et trygt samfund med it og data

Revisorerklæring.

CVR nr.: 26 22 40 20

DFF|EDB a.m.b.a.

ISAE 3402 type 2 erklæring om generelle it-kontroller for perioden
1. juni 2020 til 31. maj 2021 relateret til DFF|EDB a.m.b.a.s it-hostingløsning
Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF

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

Juni 2021

Indholdsfortegnelse

Afsnit 1: Beskrivelse af DFF|EDB a.m.b.a.s kontroller i forbindelse med drift af deres it-hosting løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF

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

Kontroller i applikationssystemerne er ikke omfattet af denne erklæring.

Generelle it-kontroller hos DFF|EDB a.m.b.a.

Indledning

I det følgende beskrives de generelle it-kontroller relateret til DFF|EDB a.m.b.a.s ydelser til kunder.

Anvendelse af underleverandører

DFF|EDB a.m.b.a. anvender Curanet A/S som væsentlig leverandør i forbindelse med drift af deres it-hosting løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF

Formål

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

DFF|EDB 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 DFF|EDB fremstår troværdig. For at fastholde DFF|EDB's 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 DFF|EDB 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 DFF|EDB's 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

DFF|EDB har en procedure for løbende risikovurdering af udvikling og vedligeholdelse af hosting-miljøet og Forsyning|FOF. Dermed kan DFF|EDB 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 DFF|EDB 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 programmers 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. 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. DFF|EDB anvender kun konsulenter, der har en høj standard, og hvor velbeskrevne it-sikkerhedsprocedurer er en del af standardaftalen.

Alle medarbejdere i DFF|EDB 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 DFF|EDB 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.

Al kildekode og programmer, der udvikles, er DFF|EDB´s 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 DFF|EDB 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.

DFF|EDB anvender et krypteret system til opbevaring af administrative kodeord.

Kommunikation af følsomt og fortroligt data sker via sikker mail.

DFF|EDB 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.

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

12 - Sikkerhed i forbindelse med drift

DFF|EDB 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 DFF|EDB.

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 er funktionsbehov.

DFF|EDB 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 DFF|EDB's 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 DFF|EDB.

DFF|EDB anvender kun konsulenter, der har en høj standard, og hvor velbeskrevne it-sikkerheds procedurer er en del af standardaftalen.

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

16 - Styring af sikkerhedshændelser

DFF|EDB 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. DFF|EDB har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer.

DFF|EDB beredskabsplan omfatter:

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

DFF|EDB har implementeret formelle nødplaner, og procedurer til beredskab for alle punkter. DFF|EDB har redundans i alle kritiske netværkskomponenter. Derudover refereres der til hosting-partnerens IT-revisionserklæring.

18 - Overensstemmelse

Hverken DFF|EDB eller vores kunder, er underlagt særlig lovgivning i forhold til vores ydelse. DFF|EDB 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 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 DFF|EDB 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 DFF|EDB's kunder antages at være ansvarlige for - både de indlysende og jf. DFF|EDB's forretningsvilkår/SLA.

DFF|EDB's kunder er, medmindre andet er aftalt, ansvarlige for selv at etablere forbindelse til DFF|EDB's hostingmiljø. Herudover er DFF|EDB's 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 2 medarbejdere fordelt på henholdsvis GIS- samt teknisk-afdeling. En enkelt medarbejder er fratrådt.
- Af væsentlig større systemmæssige ændringer er der indført krav om mere komplekst samt længere password, som følger anbefalingerne fra Center for Cybersikkerhed.
- Der er indført Password-reset portal til Forsyning|Hosting baseret på 2-faktor-løsningen
- Der er indført risikobaseret tilsyn med databehandlere
- Monitorering af 3. parts produkter samt OS på enheder
- Der er indført en bagatelgrænse til test af udviklingsopgaver, denne er baseret på en risikovurdering og vurderes hver gang af kvalitetsansvarlige
- Der har været stort fokus på understøttelse af medarbejders mulighed for at arbejde sikkert hjemmefra, grundet Covid-19

Afsnit 2: DFF|EDB a.m.b.a.s udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt DFF|EDB 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.

DFF|EDB 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 DFF|EDB 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 2020 til 31. maj 2021.

Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

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

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

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

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i perioden fra 1. juni 2020 til 31. maj 2021. Kriterierne for denne udtalelse var, at:

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

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

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

Kolding, den 25. juni 2021
DFF|EDB a.m.b.a.

Jan Elmstrøm Blaaberg
Adm. direktør

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

Til DFF|EDB a.m.b.a., deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om DFF|EDB a.m.b.a.s beskrivelse i afsnit 1 af generelle it-kontroller for drift af brugersystemer til behandling af DFF|EDB a.m.b.a.s kunders transaktioner i perioden fra 1. juni 2020 til 31. maj 2021 og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

DFF|EDB a.m.b.a. anvender serviceunderleverandøren Curanet A/S. Denne erklæring er udarbejdet efter partielmetoden, og DFF|EDB a.m.b.a.s kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Curanet A/S.

Enkelte af de kontrolmål, der er anført i DFF|EDB 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 DFF|EDB a.m.b.a. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

DFF|EDB a.m.b.a.s ansvar

DFF|EDB 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 IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

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

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

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om DFF|EDB 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 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 DFF|EDB 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

DFF|EDB 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 DFF|EDB 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 fra 1. juni 2020 til 31. maj 2021, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra 1. juni 2020 til 31. maj 2021.
(c) De testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i perioden fra 1. juni 2020 til 31. maj 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i det efterfølgende afsnit 4 om kontrolmål, udførte kontroller, test og resultater heraf.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt DFF|EDB 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 25. juni 2021

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Basel Rimon 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 DFF|EDB a.m.b.a.s kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos DFF|EDB a.m.b.a.s underleverandør Curanet A/S.

Kontroller udført hos DFF|EDB 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 DFF|EDB 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 DFF|EDB a.m.b.a.

A.4 Risikovurdering og -håndtering

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
4.1	DFF|EDB har en procedure for løbende risikovurdering af udvikling og vedligeholdelse af hosting-miljøet og Forsyning|FOF. Dermed kan DFF|EDB 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 DFF|EDB 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.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af it-risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået og godkendt af ledelsen i perioden.	Ingen afvigelser konstateret.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed

Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

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

A.6 Organisering af informationssikkerhed

A.6.1 Intern organisering
Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
6.1.1	*Roller og ansvarsområder for informationssikkerhed* Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret dokumentation, der viser, at ansvaret for informationssikkerhed er klart defineret og fordelt.	Ingen afvigelser konstateret.
6.1.2	*Funktionsadskillelse* Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har inspiceret procedurer vedrørende tildeling og opretholdelse af adskillelse af ansvarsområder og funktioner.	Ingen afvigelser konstateret.
6.1.3	*Kontakt med myndigheder* Der opretholdes passende kontakt med relevante myndigheder.	Vi har inspiceret proceduren vedrørende vedligeholdelse af reglerne for passende kontakt med relevante myndigheder.	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 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.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
6.2.1	*Politik for mobilt udstyr* Der vedtages en politik og understøttende sikkerheds-foranstaltninger 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 stikprøvevis inspiceret, at tekniske kontroller er im-plementeret på mobile enheder.	Ingen afvigelser konstateret.
6.2.2	*Fjernarbejdspladser* Der er implementeret en politik og understøttende sik-kerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.	Vi har inspiceret politik for sikring af fjernarbejdspladser, og vi har inspiceret underliggende sikkerhedsforanstaltninger til beskyttelse af fjernarbejdspladser.	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's 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 inspiceret proceduren for ansættelse af nye medarbejdere og de sikkerhedsopgaver, der skal udføres i den forbindelse. Vi har inspiceret et udvalg af ansættelsesaftaler med henblik på at konstatere, om proceduren med hensyn til baggrundscheck efterleves for nye medarbejdere.	Ingen afvigelser konstateret.
7.1.2	*Ansættelsesvilkår og -betingelser* Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har inspiceret et udvalg af kontrakter med medarbejdere og konsulenter med henblik på at konstatere om medarbejdere og konsulenter havde underskrevet kontrakten.	Ingen afvigelser konstateret.

A.7.2 Under ansættelsen

Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
7.2.1	*Ledelsesansvar* Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har inspiceret proceduren vedrørende fastsættelse af krav til medarbejdere og kontrahenter. Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde it-sikkerhedspolitikken.	Ingen afvigelser konstateret.

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

A.7.3 Ansættelsesforholdets ophør eller ændring

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

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

A.8 Styring af aktiver

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

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

A.8.2 Klassifikation af information Kontrolmål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.			
Nr.	**DFF|EDB a.m.b.a.s kontrol l**	**REVI-IT's test**	**Resultat af test**
8.2.1	*Klassifikation af information* Information klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.	Vi har inspiceret politik for klassificering af information. Vi har inspiceret dokumentation for at informationsaktiver er klassificeret i overensstemmelse med politik for klassificering af information.	Ingen afvigelser konstateret.
8.2.3	*Håndtering af aktiver* Der udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.	Vi har forespurgt til proceduren for håndtering af aktiver, og vi har inspiceret proceduren.	Ingen afvigelser konstateret.

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

A.9 Adgangsstyring

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

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

A.9.2 Administration af brugeradgang
Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
9.2.1	*Brugerregistrering-og afmelding* Der implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.	Vi har forespurgt til proceduren for registrering og afmelding af brugere, og vi har inspiceret procedurerne. Vi har inspiceret et udvalg af registrering og afmelding af brugere med henblik på at konstatere om proceduren er fulgt.	Ingen afvigelser konstateret.
9.2.2	*Tildeling af brugeradgang* Der implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har inspiceret, at proceduren for brugeradministration er implementeret.	Ingen afvigelser konstateret.

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

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
9.3.1	*Brug af hemmelig autentifikationsinformation* Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.	Vi har inspiceret retningslinjer for brug af fortrolige passwords.	Ingen afvigelser konstateret.

A.9.4 Styring af system- og applikationsadgang Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
9.4.1	*Begrænset adgang til informationer* Adgang til information og applikationssystemers funktioner begrænses i overensstemmelse med politikken for adgangsstyring.	Vi har inspiceret retningslinjer og procedurer til sikring af begrænsning af adgang til informationer.	Ingen afvigelser konstateret.
9.4.2	*Procedurer for sikker logon* Adgang til systemer og applikationer styres af en procedure for sikker logon.	Vi har forespurgt til procedure for sikkert login, og vi har inspiceret den implementerede løsning og procedure.	Ingen afvigelser konstateret.
9.4.3	*System for administration af passwords* Systemer til administration af passwords er interaktive og sikrer passwords med god kvalitet.	Vi har inspiceret, at der i politikker eller procedurer stilles krav til kvaliteten af passwords. Vi har inspiceret at systemer til administration af passwords er opsat i overensstemmelse med de stillede krav.	Ingen afvigelser konstateret.
9.4.5	*Styring af adgang til kildekoder til programmer* Adgang til kildekoder til programmer begrænses.	Vi har inspiceret procedurer for begrænsning af adgang til programmers kildekode.	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.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
10.1.1	*Politik for anvendelse af kryptografi* Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	Ingen afvigelser konstateret.
10.1.2	*Administration af nøgler* Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

A.11.1 Sikre områder
Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
11.1.1	*Fysisk perimetersikring* Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.	Vi har inspiceret proceduren for fysisk beskyttelse af faciliteter og perimetersikkerhed. Vi har inspiceret relevante lokationer og deres perimetersikring for at konstatere, hvorvidt der er sikringsforanstaltninger til at forhindre uautoriseret adgang.	Ingen afvigelser konstateret.
11.1.2	*Fysisk adgangskontrol* Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har inspiceret procedurerne for adgangskontrol til sikre områder. Vi har inspiceret udvalgte adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til produktionsfaciliteterne.	Ingen afvigelser konstateret.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
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, at der foretages inspektion af brandsluknings-udstyr, UPS-anlæg m.v. Vi har inspiceret, at der gennemføres test af generatorer, UPS-anlæg m.v.	Ingen afvigelser konstateret.
11.1.4	*Beskyttelse mod eksterne og miljømæssige trusler* Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret.	Vi har inspiceret proceduren vedrørende beskyttelse mod eksterne og miljømæssige trusler. Vi har forespurgt om implementering af sikkerhedsforanstaltninger til at forhindre trusler fra ild, varme og fugt og vi har inspiceret relevante lokationer for at konstatere, om der er installeret brandslukningsudstyr, brand- og røgalarmer.	Ingen afvigelser konstateret.
11.1.5	*Arbejde i sikre områder* Procedurer for arbejde i sikre områder er tilrettelagt og etableret.	Vi har inspiceret procedurer for arbejde i sikre områder.	Ingen afvigelser konstateret.

A.11.2 Udstyr

Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
11.2.1	*Placering og beskyttelse af udstyr* Udstyr er placeret og beskyttet, så risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes.	Vi har inspiceret proceduren vedrørende placering og beskyttelse af udstyr. Vi har inspiceret relevante lokationer for at vurdere, hvorvidt lokaler er sikkert aflåst og kontrolleret, at kun medarbejdere med et arbejdsbetinget behov har adgang hertil.	Ingen afvigelser konstateret.
11.2.2	*Understøttende forsyninger (forsyningssikkerhed)* Udstyr er beskyttet mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.	Vi har inspiceret procedurer for beskyttelse af udstyr mod strømafbrydelser og andre afbrydelser som følge af svigt i understøttende forsyninger. Vi her inspiceret at backupstrøm, UPS-anlæg og dieselgeneratorer med tilstrækkelig kapacitet har været til rådighed. Vi har inspiceret servicerapporter, der viser, at serviceinspektioner er udført i overensstemmelse med leverandørers anbefalinger, og at udstyr testes regelmæssigt.	Ingen afvigelser konstateret.
11.2.4	*Vedligeholdelse af udstyr* Udstyr vedligeholdes korrekt for at sikre dets fortsatte tilgængelig hed og integritet.	Vi har forespurgt til servicerapporter vedrørende vedligeholdelse af et udvalg af udstyr med henblik på at konstatere, om udstyret var vedligeholdt i overensstemmelse med leverandørernes anbefalinger.	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.	Ingen afvigelser konstateret.

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

A.12 Driftssikkerhed

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
12.1.1	*Dokumenterede driftsprocedurer* Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem.	Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret og vedligeholdt. Vi har stikprøvevis inspiceret, at driftsdokumentation er opdateret og tilgængeligt.	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 inspiceret, at et udvalg af ændringer er implementeret i produktionsmiljøet i overensstemmelse med Change Management proceduren.	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 proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav. Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring.	Ingen afvigelser konstateret.
12.1.4	*Adskillelse af udviklings-, test- og driftsmiljøer* Udviklings-, test- og driftsmiljøer adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.	Vi har forespurgt til sikring af adskillelse af udviklings-, test- og driftsmiljøer. Vi har stikprøvevis inspiceret, at der enten er logisk eller fysisk adskillelse mellem udvikling, test og produktion.	Ingen afvigelser konstateret.

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

A.12.3 Backup Kontrolmål: At beskytte mod tab af data.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
12.3.1	*Backup af information* Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har inspiceret, at der gennemføres overvågning af afviklingen af backup. Vi har forespurgt til test af gendannelse fra backupfiler, og vi har inspiceret dokumentation for test af gendannelse.	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning Kontrolmål: At registrere hændelser og tilvejebringe bevis.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
12.4.1	*Hændelseslogning* Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Vi har forespurgt til logning af brugeraktivitet. Vi har inspiceret logningskonfigurationerne.	Ingen afvigelser konstateret.
12.4.2	*Beskyttelse af log- oplysninger* Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har forespurgt til procedurer for sikring af logoplysninger. Vi har inspiceret logningskonfigurationer med henblik på at konstatere, om logningsinformationer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	*Administrator- og operatørlog* Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt.	Vi har inspiceret proceduren vedrørende logning af aktiviteter udført af systemadministratorer og -operatører. Vi har inspiceret logopsætninger med henblik på at konstatere, om systemadministratorers og -operatørers handlinger logges.	Ingen afvigelser konstateret.
12.4.4	*Tidssynkronisering* Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne er synkroniserede til en enkelt referencetidskilde.	Vi har forespurgt til proceduren for synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware Kontrolmål: At sikre integriteten af driftssystemer.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
12.5.1	*Softwareinstallation på driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret retningslinjer for installation af software på driftssystemer, og vi har stikprøvevis inspiceret, at retningslinjerne efterleves.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
12.6.1	*Styring af tekniske sårbarheder* Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder. Vi har inspiceret implementerede foranstaltninger for styring af tekniske sårbarheder.	Ingen afvigelser konstateret.
12.6.2	*Begrænsninger på softwareinstallation* Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.	Vi har forespurgt til procedurer for begrænsning af softwareinstallation, som foretages af brugere. Vi har inspiceret, at regler for softwareinstallation efterleves.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
13.1.1	*Netværksstyring* Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har inspiceret, at der er defineret krav om styring og kontrol af netværk, herunder krav og regler om kryptering, segmentering, firewalls, intrusion detection og andre relevante sikkerhedsforanstaltninger. 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.	Ingen afvigelser konstateret.
13.1.2	*Sikring af netværkstjenester* Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.	Vi har observeret, at der foreligger skriftlige krav til sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester.	Ingen afvigelser konstateret.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
13.1.3	*Opdeling af netværk* Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.	Vi har inspiceret retningslinjerne for segmentering af netværk. Vi har inspiceret et udvalg af adgange mellem netværkszoner med hensyn til, om de er begrænset til nødvendige tjenester.	Ingen afvigelser konstateret.

A.13.2 Informationsoverførsel Kontrolmålet: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
13.2.1	*Politikker og procedurer for informationsoverførsel* Der foreligger formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.	Vi har inspiceret politikker og procedurer for dataoverførsel.	Ingen afvigelser konstateret.
13.2.2	*Aftaler om informationsoverførsel* Aftaler omhandler sikker overførsel af forretningsinformation mellem organisationen og eksterne parter.	Vi har forespurgt til aftaler om dataoverførsel. Vi har inspiceret, at der foreligger aftaler med kunder og andre eksterne parter, der beskriver krav til sikker udveksling af data.	Ingen afvigelser konstateret.
13.2.3	*Elektroniske meddelelser* Informationer i elektroniske meddelelser beskyttes på passende måde.	Vi har forespurgt til retningslinjer for afsendelse af fortrolig information.	Ingen afvigelser konstateret.
13.2.4	*Fortroligheds- og hemmeligholdelsesaftaler* Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, identificeres, gennemgås regelmæssigt og dokumenteres.	Vi har forespurgt til procedure for etablering af fortrolighedsaftaler. Vi har inspiceret et udvalg af underskrevne fortrolighedsaftaler med henblik på at konstatere, om proceduren efterleves ved ansættelse af nye medarbejdere.	Ingen afvigelser konstateret.

A.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.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
14.1.1	*Analyse og specifikation af informations- sikkerheds-krav* Informationssikkerhedsrelaterede krav omfattes af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.	Vi har inspiceret proceduren for analyse og specifikation af informationssikkerhedskrav. 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.	Ingen afvigelser konstateret.
14.1.2	*Sikring af applikationstjenester på offentlige netværk* Informationer i forbindelse med applikationstjenester over offentlige netværk beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring.	Vi forespurgt til procedurer for sikring af applikationstjenester på offentlige netværk.	Ingen afvigelser konstateret.

A.14.2 Sikkerheds, udviklings- og hjælpeprocesser Kontrolmål: At sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's 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 regler for udvikling af software og systemer. Vi har stikprøvevis inspiceret, at reglerne har været efterlevet.	Ingen 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 inspiceret proceduren for Change Management med henblik på at konstatere, hvorvidt proceduren indeholder krav om: • Risikovurdering • Test • Godkendelse • Systemdokumentation • Fall back plan. Vi har inspiceret et udvalg af ændringer med henblik på at konstatere, om kravene til ændringshåndtering blev fulgt.	Ingen afvigelser konstateret.
14.2.3	*Teknisk gennemgang af applikationer efter ændringer af driftsplatforme* Ved ændring af driftsplatforme gennemgås forretningskritiske applikationer og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.	Vi har forespurgt til proceduren for teknisk gennemgang af applikationer efter ændringer af driftsplatforme. Vi har stikprøvevis inspiceret, at ændringer er blevet vurderet m.h.t. deres eventuelle konsekvenser for applikationssystemer inden de er blevet gennemført.	Ingen afvigelser konstateret.
14.2.4	*Begrænsning af ændringer af softwarepakker* Ændringer af softwarepakker vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer styres effektivt.	Vi har forespurgt vedrørende proceduren for begrænsning af ændringer af softwarepakker.	Ingen afvigelser konstateret.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's 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 proceduren for udvikling af systemer. Vi har stikprøvevis inspiceret, at proceduren er blevet fulgt.	Ingen afvigelser konstateret.
14.2.6	*Sikkert udviklingsmiljø* Der er etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus	Vi har inspiceret proceduren for etablering af sikkert udviklingsmiljø. Vi har inspiceret dokumentation for, at proceduren har været fulgt.	Ingen afvigelser konstateret.
14.2.8	*Systemsikkerhedstest* Test af sikkerhedsfunktionalitet udføres ved udvikling.	Vi har stikprøvevis inspiceret, at der foretages test af sikkerhedsfunktionalitet som led i systemudviklingsprocessen.	Ingen afvigelser konstateret.
14.2.9	*Systemgodkendelsestest* Der etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.	Vi har forespurgt vedrørende godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer. Vi har stikprøvevis inspiceret, at der som led i systemudviklingsprocessen foretages test af systemer.	Ingen afvigelser konstateret.

A.14.3 Testdata Kontrolmål: At sikre beskyttelse af data, som anvendes til test			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
14.3.1	Sikring af testdata Testdata udvælges omhyggeligt og beskyttes og styres.	Vi har inspiceret proceduren vedrørende udvælgelse og beskyttelse af testdata.	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.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
15.1.1	*Informationssikkerhedspolitik for leverandørforhold* Informationssikkerhedskravene til at minimere risicierne forbundet med leverandørers adgang til organisationens aktiver aftales med leverandøren og dokumenteres.	Vi har inspiceret proceduren for indgåelse af aftaler med leverandører. Vi har inspiceret proceduren vedrørende udvælgelse og beskyttelse af testdata.	Ingen afvigelser konstateret.
15.1.2	*Håndtering af sikkerhed i leverandøraftaler* Alle relevante informationssikkerhedskrav fastlægges og aftales med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information.	Vi har inspiceret proceduren for indgåelse af aftaler med leverandører. Vi har inspiceret indgåede leverandøraftaler m.h.t. aftaler om informationssikkerhedskrav.	Ingen afvigelser konstateret.

15.2 Styring af leverandørydelser Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.			
Nr.	**DFF|EDB a.m.b.a.s kontrol**	**REVI-IT's test**	**Resultat af test**
15.2.1	*Overvågning og gennemgang af leverandørydelser* Organisationer overvåger, gennemgår og auditerer leverandørydelser.	Vi har inspiceret proceduren for overvågning og gennemgang af serviceydelser leveret af underleverandører er i overensstemmelse med det aftalte. Inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører.	Ingen afvigelser konstateret.
15.2.2	*Styring af ændringer af leverandørydelser* Leverandørydelser overvåges, gennemgås og auditeres.	Vi har forespurgt til styring af ændringer hos leverandører og inspiceret dokumentation for håndteringen.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

A.16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
16.1.1	*Ansvar og procedurer* Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har forespurgt til ansvar og procedurer i forbindelse med informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har endvidere inspiceret procedure til håndtering af informationssikkerhedshændelser.	Ingen afvigelser konstateret.
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne.	Ingen afvigelser konstateret.
16.1.3	*Rapportering af informationssikkerhedssvagheder* Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester.	Vi har forespurgt til informationssikkerhedshændelser i perioden, samt inspiceret disse.	Ingen afvigelser konstateret.
16.1.4	*Vurdering af og beslutning om informations- sikkerhedshændelser* Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	Vi har inspiceret procedure for vurdering og evaluering af informationssikkerhedsbrud.	Ingen afvigelser konstateret.
16.1.5	*Håndtering af informationssikkerhedsbrud* Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer.	Vi har stikprøvevis inspiceret, at informations sikkerhedsbrud har været håndteret i overensstemmelse med de dokumenterede procedurer.	Ingen afvigelser konstateret.

16.1.6	*Erfaring fra informationssikkerhedsbrud* Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.	Vi har forespurgt vedrørende Problem Management-funktion, der analyserer informationssikkerhedsbrud med henblik på at reducere sandsynligheden for at de gentager sig.	Ingen afvigelser konstateret.

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

A.17.1 Informationssikkerhedskontinuitet

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
17.1.1	*Planlægning af informationssikkerhedskontinuitet* Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.	Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen.	Ingen afvigelser konstateret.
17.1.2	*Implementering af informationssikkerheds- kontinuitet* Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.	Vi har forespurgt om der er procedurer der sikrer, at alle relevante systemer indgår i beredskabsplanlægningen. Vi har inspiceret om beredskabsplanen vedligeholdes.	Ingen afvigelser konstateret.
17.1.3	*Verificer, gennemgå og evaluer informations- sikkerhedskontinuiteten* Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til regelmæssig revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurderingen.	Ingen afvigelser konstateret.

A.17.2 Redundans

Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
17.2.1	Tilgængelighed af informationsbehandlingsfaciliteter Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	Vi har forespurgt til etablering af redundans til sikring af tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen afvigelser konstateret.

A.18 Overensstemmelse

A.18.2 Gennemgang af informationssikkerheden

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

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
18.2.1	*Uafhængig gennemgang af informationssikkerhed* Organisationens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.	Vi har observeret, at der er etableret krav om regelmæssig uafhængig revisionsmæssig gennemgang af informationssikkerheden.	Ingen afvigelser konstateret.
18.2.2	*Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder* Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.	Vi har forespurgt vedrørende lederes sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder.	Ingen afvigelser konstateret
18.2.3	*Undersøgelse af teknisk overensstemmelse* Informationssystemer undersøges regelmæssigt for, om de er i overensstemmelse se med organisationens informationssikkerhedspolitikker og -standarder.	Vi har inspiceret, at procedurer for regelmæssig kontrol af systemers overholdelse af sikkerhedsstandarder er implementeret.	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.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's 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 forespurgt til, kontroller for opretholdelse af tidligere funktioner, og vi har inspiceret udvalgte kontroller. Vi har forespurgt til kontroller for modposteringer, og vi har stikprøvevis inspiceret kontrollerne. Vi har forespurgt til kontroller til sikring af, at der bogføres korrekt, og vi har stikprøvevis inspiceret kontrollerne. Vi har forespurgt til kontroller til sikring af, at bogføring ikke kan foretages på lukkede regnskaber, og vi har stikprøvevis inspiceret kontrollerne. Vi har forespurgt til test af, at bogført linjer tilfalder korrekte tabeller, og vi har stikprøvevis inspiceret kontrollerne.	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.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
01	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. 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.	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. Vi har forespurgt til kontroller til sikring af, at bogførte registreringer tilfalder korrekte tabeller, og vi har inspiceret kontrollerne.	Ingen afvigelser konstateret.

A7 Betalingsfil til NETS

Det primære formål med denne kontrol er at validere, at ud datering af NETS-filer valideres.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Formålet med denne testkørsel er at teste dannelsen af en PBS betalingsfil til NETS, for at sikre konsistensen for denne. Udgangspunktet er en betalingsfil til ratebetalinger uden bilag. For alle testcases gennemføres wizarden, med forskellige tilvalg/fravalg og intervaller. Til sidst i de enkelte testcases sammenlignes den dannede fil med en reference fra da testen blev oprettet; denne danner basis for en succes eller fejl.	Vi har forespurgt til kontroller for korrekt udlæsning af betalingsfiler til NETS, og vi har inspiceret datagrundlaget for testrapporterne.	Ingen afvigelser konstateret.

A8 OIOUBL og OIOXML til NemHandel

Det primære formål med denne kontrol er at validere, at ud datering af NemHandel-filer valideres.

Nr.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's test	Resultat af test
01	Dette testrun kører på genereringen af NemHandels dokumenter. Der lægges vægt på det, der er specielt for NemHandels dokumenter, herunder format og det nødvendige indhold i dokumenterne/filerne. Da der er værker med forbrugere, der modtager i OIOXML, medtages denne på lige fod med OIOUBL. Denne test har samme omfang som test A7. I A7 er filerne rettet mod NETS/PBS, hvorimod filerne i A8 bliver sendt direkte til den forbruger, som skal betale, og de skal selv sørge for at overføre/betale pengene. Denne test benytter Testdata01 databasen. Dataene er modificeret for at give et mere varieret datasæt.	Vi har forespurgt til kontroller for korrekt udlæsning af elektroniske faktura til NemHandel, og vi har inspiceret datagrundlaget for testrapporterne.	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.	DFF|EDB a.m.b.a.s kontrol	REVI-IT's 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 og 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 forespurgt til kontroller til sikring af funktionsadskillelse ved anvendelse af FOF, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til kontroller til sikring af, at der er differentiering af rettigheder, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til kontroller til sikring af, at indtastede data er korrekt på faktura, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til kontroller for validering ved inddatering af OIO filer, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B10 Tilbudskladde

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

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	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 kladde 50, uden at brugeren får det at se. 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.	Vi har forespurgt til kontroller til validering af inddatering i tilbudskladden, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til validering af ud datering i forbindelse med udskrift af tilbud, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B11 FOF scripts dataudtræk

Det primære formål med denne kontrol er at validere overensstemmelse af inddata og uddata fra appserver.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Formålet med dette test run er at teste dele af FOF-script, som bruges i tekstbehandler samt dannelsen af dataudtræk. Dette test run tager udgangspunkt i funktionaliteten af kommandoen MAT med den tilhørende funktionalitet som beskrevet i FOF-551. Hertil baseres dette test run også på et generelt data udtræk, der bruges til App-Server delen af FOF: 'AppServer - Forbrug', som kan importeres i hvilket som helst FOF.	Vi har forespurgt til kontroller for indlæsning og udlæsning af filer fra appserver, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B12 Restancekladde

Det primære formål med denne kontrol er at validere, at restancer er retvisende, korrekt beregnede og opdaterede.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Formålet med denne testcase er at teste restancekladden. Herunder med fokus på at restancelisten genereres/genberegnes konsistent, at skrivelser fra denne vises konsistent, og at aconto poster bogføres til den korrekte forbruger. Der følges op på, at det er muligt at taste i felterne som begrundelse, lukningsdato, og at de andre felter er lukket for ændringer, og at disse felter er persistente, når det vælges at genberegne restancelisten.	Vi har forespurgt til kontroller til sikring af, at det alene er muligt at inddatere i relevante felter i restancekladden, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til kontroller til sikring af, at restancer opdateres i forbindelse med genberegning, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til kontroller til sikring af, at der bogføres på den korrekte bruger, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B14 Aflæsningskladde

Det primære formål med denne kontrol er at validere, at aflæsninger er retvisende og korrekt registrerede.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Formålet med denne testcase er at teste aflæsningskladden. Dette test run vil gennemføre test cases på aflæsningskladden, herunder indtaste aflæsninger manuelt, indlæse aflæsningsfil og følge op på, at aflæsninger bliver registreret korrekt i aflæsningstabellen, med deres dertilhørende installationer.	Vi har forespurgt til kontroller til validering af data ved manuelle indtastninger og automatiske indlæsninger, og vi har inspiceret testrapporterne for applikationen. Vi har forespurgt til kontroller til sikring af, at aflæsninger kun inddateres én gang, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B15 Beregn faktura

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

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Formålet med denne testcase er at teste beregn faktura. Disse testcases vil gennemføre test i forhold til skærmbilledet "Dan opgørelse". De beskrevne test cases 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.

B17 Målerskifte

Det primære formål med denne kontrol er at validere registrering af skift af målere.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Formålet med denne testcase er at afprøve alle typer af målerskift, herunder komplet målerskift, batteriskift, nedlægning af måler. Såvel som med og uden aflæsninger, hertil også korrektioner. Og slutteligt test af kvikmålerskift-kladde, med indlæsning af flere typer filer, med korrekte og fejlbehæftede linjer.	Vi har forespurgt til kontroller til sikring af, at skift af måler registreres på korrekt forbruger, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.

B18 Brugeroprettelse

En test af kundeoprettelses wizzarden, der forsøger at aktivere alle funktionaliteter samt validere de mulige inputs i wizarden.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Der testet gennem forskellige scenarier i forbindelse med forbrugeroprettelser. Der testes med differentierede adresser og forskellige typer af betalingstyper og forsyningsformer.	Vi har forespurgt til kontroller til validering af data ved forbrugeroprettelser, og vi har inspiceret datagrundlaget for testrapporterne.	Ingen afvigelser konstateret.

B20 Moms

Denne kontrol har til formål at teste, hvordan moms håndteres på tværs af systemet.

Nr.	DFF|EDB a.m.b.a.'s kontrol	REVI-IT's test	Resultat af test
01	Alle momskoder testes gennem forskellige scenarier. Der testes oprettelse af moms koder, linjer der modposteres, fri faktura, kreditnota, m.m.	Vi har forespurgt til kontroller til validering af data ved håndtering af moms, og vi har inspiceret testrapporterne for applikationen.	Ingen afvigelser konstateret.