www.pwc.dk

Miracle 42 A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2020 til 31. december 2020 i relation til Miracle 42 A/S' drifts- og hostingydelser

Februar 2021

pwc

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Miracle 42 A/S' kunder, der har anvendt drifts- og hostingydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber.

Miracle 42 A/S anvender Global Connect A/S som serviceunderleverandør af housing-ydelser. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Global Connect A/S varetager for Miracle 42 A/S.

Miracle 42 A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af drifts- og hostingydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til Miracle 42 A/S' drifts- og hostingydelser var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret
   - De processer i både it-systemer og manuelle systemer, der er anvendt til styring af generelle it-kontroller.
   - Relevante kontrolmål og kontroller udformet til at nå disse mål
   - Kontroller, som vi med henvisning til drifts- og hostingydelsernes udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Hvordan andre betydelige begivenheder og forhold end transaktioner behandles
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til drifts- og hostingydelser foretaget i perioden fra 1. januar 2020 til 31. december 2020

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til drifts- og hostingydelser, 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 generelle it-kontroller i relation til drifts- og hostingydelser, som den enkelte kunde måtte anse vigtigt efter sine 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 2020 til 31. december 2020. Kriterierne anvendt for at give 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 udført 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 2020 til 31. december 2020.

København, den 12. februar 2021

Steen S. Knudsen
CEO, Miracle 42 A/S

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

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2020 til 31. december 2020 i relation til Miracle 42 A/S' drifts- og hostingydelser

Til: Miracle 42 A/S, Miracle 42 A/S' kunder og disses revisor

Omfang

Vi har fået som opgave at afgive erklæring om Miracle 42 A/S' beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til drifts- og hostingydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2020 til 31. december 2020 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Miracle 42 A/S anvender Global Connect A/S som serviceunderleverandør af housing-ydelser. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Global Connect A/S varetager for Miracle 42 A/S.

Miracle 42 A/S' ansvar

Miracle 42 A/S er ansvarlig for udarbejdelsen af beskrivelsen 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 effektivt fungerende kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har 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.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Miracle 42 A/S' beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør" som er udstedt af IAASB, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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 sine drifts- og hostingydelser 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 opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som Miracle 42 A/S har specificeret og beskrevet i ledelsens udtalelse.

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

Miracle 42 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 drifts- og hostingydelser, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller 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 ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af, hvordan generelle it-kontroller i relation til drifts- og hostingydelser, således som de var udformet og implementeret i hele perioden fra 1. januar 2020 til 31. december 2020, 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 2020 til 31. december 2020, 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 opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2020 til 31. december 2020.

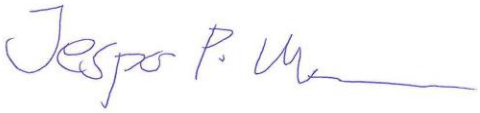
Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

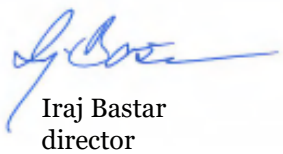
Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt Miracle 42 A/S' drifts- og hostingydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 12. februar 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab



Jesper Parsberg Madsen
statsautoriseret revisor



Iraj Bastar
director

3 Miracle 42's systembeskrivelse

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Miracle 42's kunder og deres revisorer i overensstemmelse med kravene i den danske revisionsstandard ISAE 3402 for erklæringsopgaver om kontroller hos en serviceleverandør. Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret i forbindelse med Miracle 42's leverance af serviceydelser vedr. drift og hosting.

Beskrivelsen indeholder beskrivelser af de anvendte procedurer til sikring af en betryggende afvikling af systemer. Formålet er at give tilstrækkelige informationer til, at kunders revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet, i det omfang det kan medføre en risiko for væsentlige fejl i kunders it-drift i perioden fra 1. januar 2020 til 31. december 2020.

3.2 Beskrivelse af Miracle 42 A/S' ydelser

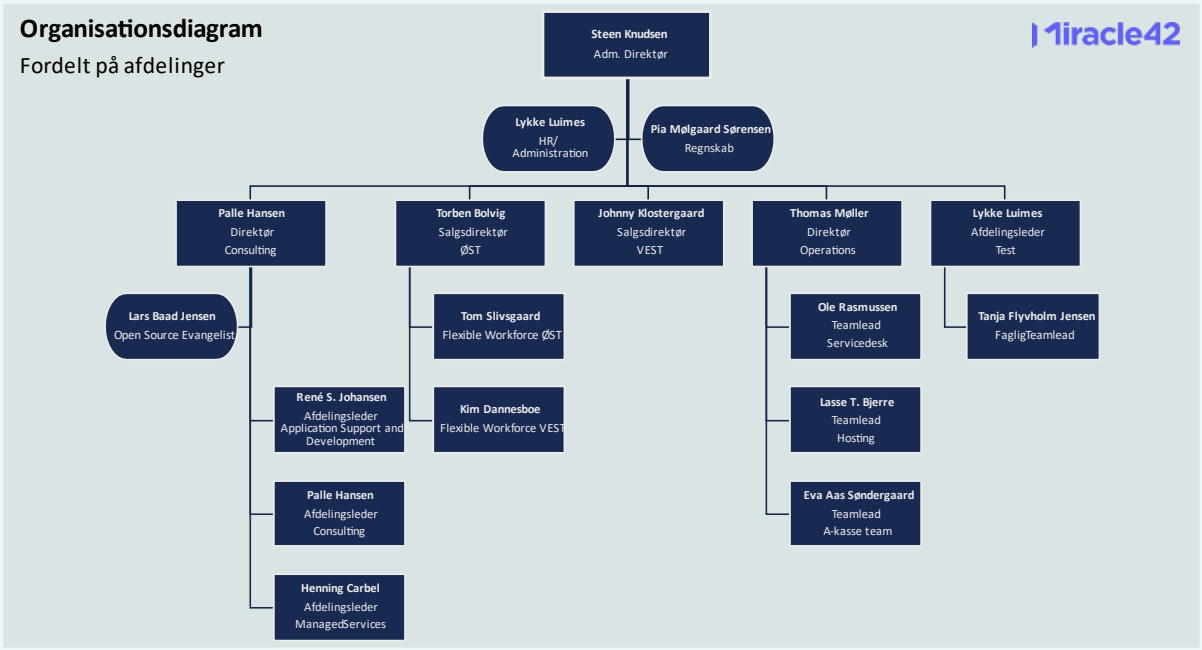
Miracle 42 leverer i dag en bred vifte af it-konsulentydelser til mere end 250 danske kunder med en samlet omsætning på mere end 80 mio. kr. Miracle 42's kerneydelser er hosting og konsulentvirksomhed inden for Microsoft og Oracle. Vores mangeårige erfaring med at drive store it-løsninger gør os i stand til at garantere meget høj kvalitet, sikkerhed og leverancestabilitet. Vi er omkring 50 fastansatte medarbejdere, alle med en solid, teoretisk baggrund og praktisk erfaring inden for bl.a. drift, projektledelse, arkitektur, database og infrastruktur.

Miracle 42 har indarbejdet processer og har fokuseret målrettet på it-drift siden 2011. Miracle 42 forholder sig løbende til opbygning af gode processer inden for projektledelse, procesledelse, teknologiledelse, kompetencestyring samt styring og gennemførelse af it-projekter. Miracle 42 har indarbejdet metoder, værktøjer og processer fra PRINCE2, DS 484/ISO 27001, ISAE 3402 og ITIL®.

Miracle 42 ser kvalitetsstyring som en løbende vurderingsproces integreret i løsningsvalg, dokumentation, projektledelse og de forskellige processer, der er i forbindelse med vedligehold, drift og support. Den bruges til at kontrollere og sikre kvaliteten af serviceydelserne og til at sikre, at tidsplaner og budgetter overholdes, og at serviceydelserne implementeres korrekt hos kunden. Kvalitetsstyring skal identificere processuelle svagheder, rette op på de identificerede svagheder og kontinuerligt forbedre dem.

3.3 Miracle 42 A/S' organisation og sikkerhed

Ansvar og organisering i Miracle 42 A/S fremgår af nedenstående organisationsdiagram.



Direktionen i Miracle 42, som er den øverst ansvarlige for it-sikkerheden, sørger for, at der til stadighed er etableret procedurer og systemer, der understøtter overholdelse af den til enhver tid gældende it-sikkerhedspolitik. For at understøtte dette har Miracle 42 A/S etableret en it-sikkerhedsgruppe, som er ansvarlig for de overordnede målsætninger for implementering af it-sikkerhed i serviceydelserne. Det er driftschefen, som er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollerbart, hvor dette overhovedet er muligt, og være et udtryk for "best practice" inden for de enkelte kontrolaktiviteter på de serviceområder, som kunderne tilbydes. It-sikkerhedsgruppen består p.t. af følgende medlemmer:

- Thomas Møller, IT-sikkerhedsansvarlig – thmol@miracle42.dk
- Lasse Taul Bjerre – labje@miracle42.dk.

Gruppen mødes månedligt for at fastsætte og følge op på målsætninger vedr. it-sikkerheden.

3.4 Risikostyring ved Miracle 42 A/S

Risikostyring gennemføres hos Miracle 42 på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering, der sigter mod interne systemer generelt. Input til denne vurdering indhentes i hele organisationen. Processen faciliteres af ansvarlige og ledere, der udarbejder et udkast til Miracle 42's ledelse. Efter intern bearbejdning godkendes vurderingen af Miracle 42's ledelse.

I projektindstillingsfasen udarbejdes der – afhængigt af projektets karakter – dels en sikkerhedsvurdering og dels en vurdering af særlige risici og usikkerheder. Dette sker efter en foruddefineret procedure.

På operationelt projektniveau gennemføres der løbende risikostyring. Der arbejdes efter en fast projektstyringsmodel, hvor ansvaret for projektrelateret risikostyring ligger hos projektlederen, som ofte vælger at inddrage projektdeltagere, eksterne partnere og evt. styregruppemedlemmer i processen.

3.5 Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering

Miracle 42 har i december måned 2015 foretaget opdatering af sikringsforanstaltninger og kontroller ud fra kontrolrammen ISO 27001:2013.

Miracle 42's it-sikkerhedspolitik, etablerede processer og kontroller omfatter alle de systemer og ydelser, kunderne tilbydes. Det fortsatte arbejde med tilpasning og forbedring af Miracle 42's sikringsforanstaltninger sker løbende i samarbejde med højt kvalificerede specialister.

På basis af ISO 27001 som kontrolramme er relevante kontrolområder og kontrolaktiviteter implementeret ud fra "best practice" til minimering af risici på de serviceydelser, som leveres af Miracle 42's hosting-afdeling. Med udgangspunkt i den valgte kontrolmodel indgår følgende kontrolområder i det samlede kontrolmiljø:

- Informationssikkerhedspolitikker (A5)
- Organisering af informationssikkerhed (A6)
- Personalesikkerhed (A7)
- Adgangssikkerhed (A9)
- Fysisk sikring og miljøsikring (A11)
- Driftssikkerhed (A12)
- Kommunikationssikkerhed (A13)
- Styring af informationssikkerhedsbrud (A16)
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring (A17).

3.6 Etableret kontrolmiljø

Hvert enkelt område er beskrevet i detaljer i de efterfølgende afsnit.

3.6.1 Informationssikkerhedspolitikker (A5)

Formål

Ledelsen har gennem godkendt it-sikkerhedspolitik fastlagt niveauet for virksomhedens anvendelse, herunder hvorledes ledelsen ønsker it-sikkerhed implementeret og kontrolleret. It-sikkerhedspolitikken er udarbejdet med udgangspunkt i en it-risikoanalyse.

Anvendte procedurer og kontroller

Miracle 42 afdækker relevante it-risici på de etablerede serviceydelser. Dette varetages gennem en løbende trussels- og risikovurdering hos Miracle 42, dels i forbindelse med alle implementeringsprojekter og ændringer i systemmiljøer, dels ved en årlig revurdering af risikoanalysen. Resultatet af den årlige gennemgang forelægges ledelsen.

På baggrund af ovenstående trussels- og risikovurdering af hostingaktiviteterne defineres it-sikkerhedspolitikken.

Miracle 42 stiller endvidere en række informationer til rådighed for kundernes revisorer til brug ved deres vurdering af Miracle 42 som serviceleverandør. Ud over driftsrelaterede forhold kan Miracle 42 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 inden udførelse af it-revision og udarbejdelse af erklæring.

Hvem udfører kontrollen?

Den årlige gennemgang udføres af sikkerhedsgruppen.

Kontroldokumentation

Der er versionsstyring på dokumenterne.

3.6.2 Organisering af informationssikkerhed (A6)

Formål

At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Anvendte procedurer og kontroller

Dokumentation for roller og ansvarsområder mht. informationssikkerhed, som dokumenterer, at Miracle 42 har en formel sikkerhedsorganisation, hvor ansvar og roller er klart defineret.

Tidspunkt for udførelse af kontrollen

Mindst én gang årligt inden udførelse af it-revision og udarbejdelse af erklæring.

Hvem udfører kontrollen?

Den årlige gennemgang udføres af sikkerhedsgruppen.

Kontroldokumentation

Kontrollen dokumenteres i Miracle 42's sikkerhedshåndbog.

3.6.3 Personalesikkerhed (A7)

Formål

Dette kontrolmål sikrer, at medarbejdere forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt og at medarbejdere er bevidste om og lever op til deres informationssikkerhedsansvar.

Der er fastlagte procedurer for screening i forbindelse med ansættelser, beskrevne ansættelsesvilkår og -betingelser, og ledelsesansvaret er klart defineret. Herudover skal det sikres, at der følges metodisk op på gennemførelse af awareness om it-sikkerhed, og at der løbende sker relevant uddannelse og træning i informationssikkerhed.

Anvendte procedurer og kontroller

Dokumentation for procedurer, beskrevne betingelser samt dokumentation for ledelsesansvar. Dokumentation for gennemførte awareness-kampagner. På PaaS-miljøer foretages brugeradministration efter samme model. Rettigheder til interne brugere hos Miracle 42 oprettes efter de samme principper og godkendes af driftschefen.

Tidspunkt for udførelse af kontrollen

Mindst én gang årligt inden udførelse af it-revision og udarbejdelse af erklæring.

Hvem udfører kontrollen?

Den årlige gennemgang udføres af sikkerhedsgruppen.

Kontroldokumentation

Kontrollen dokumenteres i Miracle 42's sikkerhedshåndbog.

3.6.4 Adgangskontrol (A9)

Formål

Tildeling af adgang til systemer og programmer administreres hensigtsmæssigt for at sikre mod uautoriserede og utilsigtede handlinger, som kan resultere i ufuldstændig, unøjagtig eller ugyldig behandling eller registrering af finansiel information. Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med kunder.

Adgangen deles op i tre områder:

- Kundens medarbejdere
- Miracle 42's medarbejdere
- Tredjepart.

Anvendte procedurer og kontroller

Det er Miracle 42's ansvar at sikre en betryggende adgang til de enkelte systemer, ved at kunden godkender tredjepartsoprettelse af brugere og tildeling af roller. Brugere oprettes på baggrund af skriftlige henvendelser/e-mails sendt til Miracle 42's driftsafdeling. Det er Miracle 42, der fastsætter, hvilken af de foruddefinerede roller brugerne skal tildeles på baggrund af kundens godkendelse. Det er endvidere kundens ansvar at meddele Miracle 42, når den tildelte rolle skal ændres eller fjernes. Rettigheder til interne brugere hos Miracle 42 oprettes efter de samme principper og godkendes af driftschefen. For interne medarbejdere er der udarbejdet formelle retningslinjer vedr. sletning af brugere. Disse sikrer bl.a., at en fratrådt medarbejder ved arbejdsophør hos Miracle 42 afleverer sine nøgler og adgangskort, således at der ikke kan opnås fysisk adgang til bygningen, og vedkommendes bruger-id spærres for login.

Tidspunkt for udførelse af kontrollen

For kunderne udføres kontrollen kun på baggrund af en skriftlig anmodning fra kunderne. Dette gælder både ift. personaleændringer hos kunderne, og når tredjepart skal tilgå kundernes system internt.

Hvem udfører kontrollen?

For kunderne er det driftsafdelingen hos Miracle 42, der har ansvaret for, at proceduren for tildeling af tredjepartsadgang til kundens miljø bliver overholdt ifølge aftale med kunden. For medarbejdere hos Miracle 42 er det driftschefen, der har ansvaret for, hvem der har adgang til hvad (kundemiljø, interne systemer).

Kontroldokumentation

Ved behov for adgang fra en tredjepart til kundens it-miljø er det kundens it-ansvarlige, der fremsender en godkendelses-e-mail til driftsafdelingen. Denne lagres herefter på kundedrevet i kundens driftsmappe. For Miracle 42's medarbejdere gemmes brugerskemaer i den enkeltes personalemappe på direktionsdrevet.

3.6.5 Fysisk sikring og miljøsikring (A11)

Miracle 42 har et datacenter til kundernes og eget udstyr. It-faciliteterne administreres hensigtsmæssigt for at sikre integriteten af finansielle informationer.

3.6.5.1 Fysisk adgangskontrol og sikring

Formål

Den fysiske adgang til systemer, data og andre it-ressourcer er begrænset og tilrettelagt i overensstemmelse med kundernes ønsker.

Anvendte procedurer og kontroller

Adgang til bygning er kontrolleret via nøglekort, som er udleveret til Miracle 42's driftspersonale ud fra et arbejdsmæssigt behov.

Serverrummet er hævet over grundniveau, og alle døre i datacenteret er sikret med en elektronisk låsemekanisme, som kun kan låses op med registrerede nøglekort. Endelig er der etableret et alarmsystem, som alarmerer vagtcentralen ved forsøg på indbrud.

Tidspunkt for udførelse af kontrollen

Der sker en periodisk gennemgang af nøglekortholdere ved udskiftning af personale eller som minimum en gang om året.

Hvem udfører kontrollen?

Driftsafdelingen.

Kontroldokumentation

Udskrift af nøglekortholdere fra nøglestyringssystemet.

3.6.5.2 Sikring mod miljømæssige hændelser

Formål

It-udstyr er beskyttet mod miljømæssige hændelser såsom strømsvigt og brand. It-faciliteterne beskyttes mod brand, vand og temperaturændringer.

Anvendte procedurer og kontroller

Datacenterets serverrum er beskyttet mod følgende miljømæssige hændelser:

- Strømsvigt
- Brand
- Klimaforandringer.

På alt vitalt it-udstyr er stabil strøm sikret med en UPS-installation, som kan holde systemerne med strøm, indtil generatoren automatisk er startet og klar. I serverrummet er der etableret røgalarm og temperaturfø-ler, der er koblet sammen med det centrale brandovervågningssystem. Serverrummet 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 serverrummet reguleres gennem det fuldautomatiske kølesystem, som sikrer den kor-rekte temperatur til sikring af stabil drift og lang holdbarhed på det anvendte it-udstyr. Der udføres lø-bende service på anlægget.

Tidspunkt for udførelse af kontrollen

- Der udføres løbende visuel kontrol af teknik- og serverrum af driftspersonalet.
- Der udføres 1 årlig kontrol/service af alarmsystemet af alarmselskabet.
- Der udføres 1 årlig kontrol/service af brandbekæmpelsesudstyr.
- Der udføres 1 årlig kontrol/service af UPS og generator.
- Der udføres 1 årlig kontrol/service af køleanlægget.

Hvem udfører kontrollen?

Kontrollen udføres af leverandørerne af systemerne.

Kontroldokumentation

Alle kontrol-/serviceskemaer forefindes hos driftschefen.

3.6.6 Driftssikkerhed (A12)

3.6.6.1 Backup

Formål

Data sikkerhedskopieres og opbevares, så de kan reetableres i overensstemmelse med gældende SLA-krav. Miracle 42 kontrollerer, om backup udføres fejlfrit, og ved fejl i backup at der foretages en vurdering af fejl og opfølgning på evt. fejlrettelse.

Anvendte procedurer og kontroller

Der er udarbejdet en udførlig beskrivelse af backupproceduren. Backupproceduren er en del af den daglige kørsel og er således automatiseret i systemet. Manuelle rutiner i forbindelse med backup er beskrevet i driftsprocedurerne. Alle backups gemmes på to lokationer med betryggende afstand. Backups testes lø-

bende, idet backups anvendes til at reetablere kundedata, ligesom der ved den årlige afprøvning af recovery-procedurer sker en efterprøvning af restore i forbindelse med en fuld reetablering af én enkelt kundes miljø, dvs. både systemopsætning og brugerdata.

På PaaS-miljøer foretages der backup med cloud-leverandørens egne værktøjer. Backup gemmes på to lokationer hos cloud-leverandøren. Der foretages ligeledes løbende test jf. de aftaler, der er indgået med kunden.

Tidspunkt for udførelse af kontrollen

Der udføres tjek af backuplogge inden for normal arbejdstid.

Hvem udfører kontrollen?

Driftsafdelingen forestår den daglige kontrol af backuplogge.

Kontroldokumentation

Daglig kontrol i Miracle 42's sagsstyringssystem.

3.6.6.2 Overvågning

Formål

Der udføres proaktiv overvågning af, at aftalte services er tilgængelige, at tilgængelige ressourcer er i overensstemmelse med de aftalte normer/tærskelværdier, og at nødvendige jobs og kørsler, såvel online som batch, afvikles rettidigt og korrekt. Miracle 42 kontrollerer, at dette sker til normal fuldførelse og med det forventede resultat.

Anvendte procedurer og kontroller

Miracle 42 har etableret et sæt skriftlige driftsprocedurer på alle væsentlige driftsaktiviteter, som er afstemt med kundens krav og den tilhørende it-sikkerhedspolitik. Driftsprocedurerne udarbejdes af driftsafdelingen i tæt samarbejde med kunden, tredjepartsleverandører og driftsafdelingen.

Der foreligger en række jobbeskrivelser for driftsafdelingen, hvor det er fastsat, hvilken overvågning og hvilke kontroller der udføres dagligt, ugentlig og årligt. Konstaterede fejl i udførte kontroller og evt. fejl fra det systemtekniske overvågningssystem korrigeres hurtigst muligt ved hjælp af procedurer eller "best practice". Kunden informeres løbende om omfanget og konsekvenserne af de konstaterede fejl. Følgende funktionsområder har adgang til kundernes it-systemer:

- Service Desk-medarbejdere
- Driftsmedarbejdere
- Konsulenter.

Tidspunkt for udførelse af kontrollen

Kontrollen udføres i primær driftstid ifølge SLA-aftalen med den enkelte kunde.

Hvem udfører kontrollen?

Kontroller udføres af Miracle 42's driftsafdeling, og uden for normal arbejdstid udføres den af en konsulent (vagten).

Kontroldokumentation

Dokumentation for udførelse af dette for kunderne sker i Miracle 42's sagsstyringssystem.

3.6.6.3 Service Desk og kundesupport

Formål

Der udføres betryggende brugersupport for brugere, der kontakter Service Desk, herunder ydes der den aftalte support i de tidsrum og på de områder, der er aftalt i kontrakten.

Anvendte procedurer og kontroller

Miracle 42 har etableret et sæt skriftlige Service Desk-procedurer på de områder, der er fastsat i aftalen med kunden. Service Desk-procedurerne udarbejdes af Service Desk i tæt samarbejde med kunden samt tredjepartsleverandører. Support til brugere sker over telefon og evt. via fjernstyringsværktøjer.

Tidspunkt for udførelse af kontrollen

Service Desk gennemgår dagligt sager, der afventer løsning.

Hvem udfører kontrollen?

Kontroller udføres af Service Desk, og uden for normal arbejdstid udføres den af Service Desk-vagten.

Kontroldokumentation

Dokumentation for henvendelser og udførelse af opgaver for kunder sker i Miracle 42's sagsstyringssystem.

3.6.6.4 Incidenthåndtering

Formål

Alle henvendelser fra kunder behandles og dokumenteres rettidigt og i overensstemmelse med de indgåede aftaler. Der gennemføres en betryggende incidenthåndtering ud fra den indgåede aftale med kunder, herunder at Miracle 42 kontrollerer, at dette sker til normal fuldførelse og med det forventede resultat.

Anvendte procedurer og kontroller

Miracle 42 anvender et sagsstyringssystem til registrering og håndtering af incidents. Der noteres følgende i sagen:

- Fejl
- Hvad der er gjort for at afhjælpe 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, og at incidenthåndtering gennemføres i overensstemmelse med de indgåede kundeaftaler.

Tidspunkt for udførelse af kontrollen

Incidenthåndtering sker inden for de aftalte SLA-tider med kunden.

Hvem udfører kontrollen?

Håndteringen af incidents udføres af Miracle 42's driftsafdeling, og uden for normal arbejdstid udføres den af en konsulent (vagten).

Kontroldokumentation

Dokumentation for incidents og udførelse af incidents for kunder sker i Miracle 42's sagsstyringssystem.

3.6.6.5 Systemsoftware

Formål

Ny systemsoftware samt ændringer til eksisterende systemsoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger. Systemsoftware vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med virksomhedens behov, og at ændringer testes og dokumenteres på tilfredsstillende vis.

Anvendte procedurer og kontroller

For Windows-servere indhentes fyldestgørende systemdokumentation efter behov. Miracle 42 har fastsat procedurer for anskaffelse og opdatering af systemsoftware på Windows-platformene. På Windows-platformen hentes opdateringer fra Microsoft, der implementeres automatisk efter aftale med kunden. Vurdering og test sker ved, at der i forbindelse med servicevinduet tages stilling til, om der er behov for de frigivne patches og fixes. Herefter testes de på mindre kritiske systemer og udvalgte testsystemer, inden de rulles ud på alle systemer.

Miracle 42 har fastsat procedurer for anskaffelse og opdatering af systemsoftware på PaaS-platformene. Miracle 42 henter opdateringerne fra relevante softwareleverandører og opdaterer manuelt systemsoftware i faste servicevinduer, der løbende aftales med kunden.

Tidspunkt for udførelse af kontrollen

Kontrollen for opdatering sker efter opsatte kontroller i Miracle 42's sagsstyringssystem.

Hvem udfører kontrollen?

Driftsafdelingen er ansvarlig for udførelse af opdateringer og kontrol heraf.

Kontroldokumentation

Det fremgår af de installerede patches på den enkelte server samt Miracle 42's sagsstyringssystem.

3.6.7 Kommunikationssikkerhed (A13)

Formål

Ny netværkssoftware samt ændringer til eksisterende netværkssoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger. Netværks- og kommunikationssoftware vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med behov, og at ændringer testes og dokumenteres på tilfredsstillende vis.

Anvendte procedurer og kontroller

Miracle 42 har fuld dokumentation for netværk og kommunikationslinjer frem til kunder, hvor der foreligger en aftale om drift af kundens netværksudstyr.

Miracle 42 vurderer løbende behovet for opdatering af firmware på netværks- og kommunikationssoftware. For at sikre en stabil drift vil der alene ske opdatering, såfremt dette er nødvendigt for at sikre kommunikationen. Inden ændringer foretages, tages der 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?

Driftsafdelingen har ansvaret for udførelse af opdateringer samt kontrol af funktionalitet.

Kontroldokumentation

Der udarbejdes dokumentation i Miracle 42s sagsstyringssystem for opgaver, der er udført på kundens system.

3.6.8 Styring af informationssikkerhedsbrud (A16)

Formål

Sikre, at der foreligger fastlagte procedurer, som benyttes ved evt. informationssikkerhedsbrud ift. ansvar og procedurer, rapportering af hændelser, vurdering af og beslutning om hændelser samt håndtering af hændelser.

Anvendte procedurer og kontroller

Miracle 42 har udarbejdet detaljerede procedurebeskrivelser, som sikrer, at evt. sikkerhedshændelser behandles ens og på kontrolleret vis, og at der gøres de fornødne tiltag ift. information, kommunikation og mitigering. Herudover er der fastlagt veldefineret ansvar ved evt. hændelser.

Tidspunkt for udførelse af kontrollen

Mindst én gang årligt inden udførelse af it-revision og udarbejdelse af erklæring.

Hvem udfører kontrollen?

Sikkerhedsgruppen udfører den årlige kontrol af sikkerhedshændelser.

Kontroldokumentation

Den årlige gennemgang dokumenteres i Miracle 42's sikkerhedshåndbog.

3.6.9 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring (A17)

Formål

En plan for genoptagelse af Miracle 42's mest kritiske interne it-baserede forretningsprocesser efter en katastrofe er udarbejdet, afprøvet og ledelsesgodkendt og vedligeholdes løbende.

Anvendte procedurer og kontroller

Miracle 42 har tegnet service på alle kritiske komponenter i datacenteret. Herudover er alle kritiske netværkskomponenter redundante for at sikre den fortsatte drift i tilfælde af nedbrud og fejl. De virtuelle servere drives primært i et VMware vSphere-cluster for at sikre høj tilgængelighed i tilfælde af nedbrud på en eller flere noder. Backup foretages dagligt, og data kopieres til en sekundær lokation efter endt backup.

De fastsatte procedurer omfatter ikke beredskabsstyring og reetablering af kundernes miljø ud over assistance ved restore af foretaget backup.

Tidspunkt for udførelse af kontrollen

Miracle 42 gennemgår årligt serviceniveauet for kritisk udstyr for at sikre høj tilgængelighed i datacenteret.

Hvem udfører kontrollen?

Sikkerhedsgruppen udfører den årlige gennemgang og tilpasning af serviceniveauer og infrastrukturarkitektur.

Kontroldokumentation

Den årlige gennemgang dokumenteres i Miracle 42's sagsstyringssystem.

3.7 Supplerende information om det etablerede kontrolmiljø og forhold, som skal iagttages af kundernes revisorer

Brugeradministration

Miracle 42 giver adgang og tildeler rettigheder i overensstemmelse med kundernes instrukser, i takt med at disse indmeldes til Service Desk. Miracle 42 er ikke ansvarlig for, at disse informationer er korrekte, og det er således kundernes eget ansvar at sikre, at de tildelte adgange og rettigheder til systemer og applikationer er tildelt i overensstemmelse med kundernes egne forventninger til en betryggende funktionsadskillelse.

Business continuity

Miracle 42 har etableret procedurer for katastrofestyring og reetablering af kritiske, interne, it-baserede forretningsprocesser i datacenteret. Disse omfatter ikke styring og sikring af kundernes forretningsprocesser ud over den aftalte restore af sikkerhedskopier. Kunderne er selv ansvarlige for at sikre, at der etableres de fornødne procedurer for katastrofehåndtering i overensstemmelse med kundernes egne forventninger til et betryggende niveau for business continuity.

Efterlevelse af relevant lovgivning

Miracle 42 har tilrettelagt procedurer og kontroller, således at de krav, som er Miracle 42's ansvar, efterleves på betryggende vis. Miracle 42 er ikke ansvarlig for applikationer, som afvikles på det hostede udstyr, og som følge af dette omfatter denne erklæring ikke sikkerhed for, at der er etableret betryggende kontroller i brugerapplikationerne, herunder at applikationerne efterlever Bogføringsloven, databeskyttelsesforordningen eller anden relevant lovgivning.

Udvikleres adgang til produktionsdata

Som udgangspunkt tildeler Miracle 42 ikke udviklere adgang til produktionsdata. Såfremt dette alligevel ønskes af kunden, sker dette ved skriftlig anvisning og accept heraf. I de tilfælde hvor kunden anvender udviklingsydelser, der tilbydes af Miracle 42, skal kundens egen revisor selv vurdere, om tildelte udvikleradgange er i overensstemmelse med kundens behov, og endvidere selv vurdere risikoen forbundet hermed.

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", og de yderligere krav, der er gældende i Danmark.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos kunder er ikke omfattet af vores testhandlinger.

Vores test af funktionaliteten har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået.

4.2 Testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af 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 være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontrollerne er implementeret og har fungeret i hele perioden fra 1. januar 2020 til 31. december 2020. Dette omfatter bl.a. vurdering af patching-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.3.1 Informationssikkerhedspolitikker (A5)

Kontrolmål: Ledelsen har gennem godkendt it-sikkerhedspolitik fastlagt niveauet for virksomhedens anvendelse, herunder hvordan ledelsen ønsker it-sikkerhed implementeret og kontrolleret. It-sikkerhedspolitikken er udarbejdet med udgangspunkt i en it-risikoanalyse.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.1.1	**It-sikkerhedspolitik** Den eksisterende it-sikkerhedspolitik bliver løbende opdateret, hvis der er behov for dette, og revurderes mindst en gang årligt. Gennemgang af sikkerhedspolitikken varetages af sikkerhedsgruppen.	Vi har inspiceret den seneste ajourførte it-sikkerhedspolitik og vurderet, om denne er betryggende. Yderligere er det konstateret, at it-sikkerhedspolitikken er godkendt.	Ingen bemærkninger.
4.3.1.2	**It-risikoanalyse** Trussels- og risikovurderinger bliver løbende opdateret, hvis der er behov for dette, og revurderes mindst en gang årligt. Opdatering af risikoanalysen varetages af driftschefen.	Vi har inspiceret den seneste ajourførte it-risikoanalyse og vurderet, om denne indeholder de relevante systemer og elementer, som anvendes i leverancen af Miracle 42 A/S' ydelser.	Ingen bemærkninger.

4.3.2 Organisering af informationssikkerhed (A6)

Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.2.1	**Roller og ansvarsområder for informationssikkerhed** Miracle 42 A/S har defineret og fordelt ansvarsområder for informationssikkerheden samt kommunikeret dette til medarbejderne.	Vi har inspiceret, at ledelsen har implementeret en it-sikkerhedsgruppe og har udpeget informationssikkerhedsansvarlige. Vi har forespurgt et udvalg af medarbejdere med henblik på at konstatere, om de var bekendte med ansvarsplaceringen mht. informationssikkerhed i organisationen.	Ingen bemærkninger.
4.3.2.2	**Funktionsadskillelse** Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har stikprøvevis inspiceret den organisatoriske fordeling i Miracle 42 A/S med henblik på at konstatere, om modstridende funktioner og ansvarsområder er adskilt.	Ingen bemærkninger.

4.3.3 *Medarbejdersikkerhed (A7)*

Kontrolmål: At sikre, at medarbejderne forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt. At sikre, at medarbejderne er bevidste om og lever op til deres informationssikkerhedsansvar.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.3.1	**Screening** Der indhentes som hovedregel udtalelser fra ansøgers oplyste referencer, før en aftale indgås, herunder indhentes straffeattester, hvis det på baggrund af stillingsindholdet vurderes relevant.	Vi har inspiceret ansættelsesproceduren og de sikkerhedsopgaver, der skal udføres i den forbindelse. Vi har endvidere inspiceret et udvalg af kommunikation mellem DPO og afdelingsledere, hvori det påpeges, at relevante referencetjek udføres.	Ingen bemærkninger.
4.3.3.2	**Ansættelsesvilkår og -betingelser** Som en del af den kontraktlige forpligtelse underskriver medarbejdere og eksterne brugere betingelserne i ansættelseskontrakten, der beskriver deres og virksomhedens ansvar for informationssikkerhed.	Vi har inspiceret ansættelsesprocedurer med henblik på at konstatere, at disse indeholder stillingtagen til information om it-sikkerhed, herunder ansvar i relation til tavshedspligt ved ansættelse. Vi har endvidere inspiceret skabelon til ansættelseskontrakter og indhentet jobbeskrivelser med henblik på at konstatere, om sikkerhedsansvar var beskrevet heri.	Ingen bemærkninger.
4.3.3.3	**Ledelsesansvar** Ledelsen kræver, at medarbejdere og eksterne brugere opretholder sikkerheden i overensstemmelse med virksomhedens fastlagte politikker og procedure.	Vi har inspiceret beskrivelsen af ledelsens krav til medarbejdere og eksterne brugere. Vi har endvidere inspiceret procedurer, hvori det påpeges, at alle har pligt til at overholde sikkerhedspolitikken, herunder sikkerhedshåndbogen.	Ingen bemærkninger.
4.3.3.4	**Bevidsthed om samt uddannelse og træning i informationssikkerhed** Virksomhedens medarbejdere og, hvor det er relevant, eksterne brugere bevidstgøres om sikkerhed og holdes regelmæssigt ajour med virksomhedens politikker og procedurer.	Vi har inspiceret, at der regelmæssigt gøres opmærksom på sikkerhedspolitikker og procedurer. Vi har desuden konstateret, at der gennemføres årlige awareness-kampagner med fokus på sikkerhed.	Ingen bemærkninger.

4.3.4 Adgangskontrol (A9)

Kontrolmål: Tildeling af adgang til systemer og programmer administreres hensigtsmæssigt for at sikre mod uautoriserede og utilsigtede handlinger, som kan resultere i ufuldstændig, unøjagtig eller ugyldig behandling eller registrering af finansiel information.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.4.1	**Brugerrettigheder – oprettelser og ændringer** Brugere oprettes kun på baggrund af skriftlige henvendelser (e-mails) modtaget i Topdesk fra de tilsluttede kunder. Brugerne oprettes med de ønskede parametre, og dette dokumenteres. Interne brugere registreres også i Topdesk.	Vi har inspiceret retningslinjer og procedure for adgangsstyring med henblik på at konstatere, at disse er betryggende. Vi har stikprøvevis inspiceret oprettede brugere og vurderet, om der er et dokumenteret grundlag for de tildelte adgange og rettigheder.	Ingen bemærkninger.
4.3.4.2	**Brugerrettigheder –udvidede rettigheder** Interne medarbejderes adgang til systemer dokumenteres i Topdesk. Driftsmedarbejdere får tildelt udvidede rettigheder, og dette godkendes formelt af driftschefen, og medarbejderen underskriver en admin-erklæring.	Vi har ved inspektion vurderet anvendte procedurer og udførte kontroller for håndtering af brugere med udvidede rettigheder. Vi har ved inspektion gennemgået brugere med udvidede rettigheder på Miracle 42 A/S' centrale infrastruktur og verificeret, at disse er godkendt til de tildelte rettigheder. Vi har desuden inspiceret de underskrevne admin-erklæringer.	Ingen bemærkninger.
4.3.4.3	**Brugerrettigheder – nedlæggelser** Den enkelte kunde har selv ansvaret for at afmelde brugere, der fratræder. Miracle 42 A/S udfører blot opgaven på baggrund af henvendelser fra kunderne. Interne brugere lukkes efter behov, og dette dokumenteres i Topdesk.	Vi har ved inspektion vurderet anvendte procedurer og udførte kontroller for nedlæggelse af brugere. Vi har stikprøvevis inspiceret, at fratrådte Miracle 42 A/S-medarbejdere har fået deres bruger-id nedlagt.	Ingen bemærkninger.
4.3.4.4	**It-sikkerhedsorganisation** Der er for Miracle 42 A/S lavet en formel rollefordeling omkring drift, support og Helpdesk.	Vi har gennemgået beskrivelser af roller og ansvarsområder og har ved interview verificeret, at disse stemmer overens med de faktiske roller og ansvarsområder hos medarbejderne.	Ingen bemærkninger.

Kontrolmål: Tildeling af adgang til systemer og programmer administreres hensigtsmæssigt for at sikre mod uautoriserede og utilsigtede handlinger, som kan resultere i ufuldstændig, unøjagtig eller ugyldig behandling eller registrering af finansiel information.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.4.5	**Anvendelse af passwords** Autentifikation af brugere gennemføres via Windows AD, hvor der er opsat en passwordpolitik, der sikrer kvaliteten og regelmæssige skift af passwords. Der er opsat kvalitetskrav for passwords, således at der kræves en minimumslængde, kompleksitet og periodisk skift af password, ligesom passwordopsætninger medfører, at password ikke kan genbruges, og at brugere bliver lukket ude ved gentagne fejlslagne forsøg på login.	Vi har inspiceret konfigurationen af passwordopsætningen på Windows AD og verificeret, at den opsatte politik anvendes som standard på domænet. Vi har endvidere gennemgået opsætningen af passwordparametre på udvalgte platforme og vurderet, om disse understøtter de beskrevne krav til passwordkvalitet.	Ingen bemærkninger.
4.3.4.6	**Anvendelse af brugerprofiler** Alle brugere er oprettet med individuelle brugerprofiler. Der anvendes serviceprofiler i Miracle 42 A/S, i det omfang det vurderes hensigtsmæssigt.	Vi har inspiceret anvendelsen af brugerprofiler på systemer og platforme og verificeret, at disse er personlige og identificerbare.	Ingen bemærkninger.
4.3.4.7	**Ændring af standardpassword** Standardbrugeres password skiftes i forbindelse med implementering af centrale applikationer og hardwarekomponenter. Der er etableret en passworddatabase, hvor adgangskoder til alle servere og udstyr er registreret.	Vi har inspiceret forhold vedr. standardpasswords og konstateret, at der er etableret beskyttet passworddatabase, hvor kun medarbejdere med et arbejdsmæssigt behov har adgang.	Ingen bemærkninger.
4.3.4.8	**Anvendelse af åbne netværk** Der anvendes ikke åbne netværk. Interne servere og kundesystemer er adskilt, og al trafik afvikles over lukkede MPLS-/VPN-forbindelser.	Vi har fået oplyst, at der ikke anvendes åbne netværk på Miracle 42 A/S' lokation. Vi har endvidere inspiceret overordnet dokumentation for netværk og segmentering heraf.	Ingen bemærkninger.
4.3.4.9	**It-sikkerhedslogning** Der er etableret logning af logins og ændringer til brugerkonti i Windows AD. Der laves ikke gennemgang af logge, medmindre der opleves fejl eller er begrundet mistanke om misbrug.	Vi har inspiceret, om der er etableret logning på logins til interne systemer. Vi har gennemgået processen for overvågning af sikkerhedshændelser og alarmer.	Ingen bemærkninger.

4.3.5 *Fysisk sikring og miljøsikring (A11)*

Kontrolmål: It-faciliteterne administreres hensigtsmæssigt for at sikre integriteten af finansielle informationer. It-faciliteterne beskyttes mod brand, vand og temperaturændringer.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.5.1	**Fysisk adgang – adgang til kritiske lokationer** Adgang til serverrum er kontrolleret via kortlæser og kode. Kun autoriseret personale fra Miracle 42 A/S har adgang til rummet.	Vi har inspiceret, om adgangen til kritiske lokationer er begrænset via personlige adgangskort, og at adgang til kritiske lokationer som serverrummet er godkendt.	Ingen bemærkninger.
4.3.5.2	**Fysisk sikkerhed – strømsikring** Der er i serverrummet forbundet UPS-anlæg samt generator på alle servere. Der er yderligere indgået kontrakt om periodisk vedligeholdelse af UPS og generatorløsning.	Vi har observeret, at der er opsat nødstrømsanlæg, og inspiceret, at der er dokumentation for periodisk gennemgang af løsningen.	Ingen bemærkninger.
4.3.5.3	**Fysisk sikkerhed – brandsikring** Serverrum er forsynet med automatisk brandslukningsudstyr og alarmer for både røg og temperatur. Der er indgået kontrakt om periodisk vedligeholdelse af brandslukningsanlægget.	Vi har observeret, at der er opsat brandalarm, og at der i serverrummet er opsat brandslukningsanlæg. Vi har endvidere konstateret, at der er udført service på anlægget.	Ingen bemærkninger.
4.3.5.4	**Fysisk sikkerhed – klimaovervågning og køling** Serverrummet er forsynet med et kølesystem, så maskinerne ikke bliver overophedet. Der er desuden indgået kontrakt om periodisk vedligeholdelse af kølesystemet.	Vi har observeret, at der er opsat et kølesystem i serverrummet, og konstateret, at der er udført service på anlægget.	Ingen bemærkninger.
4.3.5.5	**Fysisk sikkerhed – indretning** Serverrummet er indrettet, så der ikke forefindes faldstammer, vandrør mv., som vil kunne forårsage skader på maskiner, der anvendes til kritiske systemer og data. Servere er placeret i racks hævet over gulvet.	Vi har observeret indretningen af kritiske lokationer og vurderet, om der er forhold, som udgør en risiko for indtrængning af vand og fugt.	Ingen bemærkninger.

4.3.6 Driftssikkerhed (A12)

Kontrolmål: Data sikkerhedskopieres løbende for at sikre, at finansielle data forbliver nøjagtige, fuldstændige og gyldige gennem opdaterings- og lagringsprocessen.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.6.1	**Backup – strategi** Der er udarbejdet backupstrategier for alle servere og systemer. Strategierne bliver løbende opdateret, når der bliver tilføjet nye systemer eller data.	Vi har inspiceret backupstrategierne og vurderet, om disse i tilstrækkelig grad afdækker backupkrav for kritiske systemer og data, som håndteres for kunderne.	Ingen bemærkninger.
4.3.6.2	**Backup – konfiguration** Ændringer til backupkonfigurationen varetages af de ansvarlige medarbejdere i driften, der også kontrollerer de daglige kørsler. Ændringer til konfigurationen udføres i et samarbejde mellem evt. systemejere og driftsafdelingen. Den daglige kontrol dokumenteres i Topdesk.	Vi har inspiceret en stikprøve på, at backupkonfigurationen stemmer overens med den udarbejdede backupstrategi. Endvidere har vi testet den daglige efterkontrol af backupafviklingen.	Ingen bemærkninger.
4.3.6.3	**Backup – intern opbevaring** Backup afvikles til disk i datacenteret og kopieres umiddelbart herefter til et afsides datacenter. Der laves ikke backup til bånd.	Vi har inspiceret og vurderet, om den interne opbevaring af backupmedier er betryggende.	Ingen bemærkninger.
4.3.6.4	**Backup – test** Backup testes løbende i forbindelse med reetablering af filer. Årligt laves en fuld restore af et kundesystem. Der er etableret formelle recovery-procedurer for servere i datacenteret.	Vi har inspiceret etablerede procedurer for restore og har konstateret, at der har været udført test af restore for udvalgte kundesystemer, og at reetablering af disse er dokumenteret.	Ingen bemærkninger.

Kontrolmål: Der udføres løbende driftsovervågning for at sikre kontinuitet af it-programmer og processer.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.6.5	**Overvågning** Der er etableret daglige driftskontroller i Topdesk, der udføres og dokumenteres af driftsteamet. Der er opsat sensorer og alarmer på services og hardware. Ved alarm registreres dette i Topdesk og behandles herfra som en incident.	Vi har inspiceret Miracle 42 A/S' opsætning af alarmer og behandling heraf. Endvidere har vi gennemgået de daglige driftskontroller og for en stikprøve verificeret, at kontrollerne dokumenteres.	Ingen bemærkninger.

Kontrolmål: Alle henvendelser fra kunder behandles og dokumenteres rettidigt og i overensstemmelse med de indgåede aftaler.			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
4.3.6.6	**Service Desk og incidenthåndtering** Der er etableret skriftlige procedurer for Helpdesk og incidenthåndtering. Alle henvendelser behandles i Service Desk-systemet og dokumenteres.	Vi har inspiceret driftsprocedurerne og de udførte kontroller samt gennemgået Topdesk-systemet til dokumentering af kontrollerne.	Ingen bemærkninger.
Kontrolmål: Ny systemsoftware samt ændringer til eksisterende systemsoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.			
Nr.	**Serviceleverandørens kontrolaktivitet**	**PwC's udførte testhandlinger**	**Resultat af test**
4.3.6.7	**Systemsoftware – patch management** Opdateringerne indhentes fra Microsoft og rulles ud på serverne regelmæssigt. Dette udføres af driften som en fast kontrol hver anden måned. Opdatering af servere dokumenteres. Redundante servere opdateres forskudt.	Vi har stikprøvevis inspiceret, at opdateringer til servere implementeres og dokumenteres som beskrevet.	Ingen bemærkninger.
4.3.6.8	**Systemsoftware – test** Kontrol af opdateringer er etableret som en fast opgave i driften, og opdateringer frigives til mindre kritisk infrastruktur først. Hvis en ændring fejler, fjernes patchen igen, eller der foretages restore fra backup.	Vi har inspiceret proceduren for opdatering og test forud for frigivelse til brugerne og har kontrolleret procedurerne for backup.	Ingen bemærkninger.
4.3.6.9	**Systemsoftware – fallback** Fallback er etableret gennem restore af backup. Hvis muligt afinstalleres patchen.	Vi har inspiceret proceduren for opdatering. Endvidere har vi testet forhold angående reetablering af backup.	Ingen bemærkninger.
4.3.6.10	**Systemsoftware – timing** Alle servere opdateres ud fra fastsat skema/tidsplan hver anden måned. Redundante servere opdateres forskudt for at sikre driften.	Vi har inspiceret proceduren for opdatering af servere og verificeret, om der er sket kommunikering af servicevinduer.	Ingen bemærkninger.
4.3.6.11	**Systemsoftware – dokumentering af systemer** Der er etableret en serverdatabase, der indeholder alle relevante informationer om servere.	Vi har inspiceret, om dokumentationen for kundesystemer i serverdatabasen er fyldestgørende.	Ingen bemærkninger.

4.3.7 Kommunikationssikkerhed (A13)

Kontrolmål: Ny netværkssoftware samt ændringer til eksisterende netværkssoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.7.1	**Netværk og kommunikation – patch management** Relevante firmware-opdateringer vurderes løbende og implementeres efter behov. Opdateringer installeres kun, hvis det er nødvendigt for at sikre kommunikationen. Alle ændringer dokumenteres i Kiwi Cat-Tools.	Vi har inspiceret proceduren for vedligeholdelse og opdatering af netværks- og kommunikationsudstyr og for en stikprøve kontrolleret, at ændringer til netværket dokumenteres.	Ingen bemærkninger.
4.3.7.2	**Netværk og kommunikation – test** Ændringer til netværket testes i forbindelse med idriftsættelse. Kritiske netværkskomponenter kører i cluster og kan opdateres enkeltvis med mulighed for tilbagerulning.	Vi har inspiceret proceduren for vedligeholdelse og opdatering af netværks- og kommunikationsudstyr og kontrolleret, at dette dokumenteres.	Ingen bemærkninger.
4.3.7.3	**Netværk og kommunikation – fallback** Der laves automatisk backup af netværkskonfigurationer, når der foretages ændringer. Der sendes dagligt rapporter til de ansvarlige medarbejdere, hvor evt. ændringer til netværksenheder og de gemte konfigurationer er med.	Vi har stikprøvevis inspiceret, at der er arkiveret gamle konfigurationer til netværksudstyr og foretaget test af den automatiske rapportgenerering.	Ingen bemærkninger.
4.3.7.4	**Netværk og kommunikation – timing** Væsentlige ændringer til netværkskonfigurationer skal om muligt ske uden for normal arbejdstid, således at disse ikke forstyrrer driften unødigt. Hvis der planlægges større nedetid, meldes dette ud til kunder.	Vi har stikprøvevis inspiceret, at der i forbindelse med opdatering af netværkskomponenter er taget stilling til timingen af implementeringen i produktion, og at der er givet besked til de berørte brugere.	Ingen bemærkninger.
4.3.7.5	**Netværk og kommunikation – dokumentation af netværk** Netværket dokumenteres via topologitegninger. Alt aktivt udstyr er endvidere registreret i ip-oversigter.	Vi har inspiceret den seneste dokumentation for netværket og verificeret ved interview, at denne stemmer overens med det faktiske setup.	Ingen bemærkninger.

4.3.8 Styring af informationssikkerhedsbrud (A16)

Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.8.1	**Ansvar og procedurer** Der er udarbejdet en procedure vedr. informationssikkerhedshændelser, hvori der tages stilling til ansvarsplacering, rapportering, procedurer, diskretion og håndtering.	Vi har inspiceret proceduren for rapportering af informationssikkerhedshændelser med henblik på at konstatere, om der heri tages stilling til ansvarsplacering, rapportering, procedurer, diskretion og håndtering.	Ingen bemærkninger.
4.3.8.2	**Rapportering af informationssikkerhedshændelser** Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret, at der er implementeret procedurer til registrering og rapportering af informationssikkerhedshændelser.	Ingen bemærkninger.
4.3.8.3	**Vurdering af og beslutning om informationssikkerhedshændelser** Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	Vi har inspiceret, at der er implementeret procedurer for registrering, vurdering og rapportering af informationssikkerhedshændelser.	Ingen bemærkninger.
4.3.8.4	**Håndtering af informationssikkerhedsbrud** Informationssikkerhedsbrud håndteres i overensstemmelse med de dokumenterede procedurer.	Vi har inspiceret, at sikkerhedsbrud er gennemgået og vurderet efter den implementerede procedure.	Under revisionen af procedurer for håndtering af informationssikkerhedsbrud har vi observeret, at 1 ud af 3 hændelser ikke er dokumenteret i overensstemmelse med proceduren. Vi har fået oplyst, at ledelses indskærper, at de vedtagne procedurer, i forhold til sagsbehandling altid skal følges også i tilfælde af sager, der vurderes ikke sikkerhedskritiske. Ingen yderligere bemærkninger.

4.3.9 *Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring (A17)*

Kontrolmål: En plan for genoptagelse af Miracle 42's mest kritiske interne it-baserede forretningsprocesser efter en katastrofe er udarbejdet, afprøvet og ledelsesgodkendt og vedligeholdes løbende.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
4.3.9.1	**Beredskabsplanlægning** Miracle 42 har etableret en beredskabsplan, som beskriver væsentlige elementer ift. videreførelse af driften i en nødsituation, herunder aktivering af planen, roller og ansvar samt krav til test. Planen vedligeholdes løbende på baggrund af udførte tests. Servere drives primært i et VMware-cluster for at sikre høj tilgængelighed. Backup foretages dagligt, og data kopieres til en sekundær lokation efter endt backup.	Vi har inspiceret den etablerede beredskabsplan og kontrolleret, at de beskrevne elementer er indeholdt. Vi har endvidere konstateret, at seneste version af planen er ajourført på baggrund af erfaring fra seneste test. Vi har ved vores gennemgang konstateret, at et stort antal servere afvikles i virtuelle miljøer, samt gennemgået kontroller for sikring af den daglige backup.	Ingen bemærkninger.
4.3.9.2	**Beredskabstest** Miracle 42 A/S tester løbende, om backup af kundeservere kan reetableres som forventet. Dette dokumenteres i sagsstyringssystemet. Endvidere udføres der løbende service på sikkerhedsforanstaltningerne i datacenteret.	Vi har inspiceret dokumentationen for den seneste beredskabsøvelse.	Ingen bemærkninger.