



Miracle 42 A/S

ISAE 3402-erklæring om generelle it-kontroller relateret til drift og hostingydelser

Erklæringen omfatter perioden fra 01.01.2019 til 31.12.2019

Indholdsfortegnelse

	Side
1. Uafhængig revisors erklæring	1
2. Udtalelse fra Miracle 42 A/S	4
3. Systembeskrivelse fra Miracle 42 A/S	6
3.1 Introduktion	6
3.2 Beskrivelse af Miracle 42 A/S' ydelser	6
3.3 Miracle 42 A/S' organisation og sikkerhed	6
3.4 Risikostyring ved Miracle 42 A/S	7
3.5 Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering	7
3.6 Etableret kontrolmiljø	7
3.6.1 Informationssikkerhedspolitikker (A5)	8
3.6.2 Organisering af informationssikkerhed (A6)	8
3.6.3 Personalesikkerhed (A7)	9
3.6.4 Adgangskontrol (A9)	9
3.6.5 Fysisk sikring og mijøsikring (A11)	10
3.6.6 Driftssikkerhed (A12)	11
3.6.7 Kommunikationssikkerhed (A13)	14
3.6.8 Styring af informationssikkerhedsbrud (A16)	14
3.6.9 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring (A17)	14
3.7 Supplerende information om det etablerede kontrolmiljø og forhold, som skal iagttages af kundernes revisorer	15
4. Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf	16
4.1 Introduktion	16
4.2 Test af kontroller	16
4.3 Test af kontrollernes funktionalitet	16
4.4 Test af udførte kontroller hos Miracle 42 A/S	16

1. Uafhængig revisors erklæring

Til ledelsen hos Miracle 42 A/S, Miracle 42 A/S' kunder og deres revisorer

Omfang

Vi har fået til opgave at erklære os om Miracle 42 A/S' udtalelse i afsnit 2 samt de tilhørende beskrivelser af system- og kontrolmiljøet i afsnit 3 for Miracle 42 A/S' ydelser til de tilsluttede kunder, omfattende udformning, implementering og funktionalitet af de kontroller, der er anført i beskrivelsen. Miracle 42 A/S' beskrivelse omhandler drift og hosting af applikationer samt den underliggende infrastruktur (generelle it-kontroller).

Erklæringen omfatter de fælles kontroller, som varetages af Miracle 42 A/S. Denne erklæring omfatter ledelsens beskrivelse af kontrolmål og de hertil hørende kontrolaktiviteter hos Miracle 42 A/S på alle områder inden for de generelle it-kontroller, som henføres til de leverede serviceydelser. Der anvendes ikke underleverandører.

Nogle af de kontrolmål, der er anført i Miracle 42 A/S' beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Miracle 42 A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

Miracle 42 A/S' ansvar

Miracle 42 A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 2, "Serviceleverandørs udtalelse", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed i IESBA's Ethiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Deloitte anvender ISQC 1 og opretholder derfor et omfattende system til kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav i 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 funktionaliteten 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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed for beskrivelsen, udformningen og funktionaliteten af kontroller hos Miracle 42 A/S omfatter udførelse af procedurer med henblik på at opnå bevis for Miracle 42 A/S' be-

skrivelse af sit system samt for kontrollernes udformning og funktionalitet. De udvalgte procedurer afhænger af revisors vurdering, herunder vurdering af risikoen for, at beskrivelsen ikke fremstår dækkende, og at kontroller ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores procedurer omfatter en test af funktionaliteten af de kontroller, som vi anser som nødvendige for at opnå en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, bliver nået. Vores procedure omfatter endvidere en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2.

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

Begrænsninger i kontroller hos en serviceleverandør

Miracle 42 A/S' beskrivelse er udarbejdet med henblik på at imødekomme kravene fra kunderne og disses revisorer, men omfatter ikke nødvendigvis alle aspekter af kontrol i et system, som den enkelte kunde anser som værende vigtig for sit eget kontrolmiljø. Kontroller i en servicevirksomhed kan heller ikke i sagens natur forhindre eller opdage alle fejl eller udeladelser i proces- eller rapporteringstransaktioner. Derudover er forskydningen af effektivitetsvurdering udsat for den risiko, at kontroller i en servicevirksomhed kan blive utilstrækkelige eller fejle.

Endvidere vil en anvendelse af vores konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller eller i virksomhedens overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion muligvis ikke længere vil være gældende.

Konklusion

Vores konklusion er udformet på basis af de forhold, der er beskrevet i denne erklæring. De kriterier, som vi har anvendt i forbindelse med vores konklusion, er beskrevet i afsnit 2. På grundlag af den udførte revision er det vores vurdering, at:

- a) beskrivelsen af de generelle it-kontroller relateret til drift og hosting for de tilsluttede kunder, således som de var udformet og implementeret i perioden fra 01.01.2019 til 31.12.2019, 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 01.01.2019 til 31.12.2019
- 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 01.01.2019 til 31.12.2019.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring, beskrivelsen af system- og kontrolmiljøet i afsnit 3 samt vores test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der anvender Miracle 42 A/S' serviceydelser, og disses revisorer, som har tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om de tilsluttede kunders egne kontroller, når de vurderer risici for væsentlige fejlinformationer i deres årsregnskaber.

København, den 12. februar 2020

Deloitte

Statsautoriseret Revisionspartnerselskab

CVR-nr. 33 96 35 56



Thomas Kühn

partner, statsautoriseret revisor

2. Udtalelse fra Miracle 42 A/S

Denne udtalelse er udarbejdet til brug for Miracle 42 A/S' kunder, der anvender Miracle 42 A/S' serviceydelser, og disses revisorer. Vores udtalelse omfatter beskrivelsen af system- og kontrolmiljøet, herunder de kontroller, som Miracle 42 A/S udfører for kunderne i relation til de indgåede aftaler med Miracle 42 A/S. Vores beskrivelse af arbejdsprocesser og udførte kontroller er nærmere beskrevet i afsnit 3 – Systembeskrivelse fra Miracle 42 A/S.

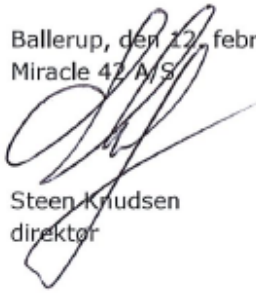
Vores beskrivelse omfatter perioden fra 01.01.2019 til 31.12.2019 og forudsætter, at kunderne og deres revisorer har tilstrækkelig forståelse af og omkring de leverede serviceydelser til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har etableret, ved vurdering af risiciene for fejlinformation i kundernes årsregnskaber.

Miracle 42 A/S bekræfter, at:

1. den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af de generelle kontroller i tilknytning til Miracle 42's outsourcingydelser, der er anvendt af kunder i perioden fra 1. januar 2019 – 31. december 2019. Kriterierne for denne udtalelse er, at den medfølgende beskrivelse:
 - a) redegør for, hvordan de generelle it-kontroller var udformet og implementeret, herunder redegør for:
 - i. de typer af ydelser, der er leveret, når det er relevant
 - ii. de processer, i både it- og manuelle systemer, der er anvendt til styringen af de generelle it-kontroller
 - iii. relevante kontrolmål, og kontroller udformet til at nå disse mål
 - iv. kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementeret af Miracle 42's kunder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
 - v. andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller
 - b) indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget i perioden fra 01.01.2019 til 31.12.2019
 - c) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer, og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte kunde måtte anse for at være vigtigt efter dennes særlige forhold.

2. de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 01.01.2019 til 31.12.2019. Kriterierne for denne udtalelse er, at:
- a) de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen var identificeret
 - b) de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
 - c) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 01.01.2019 til 31.12.2019.

Ballerup, den 12. februar 2020
Miracle 47 A/S



Steen Knudsen
direktør

3. Systembeskrivelse fra Miracle 42 A/S

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 for perioden fra 01.01.2019 til 31.12.2019.

3.2 Beskrivelse af Miracle 42 A/S' ydelser

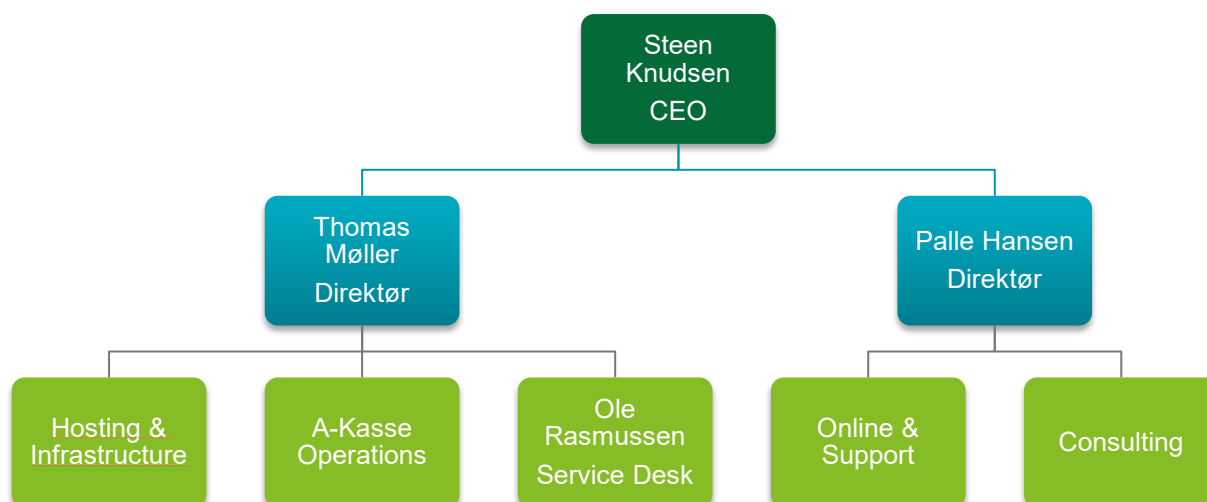
Miracle 42 leverer i dag en bred vifte af it-konsulentytelser til mere end 250 danske kunder med en samlet omsætning på mere end 80 mio. kr. Miracle 42's kerneydelser er hosting og konsulentvirksomhed inden for Microsoft og Oracle. Vores mangeårige erfaring med at drive store it-løsninger gør os i stand 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, projektlejelse, arkitektur, database og infrastruktur.

Miracle 42 har indarbejdet processer og fokuseret målrettet på it-drift siden 2011. Miracle 42 forholder sig løbende til opbygning af gode processer inden for projektlejelse, procesledelse, teknologiledelse, kompetencestyring samt styring og gennemførelse af it-projekter. Miracle 42 har indarbejdet metoder, værktøjer og processer fra PRINCE2, DS484/ISO27001, ISAE3402 og ITIL®.

Miracle 42 ser kvalitetsstyring som en løbende vurderingsproces integreret i løsningsvalg, dokumentation, projektlejelse 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 trusselvurdering, 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 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 ISO27001:2014.

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 ISO27001 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 hostingafdeling. 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 tildelt og at medarbejdere er bevidste om og lever op til deres informationssikkerhedsansvar.

Der er fastlagt procedurer for screening i forbindelse med ansættelser, beskrevne ansættelsesvilkår og -betingelser, og at ledelsesansvar er klart defineret. Herudover skal det sikres, at der følges metodisk op på gennemførelse af awareness omkring 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-kampanjer. 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 mijøsikring (A11)

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

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.

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 temperaturføler, 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 korrekte temperatur til sikring af stabil drift og lang holdbarhed på det anvendte it-udstyr. Der udføres løbende 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)

3.6.4.1 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 udføres en vurdering af fejl og opfølgning på evt. fejlretning.

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 løbende, 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 2 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.

3.6.4.2 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 onli-

ne 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.

3.6.4.3 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.

3.6.4.4 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.

3.6.4.5 Systemsoftware

Formål

Ny systemsoftware samt modifikationer 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-plattformene. På Windows-plattformen 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 frivillige 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-plattformene. 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 modifikationer 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 karenperiode, 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 mitigerende. 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 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 omkring katastrofehåndtering i overensstemmelse med kundernes egne forventninger til et betryggende niveau for Business Continuity i og omkring Modulus-systemmiljøet.

Efterlevelse af relevant lovgivning

Miracle 42 har tilrettelagt procedurer og kontroller, således at de krav, som er Miracle 42's ansvar, efterleveres 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, Persondataloven 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 udviklingsydelse, 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. Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf

4.1 Introduktion

Denne rapport er udformet med henblik på at informere Miracle 42 A/S' kunder om Miracle 42 A/S' systemer og kontroller, som kan påvirke behandlingen af forretningsrelaterede transaktioner, og samtidig informere Miracle 42 A/S' kunder om funktionaliteten af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i brugerorganisationernes forretningsprocesser, har til hensigt at hjælpe brugerorganisationens revisor til at (1) planlægge revisionen af brugerorganisationens årsregnskaber og (2) vurdere risici for fejl i årsregnskaber, som muligvis påvirkes af de generelle it-kontroller hos Miracle 42 A/S.

Vores test af Miracle 42 A/S' kontroller er begrænset til de kontrolmål og tilknyttede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller til de generelle it-kontroller, som skal være implementeret i brugerorganisationerne for at opfylde kontrolmålene. Det er hver brugerorganisations revisors ansvar at evaluere denne information ift. de kontroller, som eksisterer i hver brugerorganisation. Hvis bestemte supplerende kontroller ikke er til stede i brugerorganisationerne, kan Miracle 42 A/S' kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De test, der udføres i forbindelse med fastlæggelse af kontrollers funktionalitet, består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos Miracle 42 A/S
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelsen af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genduførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3 Test af kontrollernes funktionalitet

Vores test af kontrollernes funktionalitet inkluderer de test, som vi betragter som nødvendige for at evaluere, hvorvidt de udførte kontroller og overholdelsen af disse er tilstrækkelige til at give en høj, men ikke absolut, sikkerhed for, at de specificerede kontrolmål blev opnået i løbet af perioden fra 01.01.2019 til 31.12.2019. Vores test af kontrollernes funktionalitet var udformet til at dække et repræsentativt antal af transaktioner i løbet af perioden fra 01.01.2019 til 31.12.2019 for hver kontrol, jf. nedenfor, som er udformet til at opnå de specifikke kontrolmål. I udvælgelsen af specifikke test har vi overvejet (a) karakteren af de testede områder, (b) typerne af tilgængelig dokumentation, (c) karakteren af de revisionsmål, der skal opnås, (d) det vurderede kontrolrisikoniveau og (e) testens forventede effektivitet.

4.4 Test af udførte kontroller hos Miracle 42 A/S

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført, og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

4.4.1 Informationssikkerhedspolitikker (A5)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: 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.			
4.4.1.1 <i>It-sikkerhedspolitik</i>	Den eksisterende it-sikkerhedspolitik bliver løbende opdateret, såfremt der er behov for dette, og revurderes mindst en gang årligt. Gennemgang af sikkerhedspolitikken varetages af sikkerhedsgruppen.	Deloitte har inspiceret den seneste ajourførte it-sikkerhedspolitik og vurderet, om denne er betryggende. Yderligere er det konstateret, at it-sikkerhedspolitikken er godkendt.	Ingen bemærkninger.
4.4.1.2 <i>It-risikoanalyse</i>	Trussels- og risikovurderinger bliver løbende opdateret, såfremt der er behov for dette, og revurderes mindst en gang årligt. Opdatering af risikoanalysen varetages af driftschefen.	Deloitte 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.

4.4.2 Organisering af informationssikkerhed (A6)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.			
4.4.2.1 <i>Roller og ansvarsområder for informationssikkerhed</i>	Miracle 42 A/S har defineret og fordelt ansvarsområder for informationssikkerheden samt kommunikeret dette til medarbejderne.	Deloitte har inspiceret, at ledelsen har implementeret en it-sikkerhedsgruppe og har udpeget informationssikkerhedsansvarlige. Deloitte har forespurgt et udvalg af medarbejdere med henblik på at konstatere, om de var bekendte med ansvarsplaceringen mht. informationssikkerhed i organisationen.	Ingen bemærkninger.
4.4.2.2 <i>Funktionsadskillelse</i>	Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Deloitte har stikprøvevist inspiceret den organisatoriske fordeling i Miracle 42 A/S med henblik på at konstatere, om modstridende funktioner og ansvarsområder er adskilt.	Ingen bemærkninger.

4.4.3 Medarbejdersikkerhed (A7)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: At sikre, at medarbejdere forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt. At sikre, at medarbejdere er bevidste om og lever op til deres informationsikkerhedsansvar.			
4.4.3.1 <i>Screening</i>	Der indhentes som hovedregel udtalelser fra ansøgers oplyste referencer, før en aftale indgås, herunder indhentes straffeattester, hvis det på baggrund af stillingsindholdet vurderes relevant.	Deloitte har inspiceret ansættelsesproceduren og de sikkerhedsopgaver, der skal udføres i den forbindelse. Deloitte har endvidere inspiceret et udvalg af kommunikation mellem DPO og afdelingsledere, hvori det påpeges, at relevante referencetjek udføres.	Ingen bemærkninger.
4.4.3.2 <i>Ansættelsesvilkår og -betingelser</i>	Som en del af den kontraktlige forpligtelse underskriver medarbejdere og eksterne brugere betingelserne i ansættelseskontrakten, der beskriver deres og virksomhedens ansvar for informationsikkerhed.	Deloitte 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. Deloitte har endvidere inspiceret template til ansættelseskontrakter og indhentet jobbeskrivelser med henblik på at konstatere, om sikkerhedsansvar var beskrevet heri.	Ingen bemærkninger.
4.4.3.3 <i>Ledelsesansvar</i>	Ledelsen kræver, at medarbejdere og eksterne brugere opretholder sikkerheden i overensstemmelse med virksomhedens fastlagte politikker og procedure.	Deloitte har inspiceret beskrivelsen af ledelsens krav til medarbejdere og eksterne brugere. Deloitte har endvidere inspiceret procedurer, hvori det påpeges, at alle har pligt til at overholde sikkerhedspolitikken, herunder sikkerhedshåndbogen.	Ingen bemærkninger.
4.4.3.4 <i>Bevidsthed om samt uddannelse og træning i informationsikkerhed</i>	Virksomhedens medarbejdere og, hvor det er relevant, eksterne brugere bevidstgøres om sikkerhed og holdes regelmæssigt ajour med virksomhedens politikker og procedurer.	Deloitte har inspiceret, at der regelmæssigt gøres opmærksom på sikkerhedspolitikker og procedurer. Deloitte har desuden konstateret, at der gennemføres årlige awareness-kampagner med fokus på sikkerhed.	Ingen bemærkninger.

4.4.4 Adgangskontrol (A9)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
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.			
4.4.4.1 <i>Brugerrettigheder – Oprettelser og ændringer</i>	Brugere oprettes kun på baggrund af skriftlige henvendelser (e-mails) modtaget i Topdesk fra de tilsluttede kunder. Brugere oprettes med de ønskede parametre, og dette dokumenteres. Interne brugere registreres også i Topdesk.	Deloitte har inspiceret retningslinjer og procedure for adgangsstyring med henblik på at konstatere, at disse er betryggende. Deloitte har stikprøvevis inspiceret oprettede brugere og vurderet, om der er et dokumenteret grundlag for de tildelte adgange og rettigheder.	Ingen bemærkninger.
4.4.4.2 <i>Brugerrettigheder – Udvidede rettigheder</i>	Interne medarbejders adgang til systemer dokumenteres i Topdesk. Driftsmedarbejdere får tildelt udvidede rettigheder, og dette godkendes formelt af driftschefen, og medarbejderen underskriver en admin-erklæring.	Deloitte har ved inspektion vurderet anvendte procedurer og udførte kontroller for håndtering af brugere med udvidede rettigheder. Deloitte 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. Deloitte har desuden inspiceret de underskrevne admin-erklæringer.	Ingen bemærkninger.
4.4.4.3 <i>Brugerrettigheder – Nedlæggelser</i>	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.	Deloitte har ved inspektion vurderet anvendte procedurer og udførte kontroller for nedlæggelse af brugere. Deloitte har stikprøvevis inspiceret at fratrådte Miracle 42 A/S-medarbejdere har fået deres bruger-id nedlagt.	Ingen bemærkninger.
4.4.4.4 <i>It-sikkerhedsorganisation</i>	Der er for Miracle 42 A/S lavet en formel rollefordeling omkring drift, support og Helpdesk.	Deloitte har gennemgået beskrivelser af roller og ansvarsområder og har ved interview verificeret, at disse stemmer overens med de faktiske roller og ansvarsområder hos medarbejdere.	Ingen bemærkninger.
4.4.4.5 <i>Anvendelse af passwords</i>	Autentificering af brugere gennemføres via Windows AD, hvor der er opsat en passwordpolitik, der sikrer kvaliteten og regel-	Deloitte har inspiceret konfigurationen af passwordopsætningen på Windows AD og verificeret, at den opsatte politik anvendes som	Vi har fået oplyst, at grundet tekniske begrænsninger er det ikke muligt at gennemtvinge Miracle 42's

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
	<p>mæssige skift af passwords.</p> <p>Der er opsat kvalitetskrav for passwords, således at der kræves en minimumslængde, samt krav om kompleksitet, krav om periodisk skifte af password, ligesom passwordopsætninger medfører, at password ikke kan genbruges, og at brugere bliver lukket ude ved gentagne fejlslagne forsøg på login.</p>	<p>standard på domænet.</p> <p>Deloitte har endvidere gennemgået opsætningen af password-parametre på udvalgte platforme og vurderet, om disse understøtter de beskrevne krav til passwordkvalitet.</p>	<p>krav til passwordpolitikker fra centralt hold på SAN, Openshift-miljøet og Weblogic-applikationen.</p> <p>Ingen yderligere bemærkninger.</p>
4.4.4.6 <i>Anvendelse af brugerprofiler</i>	Alle brugere er oprettet med individuelle brugerprofiler. Der anvendes serviceprofiler i Miracle 42 A/S, i det omfang det vurderes hensigtsmæssigt.	Deloitte har inspiceret anvendelsen af brugerprofiler på systemer og platforme og verificeret, at disse er personlige og identificerbare.	Ingen bemærkninger.
4.4.4.7 <i>Ændring af standardpassword</i>	Standardbrugerens password skiftes i forbindelse med implementering af centrale applikationer og hardware-komponenter. Der er etableret en passworddatabase, hvor adgangskoder til alle servere og udstyr er registreret.	Deloitte har inspiceret forhold vedr. standardpasswords og konstateret, at der er etableret beskyttet password database, hvor kun medarbejdere med et arbejdsmæssigt behov har adgang.	Ingen bemærkninger.
4.4.4.8 <i>Anvendelse af åbne netværk</i>	Der anvendes ikke åbne netværk. Interne servere og kundesystemer er adskilt, og al trafik afvikles over lukkede MPLS-/VPN-forbindelser.	Deloitte 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.
4.4.4.9 <i>It-sikkerhedslogning</i>	Der er etableret logning af logins og ændringer til brugerkonti i Windows AD. Der laves ikke gennemgang af logs, medmindre der opleves fejl eller er begrundet mistanke om misbrug.	Deloitte har inspiceret, om der er etableret logning på logins til interne systemer. Deloitte her gennemgået processen for overvågning af sikkerhedshændelser og alarmer.	Ingen bemærkninger.

4.4.5 Fysisk sikring og miljøsikring (A11)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: It-faciliteterne administreres hensigtsmæssigt for at sikre integriteten af finansielle informationer. It-faciliteterne beskyttes mod brand, vand og temperaturændringer.			
4.4.5.1 <i>Fysisk adgang - Adgang til kritiske lokationer</i>	Adgang til serverrum er kontrolleret via kortlæser og kode. Kun autoriseret personale fra Miracle 42 A/S har adgang til rummet.	Deloitte har inspiceret, om adgangen til kritiske lokationer er begrænset via personlige adgangskort, og at adgang til kritiske lokationer som serverrummet er godkendt.	Ingen bemærkninger.
4.4.5.2 <i>Fysisk sikkerhed - Strømsikring</i>	Der er i serverrummet forbundet UPS-anlæg samt generator på alle servere. Der er yderligere indgået kontrakt om periodisk vedligeholdelse af UPS og generatorløsning.	Deloitte har observeret, at der er opsat nødstrømsanlæg, og inspiceret, at der er dokumentation for periodisk gennemgang af løsningen.	Ingen bemærkninger.
4.4.5.3 <i>Fysisk sikkerhed - Brandsikring</i>	Serverrum er forsynet med automatisk brandslukningsudstyr og alarmer for både røg og temperatur. Der er indgået kontrakt om periodisk vedligeholdelse af brandslukningsanlægget.	Deloitte 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.
4.4.5.4 <i>Fysisk sikkerhed - Klimaovervågning og køling</i>	Serverrummet er forsynet med et kølesystem, så maskinerne ikke bliver overophedet. Der er desuden indgået kontrakt om periodisk vedligeholdelse af kølesystemet.	Deloitte har observeret, at der er opsat et kølesystem i serverrummet, og konstateret, at der er udført service på anlægget.	Ingen bemærkninger.
4.4.5.5 <i>Fysisk sikkerhed - Indretning</i>	Serverrummet er indrettet således, at 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.	Deloitte har observeret indretningen af kritiske lokationer og vurderet, om der er forhold, som udgør en risiko for indtrængning af vand og fugt.	Ingen bemærkninger.

4.4.6 Driftssikkerhed (A12)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: Data sikkerhedskopieres løbende, for at sikre, at finansielle data forbliver nøjagtige, fuldstændige og gyldige gennem opdaterings- og lagringsprocessen.			
4.4.6.1 <i>Backup – Strategi</i>	Der er udarbejdet backupstrategier for alle servere og systemer. Strategierne bliver løbende opdateret, når der bliver tilføjet nye systemer eller data.	Deloitte har inspiceret backupstrategierne og vurderet, om disse i tilstrækkelig grad af-dækker backupkrav for kritiske systemer og data, som håndteres for kunderne.	Ingen bemærkninger.
4.4.6.2 <i>Backup – Konfiguration</i>	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.	Deloitte har inspireret en stikprøve på, at backupkonfigurationen stemmer overens med den udarbejdede backupstrategi. Endvidere har Deloitte testet den daglige efterkontrol af backupafviklingen.	Ingen bemærkninger.
4.4.6.3 <i>Backup – Intern opbevaring</i>	Backup afvikles til disk i datacenteret og kopieres umiddelbart herefter til et remote datacenter. Der laves ikke backup til bånd.	Deloitte har inspiceret og vurderet, om den interne opbevaring af backupmedier er betryggende.	Ingen bemærkninger.
4.4.6.4 <i>Backup – Test</i>	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.	Deloitte 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.			
4.4.6.5 <i>Overvågning</i>	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.	Deloitte har inspiceret Miracle 42 A/S' opsætning af alarmer og behandling heraf. Endvidere har Deloitte 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.			
4.4.6.6 <i>Service Desk og incidenthåndtering</i>	Der er etableret skriftlige procedurer for Helpdesk og incidenthåndtering. Alle henvendelser behandles i Service Desk-systemet og dokumenteres.	Deloitte har inspiceret driftsprocedurerne og de udførte kontroller samt gennemgået Topdesk-systemet til dokumentering af kontrollerne.	Ingen bemærkninger.

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: Ny systemsoftware samt modifikationer til eksisterende systemsoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.			
4.4.6.7 <i>Systemsoftware - Patch Management</i>	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.	Deloitte har stikprøvevis inspiceret, at opdateringer til servere implementeres og dokumenteres som beskrevet.	Ingen bemærkninger.
4.4.6.8 <i>Systemsoftware - Test</i>	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.	Deloitte har inspiceret proceduren for opdatering og test forud for frigivelse til brugerne og har kontrolleret procedurene omkring backup.	Ingen bemærkninger.
4.4.6.9 <i>Systemsoftware - Fallback</i>	Fallback er etableret gennem restore af backup. Hvis muligt afinstalleres patchen.	Deloitte har inspiceret proceduren for opdatering. Endvidere har vi testet forhold omkring reetablering af backup.	Ingen bemærkninger.
4.4.6.10 <i>Systemsoftware - Timing</i>	Alle servere opdateres ud fra fastsat schedule hver anden måned. Redundante servere opdateres forskudt for at sikre driften.	Deloitte har inspiceret proceduren for opdatering af servere og verificeret, om der er sket kommunikering af servicevinduer.	Ingen bemærkninger.
4.4.6.11 <i>Systemsoftware - Dokumentering af systemer</i>	Der er etableret en serverdatabase, der indeholder alle relevante informationer om servere.	Deloitte har inspiceret, om dokumentationen for kundesystemer i serverdatabase er fyldestgørende.	Ingen bemærkninger.

4.4.7 Kommunikationssikkerhed (A13)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: Ny netværkssoftware samt modifikationer til eksisterende netværkssoftware implementeres hensigtsmæssigt og fungerer i overensstemmelse med ledelsens forventninger.			
4.4.7.1 <i>Netværk og kommunikation – Patch Management</i>	Relevante firmware-opdateringer vurderes løbende og implementeres efter behov. Opdateringer installeres kun, såfremt det er nødvendigt for at sikre kommunikationen. Alle ændringer dokumenteres i Kiwi Cat-Tools.	Deloitte har inspiceret proceduren for vedligeholdelse og opdatering af netværk- og kommunikationsudstyr og for en stikprøve kontrolleret, at ændringer til netværket dokumenteres.	Ingen bemærkninger.
4.4.7.2 <i>Netværk og kommunikation – Test</i>	Ændringer til netværket testes i forbindelse med idriftsættelse. Kritiske netværkskomponenter kører i cluster og kan opdateres enkeltvis med mulighed for tilbagerulning.	Deloitte har inspiceret proceduren for vedligeholdelse og opdatering af netværks- og kommunikationsudstyr og kontrolleret, at dette dokumenteres.	Ingen bemærkninger.
4.4.7.3 <i>Netværk og kommunikation – Fallback</i>	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.	Deloitte har stikprøvevis inspiceret at der er arkiveret gamle konfigurationer til netværksudstyr og foretaget test af den automatiske rapportgenerering.	Ingen bemærkninger.
4.4.7.4 <i>Netværk og kommunikation – Timing</i>	Væsentlige ændringer til netværkskonfigurationer skal om muligt ske uden for normal arbejdstid, således at disse ikke forstyrrer driften unødigt. Såfremt der planlægges større nedetid, meldes dette ud til kunder.	Deloitte 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.
4.4.7.5 <i>Netværk og kommunikation – Dokumentation af netværk</i>	Netværket dokumenteres via topologitegninger. Al aktivt udstyr er endvidere registreret i ip-oversigter.	Deloitte har inspiceret den seneste dokumentation for netværket og verificeret ved interview, at denne stemmer overens med det faktiske setup.	Ingen bemærkninger.

4.4.8 Styring af informationssikkerhedsbrud (A16)

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.			
4.4.9.1 <i>Ansvar og procedurer</i>	Der er udarbejdet en procedure vedr. informationssikkerhedshændelser, hvori der tages stilling til ansvarsplacering, rapportering, procedurer, diskretion og håndtering.	Deloitte 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.
4.4.9.2 <i>Rapportering af informationssikkerhedshændelser</i>	Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Deloitte har inspiceret, at der er implementeret procedurer til registrering og rapportering af informationssikkerhedshændelser.	Vi har fået oplyst, at der ikke har været nogen informationssikkerhedshændelser i erklæringsperioden. Ingen yderligere bemærkninger.
4.4.9.3 <i>Vurdering af og beslutning om informationssikkerhedshændelser</i>	Informationssikkerhedshændelser vurderes, og det beslutes, om de skal klassificeres som informationssikkerhedsbrud.	Deloitte har inspiceret at der er implementeret procedurer for registrering, vurdering og rapportering af informationssikkerhedshændelser.	Vi har fået oplyst, at der ikke har været nogen informationssikkerhedshændelser i erklæringsperioden. Ingen yderligere bemærkninger.
4.4.9.4 <i>Håndtering af informationssikkerhedsbrud</i>	Informationssikkerhedsbrud håndteres i overensstemmelse med de dokumenterede procedurer.	Deloitte har inspiceret, at sikkerhedsbrud er gennemgået og vurderet efter den implementerede procedure.	Vi har fået oplyst, at der ikke har været nogen informationssikkerhedshændelser i erklæringsperioden. Ingen yderligere bemærkninger.

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

Kontrolaktivitet	Etableret kontrol hos Miracle 42 A/S	Testplan	Testresultat
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.			
4.4.10.1 <i>Beredskabsplanlægning</i>	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.	Deloitte har inspiceret den etablerede beredskabsplan og kontrolleret, at de beskrevne elementer er indeholdt. Deloitte 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.
4.4.10.2 <i>Beredskabstest</i>	Miracle 42 A/S tester løbende, om backup af kundeservere kan reetableres som forventet. Dette dokumenteres i sagsstyrings-systemet. Endvidere udføres der løbende service på sikringsforanstaltningerne i data-centeret.	Deloitte har inspiceret dokumentationen for den seneste beredskabsøvelse.	Ingen bemærkninger.