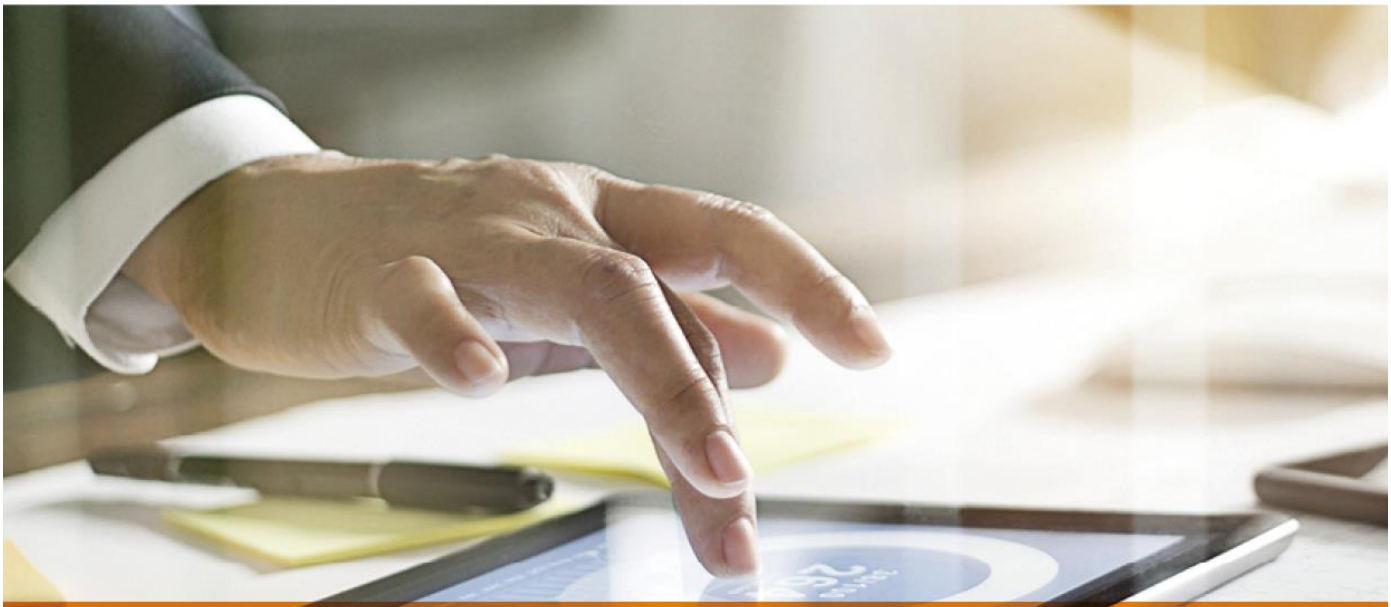
BEIERHOLM
VI SKABER BALANCE



MAJ 2022

Ambition A/S

ISAE 3402 TYPE 2 ERKLÆRING

CVR 34222282

Uafhængig revisors erklæring om kontrolmiljøet for it-driften i tilknytning til Ambition A/S.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af kontrolmiljøet for it-driften i tilknytning til Ambition A/S.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, tests og resultater heraf.

KAPITEL 1:

Ledelseserklæring

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Ambition A/S' ydelser relateret til behandling 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.

Ambition A/S bekræfter, at:

Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Ambition A/S' ydelser relateret til behandling af data i perioden til kunder i hele perioden fra d. 1. marts 2021 til d. 28. februar 2022. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

a) redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
   - de typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant.
   - de processer i både IT og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder.
   - de tilhørende regnskabsregistreringer, underliggende information og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan informationen er overført til de rapporter, der er udarbejdet til kunder.
   - hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner.
   - processen, der blev anvendt til at udarbejde rapporter til kunder.
   - 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 og rapporteringen af kunders transaktioner
b) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra d. 1. marts 2021 til 28. februar 2022,
c) 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.

- De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra d. 1. marts 2021 til d. 28. februar 2022. Kriterierne for denne udtalelse var, at:
    a) de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificerede, og
    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.
    c) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra d. 1. marts 2021 til 28. februar 2022.

København, 31. maj 2022

Ambition A/S

CVR 34222282

Peter Nyemann
CEO, partner

KAPITEL 2:

Beskrivelse af kontrolmiljøet for IT-driften i tilknytning til Ambition A/S

1. Om os og vores kerneydelser

Ambition er skabt i 2017 som en fusion af datakonsulentvirksomheden DM Partner, dialogbureauet Director og search marketingbureauet Webjuice. I 2020 udvidedes forretningen med opkøb af de nordiske aktiviteter i det digitale bureau, Artefact.

Ambition tilbyder et helt unikt koncept indenfor databaseret forretningsudvikling og markedsføring. Baseret på intelligent dataindsigt hjælper vi vores kunder med at skabe leads, kunder og salg. Hos Ambition omsætter vi data, teknologi og kreativitet til god forretning på tværs af media og kanaler. Fra prædiktive analyser og strategisk rådgivning om brug af data til målrettede kommunikationskoncepter, marketing automation, search marketing og resultatfokuseret, digital eksekvering.

Vi tilfører vores kunder værdi ved at analysere og berige kundernes egne førstepartsdata med eksterne tredjepartsdata, ved at levere data fra offentlige datakilder samt ved at indhente eller indkøbe skræddersyede data.

Ambition aktiverer desuden kundernes data gennem samarbejde om digital annoncering, data automation og marketing automation. Med digital annoncering menes i denne forbindelse custom audiences, hvor eksisterende kunder og leads eksponeres eksplicit for digital annoncering, dels til indirekte aktiviteter hvor eksisterende kunder og leads anvendes til at identificere look-a-like segmenter. Med data automation arbejdes med begreber som DMP (Data Management Platform) og CDP (Customer Data Platform) hvor kunders data samles i cloud-miljøer til brug for opnåelse af automatiserede forretningsmæssige og kommunikationsmæssige mål. Med marketing automation arbejdes med aktivering af målgrupper og kampagneeksekvering i kundernes egne CRM-systemer og marketing automation-platforme.

Ambition tilbyder desuden software- og APl-løsninger, hvor datakvalitet og -integritet er af højeste prioritet. Endelig tilbyder Ambition udvikling og drift af gamification-løsninger til at markedsføre vores kunders produkter.

2. Vores kontrolmål

Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere et stabilt og sikkert produkt til vores kunder. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige. Vores IT-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer.

3. Vores implementerede kontroller

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 handling, har en udførende ansvarshavende, og i visse tilfælde også en ansvarshavende godkender.

Vores kontroller er rettet mod dels konkrete arbejdshandlinger, dels processer for en række arbejdshandlinger, hvilket kan have konkrete kontroller tilknyttet yderligere. Konkrete arbejdshandlinger er beskrevet i Standard Operating Procedure dokumenter (SOP'er).

Tidsangivelse for en given kontrol opgives altid over en periode, også selvom en given kontrol oftest måtte blive praktisk udført i en bestemt måned år efter år.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 (Regelsæt for styring af informationssikkerhed), og er dermed helt overordnet inddelt i følgende kontrolområder:

4. Risikovurdering og -håndtering
5. Informationssikkerhedspolitikker
6. Organisering af informationssikkerhed
7. Medarbejdersikkerhed
8. Styring af aktiver
9. Adgangsstyring
10. Kryptografi
11. Fysisk sikring og miljøsikring
12. Driftssikkerhed
13. Kommunikationssikkerhed
14. Anskaffelse, udvikling og vedligeholdelse af systemer
15. Leverandørforhold
16. Styring af sikkerhedsbrud
17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetablering
18. Overensstemmelse

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område.

4. Risikostyring

Alle trusler vurderes systematisk og ensartet, og for at tilsikre transparens, overskuelighed og dokumentation, benyttes 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 er en fast del af alle arbejds- og udviklingsprocesser, både til sikring af vores produktkvalitet, forventningsafstemning med kunder, og ikke mindst, integriteten af vores forretningsplatform.

Risikovurdering foretages således både periodisk, på øverste ledelsesniveau minimum én gang årligt, samt på daglig basis når der indgår ønsker fra kunder, foretages ændringer eller implementeres nye systemer.

5. Informationssikkerhedspolitikker

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. Når vi har ændret ting i IT-sikkerhedspolitikken, og minimum efter den årlige gennemgang, fremlægges ændringerne internt ved førstkommende firmamøde for personalet. Ligeledes bliver eksterne leverandører mf. Inddraget og orienteret såfremt det har relevans.

Det er virksomhedens administrerende direktør, som er ansvarlig for virksomhedens informationssikkerhed, og som godkender denne. Virksomhedens informationssikkerhed er forhåndsgodkendt af IT-ledelsen.

6. Organisering af informationssikkerhed

6.1 Intern organisering

Ansvaret for informationssikkerhed er dokumenteret og forankret på alle niveauer. Vores dokumentation og definerede processer sikrer generelt, at vi minimerer nøglepersonsafhængighed. Vi tildeler rettigheder på baggrund af funktion, og der tildeles altid efter princip om færrest mulige rettigheder.

6.2 Mobilt udstyr og fjernarbejdspladser

Vi har udarbejdet en politik, som redegør for retningslinjer for brugen af mobile enheder (laptops, mobiltelefoner etc.), så alle medarbejdere er bekendt med reglerne før tilslutning til virksomhedens netværk eller mail system. Reglerne er del af ansættelsesforholdet.

Alle mobiltelefoner er sikret med en MDM-løsning indeholdende en række sikkerhedspolitikker. Følsomme data og persondata må alene opbevares på serverrumsmedier, i krypteret form på egen fildelingsløsning, eller som midlertidige arbejdskopier på udstyr, der ikke forlader kontoret og som bortskaffes på sikker og forsvarlig vis.

7. HR- og medarbejderrelaterede kontroller

Vi har faste procedurer for de aktiviteter og kontroller der relaterer sig til før-, under-, og efter ansættelse af medarbejdere. Det er den administrerende direktør i rollen som HR-chef i samarbejde med den ansættende leder, som er ansvarlig for de HR relaterede kontroller.

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

Det er virksomhedens administrerende direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes.

Den tekniske oprettelse af medarbejdere- såvel som konsulenter, foretages i henhold til førom-talte processer, som hver har tilknyttet et antal relevante SOP'er. Vi har desuden en proces for løbende 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 igennem strukturerede introduktioner, indlæg på firmamøder og andre tiltag.

8. Styring af aktiver

8.1 Ansvar for aktiver

Alle aktiver ejes helt og fuldstændigt af Ambition A/S. Undtaget herfra er server- og netværksudstyr, som for visse deles vedkommende er leaset af vores infrastrukturleverandør, Sentia.

Registrering af virksomhedens aktiver varetages af Sentia og kontrolleres af Ambitions IT-ansvarlige. Sentia registrerer al ejet hardware og egne softwarelicenser. Småanskaffelser som mus, tastaturer, og docking stationer registreres ikke.

Virksomheden har faste regler for brugen af aktiver, samt behandling af informationer på disse. Reglerne er integreret i ansættelseskontrakterne, i personalehåndbogen samt i den medarbejdervendte IT-sikkerhedspolitik. Alle medarbejdere er forpligtet til at læse personalehåndbogen og IT-sikkerhedspolitikken ved ansættelsens begyndelse, samt opfølgning ved ændringer der er relevant for de enkelte medarbejdere.

Virksomheden har faste procedurer til inddrivelse af IT-aktiver ved ophør af et medarbejderforhold.

8.2 Klassifikation af information

Vi har interne regler for opbevaring af særlige datatyper, eksempelvis kundedata, hr/personaledata, salgsdata osv. Personalet gøres bekendt med disse regler via den medarbejdervendte IT-sikkerhedspolitik, samt personlig introduktion i forbindelse med jobstart.

8.3 Mediehåndtering

Alle data lagret på flytbare medier skal opbevares krypteret, herunder også data synkroniseret fra virksomhedens Sharepoint-online løsning. USB sticks og eksterne harddiske tillades ikke, og i tilfælde af, at de til særlige sager skal benyttes, skal disses data krypteres.

Bortskaffelse og reparation af serverrumsmedier og infrastrukturkomponenter varetages af Sentia. Medier, som ikke længere kan/skal repareres, bliver opbevaret hos Sentia indtil de bliver sendt til destruktion. Destruktionen varetages af sikkerhedsgodkendt leverandør, og vi modtager en kvittering for sikker destruktion.

9. Adgangsstyring

9.1 Forretningsmæssige krav til adgangsstyring

Vi har en dokumenteret proces for tildeling af adgange. Dette er ligeledes en del af vores IT-sikkerhedspolitik.

9.2 Administration af brugeradgang

Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Interne brugere, herunder brugere med privilegerede rettigheder, oprettes alene på baggrund af skriftligt ønske dokumenteret i vores HR-proces Alle brugere er personhenførbare. For servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret. Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Interne brugere og deres adgangsniveau gennemgås periodisk.

9.3 Brugernes ansvar

Hver medarbejder er ansvarlig for at sikre egne logininformationer, og retningslinjer for samme oplyses i Medarbejderhåndbogen.

9.4 Styring af system- og applikationsadgang

Vores kunders brugeradgange til deres systemer og data er bestemt af dem selv. Adgange for vores medarbejdere er altid funktionsbestemt. Brug af password management system er obligatorisk for virksomhedens medarbejdere, og alle adgange bliver sporet.

Vi arbejder i segmenterede netværk, med GPO'er og alene med identificerbare brugere.

10. Kryptografi

Udveksling af kundedata udvekslet over internettet sendes over krypteret protokol.

Certifikatadministration varetages af vores infrastrukturleverandør.

11. Fysisk sikring og miljøsikring

11.1 Sikre områder

Vores kontorbygning har tyverialarm, brandalarm. Kontorbygningen har adgangskortstyring med sikkerhedszoner. Et beredskab aktiveres, såfremt alarmer aktiveres. Vores datacenter-servere er placeret hos Sentia, samt for enkelte løsningers vedkommende, i Google Compute Platform, administreret og overvåget af Sentia. I den forbindelse indhenter vi årligt en ISAE3402-II erklæring fra Sentia, og vi foretager et fysisk inspektionsbesøg hos Sentia, ligeledes årligt.

11.2 Udstyr

Vores teknikrum, som indeholder krydsfelt, linjeindgang og reserveudstyr, har eget kølingsanlæg og Inergen brandsikringsanlæg med alarm. Når udstyr skal destrueres, overdrages det til infrastrukturleverandøren Sentia til destruktion på forsvarlig vis. For serverrumsudstyr henviser vi til Sentia.

12. Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

Vi har dokumenterede driftsprocedurer og aftaler med Sentia. Vores systemdokumentation opdateres løbende.

Vores IT-leverandør Sentia har ansvar for alle IT-infrastrukturydelser og 'serverum services', herunder patch management, firmware, OS sikkerhed, monitorering af kapacitet, servicetilgængelighed og backup. Dette gælder også for produktionsservere placeret i Google Cloud Platform, hvor Sentia agerer som Google Partner. Vi håndterer alle applikationsspecifikke ændringer selv, efter en fastlagt dokumenteret proces.

Alle applikationer er under overvågning. Her monitoreres eksempelvis afvikling af vigtige jobs, fejl logs mv.

12.2 Beskyttelse mod Malware

Vi beskytter os blandt andet ved hjælp af antivirussoftware, e-mail skanning og IPS services.

12.3 Backup

Vi har en detaljeret procedurer og aftaler med Sentia for sikkerhedskopiering, continuity management og backup strategi (vurdering af differentieret backup baseret på datatyper).

12.4 Logning og overvågning

Vi har en politik for hhv. logning af netværkshandlinger og virtuelle servere. Netværkslogning (firewallens logs) gemmes på firewallens indbyggede disk og deslige på eksternt medie, for at beskytte log informationerne i fald firewallen kompromitteres.

Hændelser relateret til vores fælles platform, infrastruktur og serverrumsydelser håndteres af vores IT-leverandør, som uden for almindelig kontortid har driftsvagt.

12.5 Styring af driftssoftware

Vedligeholdelse af operativsystem og infrastrukturkomponenter foretages månedligt i et fastlagt service vindue. Vi håndterer alle applikationsspecifikke ændringer selv, efter en fastlagt dokumenteret proces.

12.6 Sårbarhedsstyring

For infrastruktur og serverrum varetages opgaven af Sentia. For vores egne applikationer og services holder vi os opdateret via relevante faglige og tekniske fora. Vi abonnerer desuden på adviseringer fra DK-Cert samt andre relevante kilder.

13. Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor personafhængighed og utilsigtede fejl minimeres.

Vi har en opdeling af både vores kontor- og servernetværk og benytter dedikerede miljøer.

Segmentering af VLAN's er implementeret for at lægge et ekstra lag af sikkerhed ind i netværket. Et VLAN tilknyttes til en port på firewallen. Servere placeret i et VLAN er derfor både fysisk og logisk isoleret fra de øvrige servere placeret i andre VLAN's.

Trafik mellem de forskellige VLANs er begrænset, således det er defineret ud fra en source IP, destinations IP samt hvilke services der skal være åbnet for.

Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv.

13.2 Informationsoverførsel

Vi har regler for udveksling af data med kunder, og behandling af kundedata må aldrig forgå over e-mail eller andre åbne kommunikationskanaler.

Implementering af- og leverancer til- nye kunder foretages i henhold til fastlagte procedurer og relevante SOP'er. Repræsentant fra vores Salg og Ledelse skal godkende kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav.

Vi har ligeledes regler for udveksling af kundedata via internettet. Vi benytter desuden krypteret VPN-tunnel til anvendelse af udstyr på distance, og vi anvender IP adressefiltrering på alle offentlige tilgængelige webservices.

Vi har databehandleraftaler med alle vores databehandlings-kunder.

14. Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

Vi har en fast procedure for vurdering af sikkerhedskrav og risici, ved anskaffelse, udvikling og vedligeholdelse af vores systemer.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

Vores retningslinjer for udvikling og ændringshåndtering indeholder faste kriterier for sikkerhedsrelaterede vurderinger, herunder ledelses- og når relevant, kundegodkendelser. Vi dertil en formel godkendelsesproces for godkendelse af opdateringer, inkluderende test og roll-back planer, for hvert udviklingstrin/produkt.

14.3 Testdata

Vi har et separat testmiljø. Testmiljø og testdata beskyttes på samme måde som produktionsdata.

15. Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

Vores leverandører (databehandler) skal til hver en tid efterleve vores IT-sikkerhedspolitik, ligesom visse leverandører skal kunne dokumentere deres kvalitet, ved at fremvise relevant revisorerklæring uden anmærkninger. Dette er en del af aftaleforholdet, og kontrolleres minimum årligt.

Kundeaftaler har tilsvarende klausuler om informationssikkerhed, særligt i forhold til hvilke forhold Kunden selv er ansvarlig for (eksempelvis egen brugeroprettelse).

15.2 Styring af leverandørydelser

De leverandører, som har adgang til vores kundedata og/eller anden fortrolig/følsom data, indhenter vi revisorerklæringer fra. Vi foretager desuden årligt en fysisk inspektion ved relevante leverandører.

For Leverandører, som får adgang til vores netværk, er forhold omhandlende fortrolighed og IT-sikkerhed altid en del af aftalegrundlaget.

16. Styring af informationssikkerhedsbrud

Såfremt et informationssikkerhedsbrud indtræffer, aktives relevant detaljeret beredskabsplan. Hvor det er relevant, indsamles beviser, kunder orienteres osv. Vurdering af sikkerhedshændelser foretages af den IT-ansvarlige. Efter en hændelse evalueres relevante retningslinjer og sikkerheds-foranstaltninger, risikoanalyse og beredskabsplanen med henblik på at sikre læring af hændelsen og at undgå at hændelse indtrækker igen (hvis muligt). Hændelser rapporteres af den IT-ansvarlige til ledelsen samt til relevante medarbejdere.

Ved kriminelle forhold, hvor der sker en politimæssig efterforskning, vil vores logføring og øvrige overvågning blive videregivet til relevante myndigheder med henblik på at benytte samme til opklaring og evaluering af sikkerhedshændelsen.

17. Beredskabsstyring

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Risikoanalyse og beredskabsplaner omfatter skadebegrænsende tiltag, etablering af temporære nødløsninger og genetablering af permanent løsning. Minimum en gang om året testes (dele af) beredskabsplanen, hvor vi foretager en simulation af et udvalgt beredskabsudløsende scenarie

Desuden er vores infrastruktur designet med særlige hensyn til redundans.

18. Overensstemmelse

Ambition A/S er ikke underlagt særlovgivning for nuværende. Ambition A/S har ikke særlige interessegrupper for nuværende. Vores kunder kan være underlagt yderligere lovgivning, og hvor det måtte være tilfældet, er vores understøttelser heraf aftalt særskilt.

Vi har en række interne kontroller for at tilsikre overensstemmelse med interne politikker, procedurer og faktisk drift til enhver tid. Disse dækker også teknisk overensstemmelse.

Vi er desuden underlagt årlig IT-revision af ekstern, uafhængig revisor.

19. Komplimenterende kontroller

Medmindre 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, vi) Anmodning om adgang til kundens servermiljø for kundens tredjepartsleverandører, og vii) Kundens anmeldelse til Datatilsynet, for hvem dette måtte være relevant.

KAPITEL 3:

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

Til kunder af Ambition A/S og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Ambition A/S beskrivelse i kapitel 2, som er en beskrivelse af kontrolmiljøet i forbindelse med IT-driften af Ambition A/S i perioden 1. marts 2021 til 28. februar 2022, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de IT-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. Erklæringen dækker ikke kontrol eller tilsyn med underleverandører i tilknytning til driften. Disse underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Erklæringen dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. virksomhedsbeskrivelsen i kapitel 2, afsnittet om komplementerende kontroller hos kunderne.

Ambition A/S' ansvar

Ambition A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i kapitel 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet 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.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR's Etiske Regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om Ambition A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til 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 overholder etiske krav samt 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 beskrivelse, udformning og funktionalitet 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 i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som Ambition A/S har specificeret og beskrevet i kapitel 2.

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

Begrænsninger i kontroller hos Ambition A/S

Ambition 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 vigtig efter deres særlige forhold. Endvidere vil kontroller hos Ambition A/S, som følge af deres art, muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos serviceleverandøren kan blive utilstrækkelige eller svigte.

Konklusion

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

a) at beskrivelsen af Ambition A/S' kontrolmiljø i tilknytning til driften af Ambition A/S, således som det var udformet og implementeret i hele perioden 1. marts 2021 til 28. februar 2022, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. marts 2021 til 28. februar 2022, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. marts 2021 til 28. februar 2022.

Beskrivelse af testede kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt Ambition A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer om kravene til kontrolmiljøet er overholdt.

Søborg, den 31. maj 2022

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Poul Halkjær Nielsen
IT-revisor, CISSP, CISM, CISA

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med ISAE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27001 og 2, version 2017.

Hvad angår periode har vi i vores test forholdt os til, om Ambition A/S har levet op til kontrolmålene i perioden 1. marts 2021 til 28. februar 2022.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som Ambition A/S jf. sin dokumentation har iværksat for at leve op til kravene.
- Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet.
- Tredje kolonne viser resultatet af vores test.

De udførte tests

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

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

KONTROLMÅL - INDLEDNING:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i driften af Ambition A/S. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
Der foretages en årlig risikovurdering, som forelægges og vurderes af ledelsen. Risikovurderingen indgår som en del af arbejdet med Ambition A/S informationssikkerhedsledelsessystem (ISMS).	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for Ambition A/S arbejdes med en løbende vurdering af de risici, som opstår som følge af de forretningsmæssige forhold og deres udvikling. Vi har kontrolleret, at risiko er en integraldel af forretningens daglige arbejdsgange.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 4:

Risikovurdering og -håndtering

Kontrolmålet er tilsikring af, at virksomheden periodisk foretager en analyse og vurdering af IT-risikobilledet

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
4.1 Formålet er at identificere og klassificere de risici, der kan påvirke organisationernes evne til at operere i henhold til de forpligtelser, virksomheden har. 4.2 Der foretaget en regelmæssig vurdering og kontrol af de udfordringer virksomheden står overfor og disse behandles i ledelsesteamet, hvor ledelsen vurderer, om nye risici er opstået og derfor kræver yderligere analyse og håndtering.	Vi har foretaget interview med relevant ledelse og personale. Vi har indhentet og gransket Ambition A/S' aktuelle og godkendte risikovurdering. Vi har verificeret, at der foretages risikovurderinger og at de rapporteres til ledelsen. Vi er blevet oplyst at risikoarbejdet sker både gennem den formelle risikovurdering samt løbende i projektarbejdet. Vi har bekræftet, at Ambition A/S' eksponering styres baseret på risikoscoren, der beregnes ud fra risikopåvirkningen og sandsynligheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Formålet er at give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
5.1 Der er udarbejdet en IT-sikkerhedspolitik og Information Security Management System (ISMS) som er godkendt af Ambition A/S' ledelse. Ambition A/S sikrer dette ved at kommunikere revisioner og opdateringer i hele organisationen via awareness-træning, e-mails såvel som på afdelings- og personalemøder.	Vi har foretaget interview med relevant ledelse og personale, og der er indhentet dokumentation. Vi har inspiceret og gennemgået Ambition 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 er oplyst, at politikken er godkendt af ledelsen og set at den er stillet til rådighed for medarbejderne på Ambition A/S' intranet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Formålet er at give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav samt relevante love og forskrifter.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
6.1 Alt ansvar for informationssikkerhed skal defineres og fordeles. Modstridende pligter og ansvarsområder bør adskilles for at reducere muligheden for uautoriseret eller utilsigtet ændring eller misbrug af organisationens aktiver. 6.2 Informationssikkerhedspolitiken inkluderer kontroller til fjernadgang og der er implementeret sikkerhedsforanstaltninger for at sikre fjernadgang.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret tildelingen af informationssikkerhedsroller og -ansvar samt opdeling af opgaver. Vi har forespurgt og er oplyst om kontrakt med myndigheder og interessegrupper. Vi har forespurgt om informationssikkerheden i projektstyring. Vi har inspiceret om politikken for styring af mobilenheder. Vi har inspiceret politikken for fjernadgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Formålet er at sikre, at medarbejder og kontrahenter er egnede til de roller de er i betragtning til og forstår at efterleve deres ansvar.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
7.1 Ambition A/S har etableret formelle procedurer for ansættelse af nye medarbejdere. 7.2 Personer, der tilbydes en stilling i Ambition A/S, vil blive genstand for en baggrundskontrol i overensstemmelse med gældende love og regler, 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. 7.3 Informationssikkerhedsansvar og forpligtelser er gældende efter ansættelsens ophør.	Vi har foretaget interview med relevant ledelse og personale. Vi har observeret, at der er en formel procedure for ansættelse af nye medarbejdere. Vi har inspiceret, at der foretages baggrundskontrol af medarbejderne før ansættelse. Vi har gennemgået skabeloner der siger, at medarbejder er forpligtet til at opretholde kontrakten og er underlagt tavshedspligt. Vi har forespurgt, om medarbejdere har modtaget undervisning og træning om informationssikkerhed og organisationens politikker. Vi har set dokumentation for og deltagerlister fra afholdte træninger. Vi har inspiceret, at informationssikkerhedsansvar og forpligtelser er gældende efter ansættelsens ophør.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 8:

Styring af aktiver

Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
8.1 Ambition A/S har registreret væsentlige IT-aktiver i en række systemer. Retningslinjer for accepteret brug af al informationsrelateret aktiver findes og er tilgængelige for relevante medarbejdere. 8.2 Alle informationsrelaterede aktiver er identificeret, er klassificeret, og har en systemejer som er ansvarlig for at aktiverne er udpeget. 8.3 Der er implementeret kontroller til at sikre håndtering af medier.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at alle informationsrelaterede aktiver har været identificeret, og at der er udpeget en systemejer til aktivet. Vi har inspiceret, at dokumentationen af aktiver er tilstrækkelig og korrekt. Vi har forespurgt om retningslinjer for klassificering af data. Vi har forespurgt om retningslinjer for håndtering af aktiver inklusiv bærbare aktiver. Vi har forespurgt om retningslinjer for bortskaffelse af medier. Vi er oplyst at det ikke er sket i perioden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

Formålet er at begrænse adgangen til information, sikre autoriseret brugeradgang og at forhindre uautoriseret adgang til systemer og services.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
9.1 Der er en politik og procedure for tildeling, ændring og tilbagekaldelse af adgangsrettigheder for medarbejdere. 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. 9.3 Adgangskoder er personlige og holdes hemmelige. 9.4 Adgang til operativsystemer og netværk er beskyttet af adgangskoder. Kvalitetskrav for længde, kompleksitet, og varighed er specificeret for adgangskoder. Desuden bliver brugeren 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 foretaget interview med relevant ledelse og personale. Vi har inspiceret politikken og proceduren for livscyklus for adgangsrettigheder. Vi har forespurgt om styring og implementeret kontrol af privilegerede adgangsrettigheder. Vi har spurgt om kontroller til periodisk gennemgang af brugeradgangsrettigheder. Vi har inspiceret, at al adgang til systemer er underlagt en prædefineret adgangskodepolitik. Vi har spurgt om retningslinjer for begrænsning af adgang til information og sikre login procedurer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 10:

Kryptografi

Formålet er at begrænse adgangen til information, tilsikre autoriseret brugeradgang og at forhindre uautoriseret adgang til systemer og services.		
Ambition A/S kontroller	**Revisors test af kontroller**	**Resultat af test**
10.1 Der er i Informationssikkerhedspolitiken sat krav om, at al kommunikation på åbne, offentlige medier, fx Internet skal være krypteret. Dette gælder både mails, internetbaseret trafik og adgang til systemer fra andre lokationer, fx VPN. 10.2 Skift af krypteringsnøgler sker efter en fastsat procedure.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at der anvendes kryptering på transmission over internettet. Vi har verificeret, at der er procedurer for skift af krypteringsnøgler.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 11:

Fysisk sikkerhed og miljøsikring

Formålet er 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.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
11.1 Alle informationsrelaterede aktiver er beskyttet mod uautoriseret adgang i datacentre og kontorer med adgangssystemer, overvågning og alarmer. Kontroller giver også rimelig sikkerhed for at adgange overvåges og tildeles i henhold til forretnings og arbejdsrelaterede behov. 11.2 Alle informationsrelaterede aktiver er beskyttet mod brand, vand og varme. Alle informationsrelaterede aktiver er beskyttet mod strømafbrydelse via UPS og nødstrømsystemer. Kabler til elektronisk kommunikation og elektricitet forsyningen er beskyttet mod manipulation. Data der bærer informationsrelaterede aktiver, bortskaffes på en sikker måde.	Vi har foretaget interview med relevant ledelse og personale. Vi har forespurgt om beskyttelse af driftsfaciliteter samt de fysiske sikkerhedsperimetre for Ambition A/S' placering. Vi har inspiceret, at teknikrummet er bag aflåste døre og er oplyst at kun relevante medarbejdere med arbejdsbetinget behov har adgang til rummet. Vi har forespurgt om at kontorer og faciliteter er beskyttet mod eksterne og miljømæssige trusler. Vi har inspiceret ISAE 3402 erklæring fra Sentia og set at den dækker redundans. Vi har inspiceret Ambitions egen rapport fra on-site inspektion af Sentias datacenter. Vi har spurgt om retningslinjer for bortskaffelse af udstyr og er oplyst at det ikke er sket i perioden. Vi er oplyst om at der i Active Directory (AD) er opsat regler for krav om skærmlås. Vi har spurgt om og inspiceret retningslinjer for "clean desk" og ubetjent brugerudstyr.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter inkl. informationer samt, at disse er beskyttet mod malware og tab af data. Derudover:
- At hændelser logføres til bevisførelse
- At integriteten af driftssystemer opretholdes.
- Forhindre, at tekniske sårbarheder udnyttes
- Forhindre indvirkningen af auditaktiviteter.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af 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 Ambition A/S har etableret en formel proces for ændringsstyring, der sikrer test og godkendelse af relevante ændringer.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at der er dokumenterede driftsprocedurer. Vi har inspiceret, at der er en dokumenteret procedure for ændringsstyring. Vi har inspiceret at der sker ændringsstyring og gennemgået udviklingsgangen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 foretaget interview med relevant ledelse og personale. Vi har inspiceret, at Informationssikkerhedspolitiken angiver, hvordan Ambition A/S skal beskyttes mod malware. Vi har bemærket, at antivirus software er installeret på relevante servere og brugerudstyr, og at denne software opdateres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.3 Der er etableret kontroller, der giver rimelige forsikring om, at processerne vedrørende backup og gendannelse af data er tilfredsstillende og i overensstemmelse med kunders leveringsaftale og Ambition A/S' kontraktlige forpligtelser også kaldet Service Level Agreement (SLA).	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at der er dokumenterede procedurer for backup, og at der er faste backupjob via Sentia Denmark A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.4 Der er implementeret kontroller for at give rimelige forsikring om, at Ambition A/S har implementeret systemer til overvågning af server og netværksdrift.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at der er implementeret et system til samling af logfiler og events fra servere og netværksenheder. Vi har inspiceret de anvendte foranstaltninger til beskyttelse af log information.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

	Vi har inspiceret, at synkronisering af tid har været implementeret.	
12.5 Der er etableret kontroller til styring af softwareinstallationen i driftssystemet.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at der er en formel procedure til versionsstyring af software. Vi har inspiceret, at der er kontroller med hvem, der må lægge ny software i drift.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.6 Kritiske softwareapplikationer og opdateringer overvåges. Der er tekniske begrænsninger for at overholde alle licensrettigheder til installeret software.	Vi har foretaget interview med relevant ledelse og personale. Vi har forespurgt om håndtering af tekniske sårbarheder. Vi har forespurgt om begrænsninger i softwareinstallation. Vi har inspiceret retningslinjer og implementerede kontroller.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12.7 Der er procedurer for periodisk revision af informationssystemerne.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret at der er udført periodisk revision på informationssystemerne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og sikre beskyttelse af understøttelse af informationsbehandlingsfaciliteter.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
13.1 Der er etableret kontroller, der giver rimelige sikkerhed for, at netværket er sikret ved brug af firewalls. 13.2 Der er etableret kontroller, der giver rimelige forsikring om, at overførslen af oplysninger er beskyttet.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at netværket administreres, dokumenteres. Vi har inspiceret, at der er tilstrækkelig adskillelse af opgaver i driften af netværkssikkerhed. Vi har inspiceret, at produktionsmiljøet er designet og implementeret som en redundant opsætning. Vi har spurgt om politikker og procedurer for informationsoverførsel.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 14:

Anskaffelse, udvikling og vedligeholdelse af systemer

Formålet er at sikre, at informationssikkerhed er en integreret del af informationssystemerne og gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
14.1 Ved udvikling af funktionalitet benyttes sikre metoder til kodning og kode review. 14.2 Der anvendes sikre udviklingsmetoder i forbindelse med udvikling af interne applikationer. Alle releases testes grundigt inden frigivelse til produktionsmiljø. Der er implementeret automatisk test af funktionalitet inden brugertest. Der er implementeret en procedure for kontrol og opfølgning på outsourcet udvikling. 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 foretaget interview med relevant ledelse og personale. Vi har observeret, at der laves kode review af udviklet kode. Vi har spurgt om udviklingspolitikken og procedurerne for systemændring. Vi har spurgt om begrænsninger vedrørende ændringer af softwarepakker. Vi har spurgt om sikre systemtekniske principper og sikre udviklingsmiljø. Vi har spurgt om outsourcet udvikling. Vi har spurgt om systemsikkerhedsprøvning og test af systemaccept. Vi har spurgt om politikken til beskyttelse af testdata.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

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.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
15.1 Risici forbundet med eksterne forretningspartnere identificeres og sikkerhed i tredjepartsaftaler og i forhold til kunder styres. 15.2 Overvågning af leverandører skal udføres regelmæssigt, herunder tilsyn med eksterne forretningspartnere.	Vi har foretaget interview med relevant ledelse og personale. Vi har forespurgt om og inspiceret processen for at vedligeholde Ambition A/S' krav til informationssikkerhed i leverandørforhold. Vi har spurgt om kontroller til overvågning af leverandørtjenester. Vi har spurgt om styring af ændringer i leverandørtjenester. Vi har bekræftet, at Ambition A/S har modtaget og evalueret ISAE 3402 Type II erklæringer fra central leverandør.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

Formålet er at sikre ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og svagheder.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
16.1 Sikkerhedshændelser rapporteres til ledelsen så snart som muligt, og de styres på en ensartet og effektiv måde.	Vi har foretaget interview med relevant ledelse og personale. Vi har spurgt om ansvar og procedurer for sikkerhedshændelser og rapportering af sikkerhedsbegivenheder. Vi har inspiceret procedurer for håndtering af sikkerhedshændelser og er oplyst at ledelsen kender deres roller og at roller er klart defineret. Vi har bekræftet at beredskabsplanen er blevet testet som udløber af en hændelse i perioden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Formålet er at sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring samt, at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
17.1 Der er etableret en sammenhængende ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og opfylder alle sikkerhedskrav og til fastlægge prioritering af test og vedligeholdelse. 17.2 Der er etableret infrastruktur med særligt hensyn til redundans.	Vi har foretaget interview med relevant ledelse og personale. Vi har inspiceret, at Ambition A/S har en beredskabsplan. og at den involverer ledelsen. Vi har verificeret, at planen er testet. Vi har inspiceret, at infrastrukturen er implementeret redundant.	Vi har ikke ved vores test konstateret væsentlige afvigelser

KONTROLMÅL 18:

Overensstemmelse med lov og kontraktskrav

Formålet er at sikre ensartet og effektiv metode til styring af informationssikkerhedsbrud herunder kommunikation om sikkerhedshændelser og -svagheder.

Ambition A/S kontroller	Revisors test af kontroller	Resultat af test
18.1 Alle vores aftaler er reguleret og indeholder krav om fortrolighed. 18.2 Der indhentes revisorerklæringer på væsentlige ydelser.	Vi har foretaget interview med relevant ledelse og personale. Vi har spurgt om kontroller til at identificere juridiske og kontraktlige krav Vi har spurgt om kontroller til validering og intellektuel ejendomsret vedrørende software. Vi har set, at der udarbejdes ISAE 3402 erklæringer på væsentlige ydelser. Vi har spurgt om implementerede kontroller for at sikre overholdelse af virksomhedens politikker og standarder. Vi har spurgt om implementerede kontroller for at sikre teknisk overholdelse af kontrol.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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."

Kim Larsen
Revisor
På vegne af: Beierholm
Serienummer: CVR:32895468-RID:34629841
IP: 212.98.xxx.xxx
2022-06-02 13:51:03 UTC
NEM ID

Poul Halkjær Nielsen
Revisor
På vegne af: Beierholm
Serienummer: CVR:32895468-RID:50750152
IP: 212.98.xxx.xxx
2022-06-02 17:06:15 UTC
NEM ID

Peter Nyemann
Direktion
Serienummer: PID:9208-2002-2-374569592814
IP: 130.185.xxx.xxx
2022-06-09 09:21:30 UTC
NEM ID