Zitcom A/S

ISAE 3402 Type 2

Uafhængig revisors erklæring om generelle it-kontroller relateret til drifts- og hosting-ydelser i perioden 1. januar 2016 til 31. december 2016

Indholdsfortegnelse

ZITCOM

1. Ledelsens 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 2016, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunden selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskab.

Zitcom A/S anvender Front-safe 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 Front-safe A/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 2016 til 31. december 2016. 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 2016 til 31. december 2016

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

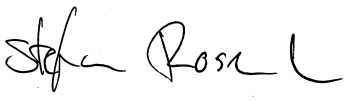
(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2016 til 31. december 2016. Kriterierne for denne udtalelse var, at:

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

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

(vi) 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 2016 til 31. december 2016.

Skanderborg, den 7. februar 2017
Zitcom A/S



Stefan Rosenlund

adm. direktør

2. Uafhængig revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet

Til: Ledelsen hos Zitcom A/S

Vi har fået som opgave at afgive erklæring om Zitcom A/S' beskrivelse af de generelle it-kontroller relateret til de af Zitcom A/S udbudte drifts- og hosting-ydelser leveret til kunder i perioden fra 1. januar 2016 til 31. december 2016 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Zitcom A/S anvender Front-safe 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 Front-safe A/S. Erklæringen er udarbejdet efter partielmetoden vedrørende Front-safe A/S, og vores test af kontroller omfatter ikke kontroller hos Front-safe A/S.

Zitcom A/S' ansvar
Zitcom A/S er ansvarlig for udarbejdelsen af beskrivelsen i afsnit 3 og tilhørende udtalelse i afsnit 1, 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 effektiviteten af 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. Vi har endvidere overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Ernst & Young Godkendt Revisionspartnerselskab er underlagt ISQC 1[1] og anvender således 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.

Vores 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 overholder, planlægger og udfører vores handlinger for at opnå

[1] "ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver"

høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er dækkende, 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.

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

Begrænsning 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 aspekter ved de generelle it-kontroller relateret til ydelserne, som hver enkelt kunde måtte anse vigtigt 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. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Zitcom A/S' udtalelse.

Det er det vores opfattelse, at:

(a) beskrivelsen af de generelle it-kontroller relateret til de af Zitcom A/S udbudte drifts- og hostingydelser, således som de var udformet og implementeret i hele perioden fra 1. januar 2016 til 31. december 2016, i alle væsentlige henseender er retvisende

(b) 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 2016 – 31. december 2016

(c) 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 2016 – 31. december 2016.

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af afsnittet "Beskrivelse af kontrolmål, kontroller samt resultat af udført arbejde".

Tiltænkte brugere og formål
Denne erklæring er udelukkende tiltænkt de kunder, der har anvendt eller anvender Zitcoms 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 fejl i deres regnskaber.

København, den 7. februar 2017

Ernst & Young
Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Claus Thaudahl Hansen
statsaut. revisor

Per Højmark
statsaut. revisor

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 den danske standard 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, i det omfang det kan medføre en risiko for væsentlige fejl i hosting-kunders it-drift for perioden 1. januar 2016 til 31. december 2016.

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.

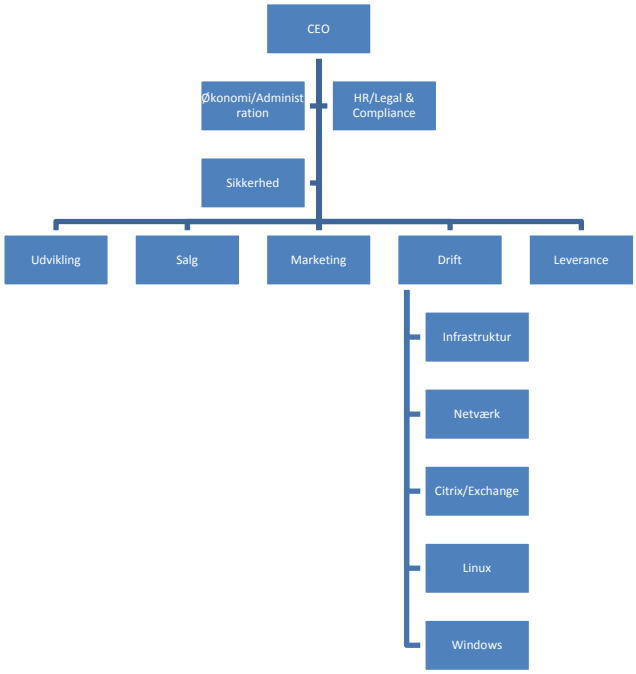
Zitcom arbejder ud fra en stræben efter at levere løsninger, der kvalitets- og servicemæssigt differentierer sig fra størstedelen af det resterende hosting-marked. Med mange års erfaring på markedet har Zitcom erfaret, at graden af kunders tilfredshed har direkte sammenhæng med niveauet på leverandørens 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) referer 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.

3.5 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 2016 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[2]
6. Drift og overvågning
7. Adgangskontrol

3.6 Etableret kontrolmiljø

Hvert enkelt område er detaljebeskrevet i de efterfølgende afsnit.

3.7 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.

[2] Opbevaring af backup er ikke inkluderet i denne rapport, da dette er håndteret af Front-safe A/S

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.

Hvem udfører kontrollen?
Den årlige gennemgang udføres af Sikkerhedsudvalget.

Kontroldokumentation
Der er versionsstyring af it-sikkerhedspolitikken.

3.7.1 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 indenfor 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.

3.7.2 Fysisk sikkerhed

Kontrolmål: 3 Fysisk adgang og sikkerhed & 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 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, som kun kan låses op med registrerede nøglekort. Endelig er der etableret et alarmsystem, som alarmerer vagten ved forsøg på indbrud.

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, som kan holde systemerne med strøm, indtil en generator automatisk er startet og klar. 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 udføres 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.

3.7.3 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 dagligt 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' sagsstyringssystem.

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)

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?
Håndteringerne 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.

3.7.4 Backup

Kontrolmål: 2 Backup[3]

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 udførlig 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 Front-safe A/S til opbevaring af daglig kopi. Processen omkring backup varetages af Zitcom.

Der erfølgende 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 servere kan genskabes på baggrund af backupdata – og herudover finder restore af data sted i forbindelse med henvendelse fra kunderne.

[3] Opbevaring af backup er ikke inkluderet i denne rapport, da dette er håndteret af Front-safe A/S

Tidspunkt for udførelse af kontrollen
Der udføres tjek af backuplogs i normal arbejdstid.

Hvem udfører kontrollen?
Driftsafdelingen forestår den daglige kontrol af backuplogs.

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

3.7.5 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 er afstemt med Zitcom A/S' krav og den tilhørende it-sikkerhedspolitik og dels med de generelle forretningsbetingelser. Driftsprocedurerne er udarbejdet af driftsafdelingen og omfatter den aftalte drift og overvågning af systemmiljøerne.

Der foreligger en række jobbeskrivelser for driftsafdelingen, hvor det er fastsat, hvilken overvågning og hvilke kontroller der udføres dagligt – ugentligt – årligt. Konstaterede fejl i udførte kontroller og eventuelle fejl fra overvågningssystemet korrigeres hurtigst muligt. Zitcom informerer løbende om omfanget og konsekvenserne af de konstaterede fejl.

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

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
Dokumentation for udførelse sker i Zitcom A/S' asset management system.

3.7.6 Adgangskontrol

Kontrolmål: 6 It-sikkerhedsadministration & 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.

Rettigheder til interne brugere hos Zitcom oprettes efter formel godkendelse af driftschefen. For interne medarbejdere er der udarbejdet formelle retningslinjer vedrørende sletning af brugere. Disse sikrer bl.a., at en fratrådt medarbejder ved arbejdsophør hos Zitcom afleverer nøgler og adgangskort, således at der ikke kan opnås fysisk adgang til bygningen, og vedkommendes bruger-id spærres for login. Der foretages ligeledes en årlig kontrol af validiteten af de oprettede brugerkonti på Zitcoms interne systemer.

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.

3.7.7 Anskaffelse og vedligeholdelse af infrastruktur

Kontrolmål: 8 Systemsoftware

Netværks- og kommunikationssoftware

Formål
Netværks- og kommunikationssoftware vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med behov, samt at ændringer testes og dokumenteres på tilfredsstillende vis.

Anvendte procedurer og kontroller
Zitcom har fuld dokumentation af netværksudstyr i sine datacentre.

Zitcom vurderer løbende behov for opdatering af firmware på netværks- og kommunikationssoftware. For at sikre en stabil drift vil der alene ske opdateringer, såfremt det er nødvendigt for at sikre kommunikationen. Inden ændringer foretages, tages backup af konfigurationsfilerne til netværkskomponenter, ligesom udskiftet udstyr beholdes i en karensperiode i tilfælde af, at nyt udstyr ikke fungerer korrekt eller optimalt. Væsentlige ændringer til netværkskonfigurationer foretages inden for de med kunderne aftalte servicevinduer.

Tidspunkt for udførelse af kontrollen
Kontrollen udføres i forbindelse med opdatering og ændring.

Hvem udfører kontrollen?
Netværksafdelingen har ansvaret for udførelse af opdateringer samt kontrol af funktionalitet.

Kontroldokumentation
Der laves dokumentation i Zitcom A/S' sagsstyringssystem omkring opgaver, der er udført på Zitcom A/S' netværksudstyr.

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. På Windows-platformen hentes opdateringer fra Microsoft, og de udrulles automatisk på serverne via Windows Server Update Services (WSUS). Vurderinger og tests sker ved, at der i forbindelse med servicevindue tages stilling til, om der er behov for de frigivne patches og fixes. Herefter lægges patch på mindre kritiske systemer, inden de lægges på alle systemer.

Tidspunkt for udførelse af kontrollen
Kontrollen for opdateringer sker via WSUS.

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.

3.8 Forhold, som skal iagttages af kundernes revisorer

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. Kundernes revisorer bør vurdere, om denne erklæring kan anvendes i forbindelse med vurdering af de generelle it-kontroller relateret til drifts- og hosting-ydelser leveret fra Zitcom A/S til kunden. Kunders revisorer 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 har tilrettelagt procedurer og kontroller, således at de områder, som er Zitcom A/S' ansvar, efterleves. 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 definerede kontrolmål og de kontroller, som sikrer opnåelse af de enkelte kontrolmål. Herudover beskrives de af EY udførte faktiske tests af Zitcoms 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 Zitcoms 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. 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 1. januar 2016 – 31. december 2016.

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. 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	Testresultat
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** Zitcom har etableret procedurer, der beskriver den daglige drift og udarbejder kontrollister med henblik på at dokumentere udførte driftskontroller.	Vi har inspiceret skriftlige driftsprocedurer, som sikrer, at de udførte driftskontroller dokumenteres. Vi har stikprøvevis inspiceret incidents og backupkontroller og undersøgt, om fejl og support er håndteret ud fra driftsprocedurer.	Ingen afvigelser konstateret.
1.2	**Driftsovervågning – generelt** Der er etableret overvågning af alle servere og relevante services. Afvigelser registreres i incident management-systemet.	Vi har stikprøvevis inspiceret, at der er installeret overvågning på serverne. Vi har ved inspektion af incident management-systemet konstateret, at eventuelle afvigelser registreres heri.	Ingen afvigelser konstateret.
1.3	**Incident-håndtering** Alle kundehenvendelser og afvigelser konstateret i driftsovervågningen registreres som en sag i sagsstyringssystemet. Henvendelserne prioriteres og tildeles de personer, som skal behandle sagen. Forløbet af sagen og løsningen dokumenteres i sagsstyringssystemet. Systemet monitorerer automatisk fremdrift i løsningen og lukningen af incidents ved automatiske påmindelser til driftspersonale.	Vi har stikprøvevis inspiceret, at incidents er blevet tildelt en relevant prioritet og ansvarlig. Vi har stikprøvevis inspiceret, at incidents løses inden for den i SLA'en definerede tidsramme, samt at der løbende via konfiguration i sagsstyringssystemet følges op på åbne sager, og at incidents dokumenteres i sagsstyringssystemet.	Ingen afvigelser konstateret.
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 med kunderne.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
2.2	**Backup – konfiguration** Backup af kundedata tages med udgangspunkt i en standardkonfiguration.	Vi har stikprøvevis inspiceret backupkonfigurationen og foretaget sammenholdelse med den udarbejdede backupbeskrivelse.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
2.3	**Backup – ekstern opbevaring** Backup spejles til en alternativ lokation for at sikre, at der altid er produktionsdata tilgængelig i tilfælde af hændelser, der kunne kræve reetablering af systemer på en anden lokation. Den sekundære lokation drives af Front-safe A/S, som er underleverandør til Zitcom.	Vi har modtaget en log over nedetid på den daglige overførsel til den eksterne lokation. Vi har stikprøvevis inspiceret, at der ikke har været væsentlige nedetider i erklæringsperioden.	Ingen afvigelser konstateret.
2.4	**Backup –restore-test** Der foretages test af, at backupdata kan anvendes til genetablering.	Vi har stikprøvevis inspiceret dokumentation for, at der i erklærings-perioden er udført test af restore af en række kundeservere.	Ingen afvigelser konstateret.
3	**Fysisk adgang: Kontrolmål – Der er etableret kontroller, som sikrer, at adgangen til it-faciliteterne tildeles udelukkende til personer med et arbejds-betinget behov herfor.**		
3.1	**Fysisk adgang – adgang til serverrum** Adgangen til serverrummet sikres med nøglekort, der skal aflæses for at låse døren op. Det er kun personer med arbejdsrelaterede behov, der får tildelt adgang.	Vi har inspiceret, at adgang til serverrummet kræver anvendelse af nøglekort. Vi har for en stikprøve af ansatte med adgang til serverrummet inspiceret, at denne adgang var tildelt i overensstemmelse med et arbejdsbetinget behov herfor.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
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 stabil strøm via UPS-anlæg og strømgenerator. Der er yderligere indgået kontrakt om et periodisk syn af UPS-anlægget og generator.	Vi har inspiceret, at der er opsat nødstrøm i datacenteret, og at der er foretaget en dokumenteret periodisk vedligeholdelse af løsningen. Vi har inspiceret, at der forefindes UPS-anlæg, og at der er foretaget dokumenteret periodisk service i løbet af erklæringsperioden.	Ingen afvigelser konstateret.
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 inspiceret, at der er opsat brandovervågning – herunder røg- og temperatursensorer, og at der i datacenteret er opsat automatisk brandslukningsanlæg, samt at der er foretaget periodisk vedligeholdelse af den samlede løsning.	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 inspiceret, at der er opsat køling i datacenteret, og at der er foretaget periodisk vedligeholdelse af løsningen.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
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.	Vi har inspiceret indretningen af datacenteret og konstateret, at der ikke forefindes faldstammer, vandrør eller andet, som vil kunne forårsage skade på kritisk udstyr.	Ingen afvigelser konstateret.
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 gennemgået 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 vurdering af, om forhold til risiko og trusler fortsat er gældende, eller om der er behov for ændring til risikoanalysen.	Vi har inspiceret senest ajourførte it-risikoanalyse og konstateret, at denne er gennemgået og opdateret inden for erklæringsperioden.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
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 relevant leder.	Vi har inspiceret relevante procedurer i forbindelse med håndtering af interne Zitcom-brugere. For en stikprøve af oprettede Zitcom-brugere har vi inspiceret dokumentation for, at oprettelse er sket på baggrund af sag i sagsstyringssystemet, og at oprettelsen er bestilt eller godkendt af relevant leder.	Ingen afvigelser konstateret.
6.2	**Brugerrettigheder – nedlæggelser** Brugere nedlægges kun på baggrund af udfyldte blanketter, som sendes til Service Desken. Alle nedlæggelser dokumenteres i sagsstyringssystemet.	Vi har inspiceret anvendte procedurer og udførte kontroller. Vi har for en stikprøve af fratrådte brugere inspiceret, at deres konti er lukket korrekt.	Ingen afvigelser konstateret.
6.3	**Brugerrettigheder – privilegerede rettigheder** Privilegerede rettigheder er begrænset til ansatte hos Zitcom med et arbejdsbetinget behov herfor.	Vi har inspiceret en samlet liste over ansatte med privilegerede adgange og har på forespørgselsbasis fået bekræftet, at de alle har et arbejdsbetinget behov for adgangen.	Ingen afvigelser konstateret
6.4	**Brugerrettigheder – periodisk opfølgning** Der foretages mindst én gang årligt opfølgning på validiteten af brugere oprettet i Windows AD hos Zitcom.	Vi har inspiceret dokumentation for den udførte kontrol og konstateret, at denne er foretaget inden for erklæringsperioden, og at gennemgangen har resulteret i deaktivering eller sletning af konti hvor nødvendigt.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
6.5	**It-sikkerhedslogning** Der er opsat krav til logning af sikkerhedsmæssige hændelser på Zitcom A/S' infrastruktur. Sikkerheds-mæssige incidents håndteres via incident management-processen.	Vi har via inspektion af konfiguration konstateret, at der er opsat logning på Zitcoms kritiske infrastruktur. Vi har stikprøvevis inspiceret, at sikkerhedsmæssige incidents hånd-teres i incident management-processen.	Ingen afvigelser konstateret.
6.6	**It-sikkerhedsorganisation** It-sikkerhedsmæssige roller og ansvarsområder er for-delt, og medarbejderne er bekendt med deres arbejds-opgaver og funktioner.	Vi har modtaget en oversigt over de faktiske roller i it-sikkerheds-organisationen. Vi har inspiceret den modtagne oversigt og konsta-teret, 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 it-sikkerhedsmæssige roller og ansvarsområder.	Ingen afvigelser konstateret.
7	**Logisk sikkerhed: Kontrolmål – Der er etableret kontroller, som sikrer, at adgange til systemer og data sker via anvendelse af passwords og bruger-profiler.**		
7.1	**Anvendelse af passwords** Autentificering af brugere sker via Windows AD, hvor relevante passwordkrav er defineret.	Vi har inspiceret konfigurationen af krav til passwords på Windows AD hos Zitcom og verificeret, at relevante brugere anvender disse.	Ingen afvigelser konstateret.
7.2	**Anvendelse af brugerprofiler** Brugere er oprettet i Windows AD, og alle anvender individuelle brugerprofiler på det interne netværk.	Vi har stikprøvevis inspiceret, at brugerprofiler på alle relevante systemer og platforme er personlige og identificerbare.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
8	**Systemsoftware: Kontrolmål – Der er etableret procedurer og kontroller, som sikrer, at servere opdateres og vedligeholdes i nødvendigt omfang.**		
8.1	**Systemsoftware – patch management** Der foretages en løbende opdatering af Windows-servere (patch).	Vi har inspiceret Zitcoms patch management-procedure vedrørende Windows-servere. Herudover har vi for en stikprøve af servere kontrolleret, at der sker løbende opdatering af disse.	Ingen afvigelser konstateret.
8.2	**Systemsoftware – fallback** Der defineres fallback-planer før opdatering af systemsoftware, hvor dette er relevant.	Vi har for en stikprøve af ændringer påset, at der i forbindelse med ændringshåndtering har været behov for og dermed beskrevet en fallback-plan.	Ingen afvigelser konstateret.
8.3	**Systemsoftware – timing** Nye opdateringer installeres inden for foruddefinerede servicevinduer.	Vi har for en stikprøve af ændringer påset, at der er taget stilling til timing i forhold til de relevante servicevinduer.	Ingen afvigelser konstateret.
9.	**Systemsoftware: Kontrolmål – Der er etableret procedurer og kontroller, som sikrer, at servere opdateres og vedligeholdes i nødvendigt omfang.**		
9.1	**Konfigurations baseline** Der foretages en årlig revurdering af konfigurations baseline for relevante teknologier for at sikre, at disse er tidssvarende.	Vi har inspiceret dokumentation for årlig gennemgang af baselines.	Ingen afvigelser konstateret.
9.2	**Konfigurations Baseline** Nye servere, der sættes i drift, er konfigureret i overensstemmelse med den til enhver tid gældende	Vi har stikprøvevist inspiceret, at servere er konfigureret i overensstemmelse med den til enhver tid gældende baseline.	Ingen afvigelser konstateret.

Nummer	Etableret kontrol hos Zitcom A/S	Tests udført af EY	Testresultat
	baseline. Denne baseline indeholder specifikke krav til passwords, patchning og logning.		