Uafhængig revisors ISAE 3402 type II – erklæring

Med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med ydelser relateret til behandling og berigelse af data i perioden 1 marts 2020 til 17 februar 2021.

IDQ A/S

CVR Nr.: 34 04 62 20

Indholdsfortegnelse

Symbol

- Vores gennemgang har ikke ført til bemærkninger.
- Der er konstateret svagheder i kontrollerne.
- Der er fundet kritiske svagheder eller mangler.

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt IDQ A/S' ydelser relateret til behandling og berigelse af data i perioden, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

IDQ A/S bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af ydelser relateret til behandling og berigelse af data og de tilhørende kontroller i perioden fra d. 1 marts 2020 til d. 17 februar 2021. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

i. redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

- de typer af ydelser, der er leveret, når det er relevant.
- de processer i både it- og manuelle systemer, der er anvendt til sikring af fortrolighed, integritet og tilgængelighed af systemer og data. relevante kontrolmål og kontroller, udformet til at nå disse mål.
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, 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.
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen.

ii. Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden d. 1 marts 2020 til d. 17 februar 2021.

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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i perioden d. 1 marts 2020 til d. 17 februar 2021 . Kriterierne for denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificerede.

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

iii. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden d. 1 marts 2020 til d. 17 februar 2021.

København, 25. juni 2021

IDQ A/S

Henrik Saustrup

Direktør

2. IDQ A/S' beskrivelse af generelle it-kontroller

1. Kontrolmiljø

Vi har i virksomheden implementeret en række kontroller med henblik på at kvalitetssikre og dokumentere kvaliteten i vores ydelser. Alle kontroller, hvad enten de relaterer sig til en processuel eller teknisk håndtering, har en udførende ansvarshavende, og i visse tilfælde også en ansvarshavende godkender. Med mindre andet er anført er den udførende ansvarshavende IDQs CTO og den ansvarshavende godkender IDQs CEO.

Vores kontroller er rettet mod dels konkrete arbejdshandlinger og dels processer for en række arbejdshandlinger, som igen kan have yderligere konkrete kontroller tilknyttet. Tidsangivelse for en given kontrol opgives altid inden for en given periode. Kontrollerne tilsigtes at blive udført inden for denne periode, men driftsmæssige omstændigheder og/eller ventetid i forbindelse med leverandører eller kunder kan betyde at den praktiske kontrol udføres senere. Oversigten over kontrollerne findes i IDQs årshjul.

2. Vores kerneydelser

IDQ A/S er en data- og softwarevirksomhed, som udvikler og markedsfører software til forøgelse af datakvalitet. Omdrejningspunktet er de tre produkter iDQ Search, iDQ Alert og iDQ Services.

iDQ Searchs formål er at tilbyde brugerne samlet adgang til søgning, opslag og overførsel af relevante markedsdata gennem et brugervenligt userinterface.

iDQ Search giver adgang til egne kundedata samt gratis datakilder og betalingstjenester. Af primære kilder kan nævnes CPR-registret, CVR-registret, OIS/BBR, Statstidende, Tinglysningen, teledata samt kreditoplysninger fra RKI og Bisnode. iDQ Search anvendes især i forbindelse med kundeoprettelse af såvel private forbrugere som virksomheder, men anvendes desuden som søgeværktøj i relation til returpost, inkassosager, kreditforespørgsler osv.

iDQ Alerts formål er at tilbyde brugerne løbende opdatering af kunde-stamdata – fx flytninger, dødsfald, navneskift og virksomhedslukninger. Desuden er formålet at give notifikationer omkring vigtige begivenheder i kundedatabasen – begivenheder som kan betyde ændringer i risikoscenariet, fx betalingsstandsninger, udlæg, tvangsauktioner osv.

iDQ Services giver adgang til en lang række webservices (også kaldet api'er), som benytter sig af de samme kilder, som anvendes i forbindelse med iDQ Search. Disse services anvendes af kunderne til at integrere data direkte i kundens egne applikationer.

3. Informationssikkerhedsrelaterede kontroller

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

Virksomhedens it-sikkerhedspolitik opdateres såfremt der foretages ændringer eller implementeres nye forretningsområder, og politikken gennemgås i sin helhed minimum én gang årligt, jf. årshjulet. Når vi har ændret ting i it-sikkerhedspolitikken, og minimum efter den årlige gennemgang, fremlægges ændringerne internt ved førstkommende månedsmøde for personalet. Ligeledes bliver eksterne leverandører inddraget og orienteret, hvis det har relevans.

Det er virksomhedens CTO, som er ansvarlig for virksomhedens informationssikkerhed.

2. IDQ A/S' beskrivelse af generelle it-kontroller

4. Risikostyring

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

Risikovurdering foretages periodisk, minimum én gang årligt, samt når der foretages ændringer eller implementeres nye systemer, som vi vurderer at have relevans i forhold til vores generelle risikovurdering.

5. HR- og medarbejderrelaterede kontroller

Forud for ansættelse af medarbejdere følges en ansættelsesprocedure udarbejdet af selskabets HR-funktion. Det er den ansættende direktør, som er ansvarlig for de HR-relaterede kontroller.

For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid opgavespecifik kontrakt, dedikeret fortrolighedserklæring, og anden relevant dokumentation indhentes.

Det er virksomhedens direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv.

Den tekniske oprettelse af medarbejdere, såvel som konsulenter, foretages i henhold til relevante procedurer. Vi har desuden en proces for kontrol af alle brugere med rettigheder til virksomhedens netværk.

Medarbejdere, og eksterne parter når relevant, bliver uddannet og trænet i vores retningslinjer for it-sikkerhed og de deraf afledte opgaver. Dette foregår som sidemandsoplæringer, ved kontormøder o. lign.

5.1 Afhængighed af nøglemedarbejdere

Via vores dokumentation og beskrivelser sikrer vi os mod personafhængighed. Vi arbejder således med dobbeltroller på de vigtigste af vores funktioner. Der afholdes månedlige one2one samtaler med nøglemedarbejdere i it-udvikling. Møderne har til formål at sikre en høj trivsel og følge op på medarbejderens ansvarsområder og på den måde minimere risikoen for og ved jobskifte.

6. Kunde-relaterede kontroller

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

7 Driftsrelaterede kontroller

7.1 Fysisk sikkerhed

Al vores udstyr er placeret hos vores datacenter leverandør. Vi har ikke fysisk adgang til datacenteret, men inspicerer dette årligt. Vores datacenter leverandør har revisorerklæring af type ISAE 3402-II, som afgives årligt, og vi indhenter årligt revisorerklæringen.

Vores fysiske kontor er placeret i Lygten 39 i København. Vi har en proces for sikring af lokationen.

7.2 Databærende medier

Alle mobiltelefoner er sikret med en MDM-løsning indeholdende en række sikkerhedspolitikker. Følsomme data må alene opbevares på serverrumsmedier eller i krypteret form på egen fildelingsløsning.

2. IDQ A/S' beskrivelse af generelle it-kontroller

7.3 Bortskaffelse af medier

Medier destrueres som en del af vores indkøbsaftale med leverandøren. Ved tyveri af mobiltelefon, foretages en fuld sletning af telefonen. Det vil derefter ikke være muligt at tilgå vores netværk via den pågældende telefon.

7.4 Styring af netværk og drift

Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor person-afhængighed og 'sjuskefejl' minimeres.

Vores tekniske set-up fokuserer på samme værdier, og værn mod uvedkommendes adgang til vores data er af højeste prioritet. Vi har desuden antivirus-systemer, e-mail skanning, og systemer til overvågning og sikring af netværk og internetbrug. Al godkendt netværkstrafik (indgående) kommer igennem vores firewall. Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv.

Adgang til netværksydelser via mobile enheder sikres via en MDM-løsning.

Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse.

Standardændringer har, i videst muligt omfang, en dedikeret SOP. Alle væsentlige ændringer drøftes, prioriteres og godkendes af ledelsen.

Ekstern datakommunikation foregår, afhængig af type, via e-mails.

7.5 Teknisk ændringsstyring - patching

Operativsystem patchning foretages månedligt i et fastlagt servicevindue. Servicevinduet fremgår af virksomhedens generelle forretningsbetingelser, og skal ikke varsles separat. For kritiske systemopdateringer, eksempelvis Windows security updates, varsles kunderne i så god tid som muligt.

7.6 Overvågning og logning

Vi foretager daglig overvågning af vores systemer via automatiserede systemer til måling af grænseværdier. Alarmering, såfremt en kritisk hændelse konstateres, tilgår vores tekniske medarbejdere. Hændelser relateret til vores fælles platform, infrastruktur og serverrumsydelser håndteres af vores it-leverandør, som uden for kontortid har driftsvagt. Hændelser for login og log-out på vores platforme logføres, og vi benytter alene personhenførbare brugerkonti, hvorfor det er muligt at identificere, hvilke personer der har været logget på.

7.7 Adgangsstyring

Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Interne brugere oprettes alene på baggrund af skriftligt ønske fra ledelsen. Alle brugere er personhenførbare. For servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentligt log-on deaktiveret.

Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Interne brugere og deres adgangsniveau gennemgås periodisk af ledelsen.

7.8 Backup og sikkerhedskopiering

Vores kunders data er lige så vigtige som vores egne data, og vi har en procedure for at sikre samme. Vi tager dagligt backup, og vi har, ved vores leverandør, en procedure for kontrol af backup, herunder hvordan der skal ageres ved fejl.

2. IDQ A/S' beskrivelse af generelle it-kontroller

7.9 Kapacitetsstyring

Tilgængelighed er en af vores kerneværdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelser til vores kunder. Et af de væsentlige parametre IDQ måles på af kunderne er svartider på søgninger gennem IDQ-systemet. Derfor overvåger vi konstant vores kapacitet, både disk, cpu og trafik, og vi kan løbende, og uden gene for kunderne, udvide vores kapacitet.

8. Håndtering af sikkerhedshændelser

Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af hændelser. Vi har en række tiltag for at forhindre at sikkerhedshændelser opstår, og vi har driftsvagtordning med vores infrastrukturleverandør således, at der reageres straks en hændelse måtte opstå. Vi holder os tillige fagligt opdaterede vha. producenternes hjemmesider, debatfora mv.

8.1 Opfølgning på sikkerhedshændelser

Alle sikkerhedsbrud dokumenteres til internt brug, og hændelsen gennemgås med alle relevante medarbejdere ved førstkommende lejlighed. Afhængig af hændelsens karakter udarbejdes nye processer og procedurer, så vi undgår at hændelsen indtræffer igen.

Sikkerhedsrelaterede emner, generelle såvel som aktuelle emner, gennemgås desuden ved interne møder.

Ved kriminelle forhold sker en politimæssig efterforskning, hvor vores logføring og øvrige overvågning kan benyttes til opklaring og evaluering af sikkerhedshændelsen.

9. Beredskabsstyring

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

10. Leverandørforhold

10.1 Sikkerhed i leverandøraftaler og kontrol af serviceydelser fra tredjepart

Alle vores leverandør og partneraftaler skal indeholde regulering af fortrolighed.

Der indhentes tillige revisorerklæring fra vores kritiske leverandører.

11. Komplementerende kontroller

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

Desuden er vores kunder selv ansvarlige for, med mindre andet er aftalt, at; i) Det aftalte niveau for backup dækker kundens behov, ii) Brugeradministration, herunder anmodninger om oprettelse og nedtagning af bruger, og periodisk gennemgang, af kundens egne brugere, iii) At sporbarhed opretholdes i tredjepartssoftware, som kunden selv administrerer, iv) At kundespecifikke softwareløsninger understøtter den af os udbudte backup teknologi, v) Særaftale for backupjobs der kræver krypteringspassword, hvor kunden alene er ansvarlig for håndtering og opbevaring af krypteringspassword, og vi) Anmodning om adgang til kundens servermiljø for kundens tredjepartsleverandører, vii) Kundens anmeldelse til Datatilsynet, for hvem dette måtte være relevant.

2. IDQ A/S' beskrivelse af generelle it-kontroller

12. Overensstemmelse med lovbestemte og kontraktlige krav

Vi er underlagt Persondataloven i forhold til vores ydelser. Gennem softwareløsninger og databehandlingsservices optræder IDQ som databehandler underlagt GDPR (Persondataforordningen). Vores kunder kan dog være underlagt særlig lovgivning, og hvor det måtte være tilfældet, er vores understøttelse heraf aftalt særskilt.

Vi lader os årlige revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne nævnt i denne beskrivelse. Vi følger rammerne inden for ISO 27002, hvilket føromtalte revisor attesterer i en ISAE3402-erklæring.

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

Til: IDQ A/S og deres kunder

Omfang

Vi har fået til opgave at afgive erklæring om IDQ A/S' beskrivelse, som er gengivet i afsnit 2, som beskriver de udførte it-kontroller i forbindelse med ydelser relateret til behandling og berigelse af data i perioden d. 1 marts 2020 til d. 17 februar 2021, samt om udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

IDQ A/S' ansvar

IDQ A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse 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.

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.

Grant Thornton 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 serviceleverandør IDQ A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB.

Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt. En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet på i afsnit 2.

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

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

Begrænsninger i kontroller hos IDQ A/S

IDQ A/S beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos IDQ A/S som følge af deres art muligvis ikke forhindre eller opdage fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i IDQ A/S' beskrivelse i afsnit 2. Det vores opfattelse, at:

a) at beskrivelsen af kontroller, således som de var udformet og implementeret i hele perioden fra d. 1 marts 2020 til d. 17 februar 2021 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 d. 1 marts 2020 til d. 17 februar 2021, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra d. 1 marts 2020 til d. 17 februar 2021

Beskrivelse af test og kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på i afsnit 4 er udelukkende tiltænkt de kunder, der har anvendt IDQ A/S' ydelser relateret til behandling og berigelse af data og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 25. juni 2021

Grant Thornton

Statsautoriserede revisionspartnerselskab

CVR-nr: 34 20 99 36

Martin Bomholtz
Statsautoriseret revisor

Anders Grønning-Kjærgaard
Director, Head of IT Audit & Advisory
(CISA,CISM,CRISC & CISSP)

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Formål og omfang

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som IDQ A/S har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været nået i perioden d. 1 marts 2020 til d. 17 februar 2021.

Vi har således ikke nødvendigvis testet alle de kontroller, som IDQ A/S har nævnt i sin beskrivelse i afsnit 2. Kontroller udført hos IDQ A/S' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

4.2 Udførte testaktiviteter

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Vi har udført vores tests af kontroller hos IDQ A/S ud fra nedenstående metoder:

Metode	Overordnet beskrivelse
Forespørgelse	Interview af udvalgte medarbejdere angående kontroller
Observation	Observation af hvordan kontroller udførelse (Design)
Inspektion	Gennemgang af politikker, procedurer og dokumentation af kontrollernes udførelse (Implementering)
Test af kontrol	Gennemførelse af kontrolhandlinger, som vi selv har udført eller som har observeret gennemført af ansvarlige medarbejdere (Udførelse)

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4. Risikovurdering og -håndtering

Kontrolmål:
At sikre, at virksomheden periodisk foretager en analyse og vurdering af it-risikobilledet.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
4.1	Kontroller er etableret, som tilvejebringer rimelig sikkerhed for, at processer for risikovurdering er implementeret, og at risikovurderingen foretages minimum årligt.	Vi har modtaget den aktuelle og godkendte risikovurdering. Vi har bekræftet, at IDQ A/S' eksponering styres baseret på risikoscoren, der beregnes ud fra risikopåvirkningen og sandsynligheden.	Ingen væsentlige afvigelser konstateret.
4.2	Kontroller er etableret, som sikre at der foretages en regelmæssig vurdering og gennemgang af risici og disse behandles i ledelsesteamet, hvor ledelsen vurderer, om nye risici er opstået og derfor kræver yderligere analyse og håndtering.	Vi har verificeret, at hyppige risikovurderinger er blevet foretaget og rapporteret til ledelsen.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

5. Informationssikkerhedspolitikker

Kontrolmål:
At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
5.1	Der er udarbejdet en it-sikkerhedspolitik som er godkendt af IDQ A/S' ledelse. IDQ A/S sikrer dette ved at kommunikere revisioner og opdateringer i hele organisationen via bevidsthed træningsprogrammer, e-mails såvel som på afdelingen og personalemøder.	Vi har inspiceret og gennemgået IDQ A/S' seneste IT-sikkerhedspolitik. Vi har verificeret, at vedligeholdelse af IT-sikkerhedspolitikken udføres regelmæssigt. Vi har under vores revision kontrolleret, at de underliggende understøttende politikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af ledelsen og stillet til rådighed for medarbejderne. Vi har inspiceret, at politikker og procedurer er blevet kommunikeret til medarbejdere via awareness-træning mv.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

6.Organisering af informationssikkerhed

Kontrolmål:
At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter samt sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
6.1	Alt ansvar for informationssikkerhed skal defineres og fordeles. Modstridende pligter og ansvarsområder er adskilt for at reducere mulighederne for uautoriseret eller utilsigtet ændring eller misbrug af organisationens aktiver.	Vi har verificeret, at ansvar og roller for informationssikkerhed er defineret og allokeret til kvalificerede medarbejdere. Vi har forespurgt om at adskillelse af opgaver og har inspiceret at der er implementeret roller i ændringsstyrringssystemet. Vi har inspiceret dokumentation for processen for kontakt med myndigheder og interessegrupper. Vi har forespurgt om evaluering af risici ifm. brug af nye systemer/services eller underleverandører.	Ingen væsentlige afvigelser konstateret.
6.2	Informationssikkerhedspolitikken inkluderer kontroller til fjernadgang og der er implementeret sikkerhedsforanstaltninger for at sikre fjernadgang.	Vi har inspiceret politikken og kontroller for styring af mobilenheder. Vi har inspiceret udvalgte sikkerhedsforanstaltninger til brug af telearbejdspladser. Vi har verificeret, at adgang til systemer tildeles via ændringsstyringsprocessen. Vi har inspiceret, at adgangsanmodninger skal godkendes af relevante medarbejdere.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

7. Medarbejdersikkerhed

Kontrolmål:
At sikre, at medarbejder og kontrahenter er egnede til deres roller og forstår og efterlever deres informationssikkerhedsansvar under og efter ansættelsen.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
7.1	IDQ A/S har etableret formelle procedurer for ansættelse af nye medarbejdere. Personer, der tilbydes en stilling i IDQ A/S, vil blive genstand for en baggrundskontrol før de begynder ansættelse. Medarbejderne bekræfter ved underskrift på deres ansættelseskontrakt, at de er forpligtet til at være bekendt med indholdet af kontrakten og er underlagt tavshedspligt.	Vi har observeret, at der er en formel procedure for ansættelse af nye medarbejdere. Vi har via stikprøver af nye ansættelser inspiceret, at proceduren for ansættelse er blevet fulgt. Vi har forespurgt til formalisering af vilkår og betingelser ved ansættelse af medarbejdere. Vi har inspiceret, at en standard medarbejderkontrakt indeholder krav om tavshedspligt.	Ingen væsentlige afvigelser konstateret.
7.2	IDQ A/S' ledelse stiller krav til at medarbejdere og kontrahenter overholder krav om informationssikkerhed. IDQ A/S udfører awareness-træning samt afdelings og personalemøder til at sikre, at medarbejdere er bekendte med politikker og procedurer. Der er implementeret sanktioner for overtrædelse af informationssikkerhedspolitikken.	Vi har forespurgt omkring ledelsens ansvar for at formidle politikker og procedurer. Vi har inspiceret dokumentation for at medarbejdere har modtaget uddannelse og træning in informationssikkerhed og virksomhedspolitikker. Vi har forespurgt til sanktionering og inspiceret vejledning hertil.	Ingen væsentlige afvigelser konstateret.
7.3	Informationssikkerhedsansvar og –forpligtelser er gældende efter ansættelsens ophør.	Vi har inspiceret processen for fratrædelse af medarbejdere. Vi har inspiceret en stikprøve på fratrædelser og verificeret at processen er blevet fulgt.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

8. Styring af aktiver

Kontrolmål:
At identificere organisationens aktiver og definere passende ansvarsområder og beskyttelse heraf samt at forhindre brud på sikkerheden på bærbare medier.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
8.1	IDQ A/S har registreret væsentlige it-aktiver i en række systemer og defineret ejerskab for kategorier af aktiver. Retningslinjer for accepteret brug af al informationsrelateret aktiver findes og er tilgængelige for relevante medarbejdere.	Vi har observeret, at aktiver er registreret i systemer hos IDQ A/S. Vi har inspiceret at kategorier af aktiver er identificeret og at der er udpeget ejere af aktiver. Vi har inspiceret at medarbejdere er informeret om, at der i politikker og procedurer er vejledninger til brug af aktiver.	Ingen væsentlige afvigelser konstateret.
8.2	Aktiver er klassificeret og mærket, hvor det er fundet relevant. Der er implementeret procedurer, som sikrer at aktiver håndteres iht. informationssikkerhedspolitikken.	Vi har forespurgt om og inspiceret, at der er klassifikation og mærkning af aktiver, data og kunder, hvor det er relevant. Vi har forespurgt om retningslinjer for håndtering af aktiver og inspiceret, hvordan aktiver håndteres i henhold til procedurer.	Ingen væsentlige afvigelser konstateret.
8.3	Der er implementeret kontroller til at sikre håndtering af bærbare medier.	Vi har forespurgt omkring håndtering af bærbare medier. Vi har forespurgt omkring vejledninger til bortskaffelse af medier samt transport af fysiske medier. Vi har inspiceret, at bærbare medier er blevet sikkert destrueret.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

9. Adgangskontroller

Kontrolmål:
At begrænse adgangen til information, sikre autoriseret brugeradgang og at forhindre uautoriseret adgang til systemer og services.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
9.1	Der er en politik og procedure for tildeling, ændring og tilbagekaldelse af adgangsrettigheder for medarbejdere.	Vi har inspiceret politikken og proceduren for tildeling, ændring og tilbagekaldelse af adgangsrettigheder. Vi har forespurgt omkring politikker for adgang til netværk og netværksservices. Vi har inspiceret de implementerede politikker.	Ingen væsentlige afvigelser konstateret.
9.2	Der findes en formel forretningsprocedure for tildeling og tilbagekalder brugeradgang. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåget. Interne brugers adgangsrettigheder gennemgås regelmæssigt i henhold til en formaliseret forretningsprocedure.	Vi har forespurgt om og inspiceret procedurer for tildeling og tilbagekaldelse af brugeradgange. Vi har stikprøvevis inspiceret tildeling og tilbagekaldelse af brugeradgange i løbet af revisionsperioden. Vi har forespurgt omkring håndtering af samt implementerede kontroller for privilegerede adgangsrettigheder. Vi har forespurgt omkring procedurer for tildeling af hemmelig autentifikationsinformation. Vi har inspiceret kontroller til periodisk gennemgang af brugeradgange samt dokumentation på at kontroller er udført.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

9. Adgangskontroller

Kontrolmål:
At begrænse adgangen til information, sikre autoriseret brugeradgang og at forhindre uautoriseret adgang til systemer og services.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
9.3	Adgangskoder er personlige og holdes hemmelige.	Vi har forespurgt omkring brugers brug af hemmelig autentifikationsinformation og inspiceret retningslinjer.	Ingen væsentlige afvigelser konstateret.
9.4	Adgang til operativsystemer og netværk er beskyttet af adgangskoder. IDQ A/S har specificeret og implementeret kvalitetskrav for længde, kompleksitet og varighed af adgangskoder. Brugeren bliver låst ud i tilfælde af gentagne mislykkede forsøg på at logge ind. Der er etableret kontroller, der giver rimelige forsikring om, at administratoradgang er begrænset til personer med et arbejdsrelateret behov for adgang.	Vi har forespurgt omkring begrænsning af adgang til information og sikker log-on procedurer. Vi har forespurgt omkring systemer til håndtering af adgangskoder samt brug af privilegerede servicekonti. Vi har inspiceret, at adgang til systemer er underlagt en prædefineret adgangskodepolitik, som sikre kravene til adgangskoder, som giver adgang til systemer og applikationer. Vi har verificeret log-on procedurer for relevante systemer og applikationer.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

10. Kryptering

Kontrolmål: **At sikre passende og effektiv brug af kryptering for at beskytte fortroligheden, autens**			
Nr.	***IDQ A/S kontrolaktivitet***	***Revisors udførte test***	***Resultat af revisors test***
10.1	Der er i informationssikkerhedspolitikken sat krav om, at al kommunikation på åbne, offentlige netværk skal være krypteret. Adgang til systemer fra andre lokationer er krypteret via VPN. Skift af krypteringsnøgler sker efter en fastsat procedure.	Vi har inspiceret, at der anvendes kryptering på transmission over internettet. Vi har inspiceret at der benyttes VPN forbindelser til adgang til systemer fra andre lokationer. Vi har verificeret, at der er procedure for skift af krypteringsnøgler.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

11. Fysisk sikring og miljøsikring

Kontrolmål:
At forhindre uautoriserede fysisk adgang til samt beskadigelse og forstyrrelse af organisationens informations- og informationsbehandlingsfaciliteter og at undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelser i organisationen.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
11.1	Alle informationsrelaterede aktiver er beskyttet mod uautoriseret adgang i datacentre og kontorer med adgangssystemer, overvågning og alarmer. Kontroller giver rimelig sikkerhed for at adgange tildeles i henhold til forretnings- og arbejdsrelaterede behov. Alle informationsrelaterede aktiver er beskyttet mod brand, vand og varme.	Vi har inspiceret de fysiske sikkerhedsparametre for IDQ A/S' lokation. Vi har inspiceret, at teknik er bag aflåste døre og at kun relevante medarbejdere med arbejdsbetinget behov har adgang til rummene. Vi har forespurgt omkring proceduren for tildeling af adgang til serverum. Vi har inspiceret understøttende forsyninger og vedligeholdelse af disse, samt at der er implementeret sikkerhedsforanstaltninger til sikring mod og opdagelse af ild, vand og varme. Vi har inspiceret leverandørers erklæringer for outsourcet drift og vedligehold af faciliteter i erklæringsperioden.	Ingen væsentlige afvigelser konstateret.
11.2	Alle informationsrelaterede aktiver er beskyttet mod strømafbrydelse via UPS og nødstrømsystemer. Kabler til elektronisk kommunikation og elektricitet forsyningen er beskyttet mod manipulation. Medarbejdere er underlagt krav om clean desk og der er implementeret skærmlås. Data der bærer informationsrelaterede aktiver, bortskaffes på en sikker måde.	Vi har inspiceret at der er implementeret UPS og nødstrømssystemer og at kabler er beskyttet mod manipulation. Vi har inspiceret beskyttelse af driftsfaciliteter og vedligeholdelse af udstyr i datacentre. Vi har inspiceret vejledning til clean desk og bruger udstyr uden for opsyn, herunder at der er skærmlås. Vi har inspiceret dokumentation for sikker bortskaffelse af medier.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

12. Driftssikkerhed

Kontrolmål:
At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.1	Der er dokumenterede driftsprocedurer for forretningskritiske systemer og disse er tilgængelige for medarbejdere med arbejdsrelaterede behov. Funktionsadskillelse er implementeret i driftsprocedurer. Der er etableret kontroller, der giver rimelige forsikring om, at IDQ A/S har etableret en formel proces for ændringsstyring, der sikrer test og godkendelse af relevante ændringer.	Vi har inspiceret, at der er dokumenterede driftsprocedurer og at de er tilgængelige for alle ansatte. Vi har gennem vores test valideret, at medarbejderne er opmærksomme på procedurerne, og at procedurerne udføres som forventet. Vi har valideret og testet kontroller i systemer der understøtter operationelle procedurer for at sikre, at automatiske kontroller er på plads og at operationelle procedurer er komplette og effektive. Vi har inspiceret, at der er funktionsadskillelse i driftsprocedurer. Vi har inspiceret, at der er en dokumenteret procedure for ændringsstyring. Vi har verificeret, at et formelt system bruges, og at systemet understøtter de dokumenterede procedurer. Vi har inspiceret og valideret at: • ændringsanmodninger registreres og beskrives • alle ændringer er underlagt formel godkendelse før implementering	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

12. Driftssikkerhed - fortsat

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

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.2	Der er etableret kontroller, der giver rimelige forsikring om, at it-aktiver er beskyttet mod vira og lignende og at de opdateres regelmæssigt med kritisk sikkerhedspatches.	Vi har inspiceret, at informationssikkerhedspolitikken angiver, hvordan IDQ A/S skal beskyttes mod malware. Vi har bekræftet informationsaktiver og faciliteter er tilstrækkeligt beskyttet mod malware. Vi har inspiceret at anti-virus software er installeret på relevante servere og brugerudstyr, samt at denne software er opdateret.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At beskytte mod tab af data

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.3	Der er etableret kontroller, der giver rimelige forsikring om, at processerne vedrørende backup og gendannelse af data er tilfredsstillende.	Vi har inspiceret, at der er dokumenterede procedurer for backup, og at der er foretaget faste backupjob. Vi har bekræftet, at backup anvendes til systemer og at backup udføres i henhold til deres skema. Vi har inspiceret, at der følges op på mislykkede sikkerhedskopieringsjob.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

12. Driftssikkerhed - fortsat

Kontrolmål:
At registrere hændelser og tilvejebringe bevis.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.4	Der er implementeret systemer til overvågning af server- og netværksdrift.	Vi har inspiceret, at der er implementeret et system til samling af logfiler og events fra servere og netværksenheder. Vi har inspiceret, at events udløser et event i overvågningssystemet, og at medarbejderne håndterer begivenhederne ud fra vigtighed og effekt. Vi har inspiceret de anvendte foranstaltninger til beskyttelse af log information. Vi har bekræftet at effektiviteten af overvågningssystemet jævnligt kontrolleres. Vi har inspiceret, at synkronisering af tid har været implementeret.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At beskytte mod tab af data

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.5	Der er etableret kontroller, der giver rimelig sikkerhed for, at driftsplatformen er patchet i henhold til retningslinjer.	Vi har inspiceret, at der er en formel procedure til patchning og opdatering af operationelle systemer. Vi har valideret, at mislykkede eller manglende patches og opdateringer registreres og håndteres.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

12. Driftssikkerhed - fortsat

Kontrolmål:
At forhindre, at tekniske sårbarheder udnyttes.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.6	Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer. Sårbarheder evalueres og der implementeres foranstaltninger for at håndtere disse. Der er opsat begrænsning i installation af software.	Vi har inspiceret at sårbarheder løbende overvåges og evalueret. Vi har forespurgt om håndtering af tekniske sårbarheder, herunder at der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko. Vi har forespurgt om begrænsninger i softwareinstallation.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
Formål: At forhindre indvirkningen af audit aktiviteter

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.7	Der gennemføres løbende revisioner af interne aktiviteter samt leverandørers overholdelse af kontrakter.	Vi har forespurgt omkring revision af interne procedurer. Vi har forespurgt om udførte revisionsaktiviteter hos leverandører.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

13. Kommunikationssikkerhed

Kontrolmål:
At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter og at opretholde informationssikkerhed ved overførelse internt i organisation til en ekstern entitet.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
13.1	Der er etableret kontroller til sikring af netværket.	Vi har inspiceret, at netværket administreres, dokumenteres og at denne dokumentation opdateres ved ændringer. Vi har verificeret, at der er passende procedurer til administration af netværksudstyr. Vi har inspiceret, at netværket er passende segmenteret og er sikres via firewalls. Vi har verificeret, at produktionsmiljøet er designet og implementeret som et redundant opsætning.	Ingen væsentlige afvigelser konstateret.
13.2	Der er etableret politikker og procedurer, samt kontroller til beskyttelse af informationer ved overførsel.	Vi har inspiceret politikker og procedurer for informationsoverførsel. Vi har spurgt om tavshedspligt eller fortrolighedserklæringer.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

14. Anskaffelse, udvikling og vedligehold af systemer

Kontrolmål:
At sikre, at informationssikkerhed er en integreret del af informationssystemerne og er tilrettelagt of implementeret inden for systemernes udviklingscyklus samt at data som anvendes til test er beskyttet.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
14.1	Der er fastlagte sikkerhedskrav til informationssystemer ifm. udvikling. Der er implementeret kontroller til beskyttelse af applikationer.	Vi har forespurgt omkring krav til sikkerhed ved udvikling og forbedring af systemer og tjenester. Vi har inspiceret at applikationstjenester offentlige netværk er passende beskyttet. Vi har spurgt om politikken til beskyttelse af testdata.	Ingen væsentlige afvigelser konstateret.
14.2	Der anvendes sikre udviklingsmetoder i forbindelse med udvikling af interne applikationer. Alle releases testes grundigt inden frigivelse til produktionsmiljø. Der er implementeret test af funktionalitet inden brugertest. Der er implementeret en procedure for kontrol og opfølgning på outsourcet udvikling.	Vi har forespurgt omkring udviklingspolitikken og procedurerne for systemændring. Vi har observeret, at der laves kode review af udviklet kode samt at udviklere er bekendt med sikker kodning. Vi har forespurgt om sikre udviklingsmiljøer, systemsikkerhedsprøvning og test af systemaccept. Vi har forespurgt om outsourcet udvikling herunder opfølgning og kontrol med outsourcet udvikling.	Ingen væsentlige afvigelser konstateret.
14.3	Det er beskrevet i politik for brug af test og produktionsdata, hvilke typer data, der må anvendes i forbindelse med test.	Vi har forespurgt omkring politikker og procedurer for brug af testdata.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

15. Leverandørforhold

Kontrolmål:
At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til og at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
15.1	Risici forbundet med eksterne forretningspartnere identificeres og sikkerhed i tredjepartsaftaler styres.	Vi har forespurgt om og inspiceret processen for at vedligeholde IDQ A/S' krav til informationssikkerhed i leverandørforhold.	Ingen væsentlige afvigelser konstateret.
15.2	Leverandører overvåges regelmæssigt, herunder styring ifm. ændringer af leverandørydelser.	Vi har spurgt om kontroller til overvågning af leverandørtjenester. Vi har spurgt om styring af ændringer i leverandørtjenester. Vi har bekræftet, at IDQ A/S har modtaget og evalueret erklæringer fra centrale leverandører.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

16. Styring af informationssikkerhedsbrud

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

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
16.1	Sikkerhedshændelser rapporteres til ledelsen så snart som muligt, og de styres på en ensartet og effektiv måde.	Vi har inspiceret procedurerne for håndtering af hændelser inklusiv rapportering af sikkerhedshændelser. Vi har inspiceret at hændelser bliver rapporteret, og at roller og ansvarsområder er defineret. Vi har stikprøvevis kontrolleret at hændelser er blevet registreret og håndteret i henhold til procedurerne.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

17. Informationssikkerhedsaspekter ved ned-, beredskabs- og reetableringsstyring

Kontrolmål:
At sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring og at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
17.1	Sikkerhedshændelser rapporteres til ledelsen så snart som muligt, og de styres på en ensartet og effektiv måde.	Vi har inspiceret procedurerne for håndtering af hændelser inklusiv rapportering af sikkerhedshændelser. Vi har inspiceret at hændelser bliver rapporteret, og at roller og ansvarsområder er defineret. Vi har stikprøvevis kontrolleret at hændelser er blevet registreret og håndteret i henhold til procedurerne.	Ingen væsentlige afvigelser konstateret.
17.2	Der er etableret kontroller til at sikre tilgængelighed af informationsbehandlingsfaciliteter.	Vi har forespurgt omkring tilgængelighed af informationsbehandlingsfaciliteter. Vi har inspiceret erklæringer fra leverandører af outsources drift.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

18. Overholdelse

Kontrolmål:
At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav, samt at sikre at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.

Nr.	*IDQ A/S kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
18.1	IDQ A/S har etableret procedurer og kontroller til at undgå brud på lov-, myndigheds- og kontraktkrav relateret til informationssikkerheds og andre sikkerhedskrav. Kontroller er etableret hvor det er relevant for at sikre privatliv og beskyttelse af personhenførbare informationer samt krav til kryptering.	Vi har forespurgt omkring kontroller til at identificere lov- og kontraktmæssige krav. Vi har inspiceret at implementerede kontroller omkring beskyttelse af privatliv og personhenførbare informationer. Vi har forespurgt omkring krav til kryptografi.	Ingen væsentlige afvigelser konstateret.
18.2	IDQ A/S har etableret kontroller til at sikre at informationssikkerhed er implementeret og håndteret i overensstemmelse med virksomhedens politikker og procedurer. Der indhentes revisorerklæringer på væsentlige ydelser.	Vi har inspiceret implementerede kontroller til at sikre overholdelse af krav i virksomhedens politikker og standarder. Vi har bekræftet, at IDQ A/S har modtaget og evalueret ISAE 3402 Type II-erklæringer fra centrale leverandører	Ingen væsentlige afvigelser konstateret.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Henrik Saustrup
Underskriver 1
Serienummer: PID:9208-2002-2-902694774292
IP: 83.221.xxx.xxx
2021-06-25 13:08:57Z
NEM ID

Anders Grønning Kjærgaard
Underskriver 2
Serienummer: PID:9208-2002-2-822661869402
IP: 194.35.xxx.xxx
2021-06-25 13:10:19Z
NEM ID

Martin Bomholtz
Underskriver 3
Serienummer: PID:9208-2002-2-013768766685
IP: 93.163.xxx.xxx
2021-06-25 14:52:42Z
NEM ID