Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med deres hostingydelse hos Zitcom A/S pr. 23. juni 2017

ISAE 3402-I

DFF|EDB a.m.b.a.

CVR-nr.: 26 22 40 20

Juni 2017

Indholdsfortegnelse

Afsnit 1: 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 hostingydelse hos Zitcom A/S, 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 2, giver en retvisende beskrivelse af DFF|EDB a.m.b.a.s hostingydelse hos Zitcom A/S til kunder pr. 23-06-2017. 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 implementeret 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 behandlingen og rapporteringen af kunders transaktioner.

(ii) 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 implementerede effektivt pr. 23-06-2017. 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.

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 2017.

Kolding, 23. juni 2017

DFF|EDB a.m.b.a.

Jan Elmstrøm Blaabjerg
Adm. direktør

Afsnit 2: DFF|EDB a.m.b.a.s beskrivelse af kontroller i forbindelse med drift af deres hostingydelser hos Zitcom A/S

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 27001. 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 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 27001.

Bemærk at dokumentation i ISO 27001 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 vedligeholdelsen af hostingmiljøet 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 årligt i april måned, 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.

Udviklingschefen og den IT ansvarlige har det overordnet ansvar for implementering af korrigerende handlinger for at minimere de identificerede risici.

5 - Sikkerhedspolitik

IT-Sikkerhedspolitikken gennemgås en gang årligt i april måned. Denne gennemgang ligger som en fast opgave i Outlook hos udviklingschefen og den IT ansvarlige.

6 - Organisering af informationssikkerhed

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

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 Citrix, 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 i Teknisk Afdeling og udviklingsafdelingen, der i samarbejde har adgang til at lave ændringer i Hosting miljøet, der kan påvirke driftsstabiliteten.

Kunder har kun kan adgang til egne data og denne adgang er for at sikre mod eksterne kilder sikret ved at brugerne anvender brugernavn og password. Al adgang til data sker desuden via en SSL eller VPN forbindelse.

7 - Sikkerhed i forhold til HR

Eksterne konsulenter skal underskrive en fortrolighedserklæring inden de får adgang til Hosting miljøet. DFF|EDB anvender kun konsulenter fra veletablerede firmaer, der har en høj standard, og hvor velbeskrevne it-sikkerheds procedurer er en del af deres standard aftale.

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 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.

Al kildekode og programmer, der udvikles, ejes af DFF|EDB, og må ikke kopieres eller overdrages til 3. part.

9 – 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 kunder 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 tre 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.

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

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

10 - 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.

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 metal gitter. 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.

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. Der er også ændringsstyring på hosting miljøet, sådan eventuelle fejl i opdateringer kan løses med det samme.

Aktiv overvågning sikrer kapacitetsstyring i Hosting miljøet.

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 DFF|EDB logger alt netværkstrafik.

Der tages daglig backup af alle data i Hosting miljøet og hver nat føres en fuld kopi af data fra DFF|EDB Hosting til en sikret sekundær lokation.

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 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.

Alle systemgrupper kører på deres eget VLAN. Opdelingen er beskrevet i systemdokumentationen.

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.

14 - Anskaffelse, udvikling og vedligeholdelse

Eneste system i DFF|EDB's eget Hosting miljøet, er Citrix platformen. Citrix platformen består af 100 % ens virtuelle servere. DFF|EDB bruger derfor ikke yderligere validering ved udvidelser, da der blot er tale om endnu en identisk virtuel server.

Udvikling af applikationer til Hosting miljøet sker primært i DFF|EDB's egen udviklingsafdeling.

15 - Leverandørforhold

Der er fortrolighedserklæringer med alle konsulenter der får adgang til systemet. Som udgangspunkt arbejder de udelukkende med hardware og software problemstillinger og har ikke adgang til data.

DFF|EDB anvender kun konsulenter fra veletablerede firmaer, der har en høj standard og hvor velbeskrevne it-sikkerheds procedurer er en del af deres standard aftale.

DFF|EDB har delvist uddelegeret driften for Hosting miljøet til Zitcom. DFF|EDB har selv driftsansvaret for Citrix miljøet, som forventes udfases efteråret 2017, hvorefter Zitcom står for alt driften af RDS miljøet.

16 - Styring af sikkerhedshændelser

DFF|EDB har klare procedurer for alle sikkerhedshændelser.

Alle hændelser bliver registret og løst uden ophold. Det er den IT ansvarlige der har det overordnede ansvar for processen.

17 - Informationssikkerhedsaspekter ved beredskabsstyring

Katastrofer søges 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 i mod 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 Zitcom 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 det nye EU direktiv (generel forordning om databeskyttelse) medfører behov for at revurdere nogle af selskabets procedurer og retningslinjer for opbevaring af data. Der pågår pt. et internt afklaringsarbejde i den anledning.

En gang årligt gennemgås den gældende sikkerhedspolitik af udviklingschefen og den IT ansvarlige, samt ved større ændringer i organisationen eller hosting miljøet.

Det er udviklingschefen og den IT ansvarlige, der har det overordnede ansvar for IT sikkerhedspolitikken.

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

Komplementerende kontroller

DFF|EDB's kunder er, medmindre andet er aftalt, ansvarlige for at etablere og vedligeholde internetforbindelse til DFF|EDB's servere. Herudover er DFF|EDB's kunder, medmindre andet er aftalt, ansvarlige for:

- At det aftalte niveau for backup dækker kundens behov
- Periodisk gennemgang af kundens egne brugere og meddele lukning af bruger
- At kundes brugere ikke lagrer ulovligt materiale på DFF|EDB's servere.

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

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

Omfang

Vi har fået til opgave at afgive erklæring om DFF|EDB a.m.b.a.s beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af DFF|EDB a.m.b.a.s ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hostingydelser hos Zitcom A/S pr. 23-06-2017, 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 a.m.b.a.s ansvar

DFF|EDB a.m.b.a. 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 a.m.b.a. 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 a.m.b.a.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 a.m.b.a.s beskrivelse i afsnit 2 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder, der anvender DFF|EDB a.m.b.a.s hostingydelse hos Zitcom A/S, 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 a.m.b.a.s beskrivelse i afsnit 2 og det er på den baggrund vores vurdering,

(a) at beskrivelsen af kontroller, således som de var udformet og implementeret pr. 23-06-2017, 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 udformet pr. 23-06-2017.

Fremhævelse af forhold i erklæringen

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt DFF|EDB a.m.b.a.s hostingydelser hos Zitcom A/S, 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, 23. juni 2017

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

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