AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. NOVEMBER 2023 TIL 31. OKTOBER 2024 OM BESKRIVELSEN AF SOFTWARE SERVICES OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

WeCode A/S

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. NOVEMBER 2023 TIL 31. OKTOBER 2024 OM BESKRIVELSEN AF SOFTWARE SERVICES OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Til: Ledelsen i WeCode A/S
WeCode A/S kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om den af WeCode A/S (serviceleverandøren) for hele perioden fra 1. november 2023 til 31. oktober 2024 udarbejdede beskrivelse i sektion 3 af software services ydelser og de tilhørende kontroller, og om udformningen og den operationelle effektivitet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandørens ansvar

Serviceleverandøren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom serviceleverandøren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

BDO Statsautoriseret revisionsaktieselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om serviceleverandørens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed kontroller hos en serviceorganisation. 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 den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risicierne for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i sektion 2.

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

Begrænsninger i kontroller hos en serviceleverandør

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

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i serviceleverandørens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af software services og de tilhørende kontroller, således som de var udformet og implementeret i hele perioden fra 1. november 2023 til 31. oktober 2024, i alle væsentlige henseender er retvisende, og

b. at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. november 2023 til 31. oktober 2024, og

c. at de testede kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. november 2023 til 31. oktober 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt serviceleverandørens software services, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundens egne kontroller, ved opnåelsen af en forståelse af kundernes informationssystemer, der er relevante for regnskabsaflæggelsen.

København, den 20. december 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. WECODE A/S UDTALELSE

WeCode A/S udvikler softwareløsninger til en række danske og internationale kunder inden for såvel den offentlige som private sektor, som har betydning for bogføringen og regnskabsaflæggelsen hos serviceleverandørens kunder.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt software services, 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, når de opnår en forståelse af kunders informationssystemer, som er relevante for regnskabsaflæggelsen.

WeCode A/S anvender serviceunderleverandører. Disse serviceunderleverandørers relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

WeCode A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af software services og de tilhørende kontroller i hele perioden fra 1. november 2023 til 31. oktober 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for software services, og hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:
   - De typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant.
   - 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

2. Indeholder relevante oplysninger om ændringer i serviceleverandørens software services foretaget i perioden fra 1. november 2023 til 31. oktober 2024.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af software services og de tilhørende kontroller under hensyntagen til, at denne beskrivelse 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 software services, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

WeCode A/S bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. november 2023 til 31. oktober 2024. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

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

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. november 2023 til 31. oktober 2024.

København, den 20. december 2024

WeCode A/S

Troels Johannesen
CEO, Ejer

3. WECODE A/S BESKRIVELSE AF SOFTWARE SERVICES

WeCode A/S beskæftiger ca. 21 medarbejdere, og har kontor på adressen, Thorsgade 59, 2. sal, 2200 København N. WeCode A/S er en softwarevirksomhed der hoster, supporterer og udvikler webapplikationer og systemer samt webshops. Der forefindes ikke fysiske servere på virksomhedens adresse, disse ligger hos leverandører. Alle servere, hvorpå der hostes kundesystemer, ligger fysisk inden for EU. I virksomheden arbejdes der på bærbare MacBooks, og alle computer-versioner overvåges via et Mobile Device Management system. Der er på alle computere opsat malware protection og sat restriktioner og regler for downloading af apps.

RISIKOVURDERING OG - HÅNDTERING

WeCode A/S logger løbende risici vedr. de systemer vi hoster og drifter. Alle identificerede risici gennemgås og vurderes i forbindelse med de kvartalsvise sikkerhedsmøder. Det er ledelsen i virksomheden, der logger og vurderer risici samt sikrer udarbejdelse af handlingsplaner for at minimere disse.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

Sikkerhedspolitik
Informationssikkerhedspolitikkerne bliver mindst 1 gang årligt revurderet af ledelsen i forbindelse med et af de kvartalsvise sikkerhedsmøder. Eventuelle ændringer til sikkerhedspolitikken skal præsenteres og godkendes af bestyrelsen ved næste forestående bestyrelsesmøde. Til Lead udvikler møder vil eventuelle ændringer i de tekniske foranstaltninger gennemgås og diskuteres, samt hvilke tiltag der eventuelt skal tages for at implementere eventuelle ændringer i retningslinjerne i de enkelte teams. Alle ændringer i politikkerne kommunikeres ud til samtlige medarbejdere via det månedlige møde. Der forefindes procesbeskrivelser og guides for alle vigtige processer, let tilgængeligt for alle relevante medarbejdere. Der er i virksomheden opsat politikker og processer for sikker udvikling og opbevaring af systemer for vores kunder. Alle vores systemer og dertilhørende kildekode versioneres. Som sikkerhedsforanstaltning er test og produktionsservere altid adskilt i tilfælde af nedbrud. Tekniske sårbarheder overvåges, logges og udbedres løbende af lead udviklerne i virksomheden i tæt dialog med de enkelte kunder. Alle ændringer foretages altid i et testmiljø, før det implementeres. Der forefindes backups af alle kundeprojekter og dertilhørende data. Der tages backup dagligt, og denne opbevares på en særskilt server. Backup bruges til genopretning ved nedbrud på en produktionsserver, og der forefindes en klar proces og ansvarsfordeling i sådanne tilfælde.

Medarbejdersikkerhed
Inden ansættelse screenes ansøgere først af CEO og HR, herefter indkaldes relevante kandidater til minimum 2 samtaler. 1. hvor HR deltager, og laver en indledende vurdering af ansøgers personlige egenskaber, og hvorvidt disse kunne være et match til det team, der ansættes til, herudover vil der være en indledende forventningsafstemning i forhold til arbejdsrammer. I 2. samtale deltager HR samt en lead udvikler eller CEO for at vurdere ansøgers tekniske færdigheder. Ved tiltrædelse forefindes der en fast proces for onboarding, der blandt andet inkluderer præsentation, gennemgang og test i virksomhedens sikkerhedspolitikker, opsætning af mobile enheder og opsætning af adgange til lokaler, skabe og systemer. Ved fratrædelse fjernes alle adgange senest den næstkommende hverdag. Alt hardware tilbageleveres. Medarbejderen holdes løbende ajour med eventuelle ændringer i virksomhedens sikkerhedspolitikker. Der afholdes test i sikkerhedspolitikkerne 1 gang i kvartalet. Styring af informationsrelaterede aktiver, servere og dertilhørende kodebaser noteres og vedligeholdes i et Google Sheet, der opdateres løbende ved ændringer og oprettelse af nye servere. Dette vedligeholdes af den sikkerhedsansvarlige lead udvikler i virksomheden, og gennemgås i samarbejde med ledelsen forud for de kvartalsvise sikkerhedsmøder. Der opretholdes fortegnelser over alle virksomhedens computere og øvrige mobile enheder.

Adgangsstyring
Der tildeles adgange og brugerrettigheder efter et need-to-have-princip. Det vil sige, at en medarbejder kun får tildelt en adgang, hvis det er nødvendigt for dem, for at udføre deres arbejde, og ligeledes tildeles kun de brugerrettigheder, der er nødvendige for medarbejderne. Adgangene logges og gennemgås minimum 1 gang årligt i forbindelse med et sikkerhedsmøde. Adgang til servere kan kun tildeles af ledelsen, og er forbeholdt lead udviklere. Adgang til servere kan kun ske via virksomhedens interne kodebeskyttede netværk, eller via VPN. Servere kan kun tilgås via SSH med en SSH nøgle. Der er påkrævet 2 faktor login eller SSO til alle vigtige systemer. Logins og adgange oprettes altid med en af virksomheden oprettet mailadresse. WeCode har en klar politik for oprettelse af sikre adgangskoder. Kodeord til virksomhedens aktiver og kundesystemer opbevares af medarbejderen i Apple Keychain, som er beskyttet af en ekstra adgangskode.

Fysisk sikkerhed
Adgang til bygningen kan ske via dørtelefon, der deles med andre organisationer og virksomheder. Ingen medarbejdere har en nøgle til hverken yderdør til ejendommen eller til selve kontoret. Adgang til ejendommen kan kun ske mellem kl. 7.00 og kl. 19.00 på hverdage. Hver medarbejder modtager ved onboarding en personlig kode til virksomhedens hoveddør. Denne kode må ikke deles med andre eller mellem medarbejdere. Ved offboarding af en medarbejder fjernes denne kode. Der logges hver gang, en kode bliver benyttet til at tilgå kontoret. Kontoret er udstyret med en alarm, der skal slåes fra med en separat kode af den først ankomne. Koden er ens for alle, men skiftes hver 6. mdr. og kommunikeres ud via den interne platform. Koden til alarmen gives ikke til studerende, praktikanter eller lignende medarbejdere ansat på deltid eller i en midlertidig stilling. Den første og den sidste, der forlader kontoret, kan derfor kun være en fuldtidsmedarbejder i virksomheden. Besøgende kan benytte en ringeklokke, der sidder ude foran hoveddøren. Der er 2 ståldøre, der giver adgang til kontoret. Alle medarbejdere er instrueret i at bruge hoveddøren. Indgang via bagdør igangsætter alarmen, hvis man er den først fremmødte. Alarmsystemet er opsat med dørafbrydere, sensorer og kameraer. Disse serviceres af et alarmselskab. Mobilt udstyr skal uden for arbejdstiden opbevares i tildelte kodebeskyttede sikkerhedsskabe.

Styring af netværk og drift
Virksomhedens servere er hostet hos pålidelige tredjepartsleverandører. Lead-udviklere er ansvarlige for at vedligeholde og overvåge softwaren på serverne. Serverne overvåges, så der hurtigt og effektivt kan identificeres eventuelle fejl eller driftsproblemer og tages øjeblikkelig handling for at løse dem. Alle medarbejdere bruger MacBooks, som administreres via et Mobile Device Management (MDM)-system. Dette muliggør regelmæssige opdateringer og sikkerhedsforanstaltninger for at beskytte vores arbejdsstationer mod trusler. MacBooks, der ikke længere kan opdateres med sikkerhedsrettelser, bliver afskaffet for at opretholde en høj sikkerhedsstandard. Netværksinfrastrukturen leveres af en netværksleverandør, og er baseret på fibernet. Netværksudstyr i virksomheden opdateres regelmæssigt af netværksleverandøren for at sikre en stabil og sikker forbindelse. Overvågning af netværket udføres af vores netværksleverandør, der proaktivt identificerer og håndterer eventuelle problemer eller trusler for at opretholde høj netværkstilgængelighed og ydeevne. Der er på virksomhedens adresse implementeret et kodebeskyttet WiFi, der kun er tilgængeligt for vores medarbejdere. Adgangskoden til dette netværk ændres kvartalsvis for øget sikkerhed. Derudover har vi et gæstenetværk, der giver besøgende en bekvem internetadgang uden at kompromittere sikkerheden på vores interne netværk.

Kommunikationssikkerhed
WeCode har forskellige politikker vedrørende datadeling og opbevaring. Procedurerne afhænger af, hvilke data der er tale om. I virksomheden er data defineret ud fra forskellige klassifikationer, og det er disse klassifikationer, der afgør, hvordan data må deles og opbevares. Data opbevares ikke lokalt på bærbare medier for

at minimere risikoen for datatab eller lækage. Data udskrives eller nedfældes ikke i fysisk form, f.eks. papirform, for at forhindre uautoriseret adgang. Data deles kun, hvis dette er nødvendigt. Dataudveksling skal altid ske via sikre protokoller som HTTPS og OAUTH for API-udveksling. Deles der databaser internt til brug for udvikling, vil persondata og lignende blive obfuscated af en lead udvikler inden deling.

Der arbejdes udelukkende med dummy data i testmiljøer, medmindre dataene er strengt nødvendig til f.eks. fejlfinding. Følsomt og kritisk data skal blandt andet gemmes som BLOB-filer, og kan kun åbnes med en nøgle, hvilket sikrer, at data forbliver utilgængelig fra samme server.

Anskaffelse, udvikling og vedligeholdelse af Informationsbehandlingssystemer
I virksomheden udføres serveropsætning via Forge med anvendelse af den seneste software, inklusive PHP, Nginx, MySQL og Ubuntu. For at beskytte adgangen til serveren implementeres en firewall, som kun tillader SSH-adgang fra godkendte IP-adresser. Kildekodeadministrationen foregår på GitHub, hvor hovedbranchen er beskyttet, og kun Lead-udviklere har kontrol over produktionen. Når data håndteres i henhold til klassifikation A eller B, følger virksomheden sikkerhedspolitikken for ansvarlig datahåndtering. I virksomheden prioriterer man sikkerheden i udviklings- og hjælpeprocesserne.

Lead-udviklere er ansvarlige for at opretholde sikkerheden i deres team, og følger strenge standarder for sikkerhedsimplementering i de anvendte teknologier. Der er implementeret monitorering for at spore kodeændringer, og der findes direkte kommunikationskanaler, hvor Lead-udviklere informeres om sikkerhedsopdateringer i projekter, hvor de er tekniske ejere. Virksomheden sikrer, at alle kildekoder gennemgår en nøje code-review-proces, og en "request-to-pull" tilgang anvendes, hvor udviklere anmoder om kodegennemgang og test af en Lead-udvikler. For større applikationer benyttes også Continuous Integration (CI) til at teste for fejl og mangler, og en pull-request kan kun godkendes, hvis koden består de nødvendige CI-tests. For at sikre sikkerheden og beskyttelsen af følsomme data håndteres testdata omhyggeligt i virksomheden. Kun Lead-udviklere har adgang til live databaser, og de har kun adgang til databaser, der er knyttet til projekter, hvor de fungerer som teknisk ansvarlige. Når databaser eksporteres til brug i et testmiljø, renses de omhyggeligt for personoplysninger.

I testmiljøet anvendes kun databaser med dummy-data eller obfuscated data for at beskytte følsomme oplysninger. Virksomheden sikrer, at testdata håndteres i overensstemmelse med sikkerhedsprotokoller for at opretholde integriteten og fortroligheden af data. I virksomheden implementeres omfattende logning og hændelseslogning. Kundespecifik logning aftales i samarbejde med kunden, mens generel logning af systemer administreret af virksomheden involverer tredjepartstjenester. Log-oplysninger er beskyttet og kun tilgængelige for Lead-udviklere. Alle handlinger udført af administratorer og operatører logges for at sikre sporbarhed og gennemsigtighed.

Leverandørforhold
I virksomheden er leverandørforholdene baseret på nøje udvalgte partnere, der overholder branchens bedste praksis. Disse leverandører er valgt ud fra standarder, der sikrer sikkerhed og pålidelighed. Relevante erklæringer fra leverandørerne indhentes og evalueres årligt. Eventuelle afvigelser eller usikkerheder i disse erklæringer diskuteres og vurderes på et dedikeret sikkerhedsmøde.

Styring af sikkerhedshændelser
Nedetid på systemer monitoreres, og lead udviklerne orienteres uden ophold ved nedetid. Der forefindes en klar ansvarsdeling og procedurer ved nedbrud på systemer eller kompromittering af data. Lead udviklerne i virksomheden vurderer løbende trusselsbilledet samt prioriterer og implementerer opdateringer.

Beredskabsstyring

WeCode A/S har en beredskabsplan ved nedbrud eller kompromittering af servere. Der laves beredskabsøvelser minimum årligt, hvor genetablering af projekter fra backups testes. Tests er planlagt mellem ledelsen og lead udviklerne i virksomheden. Øvelserne finder sted op til et internt sikkerhedsmøde, hvor øvelserne og beredskabsplanen evalueres og opdateres, hvis nødvendigt.

ÆNDRINGER I SOFTWARE SERVICES OG DE TILHØRENDE GENERELLE IT-KONTROLLER

Der er i perioden fra 1. november 2023 til 31. oktober 2024 ikke foretaget væsentlige ændringer i software services og de tilhørende generelle it-kontroller.

KOMPLEMENTERENDE KONTROLLER HOS SERVICELEVERANDØRENS KUNDER

Kunden er forpligtet til at implementere følgende tekniske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed i overensstemmelse med relevant lovgivning:

- Kunden er ansvarlig for egne data. Det betyder, at kunden er ansvarlig for de ændringer, der måtte foretages i data, når der er logget på systemet med individuelle brugernavne og adgangskoder, herunder den behandling af data, der foretages i systemet, sker i overensstemmelse med relevant lovgivning.
- Kunden styrer brugerrettighederne i softwareservicen, herunder hvilke personer hos kunden, der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed om kontroller hos en serviceorganisation.

BDO har udført handlinger for at opnå bevis for oplysningerne i WeCode A/S beskrivelse software services samt for udformningen og den operationelle effektivitet af de tilhørende kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af WeCode A/S, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden fra 1. november 2023 til 31. oktober 2024.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen og den operationelle effektivitet heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som Akamai/Linode leverer inden for hosting, har vi modtaget ISO 27001 certifikation og SoA vedrørende serviceunderleverandørens kontroller.

For de ydelser, som Backblaze leverer inden for backup, har vi modtaget en SOC 2 rapport vedrørende serviceunderleverandørens kontroller.

For de ydelser, som Amazon Web Services leverer inden for hosting af services, har vi modtaget SOC 1 rapport vedrørende serviceunderleverandørens kontroller.

Disse serviceunderleverandørers relevante kontrolmål og tilknyttede kontroller indgår ikke i WeCode A/S beskrivelse af software services og de tilhørende kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos WeCode A/S, der sikrer overvågning af serviceunderleverandørens opfyldelse af den mellem serviceunderleverandøren og WeCode A/S' indgåede aftale.

Resultat af test

Resultatet af de udførte test af kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet og implementeret eller ikke har fungeret effektivt i perioden.

Risikovurdering		
Kontrolmål ▶ *At sikre, at serviceleverandøren udfører en årlig risikovurdering i forhold til grundlaget for de tekniske og organisatoriske sikkerhedsforanstaltninger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Risikovurdering ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandør løbende identificeret trusler som bliver vurderet i forhold til selskabets it-anvendelse. Vi har inspiceret årshjulet og referat af et sikkerhedsmøde og observeret at risikovurderingen bliver opdateret løbende.	Ingen afvigelser konstateret.

A.5 Organisatoriske foranstaltninger

Kontrolmål

- *At sikre løbende egnethed, tilstrækkelighed, effektivitet af ledelsens retning og støtte til informationssikkerhed i overensstemmelse med forretningsmæssige, juridiske, lovmæssige, regulatoriske og kontraktlige krav.*
- *At etablere en defineret, godkendt og forstået struktur for implementering, drift og styring af informationssikkerhed i organisationen.*
- *At reducere risikoen for svindel, fejl og omgåelse af informationssikkerhedsforanstaltninger.*
- *At sikre, at ledelsen har forstået deres informationssikkerhedsmæssige rolle og iværksætter handlinger for at sikre, at alle medarbejdere er bevidste om og opfylder deres informationssikkerhedsansvar.*
- *At klarlægge organisationens information og understøttende aktiver for at bevare informationssikkerhed og tildele passende ejerskab.*
- *At sikre autoriseret adgang og forhindre uautoriseret adgang til information og understøttende aktiver.*
- *At give mulighed for entydig identifikation af personer og systemer, der får adgang til organisationens information og understøttende aktiver, og at muliggøre passende tildeling af adgangsrettigheder.*
- *At sikre korrekt entitetsautentifikation og forhindre fejl i autentifikationsprocesser.*
- *At sikre, at adgang til information og understøttende aktiver er defineret og autoriseret overensstemmelse med de forretningsmæssige krav.*
- *At opretholde et aftalt informationssikkerhedsniveau i leverandørforhold.*
- *At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.*
- *At angive og styre informationssikkerhed i forbindelse med brugen af cloudtjenester.*
- *At sikre hurtig, effektiv, konsekvent og velordnet håndtering af informationssikkerhedsincidents, herunder kommunikation om informationssikkerhedshændelser.*
- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
5.1 Politikker for informationssikkerhed ▶ Serviceleverandøren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Serviceleverandørens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har implementeret en informationssikkerhedspolitik. Vi har yderligere inspiceret, at informationssikkerhedspolitikken bliver gennemgået og opdateret en gang årligt.	Ingen afvigelser konstateret.
5.2 Roller og ansvar for informationssikkerhed ▶ Serviceleverandøren sikrer, at samme person ikke har adgang til at tilgå, ændre og anvende systemer, informationer eller infrastruktur, uden at dette er godkendt eller vil blive opdaget. ▶ Serviceleverandøren har en klar opdeling af organisationen i forhold til informationssikkerhed og har udførlige ansvars- og rollebeskrivelser for de enkelte medarbejdere.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og observeret, at der heri er defineret, hvem der er godkendt til at ændre i systemer.	Ingen afvigelser konstateret.

	Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og observeret, at roller og ansvar for de enkelte medarbejdere er defineret heri, herunder at bestyrelsen har det overordnede ansvar.	
5.3 Funktionsadskillelse ▶ Serviceleverandørens funktioner og ansvarsområder er adskilt, i det omfang det er muligt, taget virksomhedens størrelse i betragtning, for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af data.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og observeret serviceleverandøren heri har implementeret en adskillelse af funktioner, herunder at kun ledelsen har den fulde adgang til alle projekter og uddelegerer derefter rettigheder til de enkelte medarbejdere, hvis der foreligger et arbejdsbetinget behov. Vi har stikprøvevis inspiceret projekter og observeret, at der er etableret funktionsadskillelse.	Ingen afvigelser konstateret.
5.4 Ledelsens ansvar ▶ Ledelsen sikrer, at alle medarbejdere og relevante leverandører er orienteret, og opretholder serviceleverandørens krav til informationssikkerhed	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren halvårligt udsender en awareness test om informationssikkerhedspolitikken, som alle medarbejdere skal gennemføre. Vi har yderligere inspiceret, at information om opdateret sikkerhedspolitik er kommunikeret til medarbejderne.	Ingen afvigelser konstateret.
5.9 Fortegnelse over information og understøttende aktiver ▶ Serviceleverandøren har en fortegnelse over aktiver, der anvendes til udførelse af serviceleverandørens aktiviteter, (dette inkluderer ansattes udstyr). ▶ Anvendte aktiver er tildelt en ejer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har en fortegnelse for aktiver og en fortegnelse for servere og observeret, at alle aktiver er tildelt en ejer. Vi har inspiceret serviceleverandørens notifikationer ift. opdatering af fortegnelse.	Ingen afvigelser konstateret.

5.15 Administration af adgange ▶ Serviceleverandøren har udarbejdet en procedure for adgangsstyring, som styrer registreringer og afmeldinger af brugeradgange. ▶ Serviceleverandøren har kun givet medarbejdere adgang til netværk og netværkstjenester, som de er autoriseret til at anvende.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret serviceleverandørens procedure for adgangsstyring, hvor det fremgår, at medarbejdere hos serviceleverandøren ikke får tildelt adgange, før de er tildelt et team og at de bliver fjernet ved fratrædelser. Vi har stikprøvevis inspiceret at tildeling af adgange, og observeret, at medarbejder kun får rettigheder som er arbejdsbetinget i henhold til proceduren. Vi har stikprøvevis inspiceret afmeldinger af adgange, og observeret, at ved afmeldinger bliver der frataget adgange i henhold til proceduren. Vi har inspiceret procedure for onbording af medarbejdere og observeret, at medarbejderne hos serviceleverandøren får adgang til netværket igennem en MDM-løsning. Vi har yderligere inspiceret, at serviceleverandøren kan fjerne medarbejdernes adgang til det interne netværk. Vi har stikprøvevis inspiceret, at serviceleverandøren under onboarding tilmelder nye enheder til MDM-løsningen.	Ingen afvigelser konstateret.
5.16 Styring af identifikation ▶ Serviceleverandøren har opstillet en procedure for registrering og afmelding af bruger i forbindelse med tildeling af adgangsrettigheder.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi er ved forespørgsel blevet informeret om, at der er tre adgangstyper til systemet. Vi har foretaget inspektion af serviceleverandørens udarbejdet procedure for adgangstyper til følgende systemer. • Interne systemer	Ingen afvigelser konstateret.

	• Kundesystemer • Servere og kodebaser Vi har inspiceret stikprøvevis at serviceleverandør på tildeling af rettigheder følger deres procedure. Vi har inspiceret serviceleverandørs lister over administrative rettigheder og observeret at det kun er medarbejdere med arbejdsbetinget behov som har adgang til at tildele rettigheder.	
5.17 Autentifikationsoplysninger ▶ Serviceleverandøren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. ▶ Serviceleverandøren har opstillet systemer til administration af adgangskoder, og disse er aktive.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for adgangsstyring og observeret, at der opstillet krav ift. adgangskoder, kompleksitet og MFA. Vi har inspiceret, at serviceleverandøren har opstillet systemer til administration af adgangskoder. Vi har inspiceret password politikken på alle serviceleverandørens systemer, herunder at der på nogle services kræves MFA.	Ingen afvigelser konstateret.
5.18 Adgangsrettigheder ▶ Serviceleverandøren har opstillet en procedure for adgangsstyring af tildeling og tilbagekald af adgangsrettigheder. ▶ Serviceleverandøren foretager periodisk gennemgang af brugeres adgangsrettigheder. ▶ Serviceleverandøren inddrager og tilpasser adgangsrettigheder, når medarbejdere fratræder eller aftaler ophører.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret procedure for adgangsstyring og observeret, at der heri er anført, at ledelsen har ansvaret for tildeling og tilbagekald af adgangsrettigheder. Vi har inspiceret, at ledelsen foretager en periodisk gennemgang af brugernes adgangsrettigheder en gang pr. kvartal. Vi har inspiceret procedure for on- og offboarding og stikprøvevis observeret, at serviceleverandøren rettidigt har nedlagt fratrådte brugeres adgang.	Ingen afvigelser konstateret.

5.19 Informationssikkerhedspolitik i leverandørforhold ▶ Serviceleverandøren har fastsat informationssikkerhedskrav til anvendte underleverandører. ▶ Serviceleverandøren har begrænset underleverandørers adgang til serviceleverandørens systemer i forhold til underleverandørens arbejdsbetingede behov.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for anvendelse af underleverandører. Vi er ved forespørgsel blevet informeret om, at underleverandører ikke har adgang til hverken data eller systemer. Underleverandører foretager kun hosting. Vi har inspiceret adgangsforholdene til serverne og har observeret at det kun er ansatte hos serviceleverandøren, som har adgang.	Ingen afvigelser konstateret.
A.5.20 Håndtering af informationssikkerhed i leverandørforhold ▶ Informationssikkerhedskrav er aftalt med relevante underleverandører.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandøraftalerne indgået med underserviceleverandører, og kan se at serviceleverandøren har indgået informationssikkerhedskrav i forbindelse med aftalen med de relevante underleverandører.	Ingen afvigelser konstateret.
5.22 Overvågning, vurdering og ændringsstyring i leverandørydelser ▶ Serviceleverandøren udfører tilsyn, herunder indhenter og gennemgår underserviceleverandørens revisorerklæringer, certificeringer og lignende. ▶ Serviceleverandøren tager stilling til eventuelle ændringer af leverandørydelser.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret at serviceleverandøren har indhentet passende SOC1 rapporter og ISO 27001 certificeringer fra deres underserviceleverandørens og udført tilsyn af dem. Vi har inspiceret serviceleverandørens aftaler indgået med underleverandører og observeret, at der er ændringer til leverandørydelser. Vi har hertil observeret at serviceleverandøren har indhentet SOC 2 rapport og udført tilsyn med den nye underleverandør.	Ingen afvigelser konstateret.

	Vi har ydermere inspiceret et bridge letter udgivet fra Amazon ift. Kontrolområder forinden deres næste erklæring udgives i november 2024.	
5.23 Informationssikkerhed ved brug af cloud-tjenester ▶ Serviceleverandøren har processer for anskaffelse, brug, styring og afslutning af brugen af cloud-tjenester i overensstemmelse med organisationens informationssikkerhedskrav.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for leverandørforhold som en del af styring af brug for cloud tjenester. Vi har inspiceret at der har været ændringer i leverandørydelser indenfor erklæringsperioden, mhp. cloud-tjenester. Vi har hertil observeret at brugen af den nye cloud-tjeneste, er i overensstemmelse med serviceleverandørens informationssikkerhedskrav. Vi har inspiceret dokumentation for risikovurdering og informationssikkerhed på cloud tjenester.	Ingen afvigelser konstateret.
5.24 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents ▶ Der er fastlagt ledelsesansvar og roller i forbindelse med brud på informationssikkerheden. ▶ Serviceleverandøren har implementeret en procedure for håndtering af brud på informationssikkerheden.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for styring af informationssikkerhedsbrud og observeret, at der heri er anført, at det overordnede ansvar for håndtering af informationssikkerhedsbrud ligger hos ledelsen, herunder at alle ansatte er forpligtet til at informere ledelsen, hvis der er mistanke om brud på informationssikkerheden. Vi har inspiceret, at alle ansatte hos serviceleverandøren skal læse informationssikkerhedspolitikken 1-2 gange årligt. Vi er ved forespørgsel blevet informeret om, at der ikke har været nogle brud i nyere tid, hvorfor vi ikke kunne teste om proceduren efterleves.	Vi har konstateret, at der er etableret en procedure ved brud på informationssikkerheden. Der har dog ikke været hændelser i erklæringsperioden. Vi kan derfor ikke udtale os om kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

5.37 Dokumenterede driftsprocedurer ▶ Driftsprocedurer er udarbejdet og gjort tilgængelige for relevante ansatte.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en driftsprocedure, som er tilgængelig for alle relevante ansatte.	Ingen afvigelser konstateret.

A.6 Personrelaterede foranstaltninger

Kontrolmål

- *At sikre, at alle medarbejdere er egnet til de roller, som de er i betragtning til, og forbliver egnede under deres ansættelse.*
- *At sikre, at medarbejdere og relevante interessenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At sikre informationssikkerheden, når medarbejdere arbejder på afstand.*
- *At understøtte rettidig, konsistent og effektiv indrapportering af informationssikkerhedshændelser, som kan identificeres af medarbejdere.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.6.1 Screening ▶ Serviceleverandøren gennemlæser ansøgning og cv på potentielle medarbejdere før ansættelse.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for ansættelse. Vi er ved forespørgsel blevet informeret om, at vurdering foretages med udgangspunkt i ansøgning og CV og ud fra en vurdering af ansøgers relevante kompetencer, indkaldes den potentielle medarbejder til samtale.	Ingen afvigelser konstateret.
A.6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed ▶ Serviceleverandøren afholder awareness-træning ved ansættelse af nye medarbejdere i henhold til informationssikkerhed. ▶ Der afholdes introduktionskursus for nye medarbejdere om informationssikkerhed. ▶ Serviceleverandøren foretager løbende awareness-træning af medarbejdere i henhold til informationssikkerhed samt håndteringen heraf.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret onboarding præsentationen, som alle nye medarbejdere skal igennem og observeret, at nye medarbejdere gennemgår informationssikkerhedspolitikken efterfulgt af test i informationssikkerhed. Vi har inspiceret, at alle medarbejdere er blevet testet i informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
A.6.7 Distancearbejde (fjernarbejde) ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren.	Ingen afvigelser konstateret.

▶ Fjernadgang til serviceleverandørens systemer og data sker via en krypteret VPN-forbindelse. ▶ Fjernadgang skal foregå via to-faktor autentifikation.	Vi er ved forespørgsel blevet informeret om, at serviceleverandøren anvender Bitdefender. Vi har observeret Bitdefenders dashboard overvåger alle aktiver hos serviceleverandøren. Vi har stikprøvevis inspiceret, at Bitdefender er installeret på arbejdsstationer. Vi har inspiceret, at serviceleverandøren har installeret en VPN, som er begrænset til medarbejdere hos serviceleverandøren. Vi har inspiceret konfigurationer for serviceleverandørens VPN-løsning, herunder at der anvendes to-faktor autentifikation.	
A.6.8 Indrapportering af informationssikkerhedshændelser ▶ Serviceleverandøren rapporterer om informationssikkerhedshændelser til relevante parter. ▶ Serviceleverandøren rapporterer om informationssikkerhedssvagheder til relevante parter.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en business continuity plan, hvis en informationssikkerhedshændelse skulle finde sted. Vi har inspiceret, at serviceleverandøren har udført en skrivebordstest af business continuity planen i erklæringsperioden. Vi er ved forespørgsel blevet informeret om, at serviceleverandøren ikke har registreret nogle hændelser i erklæringsperioden, hvorfor vi ikke har kunne teste om relevante parter informeres.	Vi har konstateret, at der er etableret en procedure for indrapportering af hændelser. Der har ikke været grund til at indrapportere hændelser i erklæringsperioden. Vi kan derfor ikke udtale os om kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

A.7 Fysiske foranstaltninger

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til, beskadigelse og forstyrrelse af organisationens information og understøttende aktiver.*
- *At sikre, at der kun sker autoriseret fysisk adgang til organisationens information og understøttende aktiver.*
- *At forebygge eller reducere konsekvenserne af hændelser, der opstår på grund af fysiske og miljømæssige trusler.*
- *At reducere risici fra fysiske og miljømæssige trusler og fra uautoriseret adgang og beskadigelse.*
- *At undgå tab, beskadigelse eller kompromittering af information og understøttende aktiver eller driftsforstyrrelser i organisationen som følge af fejl og afbrydelse af understøttende forsyninger.*
- *At undgå tab, beskadigelse, tyveri eller kompromittering af information og understøttende aktiver samt driftsforstyrrelser i organisationen grundet manglende vedligeholdelse.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
7.1 Fysisk områdesikring ▸ Der er etableret fysisk områdesikring til at beskytte områder, der indeholder følsomme og kritiske informationer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for fysisk sikring og miljøsikring. Vi har inspiceret underserviceleverandørernes SOC1 rapporter og ISO 27001 certificeringer og observeret, at der ikke er observationer vedrørende fysisk områdesikring.	Ingen afvigelser konstateret.
7.2 Fysisk adgangskontrol ▸ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til serviceleverandørens kontorer og faciliteter, herunder sikring af, at kun autoriserede personer har adgang. ▸ Alle adgange registreres og logges. ▸ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til serviceleverandørens kontorer og faciliteter.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for fysisk sikring og miljøsikring. Vi har inspiceret, at alle ansatte hos serviceleverandøren har en personlig kode for adgang til serviceleverandørens kontor. Vi har observeret at døren til lokalerne bliver registreret og logget. Vi er ved forespørgsel blevet informeret om at serviceleverandør gennemgår alle ansattes adgange og nye adgangskoder halvårligt. Vi har stikprøvevis inspiceret, at fratrådte medarbejderes personlige kode rettidigt deaktiveres.	Ingen afvigelser konstateret.

7.5 Beskyttelse mod fysiske og miljømæssige trusler ▶ Serviceleverandøren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret underserviceleverandørernes SOC1 rapporter og ISO 27001 certificeringer og observeret, at der ikke er observationer vedrørende fysiske og miljømæssige trusler.	Ingen afvigelser konstateret.
7.8 Placering og beskyttelse af udstyr ▶ Serviceleverandøren har sikret, at udstyr er placeret i sikre lokaler for at beskytte mod uautoriserede adgange og miljømæssige trusler.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for fysisk sikring og miljøsikring. Vi har observeret, at medarbejderne benytter sig af serviceleverandørens skabe til opbevaring af computere udenfor arbejdstid. Vi har inspiceret underserviceleverandørernes SOC1 rapporter og ISO 27001 certificeringer og observeret, at der ikke er observationer vedrørende placering og beskyttelse af udstyr.	Ingen afvigelser konstateret.
7.11 Forsyningssikkerhed ▶ Udstyr er beskyttet mod strømsvigt og andre forstyrrelser. ▶ Kabler, der bærer data eller understøtter telekommunikation, er beskyttet.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren fører tilsyn med deres underserviceleverandør. Vi har inspiceret, at der ikke har været nogle afvigelser for underserviceleverandøren.	Ingen afvigelser konstateret.
7.13 Vedligeholdelse af udstyr ▶ Vedligeholdelse af udstyr følger en vedligeholdelsesplan, og udføres kun af autoriseret personale.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren har udarbejdet en procedure for vedligeholdelse af udstyr. Vi har yderligere inspiceret, at når udstyr ikke kan sikkerhedsopdateres eller ikke er funktionel, så vil udstyret blive destrueret.	Vi har konstateret, at der er etableret en procedure for bortskaffelse af udstyr. Der har dog ikke været destrueret forældet hardware i erklæringsperioden. Vi kan derfor ikke udtale os om kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

	Vi er ved forespørgsel blevet informeret om, at der ikke har været nogle destruerede medier i nyere tid, hvorfor vi ikke har kunne teste at proceduren følges.	

A.8 Teknologiske foranstaltninger

Kontrolmål

- *At sikre, at kun autoriserede brugere, softwarekomponenter og -tjenester har privilegerede adgangsrettigheder.*
- *At sikre udelukkende autoriseret adgang og forhindre uautoriseret adgang til information og understøttende aktiver.*
- *At forhindre uautoriseret funktionalitet, undgå utilsigtede eller skadelige ændringer og opretholde fortroligheden af værdifuld intellektuel ejendom.*
- *At sikre, at en bruger eller en entitet autentificeres på sikker vis, når der gives adgang til systemer, applikationer og tjenester.*
- *At sikre, at information og understøttende aktiver beskyttes mod malware.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At sikre, at hardware, software, tjenester og netværk fungerer korrekt med de krævede sikkerhedsindstillinger og at der ikke laves om på konfigurering ved uautoriserede eller ukorrekte ændringer.*
- *At muliggøre retablering efter tab af data eller systemer.*
- *At optegne hændelser, generere bevismateriale, sikre loginformationens integritet, forhindre uautoriseret adgang, identificere informationssikkerhedshændelser, der kan føre til informationssikkerhedsincident og understøtte undersøgelser.*
- *At sørge for sikkerhed i brugen af netværkstjenester.*
- *At inddele netværket med sikkerhedsafgrænsninger og styre trafikken mellem dem ud fra forretningsmæssige behov.*
- *At validere, om informationssikkerhedskravene er opfyldt, når applikationer eller kode implementeres i produktionsmiljøet.*
- *At beskytte produktionsmiljøet og data mod kompromittering som følge af udviklings- og testaktiviteter.*
- *At bevare informationssikkerheden ved udførelse af ændringer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
8.2 Privilegerede adgangsrettigheder ▶ Privilegerede (administrative) adgangsrettigheder til software, systemer og enheder tildeles ud fra et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at alle privilegerede adgangsrettigheder til serviceleverandøren, stemmer overens med deres arbejdsbetingede behov.	Ingen afvigelser konstateret.
8.3 Begrænset adgang til informationer ▶ Serviceleverandøren har begrænset medarbejderes og kunders adgang til informationer jf. henholdsvis arbejdsbetinget behov og gældende kontrakt med kunden.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret proceduren for styring af adgang til aktiver hos serviceleverandøren og har observeret, at alle ansatte kun har adgang til begrænset information. Vi er ved forespørgsel blevet informeret om, at kunder ikke har adgang til serviceleverandørens informationer.	Ingen afvigelser konstateret.

8.4 Adgang til kildekode ▶ Adgang til kildekode er begrænset til relevante brugere.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at det kun er ledelsen hos serviceleverandøren, som kan give adgang til kildekode, og at der er en procedure for at give adgang. Vi har stikprøvevis inspiceret ansattes adgange og observeret, at det kun tildeles hvis der er arbejdsbetinget behov.	Ingen afvigelser konstateret.
8.5 Sikker autentifikation ▶ Serviceleverandøren har etableret logisk adgangskontrol til systemer med informationer, herunder to-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret alle serviceleverandørens logiske adgangskontroller og observeret, at de er implementeret.	Ingen afvigelser konstateret.
8.7 Beskyttelse mod malware ▶ Der er implementeret kontroller til detektering, forhindring og gendannelse kombineret med passende brugerbevidsthed for at beskytte mod malware.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret proceduren for detektering, forhindring og gendannelse er passende implementeret.	Ingen afvigelser konstateret.
8.8 Styring af tekniske sårbarheder ▶ Serviceleverandøren indhenter informationer om tekniske sårbarheder. ▶ Serviceleverandøren har taget stilling til identificerede sårbarheder.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at serviceleverandøren aktivt indhenter informationer om tekniske sårbarheder. Vi har inspiceret, at serviceleverandøren tager stilling til de identificerede sårbarheder, og at kunder med kritiske sårbarheder bliver kontaktet. Vi har stikprøvevis inspiceret, at serviceleverandøren håndterer sårbarheder, som er identificeret med sikkerhedsværktøjer.	Ingen afvigelser konstateret.

8.9 Konfigurationsstyring ▶ Serviceleverandøren sørger for, at hardware, software, tjenester og netværk fungerer korrekt i forhold til sikkerhedsindstillinger, som de har prædefineret, samt sørger for, at disse konfigurationer ikke kan ændres.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspicere procedure for opsætning af server hos serviceleverandør.	Ingen afvigelser konstateret.
8.13 Backup af information ▶ Der foretages dagligt backup af systemer og data. ▶ Opbevaring af backup er outsourcet til underleverandøren. ▶ Der udføres mindst restore-tests 1 gange årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret at backup-politikken hos serviceleverandøren er implementeret. Vi er ved forespørgsel informeret om, at backup af kundedata afhænger af aftalen med kunden. Vi har for en stikprøve observeret sammenhæng mellem backup og aftale. Vi har inspiceret, at serviceleverandøren har outsourcet deres backups til en underleverandør men, at de selv styrer backupkonfigurationer igennem en backup manager. Vi har inspiceret, at restore af backup testes årligt.	Ingen afvigelser konstateret.
8.15 Logning ▶ Alle succesfulde og mislykkede adgangsforsøg til systemleverandørens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Serviceleverandøren har begrænset, hvem der kan få adgang til logdata.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at logning af succesfulde og mislykkede adgangsforsøg finder sted på serviceleverandørens systemer. Vi har inspiceret, at der logges på ændringer på serviceleverandørens systemer og databaser. Vi har inspiceret administration til logning og observeret, at det kun er de tekniske ejere eller ledelsen, som kan tilgå logs. Vi har stikprøvevis inspiceret at serviceleverandøren fører passende logs på deres servere.	Ingen afvigelser konstateret.

8.18 Brug af privilegerede understøttende systemprogrammer ▶ Kun autoriserede medarbejdere kan anvende systemprogrammer, der kan omgå system- og applikationskontroller.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret oversigt over adgange til serverne og observeret, at det kun er tekniske ejer, som har adgang til at kunne omgå system- og applikationskontroller.	Ingen afvigelser konstateret.
8.19 Softwareinstallationer i test- og produktionssystemer ▶ Serviceleverandøren har implementeret procedurer for softwareinstallation.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret proceduren for softwareinstallation og observeret, at der heri er anført, at det kun er de tekniske ejere, som må installere software. Vi har stikprøvevis inspiceret, at serviceleverandøren følger deres procedure for installation af software på nye servere.	Ingen afvigelser konstateret.
8.20 Netværkssikkerhed ▶ Netværkstopologien er struktureret således at servere, som driver applikationer, ikke kan tilgås direkte fra internettet. ▶ Serviceleverandøren anvender kendte netværksteknologier og mekanismer (Firewall/Intrusion Detection System/Intrusion Prevention System) for at beskytte serviceleverandørens interne netværk.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at netværkssikkerhed bliver på serviceleverandørens, serverer og observeret, at det er opsat så serverne kun kan tilgås sikkert igennem de tvungne regler. Vi har inspiceret at serviceleverandøren har opsat kendte netværksteknologier i form af firewall og Intrusion Detection Systems. Vi har stikprøvevis inspiceret alarmer genereret af serviceleverandørens IDS system og observeret, at serviceleverandøren løbende håndterer relevante sikkerhedsalarmer.	Ingen afvigelser konstateret.
8.21 Sikring af netværkstjenester ▶ Serviceleverandøren har implementeret/stillet krav til passende sikkerhedsforanstaltninger til beskyttelse af dens netværkstjenester.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren.	Ingen afvigelser konstateret.

	Vi har inspiceret serviceleverandørens procedure for netværkssikkerhed og observeret, at der er opstillet firewall regler og Intrusion Detection Systems som følger proceduren.	
8.22 Segmentering af netværk ▶ Serviceleverandørens netværk er segmenteret, så interne servere ikke kommunikerer direkte med internettet.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret netværk segmenteringen samt firewall regler og observeret, at man ikke kan tilgå server direkte fra nettet.	Ingen afvigelser konstateret.
8.29 Sikkerhedstest under udvikling og godkendelse ▶ Informationssikkerhedskrav og krav til behandling af informationer inddrages i en tidlig vurdering af projekter/systemer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret serviceleverandørens procedure for sikring af kildekodede. Vi har stikprøvevis inspiceret, at proceduren er fulgt.	Ingen afvigelser konstateret.
8.31 Adskillelse af udviklings-, test- og produktionsmiljøer ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Ændringer af funktionalitet testes, inden det sættes i drift. ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekoder. ▶ Udviklings- og testmiljøer er adskilte.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har observeret at funktionsadskillelse er til stedet hos serviceleverandøren mellem udvikling og drift. Vi har inspiceret processen af funktionsadskillelse og observeret at ændringer testes før drift. Vi har inspiceret at udvikling og test er adskilt fra produktion. Vi har observeret at versionsstyring er implementeret og at ændringer bliver registreret. Vi har observeret at udvikling og test er adskilte miljøer.	Ingen afvigelser konstateret.

8.32 Ændringsstyring ▶ Serviceleverandøren har oprettet procedurer for ændringsstyring. ▶ Serviceleverandøren foretager passende test af nye systemer og systemændringer. ▶ Serviceleverandøren har opstillet regler for begrænsninger af softwareinstallationer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret at serviceleverandøren har implementeret procedure for ændringsstyring og observeret, at alle ændringer sker igennem den tekniske ejer af systemet. Vi er på forespørgsel blevet oplyst af serviceleverandør, at der ikke har været test af nye systemer og systemændringer i nyere tid.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-12-20 14:32:52 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2024-12-20 14:53:54 UTC

Troels Johannesen
CEO, Ejer
Serienummer: 647e137c-c5f1-4422-929e-d919dbc26b99
IP: 87.63.xxx.xxx
2024-12-22 16:25:30 UTC