde informationssikkerhedspolitikken.</p>	Ingen afvigelser konstateret.
7.2.2	<p><i>Bevidsthed om, uddannelse og træning i informationssikkerhed</i></p> <p>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.</p>	<p>Vi har inspiceret proceduren til sikring af tilstrækkelig uddannelse og træning i informationssikkerhed.</p> <p>Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejderne.</p>	Ingen afvigelser konstateret.
7.2.3	<p><i>Sanktioner</i></p> <p>Der er etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.</p>	<p>Vi har inspiceret, at der er etableret en formel sanktionsproces, som er kommunikeret til medarbejdere og kontrahenter.</p>	Ingen afvigelser konstateret.

A.7.3 Ansættelsesforholdets ophør eller ændring

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

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
7.3.1	<p><i>Ansættelsesforholdets ophør eller ændring</i></p> <p>Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikerer til medarbejderen eller kontrahenten og håndhæves.</p>	<p>Vi har forespurgt til medarbejderen og kontrahentens forpligtelser til opretholdelse af informationssikkerhed i forbindelse med ophør af ansættelse eller kontrakt.</p> <p>Vi har inspiceret dokumentation for at informationssikkerhedsansvar og -forpligtelser ved ansættelsens ophør eller ændring er defineret og kommunikeret.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
8.1.1	<p><i>Fortegnelse over aktiver</i></p> <p>Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver.</p>	Vi har inspiceret fortegnelser over aktiver.	Ingen afvigelser konstateret.
8.1.2	<p><i>Ejerskab af aktiver</i></p> <p>Der udpeges en ejer i organisationen for hvert aktiv.</p>	Vi har inspiceret oversigt over ejerskab til aktiver.	Ingen afvigelser konstateret.
8.1.3	<p><i>Accepteret brug af aktiver</i></p> <p>Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, dokumenteres og implementeres.</p>	Vi har inspiceret reglerne for accepteret brug af aktiver.	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
8.1.4	<p><i>Tilbagelevering af aktiver</i></p> <p>Alle medarbejdere og eksterne brugere afleverer alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.</p>	<p>Vi har inspiceret proceduren til sikring af tilbagelevering af udleverede aktiver.</p> <p>Vi har stikprøvevis inspiceret, at aktiver er inddraget for fratrådte medarbejdere.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
8.2.1	<p><i>Klassifikation af information</i></p> <p>Information klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.</p>	Vi har inspiceret politik for klassificering af information.	Ingen afvigelser konstateret.
8.2.3	<p><i>Håndtering af aktiver</i></p> <p>Der er udarbejdet og implementeret procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.</p>	Vi har inspiceret proceduren for håndtering af aktiver.	Ingen afvigelser konstateret.

A.8.3 Mediehåndtering

Kontrolmål: at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
8.3.1	<p><i>Styring af bærbare medier</i></p> <p>Der er implementeret procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget.</p>	Vi har inspiceret procedurer for styring af bærbare medier.	Ingen afvigelser konstateret.
8.3.2	<p><i>Bortskaffelse af medier</i></p> <p>Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.</p>	<p>Vi har inspiceret proceduren for bortskaffelse af medier.</p> <p>Vi har inspiceret, at medier bortskaffes i overensstemmelse med procedurerne.</p>	<p>Vi er blevet informeret om, at udstyr ikke er blevet bortskaffet eller genbrugt i perioden, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

A.9 Adgangsstyring

A.9.1 Forretningsmæssige krav til adgangsstyring

Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
9.1.1	<p><i>Politik for adgangsstyring</i></p> <p>En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.</p>	Vi har inspiceret politikken for adgangsstyring.	Ingen afvigelser konstateret.
9.1.2	<p><i>Adgang til netværk og netværkstjenester</i></p> <p>Brugere har kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.</p>	<p>Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester.</p> <p>Vi har inspiceret et udvalg af brugere med henblik på at konstatere, at de kun har adgang til godkendte netværk og netværkstjenester, der er tildelt på baggrund af et arbejdsrelateret behov.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
9.2.1	<p><i>Brugerregistrering-og afmelding</i></p> <p>Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling og afmelding af adgangsrettigheder.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgangsrettigheder.</p> <p>Vi har stikprøvevis inspiceret, at brugernes adgangsrettigheder er godkendt.</p> <p>Vi har inspiceret, at fratrådte brugeres adgangsrettigheder er nedlagt.</p>	Ingen afvigelser konstateret.
9.2.2	<p><i>Tildeling af brugeradgang</i></p> <p>Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.</p>	<p>Vi har inspiceret, at der er etableret en procedure for brugeradministration.</p> <p>Vi har inspiceret, at proceduren for brugeradministration er implementeret.</p>	Ingen afvigelser konstateret.
9.2.3	<p><i>Styring af privilegerede adgangsrettigheder</i></p> <p>Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.</p>	<p>Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder.</p> <p>Vi har inspiceret et udvalg af privilegerede brugere for at konstatere, om procedurerne er blevet overholdt.</p>	Ingen afvigelser konstateret.
9.2.4	<p><i>Styring af hemmelig autentifikationsinformation om brugere</i></p> <p>Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces.</p>	<p>Vi har inspiceret proceduren vedrørende tildeling af passwords til platforme.</p> <p>Vi har stikprøvevis inspiceret, at proceduren overholdes.</p>	Ingen afvigelser konstateret.
9.2.5	<p><i>Gennemgang af brugeradgangsrettigheder</i></p> <p>Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.</p>	<p>Vi har inspiceret proceduren for regelmæssig gennemgang og evaluering af adgangsrettigheder.</p> <p>Vi har inspiceret et udvalg af gennemgang og evalueringer af adgangsrettigheder.</p>	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
9.2.6	<p><i>Inddragelse eller justering af adgangsrrettigheder</i></p> <p>Alle medarbejderes og eksterne brugeres adgangsrrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.</p>	<p>Vi har inspiceret procedurerne for inddragelse og justering af adgangsrrettigheder.</p> <p>Vi har for et udvalg af fratrådte medarbejdere inspiceret, hvorvidt medarbejderne har fået deres adgangsrrettigheder inddraget.</p>	Ingen afvigelser konstateret.

A.9.3 Brugernes ansvar

Kontrolmål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
9.3.1	<p><i>Brug af hemmelig autentifikationsinformation</i></p> <p>Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
9.4.2	<p><i>Procedurer for sikker logon</i></p> <p>Adgang til systemer og applikationer styres af en procedure for sikker logon.</p>	<p>Vi har forespurgt til procedure for sikkert login, og vi har inspiceret den implementerede løsning.</p>	<p>Ingen afvigelser konstateret.</p>
9.4.3	<p><i>System for administration af passwords</i></p> <p>Systemer til administration af passwords er interaktive og sikrer passwords med god kvalitet.</p>	<p>Vi har inspiceret, at der i politikker eller procedurer stilles krav til kvaliteten af passwords.</p> <p>Vi har inspiceret, at systemer til administration af passwords er opsat i overensstemmelse med de stillede krav.</p>	<p>Ingen afvigelser konstateret.</p>
9.4.5	<p><i>Styring af adgang til kildekoder til programmer</i></p> <p>Adgang til kildekoder til programmer begrænses.</p>	<p>Vi har inspiceret procedurer for begrænsning af adgang til programmets kildekode.</p> <p>Vi har stikprøvevis inspiceret, at adgange til kildekoder er godkendt, og baseret på et arbejdsbetinget behov.</p>	<p>Ingen afvigelser konstateret.</p>

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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
10.1.1	<p><i>Politik for anvendelse af kryptografi</i></p> <p>Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.</p>	<p>Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.</p>	Ingen afvigelser konstateret.
10.1.2	<p><i>Administration af nøgler</i></p> <p>Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.</p>	<p>Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker.</p> <p>Vi har stikprøvevis inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
11.1.1	<p><i>Fysisk perimetersikring</i></p> <p>Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.</p>	<p>Vi har inspiceret proceduren for fysisk beskyttelse af faciliteter og perimetersikkerhed.</p> <p>Vi har inspiceret relevante lokationer og deres perimetersikring for at konstatere, hvorvidt der er sikringsforanstaltninger til at forhindre uautoriseret adgang.</p>	Ingen afvigelser konstateret.
11.1.2	<p><i>Fysisk adgangskontrol</i></p> <p>Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.</p>	<p>Vi har inspiceret procedurene for adgangskontrol til sikre områder.</p> <p>Vi har inspiceret udvalgte adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til faciliteterne.</p>	Ingen afvigelser konstateret.
11.1.4	<p><i>Beskyttelse mod eksterne og miljømæssige trusler</i></p> <p>Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret.</p>	<p>Vi har inspiceret proceduren vedrørende beskyttelse mod eksterne og miljømæssige trusler.</p> <p>Vi har forespurgt om implementering af sikkerhedsforanstaltninger til at forhindre trusler fra ild, varme og fugt og vi har inspiceret relevante lokationer for at konstatere, om der er installeret brandslukningsudstyr, brand- og røgalarmer, blokering af vandførende rør, hævede gulve samt alarmer.</p>	Ingen afvigelser konstateret.

A.11.2 Udstyr			
Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen			
Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
11.2.1	<p><i>Placering og beskyttelse af udstyr</i></p> <p>Udstyr er placeret og beskyttet, så risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes.</p>	<p>Vi har inspiceret proceduren vedrørende placering og beskyttelse af udstyr.</p> <p>Vi har inspiceret relevante lokationer for at vurdere, hvorvidt lokaler er sikkert aflåst og kontrolleret, at kun medarbejdere med et arbejdsbetinget behov har adgang hertil.</p>	Ingen afvigelser konstateret.
11.2.5	<p><i>Fjernelse af aktiver</i></p> <p>Udstyr, information og software må ikke fjernes fra organisationen uden forudgående tilladelse.</p>	Vi har inspiceret retningslinjer for fjernelse af udstyr, information og software fra virksomheden.	Ingen afvigelser konstateret.
11.2.6	<p><i>Sikring af udstyr og aktiver uden for organisationen</i></p> <p>Der er etableret sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen.</p>	Vi har inspiceret retningslinjer for sikring af udstyr og aktiver uden for organisationen.	Ingen afvigelser konstateret.
11.2.7	<p><i>Sikker bortskaffelse eller genbrug af udstyr</i></p> <p>Alt udstyr med lagringsmedier verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.</p>	<p>Vi har inspiceret proceduren for sletning af data og software på lagringsmedier inden bortskaffelse af lagringsmediet.</p> <p>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.</p>	<p>Vi er blevet informeret om, at udstyr ikke er blevet bortskaffet eller genbrugt i perioden, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
11.2.8	<p><i>Brugerdstyr uden opsyn</i></p> <p>Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.</p>	Vi har inspiceret proceduren for sikring af beskyttelse af udstyr, som er uden opsyn.	Ingen afvigelser konstateret.
11.2.9	<p><i>Politik for ryddeligt skrivebord og blank skærm</i></p> <p>Der er udarbejdet en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
12.1.1	<i>Dokumenterede driftsprocedurer</i> 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	<i>Ændringsstyring</i> Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret proceduren vedrørende ændringer til informationsbehandlingsudstyr og – systemer. Vi har inspiceret, at et udvalg af ændringer foretaget på platforme, databaser og netværksudstyr er godkendt, testet, dokumenteret og implementeret i produktionsmiljøet i overensstemmelse med proceduren for ændringsstyring.	Ingen afvigelser konstateret.
12.1.3	<i>Kapacitetsstyring</i> 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	<i>Adskillelse af udviklings-, test- og driftsmiljøer</i> 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 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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
12.2.1	<p><i>Kontroller mod malware</i></p> <p>Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.</p>	<p>Vi har forespurgt til foranstaltninger mod malware.</p> <p>Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.</p>	Ingen afvigelser konstateret.

A.12.3 Backup

Kontrolmål: At beskytte mod tab af data.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
12.3.1	<p><i>Backup af information</i></p> <p>Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.</p>	<p>Vi har forespurgt til krav til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for, at opsætningen var i overensstemmelse med kravene.</p> <p>Vi har inspiceret, at der gennemføres overvågning af afviklingen af backup.</p> <p>Vi har forespurgt til test af gendannelse fra backupfiler, og vi har inspiceret dokumentation for test af gendannelse.</p>	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning

Kontrolmål: At registrere hændelser og tilvejebringe bevis.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
12.4.1	<i>Hændelseslogning</i> 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.
12.4.2	<i>Beskyttelse af log- oplysninger</i> Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har forespurgt til procedurer for sikring af logoplysninger. Vi har inspiceret et udvalg af logningskonfigurationer med henblik på at konstatere, om logningsinformationer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	<i>Administrator- og operatørlog</i> 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 på udvalgte servere og database-systemer med henblik på at konstatere, om systemadministratorers og -operatørers handlinger logges.	Ingen afvigelser konstateret.
12.4.4	<i>Tidssynkronisering</i> 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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
12.5.1	<i>Softwareinstallation på driftssystemer</i> Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret retningslinjer for installation af software på driftssystemer, og vi har stikprøvevis inspiceret, at retningslinjerne efterleves.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring

Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
12.6.1	<p><i>Styring af tekniske sårbarheder</i></p> <p>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.</p>	<p>Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder.</p> <p>Vi har stikprøvevis inspiceret servere, databasesystemer og netværkskomponenter for at konstatere, hvorvidt de er patchet rettidigt.</p>	Ingen afvigelser konstateret.
12.6.2	<p><i>Begrænsninger på softwareinstallation</i></p> <p>Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.</p>	<p>Vi har forespurgt til procedurer for begrænsning af softwareinstallation, som foretages af brugere.</p> <p>Vi har inspiceret, at regler for softwareinstallation efterleves.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
13.1.1	<p><i>Netværksstyring</i></p> <p>Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.</p>	<p>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.</p> <p>Vi har inspiceret dokumentation for design af netværket og et udvalg af sikkerhedsmæssige opsætninger af netværkskomponenter med henblik på at konstatere, om de definerede krav og regler er implementeret.</p>	Ingen afvigelser konstateret.
13.1.2	<p><i>Sikring af netværkstjenester</i></p> <p>Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcete.</p>	<p>Vi har observeret, at der foreligger skriftlige krav til sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester.</p> <p>Vi har inspiceret et udvalg af netværkskomponenter for at vurdere, hvorvidt komponenterne er opsat i overensstemmelse med kravene.</p>	Ingen afvigelser konstateret.
13.1.3	<p><i>Opdeling af netværk</i></p> <p>Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.</p>	<p>Vi har inspiceret netværksdiagrammer og anden netværksdokumentation med hensyn til opdeling af netværk.</p>	Ingen afvigelser konstateret.

A.13.2 Informationsoverførsel

Kontrolmålet: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
13.2.1	<p><i>Politikker og procedurer for informationsoverførsel</i></p> <p>Der foreligger formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.</p>	Vi har inspiceret politikker og procedurer for dataoverførsel.	Ingen afvigelser konstateret.
13.2.2	<p><i>Aftaler om informationsoverførsel</i></p> <p>Aftaler omhandler sikker overførsel af forretningsinformation mellem organisationen og eksterne parter.</p>	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	<p><i>Elektroniske meddelelser</i></p> <p>Informationer i elektroniske meddelelser beskyttes på passende måde.</p>	Vi har inspiceret retningslinjer for afsendelse af fortrolig information.	Ingen afvigelser konstateret.
13.2.4	<p><i>Fortroligheds- og hemmeligholdelsesaftaler</i></p> <p>Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, identificeres, gennemgås regelmæssigt og dokumenteres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, som sikrer, at medarbejderne underskriver en fortrolighedsaftale, og at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen.</p> <p>Vi har stikprøvevis inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale.</p>	Ingen afvigelser konstateret.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

A.14.1 Sikkerhedskrav til informationssystemer

Kontrolmål: At sikre at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
14.1.1	<p><i>Analyse og specifikation af informations- sikkerheds-krav</i></p> <p>Informationssikkerhedsrelaterede krav omfattes af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.</p>	<p>Vi har inspiceret proceduren for analyse og specifikation af informationssikkerhedskrav.</p> <p>Vi har inspiceret et udvalg af ændringsanmodninger til systemer med henblik på at konstatere, om der er beskrevet krav til sikkerhed og kontroller i nye informationssystemer eller i forbindelse med ændringer i eksisterende systemer.</p>	Ingen afvigelser konstateret.

A.14.2 Sikkerheds, udviklings- og hjælpeprocesser

Kontrolmål: At sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
14.2.1	<p><i>Sikker udviklingspolitik</i></p> <p>Der fastlægges og anvendes regler for udvikling af software og systemer i organisationen.</p>	<p>Vi har inspiceret regler for udvikling af software og systemer.</p> <p>Vi har stikprøvevis inspiceret, at reglerne har været efterlevet.</p>	Ingen afvigelser konstateret.
14.2.2	<p><i>Procedurer for styring af systemændringer</i></p> <p>Ændringer af systemer inden for udviklingslivscyklussen styres ved hjælp af formelle procedurer for ændringsstyring.</p>	<p>Vi har inspiceret proceduren for ændringsstyring med henblik på at konstatere, hvorvidt proceduren indeholder relevante krav.</p> <p>Vi har inspiceret et udvalg af ændringer med henblik på at konstatere, om kravene til ændringshåndtering blev fulgt.</p>	Ingen afvigelser konstateret.
14.2.5	<p><i>Principper for udvikling af sikre systemer</i></p> <p>Principper for udvikling af sikre systemer fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med alle implementeringer af informationssystemer.</p>	<p>Vi har inspiceret proceduren for udvikling af systemer.</p> <p>Vi har stikprøvevis inspiceret, at proceduren har været fulgt.</p>	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
14.2.6	<p><i>Sikkert udviklingsmiljø</i></p> <p>Der er etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus</p>	<p>Vi har inspiceret proceduren for etablering af sikkert udviklingsmiljø.</p> <p>Vi har stikprøvevis inspiceret, at proceduren har været fulgt.</p>	Ingen afvigelser konstateret.

A.14.3 Testdata

Kontrolmål: At sikre beskyttelse af data, som anvendes til test

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
14.3.1	<p><i>Sikring af testdata</i></p> <p>Testdata udvælges omhyggeligt og beskyttes og styres.</p>	<p>Vi har inspiceret proceduren vedrørende udvælgelse og beskyttelse af testdata.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
15.1.1	<p><i>Informationssikkerhedspolitik for leverandørforhold</i></p> <p>Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til organisationens aktiver aftales med leverandøren og dokumenteres.</p>	<p>Vi har inspiceret proceduren for indgåelse af aftaler med leverandører.</p> <p>Vi har inspiceret indgåede aftaler.</p>	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
15.1.2	<p><i>Håndtering af sikkerhed i leverandøraftaler</i></p> <p>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.</p>	<p>Vi har inspiceret proceduren for indgåelse af aftaler med leverandører.</p> <p>Vi har stikprøvevis inspiceret, at indgåede leverandøraftaler indeholder relevante informationssikkerhedskrav.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
15.2.1	<p><i>Overvågning og gennemgang af leverandørydelser</i></p> <p>Leverandørydelser overvåges, gennemgås og auditeres.</p>	<p>Vi har inspiceret, at proceduren for overvågning og gennemgang af serviceydelser leveret af underleverandører er i overensstemmelse med det aftalte.</p> <p>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.</p> <p>Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører.</p>	Ingen afvigelser konstateret.
15.2.2	<p><i>Styring af ændringer af leverandørydelser</i></p> <p>Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, - procedurer og -kontroller, styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, - systemer og -processer er, og til en revurdering af risici.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
16.1.1	<p><i>Ansvar og procedurer</i></p> <p>Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.</p>	<p>Vi har forespurgt til ansvar og procedurer i forbindelse med informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling.</p> <p>Vi har endvidere inspiceret procedure til håndtering af informationssikkerhedshændelser.</p>	Ingen afvigelser konstateret.
16.1.2	<p><i>Rapportering af informationssikkerhedshændelser</i></p> <p>Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.</p>	<p>Vi har inspiceret retningslinjer for rapportering af informationssikkerhedshændelser.</p> <p>Vi har stikprøvevis inspiceret, at informationssikkerhedshændelser er rapporteret ad passende ledelseskanaler.</p>	Ingen afvigelser konstateret.
16.1.3	<p><i>Rapportering af informationssikkerhedssvagheder</i></p> <p>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.</p>	<p>Vi har inspiceret retningslinjer for rapportering af informationssikkerhedssvagheder.</p> <p>Vi har stikprøvevis inspiceret, at medarbejderne har rapporteret svagheder eller mistanke om svagheder i informationssystemer og -tjenester.</p>	Ingen afvigelser konstateret.
16.1.4	<p><i>Vurdering af og beslutning om informationssikkerhedshændelser</i></p> <p>Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.</p>	<p>Vi har inspiceret, procedure for vurdering af informationssikkerhedshændelser.</p> <p>Vi har inspiceret, at informationssikkerhedshændelser har været håndteret i overensstemmelse med proceduren.</p>	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
16.1.5	<i>Håndtering af informationssikkerhedsbrud</i> Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer.	Vi har stikprøvevis inspiceret, at informationssikkerhedsbrud har været håndteret i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
16.1.6	<i>Erfaring fra informationssikkerhedsbrud</i> 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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
17.1.1	<i>Planlægning af Informationssikkerhedskontinuitet</i> 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	<i>Implementering af informationssikkerheds- kontinuitet</i> 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 dokumentation for at beredskabsplanen gennemgås periodisk.	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
17.1.3	<p><i>Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten</i></p> <p>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.</p>	<p>Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test.</p> <p>Vi har endvidere forespurgt til regelmæssig revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurderingen.</p>	Ingen afvigelser konstateret.

A.17.2 Redundans

Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
17.2.1	<p>Tilgængelighed af informationsbehandlingsfaciliteter</p> <p>Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.</p>	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.	Softværket a.m.b.a's kontrol	REVI-IT's test	Resultat af test
18.2.1	<p><i>Uafhængig gennemgang af informationssikkerhed</i></p> <p>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.</p>	<p>Vi har observeret, at der er etableret krav om regelmæssig uafhængig revisionsmæssig gennemgang af informationssikkerheden.</p>	<p>Ingen afvigelser konstateret.</p>
18.2.2	<p><i>Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder</i></p> <p>Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.</p>	<p>Vi har forespurgt vedrørende lederes sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder.</p> <p>Vi har inspiceret dokumentation for sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder.</p>	<p>Ingen afvigelser konstateret.</p>
18.2.3	<p><i>Undersøgelse af teknisk overensstemmelse</i></p> <p>Informationssystemer undersøges regelmæssigt for, om de er i overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder.</p>	<p>Vi har inspiceret, at procedurer for regelmæssig kontrol af systemers overholdelse af sikkerhedsstandarder er implementeret.</p>	<p>Ingen afvigelser konstateret.</p>

FOF - TestComplete

A4 Finanskladde

Det primære formål med denne kontrol er at validere, at der foretages en validering af inddata, og at data overføres korrekt til finanstabellen.

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	<p>Denne testkørsel gennemgår Finanskladden og sørger for, at alle controls er på formen, og at funktionaliteten er bibeholdt i forhold til tidligere versioner, ved forskellige linjetyper. Ligeledes går den igennem menuen Funktioner og afprøver de forskellige muligheder.</p> <p>Igennem disse testcases bliver der lavet flere gennemløb af funktionen Finansbogføring (Stored Procedure), der til sammen bredt dækker denne/disse funktioner.</p> <p>Ved bogføring bliver der testet, om det falder korrekt på plads i de respektive tabeller i FOF.</p>	<p>Vi har forespurgt til kontroller for opretholdelse af tidligere funktioner, og vi har inspiceret udvalgte kontroller.</p> <p>Vi har forespurgt til kontroller for modposterings, og vi har stikprøvevis inspiceret kontrollerne.</p> <p>Vi har forespurgt til kontroller til sikring af, at der bogføres korrekt, og vi har stikprøvevis inspiceret kontrollerne.</p> <p>Vi har forespurgt til test af, at bogførte linjer falder i korrekte tabeller, og vi har stikprøvevis inspiceret kontrollerne.</p>	Ingen afvigelser konstateret.

A5 Aconto kladde

Det primære formål med denne kontrol er at validere, at der foretages en validering af inddata, og at data overføres korrekt til aconto kladden i forbindelse med bogførte registreringer.

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	<p>Dette testrun gennemgår funktionaliteten af Aconto kladden. Herunder bogføring på forskellige forbrugere med forskellig art og med forskellige finansgrupper. Arterne indeholder både betalinger og påligninger. Et bredt udsnit af arterne er taget med.</p> <p>På issue FOF-1434 er vedhæftet det input, som indlæses i aconto kladden. Ved bogføring bliver der testet, om det falder korrekt på plads i de respektive tabeller i FOF.</p>	<p>Vi har forespurgt til kontroller til sikring af, at bogføring på forbrugere med art of finansgruppe registreres korrekt, og vi har stikprøvevis inspiceret kontroller til sikring af dette.</p> <p>Vi har forespurgt til kontroller til sikring af, at bogførte registreringer tilfalder korrekte tabeller, og vi har inspiceret kontrollerne.</p>	Ingen afvigelser konstateret.

A9 Fakturaflow

Det primære formål med denne kontrol er at validere, at faktura flowet håndteres på betryggende vis, herunder at der sikres funktionsadskillelse, brugerbegrænsninger, og at de korrekte beløb fremgår af faktura.

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	<p>Denne testcase gennemløber mulighederne i Fakturaflow og sikrer at brugerbegrænsninger, status for fordelte og godkendte faktura bibeholdes, at såvel som korrekte som ukorrekte OIO-filer kan indlæses og at data bliver håndteret korrekt, såvel som flere andre funktionaliteter.</p> <p>Skærbilleder der indgår i denne test, dækker over Fakturaflow, EDH, Bruger-opsætning, Kreditorvedligeholdelse (fanen posteringer).</p>	<p>Vi har forespurgt til kontroller til sikring af funktionsadskillelse ved anvendelse af FOF, og vi har inspiceret testrapporterne for applikationen.</p> <p>Vi har forespurgt til kontroller til sikring af, at der er differentiering af rettigheder, og vi har inspiceret testrapporterne for applikationen.</p> <p>Vi har forespurgt til kontroller til sikring af, at indtastede data er korrekt på faktura, og vi har inspiceret testrapporterne for applikationen.</p> <p>Vi har forespurgt til kontroller for validering ved inddatering af OIO filer, og vi har inspiceret testrapporterne for applikationen.</p>	Ingen afvigelser konstateret.

B10 Tilbudskladde

Det primære formål med denne kontrol er at validere kontroller i forbindelse med inddatering i tilbudskladden.

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	<p>Tilbudskladden er introduceret som en ekstra feature i forhold til finanskladderne. Den ligger i forlængelse af frifaktura-kladden og giver værket mulighed for at oprette linjer til Tilbud, udskrive, arkivere og vente på kundernes accept, hvorefter de kan bogføres igennem kladder 50, uden at brugeren får det at se.</p> <p>Dette testrun vil koncentrere sig om at teste de tilføjede felter i finanskladden, finanskladden, systemmiljøet og i forhold til EDH-arkivering på forbrugeren. Hertil vil også funktionaliteten med at udskrive, arkivere og bogføre tilbud blive testet.</p>	<p>Vi har forespurgt til kontroller til validering af inddatering i tilbudskladden, og vi har inspiceret testrapporterne for applikationen.</p> <p>Vi har forespurgt til validering af ud-datering i forbindelse med udskrift af tilbud, og vi har inspiceret testrapporterne for applikationen.</p>	Ingen afvigelser konstateret.

B15 Beregn faktura

Det primære formål med denne kontrol er at validere, at fakturaer beregnes korrekt til opgørelser.

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	Formålet med denne testcase er at teste "beregne faktura". Disse testcases vil gennemføre test i forhold til skærbilledet "dan opgørelse". De beskrevne testcases vil teste alle opgørelsestyper og undertyper (i forhold til budget). I en test case registreres opgørelsen til brug i efterfølgende test cases.	Vi har forespurgt til kontroller for korrekt beregning til opgørelser, herunder årsopgørelse, skønnet forbrug og budget, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B16 Forbrugerovervågning

Denne case sikrer at de forbrugsovervågnings specifikke funktionaliteter fungerer som det er meningen. Herunder filtrering på kladden og at dokumenter udskrives for den tilhørende linje, samt arkivering til korrekt installation.

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	Der testes gennem forskellige scenarier i forbindelse med forbrugerovervågning. Der testes med forbrug og forskellige ejendomme.	Vi har forespurgt til kontroller til validering af data ved forbrugerovervågning, og vi har inspiceret datagrundlaget for testrapporterne.	Ingen afvigelser konstateret.

B28 Dokument køen

Denne samling af test cases forsøger at teste basisfunktionaliteten som eksisterer i forhold til konceptet "Dokumentkøen".

Nr.	Softværket a.m.b.as kontrol	REVI-IT's test	Resultat af test
01	Hver test case kører både på køerne "E-Boks" og "Betalingservice", det vil sige at hver test case indeholder 2 funktioner til eksekvering, men har samme input og udfald, blot at det er 2 forskellige køer.	Vi har forespurgt til kontroller til håndtering af dokumenter i dokument køen, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.