Zitcom A/S

CVR-nr.: 29412006

Uafhængig revisors erklæring om generelle it-kontroller hos Zitcom A/S relateret til drifts- og hosting-ydelser i perioden 1. januar 2017 til 31. december 2017

Indhold

1 Serviceleverandørens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt de af Zitcom A/S' udbudte drifts- og hosting-ydelser i perioden 1. januar til 31. december 2017, 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.

Zitcom A/S anvender GlobalConnect A/S som underleverandør til ekstern opbevaring af backup. Beskrivelsen inkluderer udelukkende kontroller og kontrolmål for processer, som håndteres af Zitcom A/S, og indeholder således ikke kontroller og kontrolmål, der håndteres af GlobalConnectA/S.

Zitcom A/S bekræfter, at:

(a) den medfølgende beskrivelse giver en dækkende beskrivelse af de generelle it-kontroller relateret til de af Zitcom A/S udbudte drifts- og hosting-ydelser i perioden fra 1. januar 2017 til 31. december 2017. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

  (i) redegør for, hvordan de generelle it-kontroller relateret til drifts- og hosting-ydelser leveret til kunder i perioden var udformet og implementeret, herunder redegør for:
    - de typer af ydelser, der er leveret
    - hvordan de generelle it-kontroller behandlede andre betydelige begivenheder og forhold end transaktioner
    - de processer i både it-systemet og manuelle systemer, der er anvendt til styring af de generelle it-kontroller
    - relevante kontrolmål og kontroller udformet til at nå disse mål
    - kontroller, som vi med henvisning til de generelle it-kontrollers udformning har forudsat ville være implementeret af brugerorganisationer
    - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller

  (ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. januar til 31. december 2017.

  (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 udformet og fungerede effektivt i hele perioden fra 1. januar til 31. december 2017. Kriterierne for denne udtalelse var, at:

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

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

  (iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar til 31. december 2017.

Skanderborg, den 15. februar 2018
Zitcom A/S

Stefan Rosenlund
Adm. direktør

2 Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til: Ledelsen hos Zitcom A/S

Omfang

Vi har fået som opgave at afgive erklæring om Zitcom A/S' beskrivelse i afsnit 3 af de generelle it-kontroller i relation til Zitcom A/S' udbudte drifts- og hosting-ydelser i hele perioden fra 1. januar til 31. december 2017 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Zitcom A/S anvender GlobalConnect A/S som underleverandør til ekstern opbevaring af backup. Beskrivelsen inkluderer udelukkende kontroller og kontrolmål for processer, som håndteres af Zitcom A/S, og indeholder ikke kontroller og processer, der håndteres af GlobalConnect A/S. Erklæringen er udarbejdet efter partielmetoden vedrørende GlobalConnect A/S, og vores test af kontroller omfatter ikke kontroller hos GlobalConnect A/S.

Zitcom A/S' ansvar

Zitcom A/S er ansvarlig for udarbejdelsen af beskrivelsen i afsnit 3 og tilhørende udtalelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores 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.

Ernst & Young 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.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Zitcom A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB, og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere 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 1.

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

Zitcom A/S' beskrivelse 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 deres særlige forhold.

Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i afsnit 1. Det er vores opfattelse:

(a) at beskrivelsen af de generelle it-kontroller relateret til Zitcom A/S' udbudte drifts- og hosting-ydelser, således som det var udformet og implementeret i hele perioden fra 1. januar til 31. december, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar til 31. december 2017, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar til 31. december 2017.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller er udelukkende tiltænkt kunder, der har anvendt Zitcom A/S' udbudte drifts- og hosting-ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 15. februar 2018
ERNST & YOUNG
Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Per Højmark
statsaut. revisor
MNE-nr. mne9230

3 Beskrivelse af Zitcom A/S' services, processer, kontrolmål og kontroller

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Zitcom A/S' kunder og disses revisorer i overensstemmelse med kravene i ISAE 3402 for erklæringsopgaver med sikkerhed om kontroller hos serviceleverandør. Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret i forbindelse med Zitcom A/S' leverance af serviceydelser på drift og hosting.

Beskrivelsen indeholder omtale af de anvendte procedurer til sikring af en betryggende afvikling af systemer. Formålet er at give tilstrækkelige informationer til, at hosting-kunders revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i de omfattede generelle it-kontroller hos Zitcom A/S, i det omfang det kan medføre en risiko for væsentlige fejl i hosting-kunders it-drift for perioden 1. januar 2017 til 31. december 2017.

3.2 Beskrivelse af Zitcom A/S' ydelser

Zitcom udvikler, administrerer og servicerer en vifte af professionelle hosting- og cloud-løsninger for en lang række virksomheder og organisationer i Danmark.

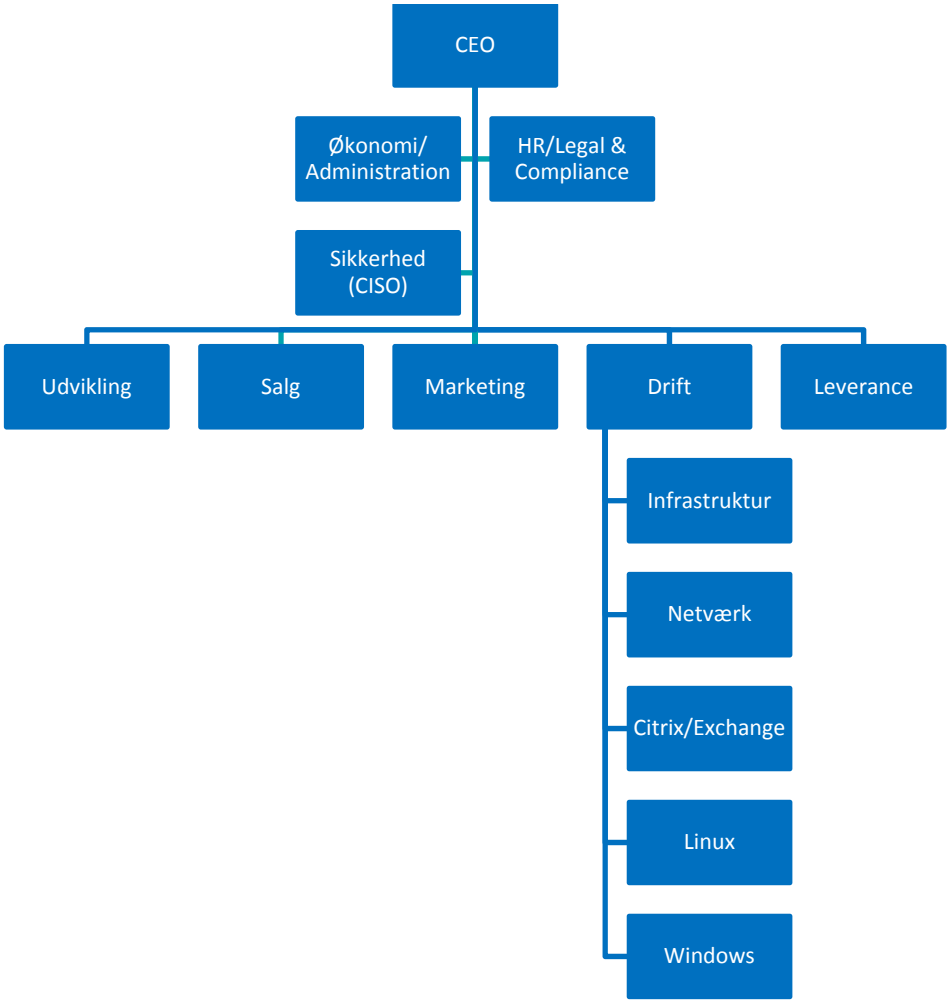
Zitcom arbejder ud fra en stræben efter at levere løsninger, der kvalitets- og servicemæssigt differentierer sig fra størstedelen af det resterende hosting-marked. Med mange års erfaring på markedet har Zitcom erfaret, at graden af kunders tilfredshed har direkte sammenhæng med niveauet på leverandørens service, tekniske kompetencer og kvaliteten af det hardware, som Zitcom A/S' løsninger driftes på. Det er derfor i stor stil de værdier, som vi baserer vores forretningsgrundlag på.

Fundamentet i forretningen er et moderne datacenter, som vi drifter med udgangspunkt i, at det skal kunne supportere stabilitet, sikkerhed og en hastighed, der kan imødekomme servicekrav fra kritiske og kvalitetsbevidste kunder. Med vores højt certificerede og fagligt erfarne medarbejdere kan vi støtte op omkring enhver type af hosting-løsninger – altid med kompetent rådgivning.

3.3 Zitcom A/S' organisation og sikkerhed

Kontrolmål 6: It-sikkerhedsadministration

Ansvar og organisering i Zitcom A/S fremgår af nedenstående organisationsdiagram. Sikkerhedschefen (CISO) refererer til den administrerende direktør (CEO).



Organisationens arbejde med sikkerhed styres og prioriteres af Sikkerhedsudvalget, som består af følgende medlemmer:

- CEO, Stefan Rosenlund
- CTO, Ole P. Jensen
- Chief Legal Officer, Bo Brandt Stisen
- CISO, Jakob Flink Schwartz

3.4 Risikostyring hos Zitcom A/S

Kontrolmål 5: IT Governance

Risikostyring gennemføres i Zitcom på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering, der sigter mod udvalgte systemer. Input til denne vurdering indhentes fra alle relevante niveauer i organisationen. Processen faciliteres af ansvarlige og ledere, der udarbejder udkast til Zitcom A/S' ledelse. Efter intern bearbejdning godkendes vurderingen af Zitcom A/S' ledelse.

Risikostyringen tager højde for forhold, som er nødvendige for at kunne styre risici i forhold til leverancen til kunderne. Dette sker gennem it-ledelsens kendskab til typer af aftaler mellem Zitcom A/S og kunderne.

Zitcom har som en del af ISO 27001-certificeringen etableret en formaliseret risikostyring, som omfatter alle relevante processer i virksomheden, der anvendes i leverancen af hosting-services. Der følges op

på risikovurderingen minimum én gang årligt ved det årlige ledelsesreview af ISO 27001-arbejdet. Arbejdet med risici er dokumenteret i et dokument, hvori både impact og sandsynlighed kan ses sammen med den samlede vægtning af hver enkelt risiko og de dertil knyttede handlinger. Relevante handlinger i forhold til væsentlige risici besluttes altid i samarbejde med ledelsen.

3.4.1 Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering

Kontrolmål 5: IT Governance

Zitcom A/S' it-sikkerhedspolitik, etablerede processer og kontroller omfatter alle systemer og ydelser, der tilbydes kunderne. Det fortsatte arbejde med tilpasning og forbedring af Zitcom A/S' sikringsforanstaltninger sker løbende i samarbejde med højt kvalificerede specialister.

Fastsættelse af kriterier og omfang for kontrolimplementering hos Zitcom er i 2017 sket ud fra ISO 27001/27002-standarderne. Med udgangspunkt i dette kontrolrammeværk er relevante kontrolområder og kontrolaktiviteter implementeret på de serviceydelser, der leveres af Zitcom.

Følgende væsentlige kontrolområder indgår i det samlede kontrolmiljø:

1. Informationssikkerhed
2. Intern organisering af it-sikkerhed
3. Fysisk sikkerhed
4. Styring af kommunikation med kunder
5. Backup[1]
6. Drift og overvågning
7. Adgangskontrol

3.4.2 Etableret kontrolmiljø

Hvert enkelt område er detaljebeskrevet i de efterfølgende afsnit.

3.4.3 Informationssikkerhed

Kontrolmål 5: IT Governance

Formål

En ledelsesgodkendt it-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse og er kommunikeret ud til relevante medarbejdere i virksomheden.

Anvendte procedurer og kontroller

Zitcom identificerer og afdækker relevante it-risici på de etablerede serviceydelser til kunderne. Dette varetages gennem en løbende trussels- og risikovurdering hos Zitcom, dels i forbindelse med alle udviklingsprojekter og ændringer i systemmiljøer, dels ved en årlig revurdering af risikoanalysen. Resultatet af den årlige revurdering forelægges ledelsen til godkendelse. Zitcom stiller endvidere en række informationer til rådighed for hosting-kundernes revisorer til brug for deres vurdering af Zitcom som serviceleverandør. Ud over driftsrelaterede forhold kan Zitcom også informere om sikkerhedsmæssige forhold, i det omfang kunderne efterspørger dette.

Tidspunkt for udførelse af kontrollen

It-risikoanalysen og it-sikkerhedspolitikken revurderes mindst én gang årligt forinden udførelse af it-revision og udarbejdelse af erklæring.

[1] Opbevaring af backup er ikke inkluderet i denne rapport, da dette er håndteret af serviceleverandør

Hvem udfører kontrollen?

Den årlige gennemgang udføres af Sikkerhedsudvalget.

Kontroldokumentation

Der er versionsstyring af it-sikkerhedspolitikken.

3.4.4 Intern organisering af it-sikkerhed

Kontrolmål 6: It-sikkerhedsadministration

Direktionen i Zitcom, som i det daglige er de øverste ansvarlige for it-sikkerheden, sørger for, at der til stadighed er etableret procedurer og tilknyttet systemer, der understøtter overholdelsen af den til enhver tid gældende it-sikkerhedspolitik. Sikkerhedsgruppen beskriver de overordnede målsætninger, og den driftsansvarlige er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollabelt ud fra en ressourcemæssig vurdering af omkostninger og risiko, ligesom de enkelte kontrolaktiviteter på de serviceområder, som tilbydes kunderne, skal være inden for rammerne af ISO 27001. Sikkerhedsudvalget består p.t. af følgende medlemmer:

- CEO, Stefan Rosenlund
- CTO, Ole P. Jensen
- Chief Legal Officer, Bo Brandt Stisen
- CISO, Jakob Flink Schwartz

Gruppen mødes én gang årligt for at fastsætte og følge op på målsætninger i relation til it-sikkerheden.

3.4.5 Fysisk sikkerhed

Kontrolmål 3: Fysisk adgang og sikkerhed og 4: Sikring mod miljømæssige hændelser

Fysisk adgangskontrol og sikring

Formål

Den fysiske adgang til systemer, data og andre it-ressourcer er begrænset til personer med godkendt behov for adgang.

Anvendte procedurer og kontroller

Adgang til bygningen er kontrolleret via nøgle og nøglekort, som er udleveret til Zitcom A/S' personale med arbejdsmæssigt behov.

Datacenteret er hævet over grundniveau, og døren ind til serverrummet samt porten til området er sikret med elektronisk låsemekanisme/alarmsystem, som kun kan slås fra med registrerede nøglekort. Alarmsystemet alarmerer vagten ved forsøg på indbrud. Der foretages årligt kontrol af, at kun personer med et arbejdsrelateret behov har adgang til serverrum.

Tidspunkt for udførelse af kontrollen

Der sker en periodisk gennemgang af nøglekortholdere minimum én gang om året samt ved udskiftning af personale.

Hvem udfører kontrollen?

Driftsafdelingen.

Kontroldokumentation

Udskrift af nøglekort fra alarmsystemet.

Sikring mod miljømæssige hændelser

Formål

It-udstyr er beskyttet mod miljømæssige hændelser som strømsvigt og brand.

Anvendte procedurer og kontroller

Datacenterets serverrum er beskyttet mod følgende miljømæssige hændelser:

- Strømsikring
- Brandsikring
- Klimahændelser

På alt kritisk it-udstyr er strøm sikret med en UPS-installation og en nødstrømsgenerator. I datacenteret er der etableret røg- og temperaturfølere, der er koblet sammen med det centrale overvågningssystem. Datacenteret er endvidere forsynet med automatisk brandbekæmpelsesudstyr (der aktiveres ved for høje værdier på enten røg eller varme). Der er indgået aftale med leverandør om at udføre løbende service på disse anlæg.

Varmeudviklingen i centeret reguleres gennem det fuldautomatiske kølesystem, som sikrer den korrekte temperatur og luftfugtighed til sikring af stabil drift og lang holdbarhed på det anvendte it-udstyr. Der udføres løbende service på anlægget.

Tidspunkt for udførelse af kontrollen

Løbende visuel inspektion af teknik- og serverum samt årligt serviceeftersyn.

Hvem udfører kontrollen?

Driftspersonalet med input fra leverandører.

Kontroldokumentation

Kontrol-/serviceskemaer opdateres og gemmes i wiki-systemet.

3.4.6 Styring af kommunikation med kunder

Kontrolmål 1: Driftsafvikling

Service Desk og Zitcom-support

Formål

Der udføres tilfredsstillende support for kunder, der kontakter Service Desk, herunder at der ydes den aftalte support i det aftalte tidsrum.

Anvendte procedurer og kontroller

Service Deskens håndtering af de enkelte kunder er baseret på et sæt skriftlige procedurer på de områder, der er aftalt med kunden. Procedurerne udarbejdes af Service Desk i et tæt samarbejde med kunden samt eventuelt tredjepartsleverandører til kunden. Support til bruger sker via e-mail, telefon og eventuelle fjernstyringsværktøjer.

Tidspunkt for udførelse af kontrollen

Service Desk gennemgår sager, der afventer løsning.

Hvem udfører kontrollen?

Kontroller udføres af Service Desk.

Kontroldokumentation

Dokumentation for henvendelser og udførelse af opgaver for kunderne sker i Zitcom A/S' sagsstyrings-system.

Incident-håndtering

Formål

Der gennemføres en betryggende incident-håndtering ud fra de indgåede aftaler med kunder.

Anvendte procedurer og kontroller

Zitcom anvender et sagsstyringssystem til registrering og håndtering af incidents, og der noteres følgende i sagen:

- Fejl
- Hvad der er gjort for afhjælpning af fejl
- Hvem der har udført opgaver
- Tidsstempling for, hvad tid der er noteret i sagen
- Tidsregistrering (om det er ifølge driftsaftale, eller det skal faktureres)
- Prioritering af fejlen

Ledelsen af driftsafdelingen er ansvarlig for overvågning af, at indkomne henvendelser i Service Desk prioriteres og tildeles ressourcer, samt at incident-håndtering gennemføres i overensstemmelse med de indgåede kundeaftaler.

Tidspunkt for udførelse af kontrollen

Incident-håndtering sker inden for de aftalte SLA-tider med kunderne.

Hvem udfører kontrollen?

Håndteringen af incidents udføres af Zitcom A/S' driftsafdeling, og uden for normal arbejdstid udføres den af bagvagten.

Kontroldokumentation

Dokumentation for incidents og udførelse af incidents for kunderne sker i Zitcom A/S' sagsstyringssystem.

DDoS-beskyttelse

Formål

Formålet med DDoS-beskyttelse er at kunne filtrere eller afvise den ondsindede trafik.

Anvendte procedurer og kontroller

Zitcom anvender DDoS-beskyttelse i flere lag. Der er konstant overvågning af pakkemængder og båndbredde, og der kigges efter mønstre. Derefter kan forskellige filtre aktiveres for at afvise de ondsindede pakker.

Tidspunkt for udførelse af kontrollen

DDoS-beskyttelseskontrollen udføres, når infrastrukturen er under angreb.

Hvem udfører kontrollen?

Netværksafdelingen har ansvaret for overvågning og administration af DDoS-beskyttelsen.

Kontroldokumentation

Dokumentation for at DDoS-beskyttelsessystemet er aktiveret, og man kan se, at Zitcom A/S' IP-adresser er dækket.

3.4.7 Backup

Kontrolmål 2: Backup[2]

Formål

Data sikkerhedskopieres og opbevares, så de kan reetableres i overensstemmelse med gældende SLA-krav. Zitcom kontrollerer, om backup udføres fejlfrit, og ved fejl i backup, at der udføres en vurdering af fejl og opfølgning på eventuel fejlretning.

Anvendte procedurer og kontroller

Der er udarbejdet en beskrivelse af backupproceduren. Backupproceduren er en del af den daglige kørsel og er således automatiseret i backupsystemet. Manuelle rutiner i forbindelse med backup er beskrevet i driftsprocedurerne. I forbindelse med backup anvendes underleverandøren GlobalConnect A/S til opbevaring af daglig kopi. Processen omkring backup varetages af Zitcom. Der er etableret kontroller, som sikrer, at backup foretages struktureret.

Der er følgende backupcyklus:

- Dagligt: backup af nye eller ændrede data
- Ugentligt: fuld backup af alle data og systemmiljøer

Backup opbevares, således at mindst én backup er fysisk placeret andetsteds end produktionsdata. Der foretages mindst én gang årligt en test af, at tilfældigt udvalgte servere kan genskabes på baggrund af backupdata, og herudover finder restore af data sted i forbindelse med henvendelse fra kunderne.

Tidspunkt for udførelse af kontrollen

Der er etableret automatisk backup, og der gennemføres restore-test minimum én gang årligt.

Hvem udfører kontrollen?

Driftsafdelingen forestår den daglige kontrol af backuplogs.

Kontroldokumentation

Kontrol af fejlede jobs udføres i Zitcom A/S' sagsstyringssystem.

3.4.8 Drift og overvågning

Kontrolmål 1: Driftsafvikling

Formål

Der udføres overvågning af, at aftalte services er tilgængelige, samt at nødvendige jobs og kørsler, såvel online som batch, afvikles rettidigt og korrekt. Afviklingen af jobs og kørsler overvåges af Zitcom.

Anvendte procedurer og kontroller

Zitcom har etableret et sæt af skriftlige driftsprocedurer på alle væsentlige driftsaktiviteter, som dels er afstemt med Zitcom A/S' krav og den tilhørende it-sikkerhedspolitik, dels med de generelle forretningsbetingelser. Driftsprocedurerne er udarbejdet af driftsafdelingen og omfatter den aftalte drift og overvågning af systemmiljøerne.

[2] Opbevaring af backup er ikke inkluderet i denne rapport, da dette er håndteret af serviceleverandør.

Konstaterede fejl i udførte kontroller og eventuelle fejl fra overvågningssystemet korrigeres hurtigst muligt. Zitcom informerer løbende om omfanget og konsekvenserne af de konstaterede fejl. Afvikling af batchjobs logges automatisk, således at der kan foretages opfølgende kontrol. Servere overvåges ved hjælp af monitoreringssoftware.

Følgende funktionsområder har adgang til kundernes it-systemer: Service Desk-medarbejdere og drifts-medarbejdere.

Tidspunkt for udførelse af kontrollen

Overvågning og opfølgning udføres 24/7 eller i primær driftstid ifølge SLA-aftalen med den enkelte kunde.

Hvem udfører kontrollen?

Kontroller udføres af Zitcom A/S' driftsafdeling, og uden for normal arbejdstid udføres den af forvagten.

Kontroldokumentation

Den automatiske overvågning dokumenteres i Zitcom A/S' asset management-system.

3.4.9 Adgangskontrol

Kontrolmål 6: It-sikkerhedsadministration og 7: Logisk sikkerhed

Formål

Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med Zitcoms retningslinjer.

Adgangen deles op i tre områder:

- Kundernes medarbejdere
- Zitcom A/S' medarbejdere
- Medarbejdere hos tredjeparter

Anvendte procedurer og kontroller

Det er kundens ansvar at sikre en betryggende adgang til de enkelte systemmiljøer, herunder at autentificere eventuel adgang til tredjepartsleverandør. Zitcom forestår den tekniske oprettelse ud fra kundernes anvisninger, men det er kundens ansvar at kontrollere, at Zitcom har oprettet brugerne i henhold til anvisningerne.

For Zitcoms interne brugere er informationssikkerhedsmæssige roller og ansvarsområder fordelt, og medarbejderne bliver gjort bekendt med deres ansvar ved tiltrædelse.

Rettigheder til interne brugere hos Zitcom oprettes efter formel godkendelse. For interne medarbejdere er der udarbejdet formelle retningslinjer vedrørende sletning af brugere. Disse sikrer bl.a., at en fratrådt medarbejder ved arbejdsophør hos Zitcom spærres for login. Der foretages ligeledes en årlig kontrol af validiteten af de oprettede brugerkonti på Zitcoms interne systemer.

Der er defineret specifikke krav til passwordkvalitet med hensyn til længde, kompleksitet, udskiftningshyppighed og historik og med hensyn til logningsniveau.

Navngivningen og opsætningen af brugerkonti til medarbejdere på de interne domæner er således, at disse brugerkonti til enhver tid vil være personhenførbare.

Nye Windows-servere, der sættes i drift, er konfigureret i overensstemmelse med den aktuelle baseline, som er defineret i en række scripts. Denne baseline indeholder specifikke krav til passwords, patchning og logning. Ansvaret for kontrol af, at konfigurationsbaselinen er blevet opsat på servere, overgår til kunder ved idriftsættelse.

Tidspunkt for udførelse af kontrollen

Kontrollen vedrørende brugeroprettelser sker, hver gang Zitcom har en intern ansættelse eller fratrædelse. Kontrollen vedrørende inaktive brugere og brugere med administrative rettigheder foregår årligt.

Hvem udfører kontrollen?

Driftsafdelingen ved Zitcom har ansvaret for, at adgangsprocedurerne bliver overholdt.

Kontroldokumentation

Dokumentation vedrørende Zitcom A/S' medarbejdere gemmes i et relevant værktøj.

3.4.10 Anskaffelse og vedligeholdelse af systemsoftware

Kontrolmål 8: Systemsoftware

Formål

Systemsoftware vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med virksomhedens behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.

Anvendte procedurer og kontroller

For Windows-servere, som Zitcom har driftsansvaret for, indhentes fyldestgørende systemdokumentation efter behov. Zitcom har fastsat procedurer for anskaffelse og opdatering af systemsoftware på Windows-platformene. Til Windows- og Linux-platformene hentes opdateringer, og de udrulles automatisk på serverne. Netværksudstyr opdateres ved behov, og der defineres fall-back-planer, inden opdatering gennemføres.

Tidspunkt for udførelse af kontrollen

Kontrollen for opdateringer sker via WSUS (Windows) eller Package Manager (Linux).

Hvem udfører kontrollen?

Driftsafdelingen er ansvarlig for udførelse af opdateringer og kontrol heraf.

Kontroldokumentation

Ud over dokumentation i WSUS fremgår installerede patches på den enkelte server.

3.4.11 Beredskabsplan

Kontrolmål 9: Beredskabsplanlægning

Formål

En plan for genoptagelse af systemmiljøer hos Zitcom, efter en katastrofe er indtruffet.

Anvendte procedurer og kontroller

Zitcom har etableret en beredskabsplan, som overordnet fastsætter retningslinjer for, hvordan en katastrofesituation skal håndteres. Beredskabsplanen godkendes årligt af Zitcom A/S' ledelse.

Beredskabsplanen indeholder beskrivelse af følgende områder:

- Information om beredskabsplanen
- Organisering og kontrakter
- Oversigt over infrastruktur og tolerancegrænser for afbrydelse af forretningsprocesser
- Reaktionsplan, herunder klassificering af en nødsituation og regler for eskalering
- Krisestyringsplan, herunder retningslinjer for:
    - Initiering af beredskab
    - Skades- og situationsvurdering
    - Fastlæggelse af handlinger
    - Implementering og logistik
- Nøddrift og reetableringsplan

Beredskabsplanen revurderes løbende og mindst én gang årligt, og der gennemføres en verifikation af den etablerede backup gennem en restore-test. Der gennemføres ikke større reetableringsøvelser eller en fuld reetablering af hele systemmiljøer.

Tidspunkt for udførelse af kontrollen

Beredskabsplanen gennemgås og risikovurderes mindst én gang årligt.

Hvem udfører kontrollen?

Sikkerhedsgruppen udfører den årlige gennemgang og tilpasning af beredskabsplanen.

Kontroldokumentation

Der er versionsstyring af beredskabsplanen. Der foreligger dokumentation for handlinger foretaget i forbindelse med 'dry run' af beredskabsplan.

3.4.12 Styring af leverandørydelser

Kontrolmål 10: Leverandørydelser – Der er etableret kontroller, som sikrer, at revisionserklæringer fra eksterne leverandører bliver gennemgået for afvigelser.

Formål

At sikre, at eventuelle afvigende kontroller hos eksterne leverandører bliver mitigeret.

Anvendte procedurer og kontroller

Der er kontrol med revisionserklæringer fra leverandører, som sikrer, at disse bliver gennemgået periodisk, samt at eventuelle afvigelser i kontroller hos leverandører bliver mitigeret, hvis relevant, hos Zitcom.

Tidspunkt for udførelse af kontrollen

Årlig gennemgang af revisionserklæringer.

Hvem udfører kontrollen?

Ledelsen.

Kontroldokumentation

Oversigt over leverandørydelser og kontrollen heraf.

3.4.13 Forhold, som skal iagttages af kunderne

Levering af serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på Zitcom A/S' standardbetingelser. Det bevirker, at indgåede kundeaftaler, som på de leverede serviceydelser er forskellige fra Zitcom A/S' standardbetingelser, ikke er omfattet af nærværende erklæring. Kunderne bør vurdere, om denne erklæring kan anvendes i forbindelse med vurdering af de generelle it-kontroller hos Zitcom A/S relateret til drifts- og hosting-ydelser leveret fra Zitcom A/S til kunden. Kunderne bør selv afdække eventuelle andre risici, der vurderes som væsentlige.

Brugeradministration

Zitcom giver adgang og tildeler rettigheder i overensstemmelse med kundernes instrukser, i takt med at disse bliver indmeldt gennem Service Desk. Zitcom er ikke ansvarlig for, at informationer om brugerne er korrekte, og det er således kundernes eget ansvar at sikre, at de tildelte adgange og rettigheder til systemer og applikationer sker i overensstemmelse med kundernes egne forventninger til en betryggende funktionsadskillelse i de systemmiljøer, som hostes og driftes hos Zitcom. Såfremt det er ønsket, kan kunden selv oprette brugere på de enkelte servere – kontroller relateret til denne proces er kundernes eget ansvar.

Konfiguration af sikkerhed

Zitcom har etableret intern sikkerhed i forbindelse med levering af drifts- og hosting-ydelser til sine kunder. Etablering og konfiguration af sikkerheden på servere er udelukkende kundens ansvar, ligesom det er kundernes ansvar at sikre, at sikkerhedskonfigurationer er i overensstemmelse med det ønskede sikkerhedsniveau for den enkelte kunde.

Efterlevelse af relevant lovgivning

Zitcom er ikke ansvarlig for applikationer, som afvikles på det hostede udstyr. Det er således kundernes ansvar, at der er etableret betryggende kontroller i brugerapplikationerne, herunder at disse understøtter efterlevelse af bogføringsloven, persondataloven og/eller anden relevant lovgivning.

4 Beskrivelse af kontrolmål, kontroller samt resultat af udført arbejde

I dette afsnit beskrives de af Zitcom A/S definerede kontrolmål og de kontroller, som sikrer opnåelse af de enkelte kontrolmål. Herudover beskrives de af EY udførte faktiske tests af Zitcom A/S' kontroller samt resultaterne af de udførte tests.

4.1 Formål og omfang

EY's test omfatter udførelse af handlinger for at opnå bevis for oplysningerne i Zitcom A/S' beskrivelse af sit system samt for kontrollernes udformning og funktionalitet.

De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risici for, at beskrivelsen ikke er dækkende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Test af kontroller er gennemført i overensstemmelse med ISAE 3402, Erklæring med sikkerhed om kontroller hos en serviceleverandør.

De udførte tests af kontrollernes design og implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af Zitcom A/S. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos kunderne er ikke omfattet af gennemgangen.

De udførte tests af design og implementering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af passende personale hos Zitcom A/S. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3 Resultat af tests

Resultatet af tests af kontroller omfatter en tilkendegivelse af, hvorvidt der i forbindelse med den beskrevne test af kontrollen er konstateret afvigelser. En afvigelse i en kontrol foreligger, når:

1. en kontrol er udformet, implementeret eller anvendt på en sådan måde, at den ikke rettidigt kan forebygge eller opdage og korrigere fejl i processer eller systemer, eller
2. der mangler en kontrol, der er nødvendig for rettidigt at forebygge eller opdage og korrigere fejl i processer eller systemer.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
1	**Driftsafvikling: Kontrolmål – Der er etableret kontroller, som sikrer, at driftsafvikling overvåges, samt at der følges op på incidents.**		
1.1	**Batch og driftsafvikling – skriftlige procedurer** Afvikling af batchjobs bliver logget automatisk, således at der kan foretages opfølgende kontrol.	Vi har inspiceret procesdokumentation for afvikling af batchjobs. Vi har stikprøvevis inspiceret dokumentation for afvikling af daglige batchjobs samt dokumentation for håndtering af fejl opstået i denne forbindelse.	Ingen afvigelser konstateret.
1.2	**Driftsovervågning – generelt** Servere overvåges ved hjælp af monitoreringssoftware.	Vi har stikprøvevis inspiceret, at der er etableret overvågning af serverne. Vi har ved inspektion af incident management-systemet konstateret, at eventuelle afvigelser registreres heri.	Ingen afvigelser konstateret.
1.3	**Incident-håndtering** Incidents registreres og prioriteres i sagsstyringssystemet, og ansvaret for løsning af den enkelte hændelse placeres hos en medarbejder.	Vi har stikprøvevis inspiceret registrering i sagsstyringssystemet med henblik på at konstatere, om registreringerne omfatter prioritering og ansvarlig, og om sagen løses i overenstemmelse med den aftalte SLA.	Ingen afvigelser konstateret.
1.4	**DDoS-beskyttelse** Der er etableret DDoS-beskyttelse, som kan aktiveres automatisk eller efter behov.	Vi har forespurgt til procedurer for overvågning af netværkstrafik i forhold til detektering og mitigering af DDoS-angreb. Vi har inspiceret dokumentation for aktivering af automatisk DDoS-beskyttelse.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
2	**Backup: Kontrolmål – Der er etableret kontroller, som sikrer, at backup foretages struktureret, ligesom læsbarheden af backup sikres.**		
2.1	**Backup – strategi** Der er etableret en backupstrategi baseret på den indgåede SLA med de enkelte kunder.	Vi har inspiceret backupstrategien for, om den i tilstrækkelig grad afdækker backupkrav ud fra defineret SLA.	Ingen afvigelser konstateret.
2.2	**Backup – konfiguration** Backup af kundedata tages med udgangspunkt i en standardkonfiguration, som omfatter automatisk backup af kundeservere.	Vi har stikprøvevis inspiceret, at servere er konfigureret til automatisk backup.	Ingen afvigelser konstateret.
2.3	**Backup – ekstern opbevaring** Sikkerhedskopier spejles til underleverandør for at sikre, at der altid er produktionsdata tilgængeligt i tilfælde af hændelser, der kunne kræve reetablering af systemer på en anden lokation.	Vi har inspiceret dokumentation for, at sikkerhedskopi hos Zitcom spejles til ekstern serviceleverandør. Vi har inspiceret serviceleverandørs ISAE 3402-erklæring vedrørende generelle it-kontroller og påset, at kontroller vedrørende backup er anført uden afvigelser.	Ingen afvigelser konstateret.
2.4	**Backup – restore-test** Der foretages en årlig restore-test af mindst én tilfældigt udvalgt server.	Vi har stikprøvevis inspiceret dokumentation for, at der er udført restore-test af en kundeserver.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
3	**Fysisk adgang: Kontrolmål – Der er etableret kontroller, som sikrer, at adgangen til it-faciliteterne tildeles udelukkende til personer med et arbejdsbetinget behov herfor.**		
3.1	**Fysisk adgang – adgang til serverrum** Adgang til bygningen er kontrolleret via nøgle og nøglekort. Der foretages årlig kontrol af, at kun personer med et arbejdsrelateret behov har adgang til serverrummet på Sverigesvej.	Vi har observeret fysisk sikring af adgang til serverrummet på Sverigesvej. Vi har inspiceret dokumentation for årlig gennemgang af medarbejdere med adgang til Zitcom A/S' datacenter på Sverigesvej.	Ingen afvigelser konstateret.
4	**Sikring mod miljømæssige hændelser: Kontrolmål – Der er etableret kontroller, som sikrer kritisk it-udstyr mod miljømæssige hændelser.**		
4.1	**Fysisk sikkerhed – strømsikring** Serverrummet er forsynet med UPS-anlæg og nødstrømgenerator. Der er yderligere indgået kontrakt om et periodisk syn af UPS-anlægget og generator.	Vi har observeret, at der er opsat nødstrøm i datacenteret. Vi har inspiceret dokumentation for kvartalsmæssig vedligeholdelsesmæssig kontrol af nødstrømsanlæg. Vi har observeret UPS-anlæg i datacenteret. Vi har inspiceret dokumentation for årlig vedligeholdelsesmæssig kontrol af UPS-anlæg.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
4 2	**Fysisk sikkerhed – brandsikring** Serverrum er forsynet med røg- og temperaturføler, der er koblet sammen med det centrale brandovervågningssystem. Serverrum er yderligere forsynet med brandslukning og detektion (både røg og temperatur). Der er yderligere indgået kontrakt om en periodisk vedligeholdelse af brandslukningsanlægget.	Vi har observeret, at der er opsat brandovervågning, herunder røg- og temperatursensorer, og at der i datacenteret er opsat automatisk brandslukningsanlæg. Vi har inspiceret dokumentation for vedligeholdelsesmæssig kontrol af Inergen-anlæg.	Ingen afvigelser konstateret.
4.3	**Fysisk sikkerhed – klimaovervågning og køling** Serverrummet er forsynet med automatisk regulerende køling for at sikre en stabil drift. Der er yderligere indgået kontrakt om en periodisk vedligeholdelse af kølesystemet.	Vi har observeret, at der er opsat køling og klimaovervågning i datacenteret. Vi har inspiceret dokumentation for årlig vedligeholdelses-mæssig kontrol af køleanlæg.	Ingen afvigelser konstateret.
4.4	**Fysisk sikkerhed – indretning** Serverrummet er indrettet, således at der ikke forefindes faldstammer, vandrør m.v., som vil kunne forårsage skader på maskiner, der anvendes til kritiske systemer og data. Desuden er gulvet hævet i serverrummet.	Vi har inspiceret indretningen af datacenteret og konstateret, at gulvet er hævet, samt at der ikke forefindes faldstammer, vandrør eller andet, som vil kunne forårsage skade på kritisk udstyr.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
5	**IT Governance: Kontrolmål – Der er etableret kontroller, som sikrer, at ledelsen har fastlagt niveauet for virksomhedens it-sikkerhed med udgangspunkt i en risikoanalyse.**		
5.1	**It-sikkerhedspolitik** Der er udarbejdet en it-sikkerhedspolitik, som bliver ajourført mindst én gang om året.	Vi har inspiceret senest ajourførte it-sikkerhedspolitik og konstateret, at denne er gennemgået og opdateret inden for erklæringsperioden.	Ingen afvigelser konstateret.
5.2	**It-risikoanalyse** Zitcom har udarbejdet it-risikoanalyse for kritiske systemer, der anvendes i den daglige drift. Der gennemføres en årlig revurdering af, om forhold til risiko og trusler fortsat er gældende, eller om der er behov for ændring til it-risikoanalysen.	Vi har inspiceret senest ajourførte it-risikoanalyse og konstateret, at denne er opdateret i erklæringsperioden.	Ingen afvigelser konstateret.
6	**Sikkerhedsadministration: Kontrolmål – Der er etableret kontroller, som sikrer, at adgangstildeling til systemer og programmer administreres hensigtsmæssigt til sikring mod uautoriserede og utilsigtede handlinger.**		
6.1	**Brugerrettigheder – oprettelser** Interne Zitcom-brugere oprettes gennem faste oprettelsesprocedurer og på baggrund af forespørgsel fra leder.	Vi har inspiceret proceduren for håndtering af interne Zitcom-brugere. Vi har stikprøvevis inspiceret, at oprettelse af Zitcom-brugere er sket på baggrund af sag i sagsstyringssystemet, og at oprettelsen er bestilt eller godkendt af en leder.	Ingen afvigelser konstateret.
6.2	**Brugerrettigheder – nedlæggelser** Nedlæggelser af interne brugere bliver gjort før eller på fratrådte medarbejders fratrædelsesdato. Dette dokumenteres i sagsstyrings-systemet.	Vi har stikprøvevist inspiceret, at fratrådte brugeres konti er lukket rettidigt.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
6.3	**Brugerrettigheder – privilegerede rettigheder** Privilegerede rettigheder er begrænset til ansatte hos Zitcom med et arbejdsbetinget behov herfor, og denne adgang bliver revurderet én gang årligt.	Vi har inspiceret dokumentation for årlig kontrol af privilegerede brugere i de interne brugerdatabaser.	Ingen afvigelser konstateret
6.4	**Brugerrettigheder – periodisk opfølgning** Der foretages mindst én gang årligt opfølgning på validiteten af brugere oprettet i de interne brugerdatabaser hos Zitcom.	Vi har inspiceret dokumentation for årlig kontrol af personhenførbare brugere i de interne brugerdatabaser.	Ingen afvigelser konstateret.
6.5	**It-sikkerhedslogning** Der er opsat krav til logning af sikkerhedsmæssige hændelser på Zitcom A/S' interne domæne. Sikkerhedsmæssige incidents håndteres via incident management-processen.	Vi har inspiceret dokumentation for opsætning af logning i de interne brugerdatabaser. Vi har stikprøvevis inspiceret incidents i incident management-systemet og konstateret, at eventuelle afvigelser registreres heri.	Ingen afvigelser konstateret.
6.6	**It-sikkerhedsorganisation** It-sikkerhedsmæssige roller og ansvarsområder er fordelt, og medarbejderne bliver gjort bekendt med deres ansvar ved tiltrædelse.	Vi har inspiceret en oversigt over roller i organisationen og konstateret, at denne indeholder oplysninger om, hvem der har hvilke ansvarsområder i organisationen. Vi har ved forespørgsel af en stikprøve af medarbejdere konstateret, at de er bekendte med deres informations-sikkerhedsmæssige roller og ansvarsområder.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
7 Logisk sikkerhed: Kontrolmål – Der er etableret kontroller, som sikrer, at adgange til systemer og data sker via anvendelse af passwords og brugerprofiler.			
7.1	**Anvendelse af passwords** Autentificering af brugere sker via Windows AD, hvor passwordkrav er defineret.	Vi har inspiceret adgangsstyringspolitikken. Vi har inspiceret konfigurationen af krav til passwords på de interne brugerdatabaser hos Zitcom A/S.	Ingen afvigelser konstateret.
7.2	**Anvendelse af brugerprofiler** Brugere er oprettet i de interne brugerdatabaser og anvender individuelle brugerprofiler på det interne netværk. Anvendelse af "Administrator" kan spores til den person, der har anvendt kontoen.	Vi har stikprøvevis inspiceret, at brugerprofiler, som benyttes af medarbejdere på relevante systemer og platforme, er personhenførbare. Vi har forespurgt til sporbarhed ved anvendelse af "Administrator" på kundeservere.	Ingen afvigelser konstateret.
7.3	**Konfigurationsbaseline – revurdering** Der foretages en årlig revurdering af konfigurationsbaselinen.	Vi har forespurgt til proceduren for årlig gennemgang af konfigurationsbaselines.	Ingen afvigelser konstateret.
7.4	**Konfigurationsbaseline – kontrol** Nye Windows-servere, der sættes i drift, er konfigureret i overensstemmelse med den aktuelle baseline, som er defineret i en række scripts. Denne baseline indeholder specifikke krav til passwords, patchning og logning.	Vi har forespurgt til proceduren for opsætning af en ny Windows-server. Vi har inspiceret opsætningen af én ny Windows-server med henblik på at konstatere, om password, patchning og logning er opsat i overensstemmelse med den aktuelle baseline.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
8	**Systemsoftware: Kontrolmål – Der er etableret procedurer og kontroller, som sikrer, at servere opdateres i nødvendigt omfang.**		
8.1	**Systemsoftware – patch management** Der foretages en løbende opdatering af Windows- og Linux-servere (patch management).	Vi har inspiceret Zitcom A/S' patch management-procedurer for Windows og Linux. Vi har stikprøvevis inspiceret dokumentation for opdatering af Windows- og Linux-servere, hvor Zitcom A/S har ansvaret for patch management.	Ingen afvigelser konstateret.
8.2	**Systemsoftware – fall-back** Der defineres fall-back-planer før opdatering af systemsoftware, hvor dette er relevant.	Vi har stikprøvevis inspiceret, at ændringer, der havde behov for en fall-back-plan, også havde én defineret i incident-håndterings-systemet.	Ingen afvigelser konstateret.
8.3	**Systemsoftware – timing** Nye opdateringer til Windows installeres inden for foruddefinerede servicevinduer.	Vi har stikprøvevis inspiceret, at nyeste opdateringer til operativsystemer er idriftsat på servere.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Resultat af test
9	**Beredskabsplanlægning: Kontrolmål – En beredskabsplan er udarbejdet og godkendt af ledelsen. Der foretages årlig test af beredskabsplanen.**		
9.1	**Udarbejdet beredskabsplan** Der er udarbejdet en beredskabsplan, som mindst én gang om året bliver opdateret og godkendt af Zitcom A/S' ledelse.	Vi har inspiceret beredskabsplanen og konstateret, at denne er opdateret og godkendt i 2017.	Ingen afvigelser konstateret.
9.2	**Test af beredskabsplan** Der udføres beredskabsøvelser mindst én gang årligt. I forbindelse med beredskabsøvelser bliver der ført log over hændelsesforløbet.	Vi har inspiceret beredskabs- og sikkerhedshændelsespolitikken. Vi har inspiceret dokumentation for hændelsesforløb og playbooks i forbindelse med tre beredskabsøvelser udført i perioden.	Ingen afvigelser konstateret.
10	**Leverandørstyring: Kontrolmål – Der er etableret kontroller, som sikrer, at revisionserklæringer fra eksterne leverandører bliver gennemgået for afvigelser.**		
10.1	**Styring af leverandørydelser** Revisionserklæringer fra underleverandører bliver gennemgået årligt af ledelsen, og eventuelle kontrolafvigelser bliver noteret.	Vi har inspiceret dokumentation for gennemgang og anførsel af kontrolafvigelser ved Zitcom A/S' gennemgang af deres underleverandørers revisionserklæringer.	Den gennemgåede erklæring for GlobalConnect A/S dækker perioden frem til 31. december 2016. Herudover, ingen afvigelser konstateret.