Revisorerklæring

Softværket a.m.b.a.

ISAE 3402 type 2 erklæring om generelle it-kontroller for perioden 1. juni 2022 til 31. maj 2023 relateret til ydelser i forbindelse med drift af it-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF.

Juli 2023

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

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

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, aftaleretslige 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 Softværkets 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 Softværkets 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 hostingmiljøet og Forsyning|FOF. Dermed kan Softværket sikre, at de risici, som er forbundet med hostingmiljøet samt udvikling og vedligeholdelse 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 risicis 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 programmers funktionalitet. Ligeledes er det kun ansatte hos vores hosting-partner, Teknisk Afdeling, GIS- og udviklingsafdelingen, der i samarbejde har adgang til at ændre i hostingmiljøet, der kan påvirke driftsstabiliteten.

Kunder har kun adgang til egne data. Brugerne 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 hostingmiljøet 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 ansvarlige 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 kundernes 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 hostingmiljøet. 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 hostingmiljøet 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.

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

Der tages daglig backup af alle data i hostingmiljøet, 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 hostingmiljøet, af både hosting-partner og Softværket.

Sikkerhed i hostingmiljøet 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, afhængigt 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 hostingmiljøet 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 registret 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 besluttes 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-revisionserklæring.

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 gennemgange foretages i forbindelse med større ændringer i organisationen eller hostingmiljøet.

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

Evaluering foretages 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.

A4, Finanskladde, er med til at sikre validering af inddata og overførelse af data til finanstabellerne. Dette ved at benytte finansbogføringsfunktionen.

A9, Fakturaflow, gennemløber funktionaliteten i faktura flowet, ved at gennemgå områderne funktionalitet i områderne EDH, Bruger opsætning, Kreditor vedligeholdelse.

B16, Forbrugerovervågning, sikre at den specifikke opsætter funktionalitet i forbrugeroverblikket fungerer efter hensigten

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 13 medarbejdere fordelt på henholdsvis GIS-, udvikling-, teknisk-, konsulent- og supportafdelingen samt administrationen. 7 medarbejdere er fratrådt.
- Nyt alarmsystem opsat i samarbejde med Dansk Fjernvarme herunder adgangskontrol.
- VPN – opgraderet med Microsoft MFA
- 1 Q/A konsulent indlejet
- Cisco Ise – netværks sikkerhed med kontrol på om PC er fra Softværket
- Umbrella – Kontrol/tjek/screening af om internet-adresser indeholder skadeligt indhold- der filtreres om sider indeholder skadeligt software.
- Hostingmiljø er opgraderet med ny antivirus løsning

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 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 underleverandørernes 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 (eller den specifikke kunde) 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.' drift af deres it-hosting løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, der har behandlet kunders transaktioner i perioden fra 1. juni 2022 til 31. maj 2023.

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 2022 til 31. maj 2023.

(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 2022 til 31. maj 2023, hvis relevante kontroller hos underleverandører var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af Softværket a.m.b.a.s kontroller i hele perioden fra 1. juni 2022 til 31. maj 2023. 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 2022 til 31. maj 2023.

Kolding, den 3. juli 2023
Softværket a.m.b.a.

Jan Elmstrøm Blaabjerg
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 til opgave at afgive erklæring om Softværket a.m.b.a.s beskrivelse i afsnit 1 af generelle it-kontroller for drift af it-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF til behandling af Softværket a.m.b.a.s kunders transaktioner i perioden 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 underleverandørernes 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 for drift af it-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF 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.

Grant Thorntons uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers 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.

Grant Thornton 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.

Revisors 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.

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

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 Softværket a.m.b.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

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 for drift af it-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, 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 for drift af it-hostingløsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, således som de var udformet og implementeret i perioden 1. juni 2022 til 31. maj 2023, 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 2022 til 31. maj 2023, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører 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 2022 til 31. maj 2023

(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 2022 til 31. maj 2023

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 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 3. juli 2023

Grant Thornton
Statsautoriseret Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Basel Rimon Obari
Executive director, 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.s 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 Grant Thornton 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*	*Grant Thorntons 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 samt offentliggjort og kommunikeret til medarbejderne og relevante eksterne parter. Vi har inspiceret, at risikovurderingen er godkendt af ledelsen.	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 inspiceret dokumentation for at informationssikkerhedspolitikken er gennemgået i perioden. Vi har inspiceret dokumentation for at risikovurderingen er blevet gennemgået i perioden	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*	*Grant Thorntons test*	*Resultat af test*
6.1.1	*Roller og ansvarsområder for informationssikkerhed* 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	*Funktionsadskillelse* Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har inspiceret politikker vedrørende tildeling og opretholdelse af adskillelse af ansvarsområder og funktioner, og påset, at der er taget stilling til funktionsadskillelse.	Ingen afvigelser konstateret.
6.1.3	*Kontakt med myndigheder* Der opretholdes passende kontakt med relevante myndigheder.	Vi har inspiceret dokumentation for, at der er retningslinjer for passende kontakt med myndigheder. Vi har stikprøvevis inspiceret dokumentation for kontakt med myndigheder i perioden.	Ingen afvigelser konstateret.
6.1.4	*Kontakt med særlige interessegrupper* Der opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.	Vi har inspiceret retningslinjer vedrørende vedligeholdelse af reglerne for passende kontakt med særlige interessegrupper, faglige sikkerhedsfora og faglige organisationer. Vi har stikprøvevis inspiceret dokumentation for oprettelse af kontakt med relevante interessegrupper.	Ingen afvigelser konstateret.

A.6.2 Mobilt udstyr og fjernarbejdspladser Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons test***	***Resultat af test***
6.2.1	*Politik for mobilt udstyr* Der er etableret 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: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

Nr.	*Softværket a.m.b.a.s kontrol*	*Grant Thorntons test*	*Resultat af test*
7.1.1	*Screening* 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.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere og de sikkerhedsopgaver, der skal udføres i den forbindelse. Vi har stikprøvevis inspiceret dokumentation for, at screening er gennemført i forbindelse med ansættelser.	Ingen afvigelser konstateret.
7.1.2	*Ansættelsesvilkår og -betingelser* Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har stikprøvevis inspiceret et udvalg af kontrakter med medarbejdere og konsulenter med henblik på at konstatere om medarbejdere og konsulenter havde underskrevet ansættelsesvilkår og -betingelser. Vi har stikprøvevis inspiceret, at ansættelseskontrakter indeholder pågældende og organisationens ansvar for informationssikkerhed.	Ingen afvigelser konstateret.

A.7.2 Under ansættelsen Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons 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 retningslinjerne for ledelsesansvar, og vi har stikprøvevis inspiceret dokumentation for, at retningslinjerne er blevet fulgt.	Ingen afvigelser konstateret.
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 retningslinjer for uddannelse og træning i informationssikkerhed. Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejderne.	Ingen afvigelser konstateret.
7.2.3	*Sanktioner* Der er etableret 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 til medarbejdere og kontrahenter.	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.' kontrol***	***Grant Thorntons 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 stikprøvevis inspiceret, at fratrådte medarbejdere, ved fratrædelse, informeres om fortsat tavshedspligt.	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***	***Grant Thorntons 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 at fortegnelser over aktiver indeholder både information samt informationsbehandlingsfaciliteter.	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, for både information og informationsbehandlingsfaciliteter.	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, og påset, at medarbejderne er forpligtet til at følge dem.	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a.s kontrol	Grant Thorntons test	Resultat af test
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 stikprøvevis inspiceret dokumentation for, at aktiver er tilbageleveret for fratrådte medarbejdere i henhold til intern procedure.	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***	***Grant Thorntons 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 politikken for klassifikation af information. Vi har stikprøvevis inspiceret information og stikprøvevis påset, at dette er klassificeret i henhold til politikken.	Ingen afvigelser konstateret.
8.2.3	*Håndtering af aktiver* Der er udarbejdet og implementeret procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.	Vi har inspiceret politikken for håndtering af aktiver. Vi har inspiceret dokumentation for implementering af politikken.	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***	***Grant Thorntons test***	***Resultat af test***
8.3.1	*Styring af bærbare medier* Der er implementeret procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget.	Vi har inspiceret politikken for håndtering og aktiver, og vi har inspiceret dokumentation for, at aktiver er styret efter risiko.	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 proceduren for bortskaffelse af medier. Vi har stikprøvevis inspiceret, at bortskaffelse i perioden har fulgt proceduren.	Ingen afvigelser konstateret.

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***	***Grant Thorntons 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. Vi har inspiceret at politikken er gennemgået og godkendt af ledelsen.	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 foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgangsrettigheder. Vi har stikprøvevis inspiceret, at brugernes adgangsrettigheder er godkendt. Vi har stikprøvevis inspiceret, at fratrådte brugeres adgangsrettigheder er nedlagt.	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**	**Grant Thorntons test**	**Resultat af test**
9.2.1	*Brugerregistrering-og afmelding* Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling og afmelding af adgangsrettigheder.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgangsrettigheder. Vi har stikprøvevis inspiceret, at brugernes adgangsrettigheder er godkendt. Vi har stikprøvevis inspiceret, at fratrådte brugeres adgangsrettigheder er nedlagt.	Ingen afvigelser konstateret.
9.2.2	*Tildeling af brugeradgang* 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.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har stikprøvevis inspiceret, at der foreligger godkendelse af tildeling af brugeradgange.	Ingen afvigelser konstateret.
9.2.3	*Styring af privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har inspiceret politikken for administrering af administrative brugere. Vi har stikprøvevis inspiceret administrative brugere, og påset, at de har et arbejdsbetinget behov.	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 politikken for styring af hemmelig autentifikationsinformation om brugere. Vi har stikprøvevis inspiceret dokumentation for implementering af politikken.	Ingen afvigelser konstateret.
9.2.5	*Gennemgang af brugeradgangsrettigheder* Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har inspiceret, at der foretages gennemgang og evalueringer af adgangsrettigheder.	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a.s kontrol	Grant Thorntons test	Resultat af test
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 stikprøvevis inspiceret at fratrådte medarbejdere har fået deres adgangsrettigheder inddraget rettidigt.	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***	***Grant Thorntons 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, og vi har inspiceret implementering af politikken.	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***	***Grant Thorntons test***	***Resultat af test***
9.4.2	*Procedurer for sikker logon* Adgang til systemer og applikationer styres af en procedure for sikker logon.	Vi har inspiceret, at der er retningslinjer for sikker logon, og vi har inspiceret dokumentation for, at logon følger retningslinjerne.	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 dokumentation for, at passwords opbevares i henhold til intern politik.	Ingen afvigelser konstateret.
9.4.5	*Styring af adgang til kildekoder til programmer* Adgang til kildekoder til programmer begrænses.	Vi har inspiceret retningslinjer for begrænsning af adgang til programmers kildekode. Vi har stikprøvevis inspiceret, at adgange til kildekoder følger retningslinjerne.	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.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons 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 inspiceret politik for kryptering, og stikprøvevis påset, at kryptering er implementeret i overensstemmelse med politikken.	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 dokumentation for, at krypteringsnøgler opbevares sikkert. Vi har stikprøvevis inspiceret dokumentation for, at der er opsat alarmer i forhold til certifikater.	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*	*Grant Thorntons 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 retningslinjer for fysisk beskyttelse af faciliteter og perimetersikkerhed. Vi har stikprøvevis inspiceret dokumentation for lokationer og perimetersikring.	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 stikprøvevis inspiceret, at der er etableret fysisk sikring af kontorer, lokaler og faciliteter. Vi har inspiceret dokumentation for, at der er opsat alarm på døre.	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***	***Grant Thorntons test***	***Resultat af test***
11.2.4	*Vedligeholdelse af udstyr* Udstyr vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet.	Vi har inspiceret retningslinjerne for vedligeholdelse af udstyr. Vi har inspiceret dokumentation for vedligeholdelse af alarmsystem.	Ingen afvigelser konstateret.
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, og vi har stikprøvevis påset, at udstyr er blevet fjernet i henhold til retningslinjerne.	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. Vi har inspiceret dokumentation for, at retningslinjerne er blevet fulgt.	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 retningslinjer for fjernelse af udstyr, information og software fra virksomheden, og vi har stikprøvevis påset, at udstyr er blevet fjernet i henhold til retningslinjerne.	Ingen afvigelser konstateret.
11.2.8	*Brugerudstyr uden opsyn* Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.	Vi har inspiceret politikken for sikring af beskyttelse af udstyr, som er uden opsyn. Vi har inspiceret dokumentation for, at skærmlås følger politikken.	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. Vi har stikprøvevis inspiceret dokumentation for ryddeligt skrivebord.	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*	*Grant Thorntons 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 relevante driftsprocedurer, som dækker driften. Vi har inspiceret at driftsprocedurerne er opdateret og tilgængelig for medarbejderne.	Ingen afvigelser konstateret.
12.1.2	*Ændringsstyring* Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret proceduren vedrørende ændringer til informationsbehandlingsudstyr og – systemer. Vi har stikprøvevis inspiceret, at ændringer er sket i overensstemmelse med ændringsproceduren.	Ingen 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 dokumentation for at der er implementeret løsning til overvågning af kapacitet i henhold til intern politik.	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 inspiceret politikken for adskillelse af miljøer, og stikprøvevis påset, at miljøer er adskilt.	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***	***Grant Thorntons 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 inspiceret politikken for beskyttelse mod malware, og vi har stikprøvevis inspiceret anvendelsen af antivirus.	Ingen afvigelser konstateret.

A.12.3 Backup Kontrolmål: At beskytte mod tab af data.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons 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 inspiceret, at der er backup implementeret i henhold til intern politik. Vi har stikprøvevis inspiceret, at backup er kørt succesfuldt i perioden. Vi har stikprøvevis inspiceret, at kontroller til backup er udført i perioden.	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning Kontrolmål: At registrere hændelser og tilvejebringe bevis.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons test***	***Resultat af test***
12.4.1	*Hændelseslogning* Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Vi har inspiceret politikken for logning og overvågning, og stikprøvevis inspiceret dokumentation for implementering af politikken.	Ingen afvigelser konstateret.
12.4.2	*Beskyttelse af log-oplysninger* Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har inspiceret politikken for beskyttelse af logfiler, og vi har stikprøvevis inspiceret dokumentation for beskyttelse af logfiler.	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 politikken for logning af administrator, og stikprøvevis inspiceret dokumentation for logning af administrator.	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 inspiceret løsningen for tidssynkronisering.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware Kontrolmål: At sikre integriteten af driftssystemer.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons test***	***Resultat af test***
12.5.1	*Softwareinstallation på driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har stikprøvevis inspiceret patching af systemer, og stikprøvevis påset, at dette følger den interne procedure herfor.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons 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 politikken for styring af tekniske sårbarheder, og vi har stikprøvevis inspiceret dokumentation for løbende kontrol af tekniske svagheder i perioden.	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*	*Grant Thorntons test*	*Resultat af test*
13.1.1	*Netværksstyring* Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har stikprøvevis inspiceret netværkskomponenter, og stikprøvevis påset, at håndteringen af disse følger intern politik herfor. Vi har inspiceret, at den løbende kontrol af firewall er blevet udført i perioden.	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 inspiceret politikken for sikring af netværkstjenester, og vi har stikprøvevis inspiceret dokumentation for implementering af tekniske foranstaltninger.	Ingen afvigelser konstateret.
13.1.3	*Opdeling af netværk* Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.	Vi har inspiceret netværksdokumentation med hensyn til opdeling af netværk.	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***	***Grant Thorntons 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. Vi har forespurgt til hentning af fysiske aktiver i perioden.	Vi er blevet informeret om, at der ikke har været behov for at hente fysiske aktiver hos kunder i perioden, og vi har derfor ikke kunnet teste effektiviteten af leverandørens procedurer. Ingen afvigelser konstateret.
13.2.2	*Aftaler om informationsoverførsel* Aftaler omhandler sikker overførsel af forretningsinformation mellem organisationen og eksterne parter.	Vi har inspiceret politikken for informationsoverførsel, og påset, at der taget stilling til aftaler om informationsoverførsler. Vi har stikprøvevis inspiceret, at der er indgået aftaler i henhold til politikken.	Ingen afvigelser konstateret.
13.2.3	*Elektroniske meddelelser* Informationer i elektroniske meddelelser beskyttes på passende måde.	Vi har inspiceret retningslinjer for afsendelse af fortrolig information. Vi har stikprøvevis inspiceret dokumentation for implementering af politikken.	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 inspiceret, at der er en formel politik for fortroligheds- og hemmeligholdelsesaftaler. Vi har stikprøvevis inspiceret dokumentation for overholdelse af politikken.	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	Grant Thorntons test	Resultat af test
14.1.1	*Analyse og specifikation af informationssikkerhedskrav* Informationssikkerhedsrelaterede krav omfattes af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.	Vi har inspiceret, at der en politik for anskaffelse og udvikling af nye systemer, og påset, at politikken indeholder krav om, at der skal laves risikovurdering. Vi har stikprøvevis inspiceret, at der er udført en risikovurdering af nye systemer i perioden.	Ingen afvigelser konstateret.

A.14.2 Sikkerhed i udviklings- og hjælpeprocesser
Kontrolmål: At sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus

Nr.	Softværket a.m.b.a.s kontrol	Grant Thorntons test	Resultat af test
14.2.1	*Sikker udviklingspolitik* Der fastlægges og anvendes regler for udvikling af software og systemer i organisationen.	Vi har inspiceret politikken for sikker udvikling, og påset, at der er taget stilling til sikkerhed i udviklingsprocessen. Vi har stikprøvevis inspiceret udviklingssager i perioden.	Vi har observeret, at der er for én ud af seks stikprøver ikke er foretaget review af kode. Vi har inspiceret, at der er blevet udført yderligere test af den pågældende stikprøve, og ændringen er godkendt af den ansvarlige. Ingen yderligere afvigelser konstateret.
14.2.2	*Procedurer for styring af systemændringer* Ændringer af systemer inden for udviklingslivscyklussen styres ved hjælp af formelle procedurer for ændringsstyring.	Vi har stikprøvevis inspiceret udviklingssager i perioden.	Vi har observeret, at der er for én ud af seks stikprøver ikke er foretaget review af kode. Vi har inspiceret, at der er blevet udført yderligere test af den pågældende stikprøve, og ændringen er godkendt af den ansvarlige. Ingen yderligere afvigelser konstateret.

Nr.	*Softværket a.m.b.a.s kontrol*	*Grant Thorntons test*	*Resultat af test*
14.2.5	*Principper for udvikling af sikre systemer* Principper for udvikling af sikre systemer fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med alle implementeringer af informationssystemer.	Vi har inspiceret politikken for principper for udvikling, og vi har stikprøvevis inspiceret dokumentation for, at principperne overholdes.	Ingen afvigelser konstateret.
14.2.6	*Sikkert udviklingsmiljø* Der er etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus	Vi har stikprøvevis inspiceret adgange til udviklingsmiljøet, og stikprøvevis påset, at der er et arbejdsbetinget behov for adgang.	Ingen afvigelser konstateret.
14.2.9	*Systemgodkendelsestest* Der etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.	Vi har stikprøvevis inspiceret dokumentation for, at der er lavet systemgodkendelsestest.	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***	***Grant Thorntons test***	***Resultat af test***
14.3.1	*Sikring af testdata* Testdata udvælges omhyggeligt og beskyttes og styres.	Vi har inspiceret, at der er en procedure til sikring af testdata. Vi har stikprøvevis inspiceret løbende kontroller til sikring af testdata, og stikprøvevis påset, at dette følger proceduren. Vi har stikprøvevis inspiceret testdata, og stikprøvevis påset, at dette er i overensstemmelse med proceduren.	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*	*Grant Thorntons test*	*Resultat af test*
15.1.1	*Informationssikkerhedspolitik for leverandørforhold* Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til organisationens aktiver aftales med leverandøren og dokumenteres.	Vi har inspiceret, at der er politikker for håndtering af leverandøraftaler, herunder indgåelse med disse.	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 stikprøvevis inspiceret leverandøraftaler, og stikprøvevis påset, at der er taget stilling til informationssikkerhed.	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***	***Grant Thorntons test***	***Resultat af test***
15.2.1	*Overvågning og gennemgang af leverandørydelser* Leverandørydelser overvåges, gennemgås og auditeres.	Vi har inspiceret, at politikken for overvågning og at gennemgang af serviceydelser leveret af underleverandører, 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* 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.	Vi har forespurgt til styring af ændringer hos leverandører og vi har 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*	*Grant Thorntons 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 inspiceret, at der er en procedure for håndtering af hændelser, som beskriver ansvar og roller.	Ingen afvigelser konstateret.
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret proceduren for håndtering af hændelser, og påset, at det er beskrevet hvordan hændelser skal rapporteres. Vi har inspiceret loggen over hændelser, og påset, at hændelser er registreret.	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 inspiceret proceduren for håndtering af hændelser, og påset, at der er taget stilling til rapportering af svagheder.	Ingen afvigelser konstateret.
16.1.4	*Vurdering af og beslutning om informationssikkerhedshændelser* Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	Vi har inspiceret proceduren for hændelser, og påset, at der er taget stilling til håndtering af informationssikkerhedsbrud. Vi har inspiceret loggen over hændelser, og påset, at der er taget stilling til hændelser.	Ingen afvigelser konstateret.
16.1.5	*Håndtering af informationssikkerhedsbrud* Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer.	Vi har inspiceret, at der er procedurer for håndtering af brud. Vi har forespurgt til, om der har været brud i perioden.	Vi er blevet informeret om, at der ikke har været informationssikkerhedsbrud i perioden, hvorfor vi ikke har kunnet teste effektiviteten af leverandørens procedurer. Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a.s kontrol	Grant Thorntons 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 inspiceret, at der er procedurer for indhentelse af erfaring vedrørende sikkerhedsbrud. Vi har forespurgt til opfølgning på sikkerhedsbrud.	Vi er blevet informeret om, at der ikke har været informationssikkerhedsbrud i perioden, hvorfor vi ikke har kunnet teste effektiviteten af leverandørens procedurer. 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 nød-, beredskabs- og reetableringsstyring.

Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons 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 inspiceret, at der er etableret en beredskabsprocedure til sikring af videreførelse af driften.	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 inspiceret at der er en beredskabsplan, som er godkendt og tilgængelig for medarbejdere.	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 inspiceret dokumentation for, at beredskabsplan er blevet testet i perioden.	Ingen afvigelser konstateret.

A.17.2 Redundans Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.			
Nr.	***Softværket a.m.b.a.s kontrol***	***Grant Thorntons test***	***Resultat af test***
17.2.1	*Tilgængelighed af informationsbehandlingsfaciliteter* Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	Vi har stikprøvevis inspiceret, at der er etableret redundant setup i henhold til intern politik.	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***	***Grant Thorntons 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 inspiceret, at der er etableret uafhængig 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 inspiceret dokumentation for, at der er udført kontrol af interne politikker i perioden.	Ingen afvigelser konstateret.

Nr.	Softværket a.m.b.a.s kontrol	Grant Thorntons test	Resultat af test
18.2.3	*Undersøgelse af teknisk overensstemmelse* Informationssystemer undersøges regelmæssigt for, om de er i overensstemmelse se med organisationens informationssikkerhedspolitikker og -standarder.	Vi har stikprøvevis inspiceret, at der er udført kontroller i perioden, som sikrer den tekniske overensstemmelse.	Ingen afvigelser konstateret.

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.a.s kontrol*	*Grant Thorntons test*	*Resultat af test*
01	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. Igennem disse testcases bliver der lavet flere gennemløb af funktionen Finansbogføring (Stored Procedure), der til sammen bredt dækker denne/disse funktioner. Ved bogføring bliver der testet, om det falder korrekt på plads i de respektive tabeller i FOF.	Vi har stikprøvevis inspiceret kontroller til validering af inddata og korrekt overførelse af data til finanstabellen, og vi har stikprøvevis påset, at kontrollerne er blevet udført.	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.a.s kontrol*	*Grant Thorntons test*	*Resultat af test*
01	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. Skærmbilleder der indgår i denne test, dækker over Fakturaflow, EDH, Bruger-opsætning, Kreditorvedligeholdelse (fanen posteringer).	Vi har stikprøvevis inspiceret kontroller til sikring af fakturaflow, og vi har stikprøvevis påset, at disse er blevet udført.	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.a.s kontrol*	*Grant Thorntons test*	*Resultat af test*
01	Der testes gennem forskellige scenarier i forbindelse med forbrugerovervågning. Der testes med forbrug og forskellige ejendomme.	Vi har stikprøvevis inspiceret kontroller for korrekt beregning til opgørelser, herunder årsopgørelse, skønnet forbrug og budget, og vi har vi har stikprøvevis påset, at kontrollerne er udført.	Ingen afvigelser konstateret.