Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med hostingydelser i perioden 01-02-2017 til 31-01-2018

ISAE 3402-II

TechBiz ApS

CVR-nr.: 27 57 79 38

Marts 2018

Indholdsfortegnelse

Afsnit 1: TechBiz ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt TechBiz ApS' hostingydelser, 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. TechBiz ApS bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af TechBiz ApS' hostingydelser til kunder i hele perioden fra 01-02-2017 til 31-01-2018. 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 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) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 01-02-2017 til 31-01-2018

(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 01-02-2017 til 31-01-2018. Kriterierne for denne udtalelse var, at:

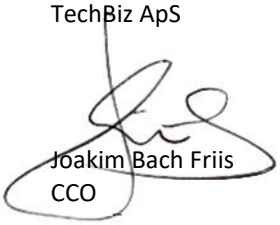
(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificerede

(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 01-02-2017 til 31-01-2018.

København, 23. marts 2018

TechBiz ApS



Joakim Bach Friis
CCO

Nikolaj Friis Krøyer
CTO

Afsnit 2: TechBiz ApS' beskrivelse af kontroller i forbindelse med drift af deres hostingydelser

Indledning

Denne beskrivelse er udarbejdet med henblik på at give oplysninger til kunder i TechBiz og deres revisorer. Beskrivelsen indeholder oplysninger om kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402.

TechBiz serviceydelser

TechBiz har arbejdet med IT drift og support siden 2000. Fokus har altid været at levere konkurrencedygtige IT-løsninger med udgangspunkt i kundens behov og med fokus på en høj oplevet værdi. TechBiz er en velkonsolideret virksomhed, hvor flere kunder, har været med helt fra begyndelsen.

TechBiz leverer følgende Hosting- og datacenter ydelser:

- Hostede Virtuelle Servere
- Hostede Dedikerede Servere
- Remote Backup

Denne kontrolbeskrivelse omhandler de ovenstående serviceydelser.

I relation hertil tilbyder TechBiz blandt andet også assistance indenfor følgende områder:

- IT-konsulentbistand indenfor IT-infrastruktur generelt
- IT-chef opgaver
- Drift af lokale servere og netværk hos kunder

Risikovurdering og håndtering

I TechBiz forstår vi, at der er en risiko ved alle ændringer i og omkring vores datacentre. Derfor opvejes altid den potentielle skade en opgave kan forsage, og sandsynligheden for at skaden indtræffer. Vurderes skaden og sandsynligheden for skaden at være høj, har vi procedurer, der sikrer, at der udvides ekstra opmærksomhed omkring sådanne opgaver.

Ud fra samme model udarbejdes løbende og som minimum årligt en samlet risikovurdering af mulige trusler i og omkring TechBiz. Ansvaret for risikovurdering ligger hos ledelsen.

Sikkerhedspolitik

Vi har defineret vores overordnede metodik og tilgang til levering af vores ydelser med hvad det indebærer, i vores it-sikkerhedspolitik og tilhørende strategiske og taktiske dokumenter.

Formålet er at sikre, at vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til forretningsstrategien – og i forhold til relevant lovgivning.

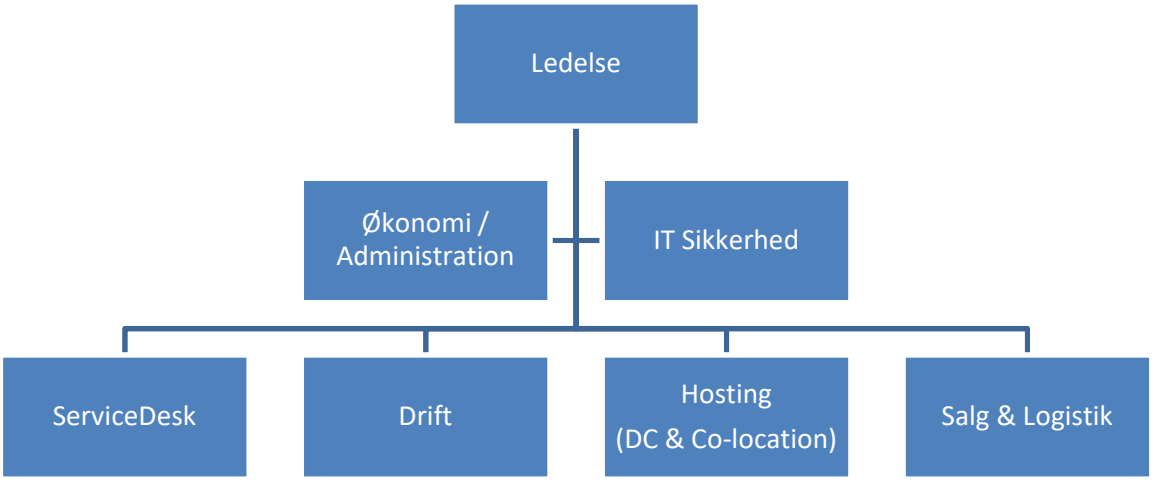
TechBiz sikkerhedspolitik skal sikre at medarbejdere i TechBiz forstår deres daglige IT-ansvarsområde og de trusler, der kan ramme TechBiz og kunder.

TechBiz tager omkring IT sikkerhedspolitikken udgangspunkt i ISO27002 (Regelsæt for styring af informationssikkerhed) og punkterne heri.

TechBiz evaluerer IT sikkerhedspolitikken minimum en gang årligt i forbindelse med IT-revision.

Organisering af informationssikkerhed

Ansvar og organisering af Informationssikkerhed fremgår af nedenstående organisationsdiagram:



Alle IT-konsulenter i TechBiz deltager i den daglige drift af TechBiz IT-løsninger. Dette sikrer at TechBiz kan reagere hurtigt på kritiske hændelser, og at alle IT-konsulenter kan bidrage til løsninger på daglige opgaver. Ligeledes skaber det en stærk forankring omkring drift og løsninger i TechBiz datacentre.

Ud fra forståelsen af at alle ændringer udgør en risiko, er der ingen medarbejdere, der udfører kritiske opgaver alene. TechBiz procedurer og ændringsstyringer sikrer, at der er klare aftaler og kontrol omkring alle kritiske opgaver.

Ligeledes holder TechBiz sig løbende orienteret fra blogs, sikkerhedsorganisationer, pressen og andre relevante feeds i forhold til nye trusler.

Informationssikkerhed som en del af projektstyring

Ved større implementeringsprojekter, nedsættes relevante teams, og foregår projekterne over længere perioder benyttes internt projektstyringsværktøj til sikring af overholdelse af deadlines og opgaver.

Mobilt udstyr og fjernarbejdspladser

Alle IT-konsulenter i TechBiz har minimum en bærbar og en mobil telefon.

Mobiltelefonerne indeholder ikke kompromitterende indhold andet end Medarbejderens TechBiz-mail. Mobiltelefonen er sikret med en adgangskode, og kan fjernslettes.

Det er ikke tilladt at gemme kompromitterende data på bærbare computere.

Jf. TechBiz Personalehåndbog skal alle medarbejdere sikre bærbare computere med adgangskode og kryptering.

TechBiz medarbejdere kan koble på interne systemer, når de ikke er på kontoret via Remote Desktop og VPN, der begge er sikret med Multi-Factor Authentication (MFA).

Medarbejdersikkerhed

Nyansættelser foretages både på egen hånd og i samarbejde med rekrutteringsbureauer. Ud over personernes tekniske kundskaber, vurderes endvidere personens serviceniveau, integritet og pålidelighed. Personens CV-gennemgås i detaljer og eventuelle referencer kontaktes.

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i enhver medarbejders ansættelseskontrakt.

Under ansættelse

Medarbejderes kundskaber vurderes løbende i forhold til deres respektive ansvarsområder og opgaver. Uddannelse tilbydes jf. beskrivelsen i TechBiz Personalehåndbog.

I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. Heri er den pågældendes stillingsbeskrivelse ligeledes klart defineret.

På ugentlige møder samles der op på den forgangene uge samt nyt tiltag eller vigtige sikkerhedsemner.

Ophør og ændring i ansættelse

Når en medarbejder stopper i TechBiz bliver alle redskaber, herunder mobil og bærbar returneret til TechBiz og alle adgange til TechBiz og eventuelle kundesystemer, bliver lukket ned. En overleveringssamtale sikrer at al nødvendig viden, som den pågældende måtte ligge inde med, bliver videregivet og dokumenteret.

Medarbejdere er underlagt deres tavshedspligt også efter ophør af deres ansættelseskontrakt.

Styring af aktiver

Vores netværk er komplekst med mange systemer og kunder, og for at sikre mod uvedkommendes adgang, og for at sikre gennemskuelighed, har vi udformet en række dokumentationer, der beskriver det interne netværk med enheder, navngivning af enheder, logisk opdeling af netværk mv.

Dokumenterne, netværkstypologier og lign. opdateres løbende ved ændringer og gennemgås minimum årligt. Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt for uvedkommende.

Når en medarbejder stopper i TechBiz afholdes et debriefing møde, hvor aktive sager gennemgås og viden overleveres. Medarbejderen skriver under på at de har afleveret alt udstyr tilhørende TechBiz eller dennes kunder og samarbejdspartnere.

Adgangskontrol

Vi har politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik.

Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores egne brugere oprettes alene på baggrund af skriftligt autorisation fra systemejer.

Ved fratrædelse sikrer vores procedurer aflevering af materiale og lukning af medarbejderens konti.

Adgang til systemer og data fjernes alene på baggrund af skriftligt ønske fra kunde, system- eller dataejer.

Alle brugere skal være personhenførbare, dvs. have tydeligt mærke med personnavn.

Vores it-sikkerhedspolitik foreskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.

Medarbejdere skriver årligt under på, at de har læst og forstået seneste version af vores it-sikkerhedspolitik.

Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen. Vores kunders brugeradgange til kundens systemer og data, bestemmes af vores kunder.

Passwords til TechBiz' interne servere skal som minimum skiftes hver 90 dag, minimum være på 7 karakterer og Complexity Requirements i Windows Server skal være slået til.

Kryptografi

Vi har en formel politik for anvendelse af kryptografi til beskyttelse af data og forbindelser, samt administrering af krypteringsnøgler. Vi foretager kryptering i den grad det giver mening i forhold til den pågældende tjeneste og/eller enhed. Beslutningen træffes af den øverste ledelse.

Alle computere i TechBiz skal være krypteret med enten Microsoft BitLocker eller MacOS FileVault. Det er medarbejderens ansvar at sørge for at IT-udstyr er krypteret, og således også at spørge om hjælp, hvis der er behov for dette.

Eksterne kommunikationsforbindelser skal sikres med krypterede VPN-forbindelser for at sikre at uvedkommende ikke gennem disse forbindelser får adgang til data.

Fysiske og miljømæssige sikringer

TechBiz´ udstyr er placeret i datacentre hos GlobalConnect og Nianet. Faciliteterne er sikret efter højeste standarder og lever op til de høje internationale standarder, der ligger i en ISAE 3402-godkendelse, herunder:

- Redundant dieselgenerator som slår til i tilfælde af strømafbrydelse
- Brandsikring (aspirationsanlæg og Inergen/Argonite)
- Redundant køleanlæg
- UPS'er som sikrer stabilitet i strømmen
- Faciliteterne overvåges af en lang række tekniske alarmer og censorer
- Adgangskontrol (personlige adgangskort, fingerscanner, kode)
- Videoovervågning

Alene autoriserede personer får adgang til datacentrene via den etablerede procedure. Vi følger periodisk, minimum årligt, op på hvilke personer, der har denne adgang. Skal eksterne personer (leverandører eller kunder) have adgang til datacentrene, er det i følgeskab med en af vores autoriserede medarbejdere.

Alle vores lokaler er monteret med tyverialarm, i tilfælde af indbrud alarmeres den private vagtcentral, og relevante personer hos TechBiz alarmeres via telefonopkald.

TechBiz udstyr er sikret i mindre celler, og står i aflåste rackskabe. Kun autoriserede personer har adgang til TechBiz udstyr.

Foruden den almindelige overvågning og alarmering af uregelmæssigheder i datacentrene tilses TechBiz udstyr løbende af TechBiz egne ansatte.

Sikkerhed i forbindelse med drift

Ændringsstyring

Alle ændringer udgør en risiko. TechBiz vurderer derfor, hvad der kan gå galt ved implementering af en ændring og hvad sandsynligheden er for at det vil ske.

TechBiz foretager løbende risikovurderinger af de ydelser TechBiz leverer. Derudover foretages kontrol af alle ændringer jf. TechBiz Change Management politik.

Formålet med TechBiz Change Management politik er at kontrollere og sikre at ændringer foretages med et minimum af afbrydelser i driften.

TechBiz Change Management politik gør TechBiz i stand til at følge ændringer, godkendelser og eventuelle problemer og hændelser i forbindelse med implementerede ændringer.

Ændringer skal godkendes af et Change Advisory Board, der varierer alt efter hvilken ændring, der forespørges på.

Kapacitetsstyring

Kapaciteten i TechBiz datacentre udvides løbende efterhånden, som eksisterende kunders behov stiger og nye kunder kommer til. Således foretages løbende gennemgang af kapacitet og optimeringsmuligheder af konsulent-teamet samtidig med at TechBiz interne overvågningssystem advarer om grænseværdier, der er ved at blive overskredet.

Adskillelse af miljøer

TechBiz datacentre er at betragte som en intern kunde hos TechBiz. De forskellige systemer i TechBiz datacentre er logisk adskilt på Domæne niveau, hvilket betyder, at de er at betragte som logiske enheder med de nødvendige adgangskontroller. Det er kun autoriseret personale der kan tilgå de relevante miljøer.

Malware

TechBiz har implementeret flere sikkerhedsforanstaltninger for at undgå Malware på vores datacentre. Der er redundante firewalls, som har til hensigt at beskytte mod udefrakommende trusler og antivirus er installeret på alle relevante servere.

TechBiz overvåger systemerne igennem overvågningssystemer, som kan rapportere om fejl og uregelmæssigheder.

Backup

TechBiz opererer med flere typer af backup rettet mod vores egne og kunders systemer.

TechBiz har lavet flere foranstaltninger som har til formål at kunne levere høj driftsstabilitet og sikre vores kunders og egne data bedst muligt.

TechBiz cluster sikrer at kundernes VMer kan flyde over flere fysiske servere og storagelag.

Backup af VMer i TechBiz cluster er inkluderet i alle hosted VM-aftaler.

Backuppen bliver monitoreret igennem TechBiz overvågningssystem, som realtime sikrer, at TechBiz er orienteret omkring helbredet på backupserverne.

Restoretests foretages flere gang årligt, herunder verificering af backup-data.

Vedligeholdelse af backup-systemerne fortages indenfor normal arbejdstid, og har ingen indflydelse på backuppen, da denne kører om natten/aftenen.

Logning og overvågning

Overvågning og logning af netværkstrafik, logs og serverperformance, følges løbende af TechBiz konsulentteam. Mistænkelig adfærd efterforskes altid og eventuelle tilpassede overvågningsscripts og -metoder udarbejdes efter behov og alt efter hændelsestype.

Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident og problem management procedurer til sikring af, at hændelser registreres, prioriteres, styres, eskaleres og at der foretages de nødvendige handlinger.

Sikkerhedslogs opbevares på særskilt syslog server for ekstra sikkerhed.

Styring af software på driftssystemer

Installation af software fortages kun af TechBiz konsulenter med de fornødne rettigheder til det pågældende system.

Kundespecifikke programmer som ønskes afviklet fra TechBiz datacentre bliver evalueret i forhold til TechBiz Sikkerhedspolitik.

Opdatering af software herunder sikkerhedsopdateringer, foretages efter instrukser fra system-ejer og af CTO i tilfælde af opdatering af host-systemer.

Styring af tekniske sårbarheder

TechBiz holder sig opdateret omkring sårbarheder via fora, nyhedsbreve og WSUS. Eventuelle risici bliver omdelt i organisationen på den til enhver lejlighed hurtigste facon (mobil, SMS, opkald, e-mail mv.) og nødvendige tiltag foretages rettidigt.

Kommunikationssikkerhed

TechBiz datacentre er opbygget med redundante switche og firewalls. Endvidere benyttes VLANs for at sikre adskillelse af netværk og servere. Servere og hosts kan tilgås gennem lukkede VPN-forbindelser eller kundetilpassede fjernskrivebord. Forbindelser og adgang kan endvidere sikres med 3-faktor login samt SSL.

Sikkerhedshændelser

Vores IT Service Management system, hvori vi håndterer langt de fleste sager for kunder og interne forhold, er samtidig vores system til håndtering af sikkerhedshændelser. Heri kan vi eskalere forhold således, at nogle opgaver får højere prioritet end andre. Sikkerhedshændelser bliver kommunikeret til hele virksomheden, således at alle kan samarbejde om løsning af hændelsen og arbejde ud fra et informeret niveau. TechBiz har procedurer for, hvordan vi vurderer og reagerer på sikkerhedshændelser.

Leverandørforhold

Eksterne partnere, der skal have adgang til TechBiz´ interne systemer gives kun til lukkede miljøer eller under overvågede forhold. Eksterne partnere, der skal have adgang til kunde-systemer, der ligger under TechBiz ansvar gives kun efter aftale med kunden.

Beredskabsstyring

TechBiz har beredskabsplaner til gendannelse af TechBiz datacentre i forbindelse med katastrofer og/eller større nedbrud. Disse planer vedligeholdes, efterprøves og tilpasses løbende efterhånden som TechBiz datacentre vokser. Metoderne og systemerne, med hvilke backup og restore foretages, evalueres løbende og minimum årligt i forbindelse med gennemgang af TechBiz sikkerhedspolitik.

En del af beredskabsplanerne i TechBiz er sikring af redundans og således muligheden for at "fejle-over" på et tilsvarende system og dermed undgår nedetid for TechBiz og TechBiz´ kunder.

Kommunikation omkring nedbrud foretages som minimum på TechBiz hjemmeside forbeholdt driftsstatus, http://www.techbiz.dk/status-side/. Derudover kommunikeres til eventuelt berørte kunder, efter kundespecifikke aftaler.

TechBiz beredskabsstyring er konstrueret omkring en overordnet beredskabsplan for TechBiz datacentre. Der kan udarbejdes individuelle og kundespecifikke beredskabsplaner efter behov og ønsker fra kunden.

Overensstemmelse

TechBiz IT-politikker og kontrolbeskrivelser revideres en gang årligt af ekstern certificeret IT-revisor.

Ændringer i perioden

Gennem perioden 01-02-2017 til 31.01.2018 er der sket følgende væsentlige ændringer:

- Vi har udbygget og optimeret vores sikkerhedspolitik
- Vi har forbedret vores håndtering og styring af incidents og changes
- Vi har tilføjet flere ressourcer til daglig drift
- Vi har optimeret dokumentations- og event procedurer
- Vi har investeret i nyt udstyr og udbygget datacentrene

Komplementerende kontroller hos kunderne

Ovenstående kontrolbeskrivelse tager udgangspunkt i de overordnede rammer i TechBiz, og der er således ikke taget højde for kundespecifikke forhold.

- Ansvaret for de forretningssystemer, som drives fra TechBiz datacentre, er kundernes eget ansvar. Kunderne har ansvaret for at de nødvendige kontroller i forbindelse med f.eks. systemudvikling, anskaffelse og ændringshåndering.
- TechBiz er ikke ansvarlig for tildeling, ændring og nedlæggelse af adgangsrettigheder for den enkelte kundes brugere. TechBiz kan være behjælpelig med udførelse af opgaven, men kunden er selv forpligtet til at sikre de nødvendige kontroller forbundet hermed.
- Det er kundens eget ansvar at sikre dataforbindelse til TechBiz datacentre og sikre de relevante kontrolmål.

TechBiz vil i langt de fleste tilfælde kunne varetage eller være behjælpelig med ovenstående ansvarsområder og kontrolpunkter, men der skal i så fald foreligge en kundespecifik aftale herpå.

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

Til ledelsen hos TechBiz ApS, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om TechBiz ApS' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af TechBiz ApS' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hostingydelser i perioden 01-02-2017 til 31-01-2018, 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.

TechBiz ApS' ansvar

TechBiz ApS er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. TechBiz ApS 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 TechBiz ApS' 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 udformet 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 præ-

sentation 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

TechBiz ApS' 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 TechBiz ApS' 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 01-02-2017 til 31-01-2018, 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 01-02-2017 til 31-01-2018
(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 01-02-2017 til 31-01-2018.

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 TechBiz ApS' hostingydelser, 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. marts 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 TechBiz ApS 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 01-02-2017 til 31-01-2018.

Vi har således ikke nødvendigvis testet alle de kontroller, som TechBiz ApS har nævnt i sin beskrivelse i afsnit 2.

Kontroller, udført hos TechBiz ApS' 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 TechBiz ApS 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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
4.1	Der udarbejdes løbende og som minimum årligt en samlet risikovurdering af mulige trusler i og omkring TechBiz. Ansvaret for risikovurdering ligger hos ledelsen.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af it-risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået og godkendt af ledelsen i revisionsperioden. Vi har forespurgt til kontrol for periodisk gennemgang af it-risikoanalysen, og vi har inspiceret kontrol for periodisk gennemgang af dokumentet.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
5.1	Vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til forretningsstrategien – og i forhold til relevant lovgivning. TechBiz tager omkring IT sikkerhedspolitikken udgangspunkt i ISO27002 (Regelsæt for styring af informationssikkerhed) og punkterne heri. TechBiz evaluerer IT sikkerhedspolitikken en gang årligt i forbindelse med IT-revision.	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.	Ingen væsentlige afvigelser konstateret.

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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
6.1	Alle IT-konsulenter i TechBiz deltager i den daglige drift af TechBiz IT-løsninger. Ud fra forståelsen af at alle ændringer udgør en risiko, er der ingen medarbejdere, der udfører kritiske opgaver alene. Ligeledes holder TechBiz sig løbende orienteret fra blogs, sikkerhedsorganisationer, pressen og andre relevante feeds i forhold til nye trusler. Ved større implementeringsprojekter, nedsættes relevante teams, og foregår projekterne over længere perioder benyttes internt projektstyringsværktøj til sikring af overholdelse af deadlines og opgaver.	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 procedure for styring af projekter, og vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter.	Ingen væsentlige afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser

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

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
6.2	Mobiltelefonerne indeholder ikke kompromitterende indhold andet end Medarbejderens TechBiz mail. Mobiltelefonen er sikret med en adgangskode, og kan fjernslettes. Det er ikke tilladt at gemme kompromitterende data på bærbare computere. Jf. TechBiz Personalehåndbog skal alle medarbejdere sikre bærbare computere med adgangskode og kryptering. TechBiz medarbejdere kan koble på interne systemer, når de ikke er på kontoret via Remote Desktop og VPN, der begge er sikret med Multi-Factor Authentication (MFA).	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.	Ingen væsentlige afvigelser konstateret.

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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
7.1	Nyansættelser foretages både på egen hånd og i samarbejde med rekrutteringsbureauer. Ud over personernes tekniske kundskaber, vurderes endvidere personens serviceniveau, integritet og pålidelighed. Personens CV-gennemgås i detaljer og eventuelle referencer kontaktes. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har 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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
7.2	Medarbejderes kundskaber vurderes løbende i forhold til deres respektive ansvarsområder og opgaver. Uddannelse tilbydes jf. beskrivelsen i TechBiz Personalehåndbog. I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. Heri er den pågældendes stillingsbeskrivelse ligeledes klart defineret. På ugentlige møder samles der op på den forgangene uge samt nyt tiltag eller vigtige sikkerhedsemner.	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, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring

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

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
7.3	Medarbejdere er underlagt tavshedspligt, også efter ophør af deres ansættelseskontrakt.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
8.1	Vi har udformet en række dokumentationer, der beskriver det interne netværk med enheder, navngivning af enheder, logisk opdeling af netværk mv. Dokumenterne, netværkstypologier og lign opdateres løbende ved ændringer og gennemgås minimum årligt.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har forespurgt til kontroller for opdatering over fortegnelser, og vi har stikprøvevis inspiceret de implementerede kontroller. Vi har forespurgt til oversigt af ejerskab for aktiver, og vi har inspiceret dokumentation for tildeling af ejerskab over aktiver. 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. Vi har stikprøvevis inspiceret dokumentation for, at proceduren er fulgt.	Ingen væsentlige afvigelser konstateret.

Klassifikation af information

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

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
8.2	Vi har udformet en række dokumentationer, der beskriver det interne netværk med enheder, navngivning af enheder, logisk opdeling af netværk mv. Dokumenterne, netværkstypologier og lign opdateres løbende ved ændringer og gennemgås minimum årligt.	Vi har forespurgt til politik for klassificering af data, og vi har inspiceret dokumentation for klassificering af data. Vi har forespurgt til 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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
8.3	Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt for uvedkommende.	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 retningslinjer for transport af bærbare medier, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring

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

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
9.1	Vi har politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik.	Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
9.2	Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores egne brugere oprettes alene på baggrund af skriftligt autorisation fra systemejer. Ved fratrædelse sikrer vores procedurer aflevering af materiale og lukning af medarbejderens konti. Adgang til systemer og data fjernes alene på baggrund af skriftligt ønske fra kunde, system- eller dataejer. Alle brugere skal være personhenførbare, dvs. have tydeligt mærke med personnavn.	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. Vi har forespurgt til proces for periodisk gennemgang af brugere, og vi har inspiceret dokumentation for seneste gennemgang.	Ingen væsentlige afvigelser konstateret.

Brugernes ansvar

Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
9.3	Vores it-sikkerhedspolitik foreskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
9.4	Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen. Vores kunders brugeradgange til kundens systemer og data, bestemmes af vores kunder. Passwords til TechBiz' interne servere skal som minimum skiftes hver 90 dag, minimum være på 7 karakterer og Complexity Requirements i Windows Server skal være slået til.	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, og 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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
10.1	Vi har en formel politik for anvendelse af kryptografi til beskyttelse af data og forbindelser, samt administrering af krypteringsnøgler. Vi foretager kryptering i den grad det giver mening i forhold til den pågældende tjeneste og/eller enhed. Beslutningen træffes af den øverste ledelse.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
11.1	Alene autoriserede personer får adgang til datacentrene via den etablerede procedure. Vi følger periodisk, minimum årligt, op på hvilke personer, der har denne adgang. Skal eksterne personer (leverandører eller kunder) have adgang til datacentrene, er det i følgeskab med en af vores autoriserede medarbejdere. Alle vores lokaler er monteret med tyverialarm, i tilfælde af indbrud alarmeres den private vagtcentral, og relevante personer hos TechBiz alarmeres via telefonopkald. TechBiz udstyr er sikret i mindre celler, og står i aflåste rackskabe. Kun autoriserede personer har adgang til TechBiz udstyr. Foruden den almindelige overvågning og alarmering af uregelmæssigheder i datacentrene tilses TechBiz udstyr løbende af TechBiz egne ansatte.	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 hos 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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
11.2	TechBiz' udstyr er placeret i datacentre hos GlobalConnect og Nianet. Faciliteterne er sikret efter højeste standarder og lever op til de høje internationale standarder, der ligger i en ISAE 3402-godkendelse, herunder: • Redundant dieselgenerator som slår til i tilfælde af strømafbrydelse • Brandsikring (aspirationsanlæg og Inergen/Argonite) • Redundant køleanlæg • UPS'er som sikrer stabilitet i strømmen • Faciliteterne overvåges af en lang række tekniske alarmer og censorer • Adgangskontrol (personlige adgangskort, fingerscanner, kode) • Videoovervågning	Vi har forespurgt til erklæringer fra underleverandører af fysiske forhold. Vi har inspiceret erklæringerne for betryggende fysisk sikring, og vi har observeret, at erklæringerne dækker perioden. Vi har inspiceret erklæringer fra underleverandører 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 periodisk eftersyn af eksterne lokationer, og har stikprøvevis inspiceret dokumentation for eftersyn. 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 observeret følgende i Nianets erklæring: - For 3 af de 15 udvalgte stikprøver var der ikke en testplan samt fallback-strategi i forbindelse med projektstyring. - Der er i revisionsperioden ikke gennemført en gennemgang af tildelte systemadgange og rettigheder. Ingen væsentlige afvigelser konstateret i øvrigt.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

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

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
12.1	TechBiz foretager løbende risikovurderinger af de ydelser TechBiz leverer. Derudover foretages kontrol af alle ændringer jf. TechBiz Change Management politik. TechBiz Change Management politik gør TechBiz i stand til at følge ændringer, godkendelser og eventuelle problemer og hændelser i forbindelse med implementerede ændringer. Ændringer skal godkendes af et Change Advisory Board, der varierer alt efter hvilken ændring, der forespørges på. Der foretages løbende gennemgang af kapacitet og optimeringsmuligheder af konsulentteamet samtidig med at TechBiz interne overvågningssystem advarer om grænseværdier, der er ved at blive overskredet. De forskellige systemer i TechBiz datacentre er logisk adskilt på Domæne niveau, hvilket betyder at de er at betragte som logiske enheder med de nødvendige adgangskontroller. Det er kun autoriseret personale der kan tilgå de relevante miljøer.	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 anvendelsen af testmiljø, og vi har inspiceret dokumentation for eksistens af testmiljø.	Ingen væsentlige afvigelser konstateret.

Malwarebeskyttelse

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

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
12.2	TechBiz har implementeret flere sikkerhedsforanstaltninger for at undgå Malware på vores datacentre. Der er redundante firewalls, som har til hensigt at beskytte mod udefrakommende trusler og antivirus er installeret på alle relevante servere. TechBiz overvåger systemerne igennem overvågningssystemer, som kan rapportere om fejl og uregelmæssigheder.	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen væsentlige afvigelser konstateret.

Backup **Kontrolmål: Formålet er at beskytte mod tab af data.**			
Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
12.3	TechBiz cluster sikrer at kundernes virtuelle maskiner (VM) kan flyde over flere fysiske servere og storagelag. Backup af VM 'er i TechBiz cluster er inkluderet i alle hosted VM-aftaler. Backuppen bliver monitoreret igennem TechBiz overvågningssystem, som realtime sikrer, at TechBiz er orienteret omkring helbredet på backupserverne. Restoretests foretages flere gang årligt, herunder verificering af backup-data. Vedligeholdelse af backupsystemerne fortages indenfor normal arbejdstid, og har ingen indflydelse på backuppen, da denne kører om natten/aftenen.	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 i øvrigt.
Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
12.4	Overvågning og logning af netværkstrafik, logs og serviceperformance følges løbende af TechBiz konsulentteam. Mistænkelig adfærd efterforskes altid og eventuelle tilpassede overvågningsscripts og -metoder udarbejdes efter behov og alt efter hændelsestype.	Vi har forespurgt til logning af brugeraktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger, og vi har inspiceret løsningen. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.
Styring af driftssoftware **Kontrolmål: Formålet er at sikre integriteten af driftssystemer.**			
Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
12.5	Installation af software fortages kun af TechBiz konsulenter med de fornødne rettigheder til det pågældende system. Kundespecifikke programmer som ønskes afviklet fra TechBiz datacentre bliver evalueret i forhold til TechBiz sikkerhedspolitik. Opdatering af software herunder sikkerhedsopdateringer, foretages efter instrukser fra system-ejer og CTO i tilfælde af opdatering af host-systemer.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
12.6	TechBiz holder sig opdateret omkring sårbarheder via fora, nyhedsbreve og WSUS. Eventuelle risici bliver omdelt i organisationen på den til enhver lejlighed hurtigste facon (mobil, SMS, opkald, e-mail mv.) og nødvendige tiltag foretages rettidigt.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
13.1	TechBiz datacentre er opbygget med redundante switche og firewalls. Endvidere benyttes VLANs for at sikre adskillelse af netværk og servere. Servere og hosts kan tilgås gennem lukkede VPN-forbindelser eller kundetilpassede fjernskrivebord. Forbindelser og adgang kan endvidere sikres med 3-faktor login samt SSL.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
13.2	Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.	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, og vi har inspiceret retningslinjerne. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen væsentlige afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold

Kontrolmål: Formålet er at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
15.1	Eksterne partnere, der skal have adgang til TechBiz´ interne systemer gives kun til lukkede miljøer eller under overvågede forhold. Eksterne partnere, der skal have adgang til kunde-systemer, der ligger under TechBiz ansvar gives kun efter aftale med kunden. TechBiz' udstyr er placeret i GlobalConnects datacentre. Faciliteterne er sikret efter højeste standarder og lever op til de høje internationale standarder, der ligger i en ISAE 3402-godkendelse.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
15.2	Foruden den almindelige overvågning og alarmering af uregelmæssigheder i datacentrene tilses TechBiz udstyr løbende af TechBiz egne ansatte.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
16.1	Sikkerhedshændelser bliver kommunikeret til hele virksomheden, således at alle kan samarbejde om løsning af hændelsen og arbejde ud fra et informeret niveau. TechBiz har procedurer for, hvordan vi vurderer og reagerer på sikkerhedshændelser.	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 procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren. Vi har forespurgt til informationssikkerhedshændelser i perioden, og vi har via stikprøve inspiceret, om procedurer ved informationssikkerhedshændelser er fulgt.	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.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
17.1	TechBiz har beredskabsplaner til gendannelse af TechBiz datacentre i forbindelse med katastrofer og/eller større nedbrud. Disse planer vedligeholdes, efterprøves og tilpasses løbende efterhånden som TechBiz datacentre vokser. Metoderne og systemerne, med hvilke backup og restore foretages, evalueres løbende og minimum årligt i forbindelse med gennemgang af TechBiz sikkerhedspolitik.	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 beredskabstest, og vi har inspiceret dokumentation for implementeringen. Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurdering.	Ingen væsentlige afvigelser konstateret.

Redundans **Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.**			
Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
17.2	En del af beredskabsplanerne i TechBiz er sikring af redundans og således muligheden for at "fejle-over" på et tilsvarende system og dermed undgå nedetid for Tech-Biz og TechBiz´ kunder.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Overensstemmelse

Gennemgang af informationssikkerheden **Kontrolmål: Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.**			
Nr.	TechBiz ApS' kontrol	REVI-IT's test	Resultat af test
18.2	TechBiz IT-politikker og kontrol-beskrivelser revideres en gang årligt af ekstern certificeret IT-revisor.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerheds-politik og procedurer, og vi har inspiceret udvalgte kontroller. Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning.	Ingen væsentlige afvigelser konstateret.