Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning, implementering og effektivitet i relation til DFF|EDB's it-hosting-løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF i perioden 1. juli 2017 – 31. maj 2018

ISAE 3402-II

DFF|EDB

CVR-nr.: 26 22 40 20

Juli 2018

Indholdsfortegnelse

Afsnit 1: DFF|EDB's udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt DFF|EDB's it-hosting-løsning 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 bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af DFF|EDB's it-hosting-løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF til kunder i hele perioden fra 01-07-2017 til 31-05-2018. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
- De typer af ydelser, der er leveret, når det er relevant
- De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- Relevante kontrolmål og kontroller, udformet til at nå disse mål
- Kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificerede i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner.

(ii) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. juli 2017 – 31. maj 2018

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

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra 1. juli 2017 – 31. maj 2018. Kriterierne for denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. juli 2017 – 31. maj 2018.

Arbejdet med at indarbejde rutiner og kontroller med tilhørende tekniske anordninger gennem det seneste år har været intensivt, men har givet anledning til langt større transparens for os og dermed vores kunder.

Vi har igennem det seneste år arbejdet intensivt med opbygning af vores kontrolmiljø, herunder udarbejdelse af politikker, procedurer, kontroller samt dokumentation heraf. Dette arbejde fortsætter vi med i løbet af 2018.

Kolding, 6. juli 2018

DFF|EDB

Jan Elmstrøm Blaabjerg
Adm. direktør

Afsnit 2: DFF|EDB's beskrivelse af kontroller 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 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 troværdigt. 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 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 i ISO 27002.

Risikovurdering og -håndtering

DFF|EDB har en procedure for løbende risikovurdering af udvikling og vedligeholdelsen 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. Alle i kategori Gul og Rød risici bliver behandlet af den samlede ledergruppe i DFF|EDB.

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

Sikkerhedspolitik

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

Organisering af informationssikkerhed

Det er kun ansatte i udviklingsafdelingen, der har adgang til vores kildekode i Subversion. Opsætning og administration af testmaskiner, build-serverer administreres ligeledes af udviklingsafdelingen og teknisk afdeling.

Den enkelte udvikler har ikke direkte adgang til produktionsserverne fra en udvikler PC. Er det nødvendigt at tilgå værkernes data for at yde support eller fejlfinde, sker dette igennem RDS, hvor der er sporbarhed af hvem der logger på. Det bevirker også, at der ikke ved et uheld kommer til at blive ændret i produktionsdata, fra en udvikler PC.

Det er kun ansatte hos hosting-partner, Teknisk Afdeling 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 bruger, og anvender personligt brugernavn og password. Alt adgang til data, sker via en SSL eller VPN forbindelse.

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-sikkerheds procedurer 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.

Styring af aktiver

Alle data i Hosting-miljøet er klassificeret 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 kildekode og programmer, der udvikles, ejes af DFF|EDB, og må ikke kopieres eller overdrages til 3. part.

Adgangskontrol

Det er kun Teknisk Afdeling i DFF|EDB, 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 i DFF|EDB, 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 skal skiftes hver 3. måned. 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.

Bemærk at DFF|EDB af supportmæssige årsager har rettigheder til at logge på alle systemer i Forsyning|Hosting.

Det er ikke muligt for kunderne selv at lave ændringer i Forsyning|Hosting.

Det er kun udviklingsafdelingen, der har adgang til at oprette brugere i Subversion.

Kryptografi

Al adgang til Hosting miljøet sker via en SSL eller VPN forbindelse.

DFF|EDB anvender et SHA-256 krypteret system til opbevaring af administrative kodeord.

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. 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 er placeret en backupserver på en sikret ekstern lokation, hvor der dagligt bliver overført en kopi af Hosting-miljøet til. Ved udskiftning af databærende udstyr, bliver alle data slettet og udstyret efterfølgende fysisk destrueret.

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.

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.

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 opbevaret sammen med systemdokumentationen.

Adgang til Hosting-miljøet sker altid via SSL. Der er opsat overvågning og logning af netværkstrafik. Alene godkendt netværkstrafik kommer gennem vores firewall. Dette gælder både indgående og udgående trafik.

Der er en segmentering af netværket, afhængig af funktionsbehov.

DFF|EDB overfører ikke, medmindre andet er aftalt, kunders data eller dele deraf til 3. part. Der er etableret fortrolighedsaftaler eller NDA for alle involveret med kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.

Anskaffelse, udvikling og vedligeholdelse

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

Udvikling af Forsyning|FOF sker primært af DFF|EDB's egen udviklingsafdeling.

Leverandørforhold

Der er fortrolighedserklæringer med alle konsulenter, der får adgang til systemet. Som udgangspunkt arbejder de udelukkende med hardware- og software-problemstillinger, 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 Zitcom. DFF|EDB har selv driftsansvaret for eget servermiljø hos DFF|EDB.

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.

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 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 til Zitcom IT revisionserklæring.

Overensstemmelse

Hverken DFF|EDB eller vores kunder, er underlagt særlig lovgivning i forhold til vores ydelse. DFF|EDB er dog opmærksom på, at persondataforordningen medfører behov for at revurdere nogle af selskabets procedurer og retningslinjer for opbevaring af data. Der pågår internt afklaringsarbejde i den anledning.

En gang årligt gennemgås den gældende sikkerhedspolitik af IT-sikkerhedsudvalget, samt ved 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.

FOF – Testcomplete

Udgangspunktet for test og kvalitetssikring i DFF|EDB er at alle moduler, forbedringer og fejl, som bliver udviklet, også bliver testet enten manuelt eller via automatiske tests inden de bliver committed og frigivet til en ny release af Forsyning|FOF.

Vi anvender TestComplete til udvikling af vores automatiserede tests. De automatiserede tests udvikles og renoveres løbende i TestComplete. TestComplete kører hver nat en automatisk test på den version af Forsyning|FOF, som ligger i trunk i subversion. Er der fejl i de afviklede tests, undersøger testansvarlige årsagen og tager fat i den rette udvikler for at finde en løsning. Alt efter årsagens betydning for Forsyning|FOF, kan løsningen enten være at tilrette kode til Forsyning|FOF eller tilrette kode til TestComplete pga. implementering af ny funktionalitet. Der udgives ikke en release af Forsyning|FOF, før der er fundet en løsning på fejlen i fejlloggen, og en godkendt automatisk test kørsel er gennemført.

A1: Opsætning og Login

Formålet med dette test run er at indsætte en ren test database, som andre test runs kan køre videre på. Hele kørslen genopretter databasen og giver mulighed for at logge ind med DFF Bruger og ADM bruger.

A2: Login procedure

Opgave for denne test run er at teste login proceduren, både med DFF bruger, en almindelig bruger, ved flere brugere logins, og når der skal køres opgraderings scripts.

Klient håndtering og ind/udlæsning af sikkerhedskopier testes ikke.

A4: Finanskladde

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.

A5: Acontokladde

Dette testrun gennemgår funktionaliteten af Acontokladden. 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.

Ved bogføring bliver der testet om det falder korrekt på plads i de respektive tabeller i FOF.

A6: Flytteprocedure

Dette testrun har til opgave at gennemløbe Flyttewizarden med udgangspunkt i kvikflyt. Wizarden bliver gennemløbet med forskellige forbruger, der alle har forskellige forudsætninger i forhold til aflæsninger, opgørelser med videre.
Nogle testcases har et navn, der slutter på et forbrugernummer. Forbrugernummeret identificerer sig med en kolonne i det tilknyttede Excel ark, dette ark beskriver hvilke specielle forløb, der bliver testet af den konkrete testcase.

A7: Betalingsfil til NETS

Formålet med denne testkørsel er at teste dannelsen af en PBS betalingsfil til NETS, 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.

A8: OIOUBL og OIOXML til Nemhandel

Dette testrun kører på genereringen af nemhandelsdokumenter. Der lægges vægt på det, der er specielt for nemhandelsdokumenter, 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.

A9: Fakturaflow

Denne testcase gennemløber mulighederne i Fakturaflow og sikrer at brugerbegrænsninger, status for fordelte og godkendte faktura bibeholdes, at såvel 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, Brugeropsætning, Kreditorvedligeholdelse (fanen posteringer).

B10: Tilbudskladde

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, system miljøet og i forhold til EDH arkivering på forbrugeren. Hertil vil også funktionaliteten med at udskrive, arkivere og bogføre tilbud blive testet.

B11: FOF scripts dataudtræk

Formålet med dette test run er at tester 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. Hertil baseres dette test run også på et generelt dataudtræk, der bruges til App-Server delen af FOF: 'AppServer - Forbrug', som kan importeres i hvilket som helst FOF.

B12: Restancekladde

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 acontoposter, 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.

B13: E|Forsyning

Formålet med denne test, er udarbejdet i forbindelse med modulet til optegning af eForsyning, og dækker de FOF relaterede ændringer til håndtering af eBruger og eBrugerrelation.

B14: Aflæsningskladde

Formålet med denne testcase er at teste aflæsningskladden. Dette test run vil gennemføre test cases på aflæsnings kladden, herunder indtaste aflæsninger manuelt, indlæse aflæsnings fil og følge op på at aflæsninger bliver registreret korrekt i aflæsnings tabellen, med deres dertilhørende installationer.

B15: Beregn faktura

Formålet med denne testcase er at teste beregn faktura. Disse testcases vil gennemføre test i forhold til skærmbilledet "Dan opgørelse". De beskrevne testcases vil teste alle opgørelsestyper og undertyper (i forhold til budget). I et testcase registreres opgørelsen til brug i efterfølgende testcases.

B16: Forbruger overvågning

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.

B17: Målerskifte

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.

B18: Forbruger Oprettelse

En test af kundeoprettelses-wizarden, der forsøger at aktivere alle funktionaliteter samt validere de mulige inputs i wizarden. Denne test holdes i rent scripting-sprog fremfor keyword test.

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 hosting-miljø. Herudover er DFF|EDB's kunder, medmindre andet er aftalt, ansvarlige for:

- At det aftalte niveau for backup dækker kundens behov
- At kunder, der ikke benytter Forsyning|Hosting, selv er ansvarlige for sikkerhedsniveau, beredskab, backup, løbende opdateringer, drift osv.

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

Til ledelsen hos DFF|EDB, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om DFF|EDB's beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af DFF|EDB's ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens it-hosting-løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF i perioden 01-07-2017 til 31-05-2018, samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

DFF|EDB's ansvar

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

REVI-IT A/S' uafhængighed og kvalitetsstyring

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

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

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om DFF|EDB's beskrivelse (afsnit 2) og om udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede og fungerer effektivt.

Opgaven med afgivelse af en erklæring med sikkerhed om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformede eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2.

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

Begrænsninger i kontroller hos en serviceleverandør

DFF|EDB's beskrivelse i afsnit 2 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

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

(a) at beskrivelsen af kontroller, således som de var udformede og implementerede i hele perioden 01-07-2017 til 31-05-2018, i alle væsentlige henseender er retvisende
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformede i hele perioden fra 01-07-2017 til 31-05-2018
(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 01-07-2017 til 31-05-2018.

Fremhævelse vedrørende centrale forhold i revisionen

Uden at det har påvirket vores konklusion, skal vi henlede opmærksomheden på ledelsens udsagn i afsnit 1, hvor de beskriver de igangværende processer omkring det videre arbejde med politiker, procedurer, kontroller samt dokumentation heraf.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt DFF|EDB's it-hosting-løsning Forsyning|Hosting samt finans- og forbrugersystemet Forsyning|FOF, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 6. juli 2018

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

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

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

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som DFF|EDB har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 01-07-2017 til 31-05-2018.

Vi har således ikke nødvendigvis testet alle de kontroller, som DFF|EDB har nævnt i sin beskrivelse i afsnit 2.

Kontroller udført hos DFF|EDB's kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos DFF|EDB via følgende handlinger:

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

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

Risikovurdering og -håndtering

Risikovurdering

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
4.1	DFF|EDB har en procedure for løbende risikovurdering af udvikling og vedligeholdelsen 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.	Vi har forespurgt til udarbejdelsen af en it-risikoanalyse, og vi har inspiceret den udarbejdede it-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 revisionsperioden.	Ingen væsentlige afvigelser konstateret.

Informationssikkerhedspolitikker

Retningslinjer for styring af informationssikkerhed

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
5.1	IT-Sikkerhedspolitikken gennemgås en gang årligt. Denne gennemgang ligger som en fast opgave i Outlook hos IT-sikkerhedsudvalget.	Vi har forespurgt til udarbejdelsen af en informationssikkerhedspolitik, og vi har inspiceret dokumentet. Vi har forespurgt til periodisk gennemgang af informationssikkerhedspolitikken, og vi har inspiceret, at dokumentet er gennemgået i revisionsperioden. Vi har desuden inspiceret kontrol for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Vi har observeret, at informationssikkerhedspolitikken tager udgangspunkt i ISO 27002:2013. Dog er der for dele af perioden kun taget stilling til punkterne 5-10, og dermed mangler der stillingtagen til punkterne 11-18, der bl.a. indeholder væsentlige dele for styring af driften, styring af udvikling, og styring af leverandører. Vi har påset, at forholdet er udbedret i Q2 2018. Ingen væsentlige afvigelser konstateret i øvrigt.

Organisering af informationssikkerhed

Intern organisering

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
6.1	Det er kun ansatte i udviklingsafdelingen, der har adgang til vores kildekode i Subversion. Opsætning og administration af testmaskiner, build-serverer administreres ligeledes af udviklingsafdelingen og tekniskafdeling. Den enkelte udvikler har ikke direkte adgang til produktionsserverne fra en udvikler PC. Er det nødvendigt at tilgå værkernes data for at yde support eller fejlfinde, sker dette igennem RDS, hvor der er sporbarhed af hvem der logger på. Det er kun ansatte hos hosting partner, Teknisk Afdeling og udviklingsafdelingen, der i samarbejde har adgang til at lave ændringer i Hosting miljøet, der kan påvirke driftsstabiliteten.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen og vedligeholdelsen af ansvarsbeskrivelser. Vi har forespurgt til adskillelse af adgang i forhold til funktion, og vi har inspiceret dokumentation for differentieret adgang. Vi har forespurgt til retningslinjer for kontakt med myndigheder. Vi har forespurgt til kontakt med interessegrupper, og vi har inspiceret dokumentation for kontakt. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter. Vi har stikprøvevis inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
6.2	Alt adgang til data, sker via en SSL eller VPN forbindelse.	Vi har forespurgt til styring af mobile enheder, og vi har inspiceret løsningen. Vi har forespurgt til sikring af fjernarbejdspladser, og vi har inspiceret løsningen.	Vi har observeret, at der ikke er retningslinjer eller kontroller til sikring af mobile enheder og fjernarbejdspladser. Ingen væsentlige afvigelser konstateret i øvrigt.

Medarbejdersikkerhed

Før ansættelsen

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
7.1	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.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har endvidere stikprøvevis inspiceret dokumentation for, at proceduren er fulgt. Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevis inspiceret indholdet af kontrakter.	Ingen væsentlige afvigelser konstateret.

Under ansættelsen

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
7.2	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.	Vi har forespurgt til ledelsens ansvar for videreformidling af politikker og procedurer, og vi har inspiceret dokumentation for tildeling af ansvar. Vi har forespurgt til videreuddannelse af personale, og vi har stikprøvevis inspiceret dokumentation for videreuddannelse. Vi har forespurgt til retningslinjer for sanktionering.	Ingen væsentlige afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring

Kontrolmål: Formålet er at beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
7.3	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.	Vi har forespurgt til medarbejderes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør i ansættelse, og vi har inspiceret dokumentation for medarbejdernes forpligtelser.	Ingen væsentlige afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
8.1	DFF|EDB opererer med systemejere, der er ansvarlig for forskellige aktiver. Herigennem sikrer vi individuel fokus på sikkerheden i alle delelementer.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har forespurgt til oversigt af ejerskab for aktiver, og vi har inspiceret oversigten. Vi har forespurgt til retningslinjer for brugen af aktiver, og vi har inspiceret retningslinjerne. Vi har forespurgt til procedure til sikring af tilbagelevering af udleverede aktiver, og vi har inspiceret proceduren.	Det har ikke været muligt at teste effektiviteten af procedure for tilbagelevering af aktiver, idet der ikke har været fratrædelser i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.

Klassifikation af information

Kontrolmål: Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
8.2	Alle data i Hosting-miljøet er klassificeret som fortrolige kundedata.	Vi har forespurgt til politik for klassificering af data, og vi har inspiceret politikken. Vi har forespurgt til mærkning af data, og vi har inspiceret retningslinjerne for mærkning af data. Vi har forespurgt til retningslinjer for håndtering af aktiver, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Mediehåndtering

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
8.3	Ved udskiftning af databærende udstyr, bliver alle data slettet og udstyret efterfølgende fysisk destrueret.	Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen. Vi har forespurgt til retningslinjer for bortskaffelse af medier. Vi har forespurgt til transport af bærbare medier.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
9.1	Det er kun Teknisk Afdeling i DFF|EDB, 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 i DFF|EDB, 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 skal skiftes hver 3. måned.	Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken. Vi har forespurgt til håndtering af adgang til netværk og netværksservices, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Administration af brugeradgange

Kontrolmål: Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
9.2	Det er kun Teknisk Afdeling i DFF|EDB, 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 i DFF|EDB, 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 skal skiftes hver 3. måned.	Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret dokumentation for oprettelse og nedlæggelse af brugere. Vi har forespurgt til proces for tildeling af rettigheder, og vi har inspiceret processen. Vi har forespurgt til overvågning af anvendelsen af privilegerede adgangsrettigheder, og vi har stikprøvevis inspiceret dokumentation for overvågning. Vi har forespurgt til opbevaring af fortrolige adgangskoder, og vi har inspiceret dokumentation for betryggende opbevaring. Vi har forespurgt til proces for periodisk gennemgang af brugere. Vi har forespurgt til procedure for inddragelse af rettigheder, og vi har inspiceret proceduren.	Det har ikke været muligt at teste effektiviteten for nedlæggelse af brugere, da der ikke har været fratrædelser hos DFF|EDB i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.

Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
9.3	DFF|EDB's medarbejdere bliver uddannet i it-sikkerhed, herunder håndtering af fortrolige informationer såsom deres logon informationer mv. Er personlige og fortrolige, og deles dermed ikke med andre.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Styring af system- og applikationsadgang **Kontrolmål: Formålet er at forhindre uautoriseret adgang til systemer og applikationer.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
9.4	Der er sporbarhed af, hvem der logger på hvilke produktionsservere og der er opdeling i medarbejdes rettigheder, jf. funktionsbeskrivelse i DFF|EDB's interne netværk.	Vi har forespurgt til begrænsning af adgang til data, og vi har inspiceret dokumentation for begrænsning. Vi har forespurgt til procedure for sikker logon, og vi har inspiceret løsningen. Vi har forespurgt til system til styring af adgangskoder. Vi har inspiceret løsningen og udvalgte konfigurationer.	Ingen væsentlige afvigelser konstateret.

Kryptografi

Kryptografiske kontroller **Kontrolmål: Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
10.1	Al adgang til Hosting miljøet sker via en SSL eller VPN forbindelse. DFF|EDB anvender et SHA-256 krypteret system til opbevaring af administrative kodeord.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	Ingen væsentlige afvigelser konstateret.

Fysisk sikring og miljøsikring

Sikre områder

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
11.1	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 metal gitter.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør, og vi har stikprøvevis inspiceret dokumentation for tildeling af adgang til driftsfaciliteter. Vi har inspiceret de fysiske forhold ved virksomhedens kontorer med henblik på at kontrollere den fysiske sikring. Vi har forespurgt til levering af pakker og varer.	Ingen væsentlige afvigelser konstateret.

Udstyr **Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
11.2	Vores servere er fysisk placeret i aflåst lokale, som har monteret køling. Adgangen til eksternt driftscenter sker i henhold til leverandørs anvisninger.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere understøttende forsyninger og sikring af regelmæssig vedligeholdelse af udstyret. Vi har forespurgt til sikring af kabler, og vi har inspiceret erklæring fra leverandør. Vi har forespurgt til politik for bortskaffelse af udstyr. Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler. Vi har inspiceret erklæring fra underleverandør. Vi har observeret, at erklæring fra underleverandør dækker til og med 31. december 2017. Vi har forespurgt til periodisk eftersyn af ekstern lokation, og vi har stikprøvevis inspiceret dokumentation for eftersyn. Vi har endvidere ved genudførelse af kontrol inspiceret den eksterne lokation. Vi har forespurgt til politik for bortskaffelse af databærende medier. Vi har forespurgt til sikring af brugerudstyr uden opsyn, og vi har stikprøvevis inspiceret, at brugerudstyr låses ved inaktivitet. Vi har forespurgt til politik for ryddeligt skrivebord.	Vi har fået oplyst, at der ikke er implementeret retningslinjer eller kontroller til sikring af brugerudstyr, når det ikke anvendes, såsom pauseskærm eller timeout. Vi har endvidere påset, at virksomheden har påbegyndt tiltag til udbedring af forholdet. Ingen væsentlige afvigelser konstateret i øvrigt.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
12.1	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.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til ændringsstyring, og vi har stikprøvevis inspiceret dokumentation for håndtering af ændringer i perioden. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Vi har forespurgt til erklæring fra underleverandør, og vi har inspiceret erklæringen. Vi har forespurgt til anvendelsen af testmiljø, og vi har inspiceret dokumentation for eksistensen af testmiljø.	Vi har observeret, at virksomheden ikke har formuleret eller implementeret formelle procedurer for indberetning eller fremsending af ændringer til leverandøren. Vi har endvidere fået oplyst, at ændringer ikke dokumenteres af DFF|EDB. Vi har dog observeret, at der ikke er observationer vedrørende styring af ændringer i erklæringen fra underleverandøren. Ingen væsentlige afvigelser konstateret i øvrigt.

Malwarebeskyttelse

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
12.2	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.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til erklæring fra underleverandøren, og vi har inspiceret erklæringen.	Vi har observeret, at der i erklæring fra underleverandøren ikke er taget stilling til beskyttelse mod malware. Ingen væsentlige afvigelser konstateret i øvrigt.

Backup

Kontrolmål: Formålet er at beskytte mod tab af data.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
12.3	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.	Vi har forespurgt til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for opsætningen. Vi har forespurgt til opbevaring af backup, og vi har inspiceret erklæring fra underleverandør med henblik på at se, at backup opbevares forsvarligt. Vi har forespurgt til test af genopprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genopprettelse.	Ingen væsentlige afvigelser konstateret.

Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
12.4	Der er opsat overvågning og logning af netværkstrafik.	Vi har forespurgt til logning af brugeraktivitet, og vi har inspiceret løsningen. Vi har forespurgt til sikring af logoplysninger. Vi har forespurgt til synkronisering op imod en betryggende tidsserver.	Vi har observeret, at virksomheden ikke har implementeret en logningsstrategi, hvori forretningen har taget stilling til logningsniveauet. Vi har endvidere observeret, at virksomheden i begrænset omfang foretager central opsamling og proaktiv logmonitorering. Ingen væsentlige afvigelser konstateret i øvrigt.
Styring af driftssoftware **Kontrolmål: Formålet er at sikre integriteten af driftssystemer.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
12.5	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.	Vi har forespurgt til retningslinjer for installation af software på driftssystemer, og vi har inspiceret retningslinjerne. Vi har forespurgt til rettidig opdatering af driftssystemer, og vi har inspiceret dokumentation for opdatering af driftssystemerne.	Ingen væsentlige afvigelser konstateret.
Sårbarhedsstyring **Kontrolmål: Formålet er at forhindre, at tekniske sårbarheder udnyttes.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
12.6	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.	Vi har forespurgt til styring af tekniske sårbarheder, og vi har inspiceret dokumentation for styringen. Vi har forespurgt til styring af adgang til programinstallation, og vi har inspiceret dokumentation for begrænsningen af brugere med rettighed til programinstallation.	Ingen væsentlige afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
13.1	Alt er sikret via firewall, og der er udarbejdet procedurer, vejledninger og dokumentation til anvendelse i forbindelse med drift og vedligehold af netværket. Der er en segmentering af netværket, afhængig er funktionsbehov	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall og patching af firewall. Vi har forespurgt til sikring af netværkstjenester, og vi har inspiceret dokumentation for betryggende sikring.	Ingen væsentlige afvigelser konstateret.

Informationsoverførsel

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
13.2	Adgang til Hosting miljøet sker altid via SSL. Der er opsat overvågning og logning af netværkstrafik. Alene godkendt netværkstrafik kommer gennem vores firewall. Dette gælder både indgående og udgående trafik. DFF|EDB overfører ikke, med mindre andet er aftalt, kunders data eller dele deraf til 3. part. Der er etableret fortrolighedsaftaler eller NDA for alle involveret med kunders data. Dette gælder både personale, underleverandører og samarbejdspartnere.	Vi har forespurgt til politikker og procedurer for dataoverførsel. Vi har forespurgt til aftaler om dataoverførsel. Vi har forespurgt til retningslinjer for afsendelse af fortrolig information. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen væsentlige afvigelser konstateret.

Anskaffelse, udvikling og vedligeholdelse af systemer

Sikkerhedskrav til informationssystemer

Kontrolmål: Formålet er 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's kontrol	REVI-IT's test	Resultat af test
14.1	Der er fastsatte procedure ifm. egen udvikling og indkøb/implementering af software. Disse dækker over procedure, før-, under- og efter i idriftsættelse. Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, med mindre at ledelsen accepterer den øgede risiko.	Vi har forespurgt til informationssikkerhedsrelaterede krav til virksomhedens løsning, og vi har inspiceret de opstillede krav. Vi har forespurgt til sikring af løsningen på offentlige netværk, og vi har inspiceret løsningen. Vi har forespurgt til sikring af transmissioner, og vi har inspiceret dokumentation for beskyttelse af transmissioner.	Ingen væsentlige afvigelser konstateret.

Sikkerhed i udviklings- og hjælpeprocesser **Kontrolmål: Formålet er at sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingscyklus.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
14.2	Udvikling af Forsyning|FOF, sker primært af DFF|EDB's egen udviklingsafdeling. DFF|EDB har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder og tilrettelagt hensigtsmæssigt i forhold til interne forhold. Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer.	Vi har forespurgt til politik for styring af udvikling, og vi har inspiceret politikken. Vi har forespurgt til procedure for styring af systemændringer, og vi har inspiceret proceduren. Vi har forespurgt til test af applikationer i forbindelse med ændringer og opdatering af driftsplatformen, og vi har inspiceret dokumentation for test. Vi har forespurgt til begrænsning af ændringer på softwarepakker, og vi har inspiceret dokumentation for prioritering af ændringer på software. Vi har forespurgt til principper for sikker udvikling, og vi har inspiceret udarbejdede principper. Vi har forespurgt til sikkert udviklingsmiljø, og vi har inspiceret dokumentation for adskillelse mellem udviklingsmiljø og produktionsmiljø. Vi har forespurgt til systemsikkerhedstest, og vi har stikprøvevis inspiceret dokumentation for systemsikkerhedstest. Vi har forespurgt til systemgodkendelsestest, og vi har stikprøvevis inspiceret dokumentation for systemaccept i forbindelse med udvikling.	Vi har observeret, at virksomheden ikke har dokumenteret udvalgte aktiviteter omkring ændringshåndtering i applikationen Forsyning|FOF. Vi har fået oplyst, at DFF|EDB i Q3 2018 har etableret en plan for udbedring af forholdet. Ingen væsentlige afvigelser konstateret i øvrigt.

Testdata **Kontrolmål: Formålet er at sikre beskyttelse af data, som anvendes til test.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
14.3	Der foreligger en proces beskrivelse for brug af testdata, således at data bliver anonymiseret og ikke er personhenførbare.	Vi har forespurgt til anvendelse af testdata, og vi har inspiceret retningslinjerne for produktion af testdata.	Vi har fået oplyst, at der anvendes testdata fra produktionsdatabasen i forbindelse med fejlsøgning og test på de pågældende værkers data. I disse tilfælde foreligger værkernes data til tider på lokale maskiner, og der er dermed ikke kontrol med, at testdata bliver slettet. Ingen væsentlige afvigelser konstateret i øvrigt.

Leverandørforhold

Informationssikkerhed i leverandørforhold **Kontrolmål: Formålet er at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
15.1	DFF|EDB har delvist uddelegeret driften for Hosting miljøet til Zitcom. DFF|EDB har selv driftsansvaret for eget server miljø hos DFF|EDB.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret aftalen med henblik på at efterse hensyntagen til informationssikkerhed. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere, om der er væsentlige bemærkninger, og om den er dækkende i forhold til virksomhedens aftale med leverandøren.	Ingen væsentlige afvigelser konstateret.

Styring af leverandørydelser **Kontrolmål: Formålet er at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
15.2	Anvendelsen af ekstern databehandler skal ske med respekt for gældende ret. Sikkerhedsregler skal i hvert enkelt tilfælde aftales med eksterne serviceleverandører. I forhold til leverandører og samarbejdspartnere, skal der i databehandleraftaler og andre kontrakter fremgå krav til tavshedserklæringer. Der skal under samarbejde med serviceleverandører ske kontrol med overholdelse af gældende aftaler.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører.	Ingen væsentlige afvigelser konstateret.

Styring af informationssikkerhedsbrud

Styring af informationssikkerhedsbrud og forbedringer

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
16.1	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.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden inspiceret procedure til håndtering af informationssikkerhedshændelser. Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne. Vi har forespurgt til informationssikkerhedshændelser i perioden. Vi har forespurgt til procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren.	Ingen væsentlige afvigelser konstateret.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Informationssikkerhedskontinuitet

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
17.1	Katastrofer forsøges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. DFF|EDB har implementeret formelle nødplaner, og procedurer til beredskab.	Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen. Vi har forespurgt til implementering af kompenserende tiltag i forbindelse med test af beredskabsplan, og vi har inspiceret dokumentation for implementeringen. Vi har forespurgt til test af beredskabsplanen. Vi har endvidere forespurgt til revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurdering.	Vi har fået oplyst, at virksomhedens beredskabsplan ikke har været testet i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.

Redundans **Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
17.2	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 imod sikringsomkostninger. DFF|EDB har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Gennemgang af informationssikkerheden **Kontrolmål: Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.**			
Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
18.2	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.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer, og vi har inspiceret udvalgte kontroller. Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning.	Vi har observeret, at der er implementeret kontroller til sikring af, at procedurerne er fulgt, men der er ikke dokumentation for udført arbejde i forbindelse med kontrollerne. Ingen væsentlige afvigelser konstateret i øvrigt.

FOF - TestComplete

A1 Opsætning og login

Det primære formål med denne kontrol er at validere anvendelsen af en test-database og mulighed for at logge ind med DFF Bruger og ADM bruger.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
01	Formålet med dette test run er at indsætte en ren test database, som andre test runs kan køre videre på. Hele kørslen genopretter databasen og giver mulighed for at logge ind med DFF Bruger og ADM bruger.	Vi har forespurgt til verificering af korrekt opsat test-database, og vi har stikprøvevis inspiceret dokumentation for test af den opsatte database. Vi har forespurgt til validering af forskel på rettighed for DFF bruger og ADM bruger, og vi har inspiceret dokumentation for differentiering i rettigheder.	Ingen væsentlige afvigelser konstateret.

A2 Login-procedure

Det primære formål med denne kontrol er at validere login-proceduren for forskellige brugere og kørsel af scripts.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
01	Opgave for denne test run er at teste login proceduren, både med DFF bruger, en almindelig bruger, ved flere brugere logins, og når der skal køres opgraderingsscripts.	Vi har forespurgt til validering af forskel på rettighed for DFF-bruger og ADM-bruger, og vi har inspiceret dokumentation for differentiering af rettigheder.	Ingen væsentlige 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'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 i finanskladden, 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 bogførte linjer tilfalder korrekte tabeller, og vi har stikprøvevis inspiceret kontrollerne.	Ingen væsentlige afvigelser konstateret.

A5 Acontokladde

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
01	Dette testrun gennemgår funktionaliteten af Acontokladden. 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 acontokladden. 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 væsentlige afvigelser konstateret.

A6 Flytteprocedure

Det primære formål med denne kontrol er at validere, at registreringer af flytteoplysninger registreres korrekt.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
01	Dette testrun har til opgave at gennemløbe Flyttewizarden med udgangspunkt i kvikflyt. Wizarden bliver gennemløbet med forskellige forbrugere, der alle har forskellige forudsætninger i forhold til aflæsninger, opgørelser med videre. Nogle testcases har et navn, der slutter på et forbrugernummer. Forbrugernummeret identificerer sig med en kolonne i det tilknyttede Excel ark; dette ark beskriver, hvilke specielle forløb der bliver testet af den konkrete testcase.	Vi har forespurgt til kontroller for, at flyttewizard medtager informationer, der indtastes, og vi har stikprøvevis inspiceret kontroller for, at data registreres korrekt i tabellerne.	Ingen væsentlige afvigelser konstateret.

A7 Betalingsfil til NETS

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

Nr.	DFF|EDB'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 stikprøvevis inspiceret kontroller for, at filerne indeholder korrekte informationer.	Ingen væsentlige afvigelser konstateret.

A8 OIOUBL og OIOXML til NemHandel

Det primære formål med denne kontrol er at validere, at uddatering af Nemhandel-filer valideres.

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
01	Dette testrun kører på genereringen af NemHandelsdokumenter. Der lægges vægt på det, der er specielt for NemHandelsdokumenter, 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 stikprøvevis inspiceret kontroller for, at filerne indeholder korrekte informationer.	Ingen væsentlige afvigelser konstateret.

A9 Fakturaflow

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

Nr.	DFF|EDB's kontrol	REVI-IT's test	Resultat af test
01	Denne testcase gennemløber mulighederne i Fakturaflow og sikrer at bruger-begrænsninger, 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 udvalgte kontroller. Vi har forespurgt til kontroller til sikring af, at der er differentiering af rettigheder, og vi har stikprøvevis inspiceret kontrollerne. Vi har forespurgt til kontroller til sikring af, at indtastede data er korrekt på faktura, og vi har stikprøvevis inspiceret kontrollerne. Vi har forespurgt til kontroller for validering ved inddatering af OIO filer, og vi har stikprøvevis inspiceret kontrollerne.	Ingen væsentlige afvigelser konstateret.

B10 Tilbudskladde

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

Nr.	DFF|EDB'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 stikprøvevis inspiceret kontrollerne. Vi har forespurgt til validering af uddatering i forbindelse med udskrift af tilbud, og vi har stikprøvevis inspiceret kontrollerne.	Ingen væsentlige 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'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 stikprøvevis inspiceret kontroller for validering af data, der indlæses og udlæses fra App-serveren.	Ingen væsentlige afvigelser konstateret.

B12 Restancekladde

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

Nr.	DFF|EDB'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 acontoposter 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 stikprøvevis inspiceret kontrollerne. Vi har forespurgt til kontroller til sikring af, at restancer opdateres i forbindelse med genberegning, og vi har stikprøvevis inspiceret de implementerede kontroller. Vi har forespurgt til kontroller til sikring af, at der bogføres på den korrekte bruger, og vi har stikprøvevis inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

B14 Aflæsningskladde

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

Nr.	DFF|EDB'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 stikprøvevis inspiceret kontrollerne. Vi har forespurgt til kontroller til sikring af, at aflæsninger kun inddateres én gang, og vi har stikprøvevis inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

B15 Beregn faktura

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

Nr.	DFF|EDB'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 stikprøvevis inspiceret kontrollerne.	Ingen væsentlige afvigelser konstateret.

B17 Målerskifte

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

Nr.	DFF|EDB'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 stikprøvevis inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

B18 Brugeroprettelse

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

Nr.	DFF|EDB'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. Vi har forespurgt til kontroller til sikring af, at forbrugeroplysninger registreres korrekt.	Vi har observeret, at dokumentationen for de definerede tests ikke er i overensstemmelse med de udførte tests. Vi har endvidere observeret, at testgrundlaget ikke indeholder validering af forsyningsformer registreret på den enkelte forbruger. Vi har yderligere observeret, at testen af registrerede forsyningsformer for den enkelte forbruger ikke er i overensstemmelse med de definerede parametre for udførsel af testen. Ingen væsentlige observationer konstateret i øvrigt.