Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med salg og drift af hosting-platform i perioden 01-11-2017 til 31-10-2018

ISAE 3402-II

Zentura IT A/S

CVR-nr.: 32 89 08 06

November 2018

Indholdsfortegnelse

Afsnit 1: Zentura IT A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Zentura IT A/S' hostingplatform, 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. Zentura IT A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Zentura IT A/S' salg og drift af hosting-platform til kunder i hele perioden fra 01-11-2017 til 31-10-2018. 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 01-11-2017 til 31-10-2018

(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 01-11-2017 til 31-10-2018. 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 01-11-2017 til 31-10-2018.

Vipperød, 28. november 2018
Zentura IT A/S

Christian Pedersen
Adm. direktør

Afsnit 2: Zentura IT A/S' beskrivelse af kontroller i forbindelse med deres salg og drift af hosting-platform

0. Indledning

Vi har i virksomheden implementeret en række kontroller med henblik på at kvalitetssikre og dokumentere kvaliteten i vores ydelser. Alle kontroller, hvad enten de relaterer sig til en processuel eller teknisk handling, har en udførende ansvarshavende, og i visse tilfælde også en ansvarshavende godkender.

Vores kontroller er rettet mod dels konkrete arbejdshandlinger, dels processer for en række arbejdshandlinger, hvilke tillige kan have konkrete kontroller tilknyttet yderligere. Konkrete arbejdshandlinger er beskrevet i Standard Operating Procedure dokumenter (SOP'er).

Tidsangivelse for en given kontrol opgives altid over en periode, også selvom en given kontrol oftest måtte blive praktisk udført i en bestemt måned år efter år.

1. Anvendelsesområde

Vi er specialister i rådgivning, implementering, drift- og vedligeholdelse af forretningskritiske it-løsninger, og vi tilbyder vores kunder forskellige typer af hosting. Vi har særlig fokus og kompetencer inden for rådgivning, opsætning, opgradering, drift og vedligehold af Citrix løsninger. Vi sætter kvalitet og pålidelighed i højsædet, og da langt de fleste af vores produkter og services leveres i realtid, har vi naturligvis 24/7/365 kundeservice, monitorering og lover aldrig mindre end 99,7% tilgængelighed.

For at garantere vores ydelser vedligeholder vi løbende vores systemer, vores kompetencer og vores dokumentation.

Vi er vores kunders it-afdeling og håndterer alle aspekter forbundet hermed.

4. Risikohåndtering

Registrering, vurdering, mitigering og evaluering af risici er en integreret del af alle vores forretningsprocesser. Kvalitet og pålidelighed er af største betydning for os, og for vores kunder, hvorfor vi løbende tager stilling til alle forhold der måtte vedrøre kvaliteten af vores ydelser og vores forretning generelt. Alt sammen med behørig hensyn til vores omverden og det evigt fluktuerende trusselsbillede.

Alle trusler vurderes systematisk og ensartet, og for at tilsikre transparens, overskuelighed og dokumentation, benyttes fastlagt klassifikationsmetode. Identifikation, analyse og vurdering af risici med betydning for vores forretning kan tage afsæt i både udefrakommende trusler såvel som interne forhold.

Risikoanalysen er ledelsesgodkendt og gennemgås mindst 1 gang årligt.

5. Informationssikkerhedspolitikker

5.1 Retningslinjer for styring af informationssikkerhed

Vi har i vores it-sikkerhedspolitik beskrevet hvordan vi tilsikrer informationssikkerhed i vores forretning. Vores it-sikkerhedspolitik kan ikke fraviges, hverken for kunder, ansatte eller leverandører, og det er virksomhedens ledelse der godkender retningslinjer og foretager de nødvendige opdateringer af samme.

Virksomhedens it-sikkerhedspolitik opdateres såfremt der foretages ændringer eller implementeres nye forretningsområder, og politikken gennemgås i sin helhed minimum én gang årligt.

6. Organisering af informationssikkerhed

6.1. Intern organisering

Når vi har ændret ting i it-sikkerhedspolitikken, og minimum efter den årlige gennemgang, fremlægges ændringerne internt ved førstkommende månedsmøde for personalet. Ligeledes bliver eksterne leverandører mf. Inddraget og orienteret såfremt det har relevans. Det er virksomhedens administrerende direktør og partner, som er ansvarlig for virksomhedens informationssikkerhed.

6.2. Mobilt udstyr (databærende medier) og fjernarbejdspladser

Vi har ingen databærende medier, undtaget serverrumsmedier og mobiltelefoner. Vi har alene adgang til mail, kalender og kontakter via vores mobiltelefoner, ligesom vi har tilkoblet en række sikkerhedspolicies. Vi anvender ikke lokale medier som eksempelvis USB-sticks.

Politikken for mobilt udstyr er en del af Zenturas IT Sikkerhedspolitik.

7. Medarbejdersikkerhed

7.1. Før ansættelsen

Forud for ansættelse af medarbejdere følges en ansættelsesprocedure. Det er den ansættende medarbejder/partner, som er ansvarlig for de HR relaterede kontroller. For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid opgavespecifik kontrakt, dedikeret fortrolighedserklæring, og anden relevant dokumentation indhentes. Det er virksomhedens direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv. Den tekniske oprettelse af medarbejdere såvel som konsulenter, foretages i henhold til relevante SOP'er. Vi har desuden en proces for kontrol af alle brugere med rettigheder til virksomhedens netværk.

7.2 Under ansættelsen

Medarbejdere, og eksterne parter når relevant, bliver uddannet og trænet i vores retningslinjer for it-sikkerhed og de deraf afledte opgaver. Dette foregår som sidemandsoplæringer, ved kontormøder o. lign. Vi har desuden en procedure for træning/uddannelse/certificering af medarbejdere.

Afhængighed af nøglemedarbejdere

Via vores dokumentation og beskrivelser sikrer vi os mod personafhængighed, ligesom vi arbejder med dobbeltroller på alle funktioner i videst muligt omfang.

7.3. Ansættelsesforholdets ophør eller ændring

Den tekniske afvikling af medarbejdere- såvel som konsulenter, foretages i henhold til relevante SOP'er. Vi har desuden en proces for kontrol af alle brugere med rettigheder til virksomhedens netværk.

8 Styring af aktiver

8.1 Ansvar for aktiver

Alle aktiver er ejet af virksomheden og der foreligger fortegnelser over samme.

8.2 Klassifikation af information

Al virksomhedens data, såvel egne data som kundernes data, nyder samme beskyttelse. Der kan være helt særlige forhold aftalt for visse kunder, og disse forhold vil være reguleret og håndteret efter særlig aftale.

8.3 Mediehåndtering

Vi har ingen databærende medier, undtaget serverrumsmedier og mobiltelefoner. Alle mobiltelefoner er sikret med sikkerhedspolicies, herunder forbindelsesgodkendelse per enhed. Vi anvender ikke lokale medier som eksempelvis USB-sticks.

9. Adgangsstyring

9.1. Forretningsmæssige krav til adgangsstyring

Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Interne brugere oprettes alene på baggrund af skriftligt ønske fra ledelsen. Alle brugere er personhenførbare. Servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret. Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Interne brugere og deres adgangsniveau gennemgås periodisk af ledelsen. Alle medarbejdere er oprettet med differentieret adgang, og har således alene adgang til de systemer og de data som er relevant for deres respektive jobfunktioner. Vi benytter desuden 2-faktor autentifikation, som er obligatorisk, også for kunder.

9.2 Administration af brugeradgang

Onboard af nye kunder foretages i henhold til fastlagte procedurer og relevante SOP'er. Repræsentant fra vores Salg og Ledelse godkender kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav. Hver kundekontrakt indeholder desuden specifikation af hvem, hos kunden, der har rettigheder til at fremsende og/eller godkende it-ændringsønsker på vegne af den pågældende virksomhed til Zentura, hvormed der aldrig opstår tvivl om hvem der er ansvarlig for en udført handling/ændring.

9.3 Brugernes ansvar

Administration af brugeradgange foretages i henhold til fastlagte procedurer og relevante SOP'er. Retningslinjer for brugeransvar er tilgængelige i virksomhedens it-sikkerhedspolitik og medarbejderhåndbog.

9.4. Styring af system- og applikationsadgang

Administration af system- og applikationsadgange foretages i henhold til fastlagte procedurer og SOP'er.

10. Kryptografi

10.1 Kryptografiske kontroller

Al netværkskommunikation mellem os og vores kunder er beskyttet med kryptering. Adgang til, og administration af, krypteringsnøgler varetages alene af virksomhedens ledelse. Al trafik til og fra Zenturas netværk er beskyttet med SSL-certifikater, som er trusted af GlobalSign.

11 Fysisk sikring og miljøsikring

11.1 Sikre områder

Al vores udstyrer er placeret i eget rack hos vores datacenter leverandør. Her er det kun vores tekniske personale har adgang. Vores backup udstyr er placeret i eget rack på alternativ datacenter lokation, ved anden datacenter leverandør. Vores datacenter leverandører har revisorerklæringer af type ISAE 3402-II, som afgives årligt, og vi indhenter årligt samme. Dertil fører vi selv tilsyn med vores fysiske udstyr, når vi med jævne mellemrum er lokationen for at udføre nødvendigt hardware relateret arbejde. Vores fysiske kontor er placeret i Vipperød. Vi har en proces for sikring af lokationen.

11.2 Udstyr

Bortskaffelse af medier

Vi ejer alle serverrumsmedier. Medier destrueres som en del af vores indkøbsaftale med leverandøren. Ved tyveri af mobiltelefon, foretages fjernsletning af telefonen. Det vil derefter ikke være muligt at tilgå mail og kalenderdata fra telefonen.

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor personafhængighed og 'sluske-fejl' minimeres. Ændringer i systemerne følger vores ITIL Change Management-proces, hvorved de skal godkendes af vores "Change Advisory Board" inden implementering.

12.2 Kapacitetsstyring

Tilgængelighed er en af vores kerneværdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelsen til vores kunder. Vi overvåger vores kapacitet, både disk, cpu og trafik, og vi kan løbende, og uden gene for kunderne, udvide vores kapacitet.

12.3 Malwarebeskyttelse

Vi anser malware som en af de største trusler mod vores forretning, og vores tekniske foranstaltninger sikrer den højst mulige grad af sikkerhed for, at malware ikke kan afvikles i vores miljøer. Vi minimerer risikoen både i form af perimeter sikkerhed, men også skadesafgrænsning, skulle en utilsigtet hændelse opstå. Vi har desuden et decideret beredskab, skulle en utilsigtet hændelse kræve iværksættelse af ekstraordinære foranstaltninger.

12.4 Backup og sikkerhedskopiering

På Zenturas hosting platform laves der snapshot backup hver nat. Det vil sige at der laves en fuld kopi af samtlige data: serversystem filer, brugerdata, fil-services, databaser og alle andre data. Et snapshot udgør en komplet kopi af serveren i det øjeblik snapshottet tages - uden datatab overhovedet. Efter hvert snapshot kopieres en kopi af snapshottet over i det modsatte datacenter. Disse snapshots opbevares i 4 dage på det primære site, således at restore kan udføres uden forudgående kopiering fra det sekundære datacenter. Alle snapshots opbevares i 30 dage på det sekundære datacenter. Denne politik benyttes både på Zenturas og kundernes servere og data.
På kunder med egen infrastruktur benyttes kundes eget backup system til backup og kundens egen politik følges.

12.5 Logning og overvågning

Vores tekniske set-up fokuserer på samme værdier, og værn mod uvedkommendes adgang til vores data er af højeste prioritet. Vi har systemer til overvågning og sikring af netværk og internetbrug, og alle e-mails (indgående og udgående) skannes for virus hos en ekstern leverandør. Vi foretager daglig overvågning af vores systemer via automatiserede systemer til måling af grænseværdier.

Alarmering, såfremt en kritisk hændelse konstateres, tilgår vores driftsmedarbejdere og uden for kontortiden til vores driftsvagt. Hændelser for login og logout på vores platforme logføres, og vi benytter alene personhenførbare brugerkonti, hvorfor det er muligt at identificere hvilke personer der har været logget på.

12.6 Styring af driftssoftware

Patching foretages ugentligt i et fastlagt servicevindue. Servicevinduet fremgår af virksomhedens generelle forretningsbetingelser, og skal ikke varsles separat. For eksempel installeres alle kritiske Microsoft system-opdateringer, Windows security-updates klassificeret som "Critical" og "Security Updates", automatisk i det

aftalte service vindue. En række 3. parts programmer som f.eks. Java, Adobe Reader, mfl. opdateres sammen med diverse Microsoft patches.

Alle "Critical" og "Security" patches er installeret senest 2 måneder efter frigivelse.

12.7 Sårbarhedsstyring

Vores systemer er beskyttet mod ukontrolleret installation af software. Vores kunder er ligeledes afskærmet fra muligheden for at installere software.

12.8 Overvejelser i forbindelse med audit af informationssystemer

Vi prioriterer løbende intern audit, herunder interne stikprøvekontroller, og ansvaret er forankret hos vores driftschef. Tidspunkt for udførelse af den årlige eksterne audit planlægges i samarbejde med vores auditører.

13 Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

Al godkendt netværkstrafik (indgående) kommer igennem vores firewall, og vi har MPLS forbindelser til alle kunder. Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv. Adgang til virksomhedens services via mobile enheder tillades ikke, dog tillades adgang til mail, kalender og adressebog. For at have denne adgang, pålægges en række sikkerhedspolicies til telefonen, hvilket er en fast del af vores proces for opsætning af enheder. Alle standard ændringer har en dedikeret SOP. Alle væsentlige ændringer drøftes, prioriteres og godkendes af ledelsen.

13.2 Informationsoverførsel

Ekstern datakommunikation sker alene via e-mails, idet vores kunders adgang og brug af vores servere ikke betragtes som ekstern datakommunikation.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

Informationssikkerhedsrelaterede krav er en del af vores processer, og ændringer/nyindkøb vurderes altid ud fra et sikkerhedsmæssigt perspektiv, jf. vores risikoanalyse.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

Alle ændringer til systemer håndteres via change-procedure.

14.3 Testdata

Testdata må aldrig være personfølsom eller fortrolig data. Testdata nyder samme beskyttelse som al anden data.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

Alle vores leverandør- og partneraftaler indeholder regulering af fortrolighed.

15.2. Styring af leverandørydelser

Vi har en proces til at sikre at vores leverandøraftaler indeholder relevante sikkerhedsmæssige forhold, eksempelvis forhold om monitorering, fortrolighed, immaterielle rettigheder og leverancesikkerhed. Der indhentes tillige revisorerklæring(er) fra vores kritiske leverandører.

16 Styring af informationssikkerhedsbrud

16.1 Styring af informationssikkerhedsbrud og forbedringer

Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af disse hændelser. Vi har etableret en række tiltag for at forhindre at sikkerhedshændelserne opstår, og dertil har vi driftsovervågning med vagtordning, hvormed vi kan reagere straks en utilsigtet hændelse måtte opstå. Vi modtager dagligt sikkerhedsinformation fra CSIS, og vi har SikkerDNS, som hjælper os med at være på forkant. Vi holder os tillige fagligt opdaterede vha. producenternes hjemmesider, debatfora mv.

Opfølgning på informationssikkerhedsbrud

Alle sikkerhedsbrud dokumenteres til internt brug, og hændelsen gennemgås med alle relevante medarbejdere ved førstkommende lejlighed. Afhængig af hændelsens karakter udarbejdes nye processer og procedurer, så vi undgår at hændelsen indtræffer igen. Sikkerhedsrelaterede emner, generelle såvel som aktuelle emner, gennemgås desuden ved interne møder. Ved kriminelle forhold sker en politimæssig efterforskning, hvor vores logføring og øvrige overvågning kan benyttes til opklaring og evaluering af sikkerhedshændelsen.

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

17.1. Informationssikkerhedskontinuitet

Der er etableret en Risiko Analyse, der lister de mulige scenarier, der kan påvirke driften af vores systemer og der er etableret beredskabsplaner der beskriver hvordan driften skal reetableres efter nedbrud.

17.2 Redundans

Vi benytter to separate datacentre, og skulle et datacenter blive utilgængeligt, skiftes automatisk over på det sekundære site.

18 Overensstemmelse

18.1 Overensstemmelse med lovbestemt og kontraktlige krav

Vi er ikke underlagt særlig lovgivning i forhold til vores ydelser. Vores kunder kan dog være underlagt særlig lovgivning, og hvor det måtte være tilfældet, er vores understøttelser heraf aftalt særskilt.

Databehandleraftaler

Vi har databehandleraftaler med alle vores kunder.

Beredskab

Skulle en nødsituation opstå, har Zentura udarbejdet en beredskabsplan. Beredskabsplanen er udarbejdet i henhold- og overensstemmelse med vores it-sikkerhedspolitik og vores risikoanalyse, og den vedligeholdes minimum årligt. Planen testes, og både plan og procedurer er forankret i vores driftsdokumentation- og procedurer. Vores beredskabsplanlægning tager højde for at vi til hver en tid kan levere vores ydelser rettidigt – næsten uanset hvad der sker.

18.2 Gennemgang af informationssikkerhed

Vi lader os årligt revidere af ekstern revisor med henblik på at opnå erklæring uden forbehold for overholdelsen af kontrollerne nævnt i denne beskrivelse. Vi følger rammerne inden for ISO 27002, hvilket føromtalte revisor attesterer i en ISAE3402-II erklæring.

19 Komplementerende kontroller

Med mindre andet er aftalt, er vores kunder selv ansvarlige for at etablere forbindelse til vores servere. Desuden er vores kunder selv ansvarlige for, med mindre andet er aftalt, at;

i) det aftalte niveau for backup dækker kundens behov,
ii) brugeradministration, herunder anmodninger om oprettelse og nedtagning af bruger, og periodisk gennemgang af kundens egne brugere
iii) at sporbarhed opretholdes i tredjepartssoftware, som kunden selv administrerer,
iv) at kundespecifikke softwareløsninger understøtter den af os udbudte backup teknologi,
v) særaftale for backupjobs der kræver krypteringspassword, hvor kunden alene er ansvarlig for håndtering og opbevaring af krypteringspassword, og
vi) anmodning om adgang til kundens servermiljø for kundens tredjepartsleverandører, vii) kundens anmeldelse til Datatilsynet, for hvem dette måtte være relevant.

Dette er en fast del af aftalegrundlaget med kunden.

20 Ændringer i perioden

Ændringer i perioden

Vi har i perioden moderniseret og tilpasset hele platformen, som er gennemgribende ændret både teknologisk-, hardware og i fysisk logkation i vores datacentre. Vi har migreret samtlige kunder over på den nye platform. Vi er desuden blevet registreret ISP og ejer dermed vores egne ip-adresser.

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

Til ledelsen hos Zentura IT A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om Zentura IT A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af Zentura IT A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hosting-platform i perioden 01-11-2017 til 31-10-2018 samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Zentura IT A/S' beskrivelse (afsnit 2) indeholder en række forhold, som virksomheden skal leve op til jf. virksomhedens medlemskab af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark). Vores revision har omfattet disse forhold, og består udover de fysiske forhold, herunder server hardware, LAN, WAN og firewalls, af:

- hvorvidt Zentura IT A/S implementerer kritiske sikkerhedsopdateringer inden for 2 måneder fra frigivelse
- hvorvidt Zentura IT A/S kan retablere enheder i datacenter inden for 3 dage
- hvorvidt Zentura IT A/S lever op til BFIH's krav for "mindstemål for god hosting".

Vores konklusion udtrykkes med høj grad af sikkerhed.

Zentura IT A/S' ansvar

Zentura IT A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. Zentura IT A/S 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 Zentura IT 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

Zentura IT A/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 Zentura IT 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 i hele perioden 01-11-2017 til 31-10-2018, 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 01-11-2017 til 31-10-2018
(c) at kontrollerne for de særlige krav, som er foranlediget af virksomhedens medlemskab af BFIH jf. beskrivelsen i kapitel 2, var hensigtsmæssigt udformede i hele perioden fra 01-11-2017 til 31-10-2018
(d) 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 01-11-2017 til 31-10-2018.

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 Zentura IT A/S' hosting-platform, 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, 28. november 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 Zentura IT A/S 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 01-11-2017 til 31-10-2018.

Vi har således ikke nødvendigvis testet alle de kontroller, som Zentura IT A/S har nævnt i sin beskrivelse i afsnit 2.

Kontroller udført hos Zentura IT A/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 Zentura IT A/S 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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
4.1	Alle trusler vurderes systematisk og ensartet, og for at tilsikre transparens, overskuelighed og dokumentation, benyttes fastlagt klassifikationsmetode. Identifikation, analyse og vurdering af risici med betydning for vores forretning kan tage afsæt i både udefrakommende trusler såvel som interne forhold. Risikoanalysen er ledelsesgodkendt og gennemgås mindst én gang årligt.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret dokumentet. Vi har forespurgt til periodisk gennemgang af risikoanalyse, 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 risikoanalysen, og vi har inspiceret dokumentation for ledelsesgodkendelse.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
5.1	Vores it-sikkerhedspolitik kan ikke fraviges, hverken for kunder, ansatte eller leverandører, og det er virksomhedens ledelse der godkender retningslinjer og foretager de nødvendige opdateringer af samme. Virksomhedens it-sikkerhedspolitik opdateres såfremt der foretages ændringer eller implementeres nye forretningsområder, og politikken gennemgås i sin helhed minimum én gang årligt.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
6.1	Det er virksomhedens administrerende direktør og partner, som er ansvarlig for virksomhedens informationssikkerhed. Via vores dokumentation og beskrivelser sikrer vi os mod personafhængighed, ligesom vi arbejder med dobbeltroller på alle funktioner i videst muligt omfang. Vi modtager dagligt sikkerhedsinformation fra CSIS, og vi har SikkerDNS, som hjælper os med at være på forkant. Vi holder os tillige fagligt opdaterede vha. producenternes hjemmesider, debatfora mv. Ændringer i systemerne følger vores ITIL Change Management proces.	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 funktionsadskillelse. Vi har forespurgt til retningslinjer for kontakt med myndigheder, og vi har inspiceret retningslinjerne. 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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
6.2	Politikken for mobilt udstyr er en del af Zenturas it-sikkerhedspolitik. Vi har alene adgang til mail, kalender og kontakter via vores mobiltelefoner, ligesom vi har tilkoblet en række sikkerhedspolicies. Vi anvender ikke lokale medier som eksempelvis USB-sticks. Ved tyveri af mobiltelefon foretages fjernsletning af telefonen.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
7.1	Forud for ansættelse af medarbejdere følges en ansættelsesprocedure. Det er den ansættende medarbejder/partner, som er ansvarlig for de HR relaterede kontroller. For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid opgavespecifik kontrakt, dedikeret fortrolighedserklæring, og anden relevant dokumentation indhentes. Det er virksomhedens direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv.	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.	Vi har observeret, at virksomheden i én ud af tre stikprøver ifm. ansættelsesproces ikke har fulgt virksomhedens egen procedure, idet straffeattest først er indhentet fire dage efter, at medarbejderen har fået adgang til virksomhedens systemer. Ingen væsentlige afvigelser konstateret i øvrigt.

Under ansættelsen

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

Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
7.2	Det er virksomhedens administrerende direktør og partner, som er ansvarlig for virksomhedens informationssikkerhed. Medarbejdere, og eksterne parter når relevant, bliver uddannet og trænet i vores retningslinjer for it-sikkerhed og de deraf afledte opgaver. Dette foregår som sidemandsoplæringer, ved kontormøder o. lign. Vi har desuden en procedure for træning/uddannelse/certificering af medarbejdere.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
7.3	Den tekniske afvikling af medarbejdere såvel som konsulenter, foretages i henhold til relevante SOP'er.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
8.1	Alle aktiver er ejet af virksomheden og der foreligger fortegnelser over samme. Politikken for mobilt udstyr er en del af Zenturas it-sikkerhedspolitik.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har forespurgt til kontrol for periodisk gennemgang af aktiver, og vi har stikprøvevis inspiceret, at fortegnelser er gennemgået i perioden. 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.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
8.2	Al virksomhedens data, såvel egne data som kundernes data, nyder samme beskyttelse. Der kan være helt særlige forhold aftalt for visse kunder, og disse forhold vil være reguleret og håndteret efter særlig aftale.	Vi har forespurgt til politik for klassificering af data, og vi har inspiceret politikken. 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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
8.3	Vi har ingen databærende medier, undtaget serverrumsmedier og mobiltelefoner. Alle mobiltelefoner er sikret med sikkerhedspolicies, herunder forbindelsesgodkendelse per enhed. Vi anvender ikke lokale medier som eksempelvis USB-sticks. Vi ejer alle serverrumsmedier. Medier destrueres som en del af vores indkøbsaftale med leverandøren.	Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen. Vi har forespurgt til procedure for bortskaffelse af medier, og vi har inspiceret proceduren. Vi har endvidere inspiceret lokationen for medier til kassation. 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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
9.1	Alle medarbejdere er oprettet med differentieret adgang, og har således alene adgang til de systemer og de data som er relevant for deres respektive jobfunktioner.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
9.2	Onboard af nye kunder foretages i henhold til fastlagte procedurer og relevante SOP'er. Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Hver kundekontrakt indeholder desuden specifikation af hvem, hos kunden, der har rettigheder til at fremsende og/eller godkende it-ændringsønsker på vegne af den pågældende virksomhed til Zentura, hvormed der aldrig opstår tvivl om hvem der er ansvarlig for en udført handling/ændring. Interne brugere oprettes alene på baggrund af skriftligt ønske fra ledelsen. Alle brugere er personhenførbare. Servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret. Interne brugere og deres adgangsniveau gennemgås periodisk af ledelsen.	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.	Vi har observeret, at virksomheden har disabled en fratrædende medarbejder 4 dage efter sidste arbejdsdag. Virksomheden har begrundet diskrepansen, og vi har ikke observeret forhold, der har givet anledning til yderligere observationer. Ingen væsentlige afvigelser konstateret i øvrigt.

Brugernes ansvar

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

Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
9.3	Retningslinjer for brugeransvar er tilgængelige i virksomhedens it-sikkerhedspolitik og medarbejderhåndbog.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
9.4	Alle medarbejdere er oprettet med differentieret adgang, og har således alene adgang til de systemer og de data som er relevant for deres respektive jobfunktioner. Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Vi benytter desuden 2-faktor autentifikation, som er obligatorisk, også for kunder. Administration af system- og applikationsadgange foretages i henhold til fastlagte procedurer og SOP'er.	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.	Vi har observeret, at der er uoverensstemmelser mellem virksomhedens kodeordspolitik og den implementerede kodeordspolitik hvad angår minimumslængde og lockout ved gentagne fejllogin. Ingen væsentlige afvigelser konstateret i øvrigt.

Kryptografi

Kryptografiske kontroller **Kontrolmål: Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.**			
Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
10.1	Al netværkskommunikation mellem os og vores kunder er beskyttet med kryptering. Adgang til, og administration af, krypteringsnøgler varetages alene af virksomhedens ledelse. Al trafik til og fra Zenturas netværk er beskyttet med SSL certifikater som er trusted af GlobalSign.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
11.1	Al vores udstyrer er placeret i eget rack hos vores datacenter leverandør. Her er det kun vores tekniske personale har adgang. Vores backup udstyr er placeret i eget rack på alternativ datacenter lokation, ved anden datacenter leverandør. Vores datacenter leverandører har revisorerklæringer af type ISAE 3402-II, som afgives årligt, og vi indhenter årligt samme. Dertil fører vi selv tilsyn med vores fysiske udstyr, når vi med jævne mellemrum er lokationen for at udføre nødvendigt hardware relateret arbejde. Vores fysiske kontor er placeret i Vipperød. Vi har en proces for sikring af lokationen.	Vi har forespurgt til erklæringer fra underleverandører af fysiske forhold, og vi har inspiceret erklæringerne for betryggende fysisk sikring. Vi har inspiceret, at erklæringer fra underleverandører er nyeste tilgængelige udgave. Vi har forespurgt til dokumentation for periodisk eftersyn på eksterne lokationer, og vi har stikprøvevis inspiceret dokumentation for eftersyn hos underleverandørerne. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandører, 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.	Vi har observeret, at der i erklæringerne for væsentlige underleverandører af fysisk sikkerhed har været konstateret afvigelser. I Nianets erklæring er konstateret følgende afvigelser: - For én af de 25 udvalgte stikprøver ifm. informationssikkerhed ved projektstyring var der ikke en formel CAB-godkendelse. - For én af de 25 udvalgte stikprøver ifm. informationssikkerhed ved projektstyring forelå der ikke fallback- og testplan. - Fire ud af 25 eksterne brugere har ikke underskrevet tavshedserklæring. - I to tilfælde har der ikke foreligget godkendelse fra nærmeste leder ifm. tildeling af Domain Admin-rettigheder på AD. - I seks ud af 25 stikprøver for incidents var de ikke prioriterede. - I én ud af 25 stikprøver for incidents var den kategoriseret som medium, hvorimod den burde have været kategoriseret som high iflg. incident management-proceduren. Den gennemgåede erklæring for Nianet dækker perioden frem til 7. juni 2018. I InterXions erklæring er konstateret følgende afvigelser: - Den yderste fysiske perimetersikring af ét af underleverandørens datacentre har ifm. igangværende bygningsarbejde ikke været forseglet, og underleverandøren har i den forbindelse ikke haft indsat ekstra foranstaltninger for at imødegå den øgede risiko. Således har generatorer og køleanlæg kunnet tilgås uden barriere. - Overvågningen på én af underleverandørens datacentre har ved inspektion vist det forkerte tidsstempel. Forholdet blev udbedret indenfor 48 timer. Den gennemgåede erklæring for InterXion dækker perioden frem til 31. december 2017. Ingen væsentlige afvigelser konstateret i øvrigt.

Udstyr **Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.**			
Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
11.2	Vi ejer alle serverrumsmedier. Medier destrueres som en del af vores indkøbsaftale med leverandøren. Ved tyveri af mobiltelefon, foretages fjernsletning af telefonen. Det vil derefter ikke være muligt at tilgå mail og kalenderdata fra telefonen.	Vi har forespurgt til erklæringer fra underleverandører af fysiske forhold, og vi har inspiceret erklæringerne for betryggende fysisk sikring. Vi har observeret, at erklæringer fra underleverandører er nyeste tilgængelige. Vi har inspiceret erklæringer fra underleverandører med henblik på at identificere understøttende forsyninger, sikring af regelmæssig vedligeholdelse af udstyret og sikring af kabler. Vi har forespurgt til periodisk eftersyn af ekstern lokation, og vi har stikprøvevis inspiceret dokumentation for eftersyn. Vi har forespurgt til politik for bortskaffelse af udstyr. Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler. 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.	Se bemærkning i 11.1. Den gennemgåede erklæring for Nianet dækker perioden frem til 7. juni 2018. Den gennemgåede erklæring for Inter-Xion dækker perioden frem til 31. december 2017. Ingen væsentlige afvigelser konstateret i øvrigt.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

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

Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
12.1	Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor personafhængighed og 'sluske-fejl' minimeres. Ændringer i systemerne følger vores ITIL Change Management proces, hvorved de skal godkendes af vores "Change Advisory Board" inden implementering. Tilgængelighed er en af vores kerneværdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelsen til vores kunder. Vi overvåger vores kapacitet, både disk, cpu og trafik, og vi kan løbende, og uden gene for kunderne, udvide vores kapacitet.	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.	Ingen væsentlige afvigelser konstateret.

Malwarebeskyttelse

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

Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
12.2	Vi anser malware som en af de største trusler mod vores forretning, og vores tekniske foranstaltninger sikrer den højst mulige grad af sikkerhed for, at malware ikke kan afvikles i vores miljøer. Vi minimerer risikoen både i form af perimeter sikkerhed, men også skadesafgrænsning, skulle en utilsigtet hændelse opstå. Alle e-mails (indgående og udgående) skannes for virus hos en ekstern leverandør. Vi har desuden et decideret beredskab, skulle en utilsigtet hændelse kræve iværksættelse af ekstraordinære foranstaltninger.	Vi har forespurgt til foranstaltninger mod malware, og vi har inspiceret dokumentation for anvendelsen. Vi har forespurgt til anvendelsen af antivirusprogrammer.	Ingen væsentlige afvigelser konstateret.

Backup **Kontrolmål: Formålet er at beskytte mod tab af data.**			
Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
12.3	På Zenturas hosting platform laves der snapshot backup hver nat. Det vil sige at der laves en fuld kopi af samtlige data: serversystem filer, brugerdata, fil-services, databaser og alle andre data. Et snapshot udgør en komplet kopi af serveren i det øjeblik snapshottet tages - uden datatab overhovedet. Efter hvert snapshot kopieres en kopi af snapshottet over i det modsatte datacenter. Disse snapshots opbevares i 4 dage på det primære site, således at restore kan udføres uden forudgående kopiering fra det sekundære datacenter. Alle snapshots opbevares i 30 dage på det sekundære datacenter. Denne politik benyttes både på Zenturas og kundernes servere og data. På kunder med egen infrastruktur benyttes kundes eget backup system til backup og kundens egen politik følges.	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 underleverandører med henblik på at se, at backup opbevares forsvarligt. Vi har forespurgt til test af genoprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse.	Ingen væsentlige afvigelser konstateret.
Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
12.4	Vi har systemer til overvågning og sikring af netværk og internetbrug, og alle e-mails (indgående og udgående) skannes for virus hos en ekstern leverandør. Vi foretager daglig overvågning af vores systemer via automatiserede systemer til måling af grænseværdier. Alarmering, såfremt en kritisk hændelse konstateres, tilgår vores driftsmedarbejdere og uden for kontortiden til vores driftsvagt. Hændelser for login og logout på vores platforme logføres, og vi benytter alene personhenførbare brugerkonti, hvorfor det ter muligt at identificere hvilke personer der har været logget på.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
12.5	Patching foretages ugentligt i et fastlagt servicevindue. Servicevinduet fremgår af virksomhedens generelle forretningsbetingelser, og skal ikke varsles separat. Fx installeres alle kritiske Microsoft systemopdateringer, Windows security updates klassificeret som "Critical" og "Security Updates", automatisk i det aftalte service vindue. En række 3. parts programmer som f.eks. Java, Adobe Reader, mfl. opdateres sammen med diverse Microsoft patches.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
12.6	Vores systemer er beskyttet mod ukontrolleret installation af software. Vores kunder er ligeledes afskærmet fra muligheden for at installere software.	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 retningslinjer for begrænsningen af programinstallation.	Ingen væsentlige afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed **Kontrolmål: Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.**			
Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
13.1	Al godkendt netværkstrafik (indgående) kommer igennem vores firewall, og vi har MPLS forbindelser til alle kunder. Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv. Adgang til virksomhedens services via mobile enheder tillades ikke, dog tillades adgang til mail, kalender og adressebog. For at have denne adgang, pålægges en række sikkerhedspolicies til telefonen, hvilket er en fast del af vores proces for opsætning af enheder.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
13.2	Ekstern datakommunikation sker alene via e-mails, idet vores kunders adgang og brug af vores servere ikke betragtes som ekstern datakommunikation. For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid opgavespecifik kontrakt, dedikeret fortrolighedserklæring, og anden relevant dokumentation indhentes.	Vi har forespurgt til politikker og procedurer for dataoverførsel, og vi har inspiceret disse. 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.	Ingen væsentlige afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold

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

Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
15.1	Alle vores leverandør- og partneraftaler indeholder regulering af fortrolighed.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret hensyntagen til informationssikkerhed i leverandørforhold. 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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
15.2	Vi har en proces til at sikre at vores leverandøraftaler indeholder relevante sikkerhedsmæssige forhold, eksempelvis forhold om monitorering, fortrolighed, immaterielle rettigheder og leverancesikkerhed. Der indhentes tillige revisorerklæring(er) fra vores kritiske leverandører.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører.	Se bemærkning i 11.1. Den gennemgåede erklæring for Nianet dækker perioden frem til 7. juni 2018. Den gennemgåede erklæring for InterXion dækker perioden frem til 31. december 2017. Ingen væsentlige afvigelser konstateret i øvrigt.

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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
16.1	Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af disse hændelser. Vi har etableret en række tiltag for at forhindre at sikkerhedshændelserne opstår, og dertil har vi driftsovervågning med vagtordning, hvormed vi kan reagere straks en utilsigtet hændelse måtte opstå. Alle sikkerhedsbrud dokumenteres til internt brug, og hændelsen gennemgås med alle relevante medarbejdere ved førstkommende lejlighed. Afhængig af hændelsens karakter udarbejdes nye processer og procedurer, så vi undgår at hændelsen indtræffer igen. Sikkerhedsrelaterede emner, generelle såvel som aktuelle emner, gennemgås desuden ved interne møder. Ved kriminelle forhold sker en politimæssig efterforskning, hvor vores logføring og øvrige overvågning kan benyttes til opklaring og evaluering af sikkerhedshændelsen.	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, og vi har stikprøvevis inspiceret, at håndtering af hændelser har fulgt proceduren. 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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
17.1	Der er etableret en risikoanalyse, der lister de mulige scenarier, der kan påvirke driften af vores systemer og der er etableret beredskabsplaner der beskriver hvordan driften skal reetableres efter nedbrud.	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 periodisk gennemgang af beredskabsplanen, og vi har inspiceret, at dokumentet er gennemgået i revisionsperioden, samt inspiceret kontrol for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af beredskabsplanen, og vi har inspiceret dokumentation for ledelsesgodkendelse. Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test samt overvejelser om kompenserende tiltag i forbindelse med test af beredskabstest.	Ingen væsentlige afvigelser konstateret.

Redundans

Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
17.2	Vi benytter to separate datacentre, og skulle et datacenter blive utilgængeligt, skiftes automatisk over på det sekundære site.	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.	Zentura IT A/S' kontrol	REVI-IT's test	Resultat af test
18.2	Vi lader os årligt revidere af ekstern revisor med henblik på at opnå erklæring uden forbehold for overholdelsen af kontrollerne nævnt i denne beskrivelse. Vi følger rammerne inden for ISO 27002, hvilket føromtalte revisor attesterer i en ISAE3402-II erklæring.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer. Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning.	Ingen væsentlige afvigelser konstateret.