Revisorerklæring

Perspektiva IT ApS

ISAE 3402 type 2 erklæring om generelle it-kontroller for perioden
18. april 2023 til 30. april 2024 relateret til leverance af Hosting Services

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

August 2024

Indholdsfortegnelse

Sektion 1:	Perspektiva IT ApS' udtalelse	1
Sektion 2:	Uafhængig revisors erklæring om beskrivelsen af kontroller, deres design og operationelle effektivitet	3
Sektion 3:	Beskrivelse af Perspektiva IT ApS' ydelser i forbindelse med leverance af Hosting Services samt generelle it-kontroller relateret hertil	5
Sektion 4:	Kontrolmål, udførte kontroller, test og resultater heraf	12

Sektion 1: Perspektiva IT ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Perspektiva IT ApS' leverance af Hosting 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, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

Perspektiva IT ApS anvender underleverandørerne Penta Infra ApS og Microsoft. Denne erklæring er udarbejdet efter partielmetoden, og Perspektiva IT ApS' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Penta Infra ApS og Microsoft. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Perspektiva IT ApS' beskrivelse i Sektion 3 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er passende designet og er operationelt effektive sammen med kontrollerne hos Perspektiva IT ApS. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

Perspektiva IT ApS bekræfter, at:

(a) Den medfølgende beskrivelse i Sektion 3, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Perspektiva IT ApS' leverance af Hosting Services der har behandlet kunders transaktioner i perioden fra 18. april 2023 til 30. april 2024. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været designet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret.
- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål og kontroller designet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes design har forudsat ville være implementerede af brugervirksomheder, 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 og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

(ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget i perioden fra 18. april 2023 til 30. april 2024.

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

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i perioden fra 18. april 2023 til 30. april 2024, hvis relevante kontroller hos underleverandører var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af Perspektiva IT ApS kontroller i hele perioden fra 18. april 2023 til 30. april 2024. Kriterierne for denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 18. april 2023 til 30. april 2024.

Holbæk, den 30. august 2024
Perspektiva IT ApS

Martin Krogh Nielsen
Adm. direktør

Sektion 2: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres design og operationelle effektivitet

Til Perspektiva IT ApS, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om Perspektiva IT ApS' beskrivelse i Sektion 3 af generelle it-kontroller for drift af brugersystemer til behandling af Perspektiva IT ApS' leverance af Hosting Services i perioden og om design og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Perspektiva IT ApS anvender underleverandørerne Penta Infra ApS og Microsoft. Denne erklæring er udarbejdet efter partielmetoden, og Perspektiva IT ApS' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Penta Infra ApS og Microsoft. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af Perspektiva IT ApS´ kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos Perspektiva IT ApS.

Enkelte af de kontrolmål, der er anført i Perspektiva IT ApS' beskrivelse i Sektion 3 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne (eller den specifikke kunde) er hensigtsmæssigt designet og operationelt effektive sammen med kontrollerne hos Perspektiva IT ApS. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

Perspektiva IT ApS' ansvar

Perspektiva IT ApS er ansvarlig for udarbejdelsen af beskrivelsen i Sektion 3 og tilhørende udtalelse i Sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for designet og implementeringen af operationelt effektive kontroller for at nå de anførte kontrolmål.

Grant Thorntons 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.

Grant Thornton 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 Perspektiva IT ApS' beskrivelse (Sektion 3) og om designet og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning.

Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes design og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er

operationelt effektive. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået.

En erklæringsopgave med sikkerhed af denne type omfatter desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet Perspektiva IT ApS' udtalelse i Sektion 1.

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

Perspektiva IT ApS' beskrivelse i Sektion 3 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 de generelle it-kontroller, 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 afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Perspektiva IT ApS' udtalelse i Sektion 1. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var designet og implementeret i perioden 18. april 2023 til 30. april 2024, i alle væsentlige henseender er retvisende

(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden fra 18. april 2023 til 30. april 2024, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, og hvis kunderne har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Perspektiva IT ApS' kontroller i perioden fra 18. april 2023 til 30. april 2024

(c) De testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har været operationelt effektive i perioden 18. april 2023 til 30. april 2024

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i den efterfølgende Sektion 4 om kontrolmål, udførte kontroller, test og resultater heraf.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i Sektion 4 er udelukkende tiltænkt kunder, der har anvendt Perspektiva IT ApS' leverance af Hosting Services, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 30. august 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Andreas Moos
Director, CISA, CISM

Sektion 3: Beskrivelse af Perspektiva IT ApS' ydelser i forbindelse med leverance af Hosting Services samt generelle it-kontroller relateret hertil

Beskrivelse af Perspektiva IT's ydelser der er omfattet af erklæringen

I det følgende beskrives Perspektiva IT ApS' ydelser til kunder, som er omfattet af de generelle it-kontroller, som erklæringen omhandler. Erklæringen omfatter generelle processer og systemopsætninger m.v. hos Perspektiva IT. Processer og systemopsætninger m.v., der er individuelt aftalt med Perspektiva IT's kunder er ikke omfattet af erklæringen. Vurdering af eventuelle kundespecifikke processer og systemopsætninger m.v. vil fremgå af specifikke erklæringer til kunder, der har bestilt sådanne.

Perspektiva IT er en moderne og innovativ virksomhed, grundlagt i 1996, og beskæftiger mere end 20 medarbejdere. Hovedkontoret er placeret i Holbæk. Perspektiva IT tilbyder en række IT-support og driftsydelser som driftes i HostingCenter. Hostingcenteret er lokaliseret i Glostrup hos virksomheden Penta Infra som driver en række datacentre i Europa. Perspektiva IT driver ikke selve omgivelserne (strøm/nødstrøm, fysisk sikring mv.) men udelukkende den hardware og software som udgør selve hosting ydelsen.

Perspektiva IT servicerer kunder i hele Danmark og tilbyder ligeledes support til kundernes udenlandske afdelinger.

Målsætningen for Perspektiva IT er at være kundernes foretrukne IT-outsourcing leverandør. Det med udgangspunkt i det egenudviklede SAFE koncept – (**S**ikkerhed, **A**nsvar, **F**remtid, **E**ffektivitet).

Perspektiva IT håndterer kundernes support og IT-drift så kundernes medarbejdere altid kan arbejde sikkert og effektivt, hvilket sikrer at kunderne kan fokusere på deres kerneforretning. Perspektiva IT leverer løsninger med høj fleksibilitet, som kan skræddersyes til kunders behov og krav.

Generelle it-kontroller hos Perspektiva IT

I det følgende beskrives de generelle it-kontroller relateret til Perspektiva IT ApS' ydelser til kunder.

Risikostyring

Perspektiva IT ApS' har udarbejdet faste procedurer for risikovurdering af forretningen og hostingcenteret. Dette er med henblik på at sikre, at alle risici er minimeret til et acceptabelt niveau, så Perspektiva IT ApS' kan opretholde en normal drift i tilfælde af risici indtræffer. Der gennemføres periodisk evaluering af risikoanalysen samt en årlig gennemgang med efterfølgende godkendelse af ledelsen. Med udgangspunkt i risikovurderingen og ISO 27002:2013, har Perspektiva IT ApS' udvalgt hovedområder og kontrolmål for styring af it-sikkerheden, der er nærmere beskrevet i det følgende:

Organisering af it-sikkerheden

Organiseringen af it-sikkerheden sker med udgangspunkt i Perspektiva IT ApS' IT-sikkerhedspolitik og tager udgangspunkt i ISO 27001/2:2013, som indeholder følgende hovedområder:

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

Tilrettelæggelsen af it-sikkerheden indenfor de enkelte områder er beskrevet nedenfor.

Informationssikkerhedspolitikker

Den udarbejdede IT-sikkerhedspolitik sikrer, at alle medarbejdere er indforstået med de fastlagte krav og rammer for IT-sikkerhed i Perspektiva IT, samt at disse overholdes. Der gennemføres minimum en årlig revidering af IT-sikkerhedspolitikken. IT-sikkerhedspolitikken tager udgangspunkt i, at Perspektiva IT ønsker at være en stærk samarbejdspartner inden for IT-løsninger samt sikrer levering af en stabil og sikker IT-drift

Perspektiva IT's it-sikkerhed er baseret på:

- Almindeligt accepterede metoder og politikker for informationssikkerhed.
- Alle relevante regler, lovkrav, retningslinjer, vejledninger og kontrakter
- En ledelsesgodkendt it-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse, og kommunikeret ud til alle medarbejdere i virksomheden.

Procedurer og kontroller
Perspektiva IT afdækker relevante it-risici på driftsydelserne. Dette varetages gennem en løbende trussels- og risikovurdering hos Perspektiva IT i forbindelse med en årlig revurdering af risikoanalysen.

Resultatet af den årlige gennemgang forlægges for ledelsen. Perspektiva IT stiller desuden en række informationer til rådighed for drift-kundernes revisorer, til brug for deres vurdering af Perspektiva IT som driftsleverandør.

Udførsel af kontrollen
It-sikkerhedspolitikken revurderes mindst en gang årligt forinden udførelse af it-revisionen og udarbejdelse af erklæring.

Den årlige gennemgang udføres af IT sikkerhedsgruppen:

- Direktør Martin Krogh Nielsen.
- IT Sikkerhedschef Claus Daugaard Hansen
- IT Driftschef Peter Korva Hertz

Kontrol dokumentation
Der er versionsstyring af it-sikkerhedspolitikken

Organisering af informationssikkerhed

Perspektiva IT har en standard procedure for oprettelse og ansættelse af nye medarbejdere. Der er tilsvarende udarbejdet faste kontroller, som sikrer at proceduren bliver overholdt samt at organisationsdiagrammet (Accountability Chart) bliver løbende opdateret i forbindelse med ændringer i medarbejderstaben.

Intern organisering

IT-sikkerhedsudvalg
Gennem vidensdeling og efteruddannelse sikrer Perspektiva IT ApS at alle medarbejdere efterlever den rolle, som er tiltænkt dem, samt at alle procedurer fra IT-sikkerhedspolitikken bliver overholdt. Det sikrer, at sikkerhedsrelaterede forhold bliver eskaleret og håndteres jf. IT-sikkerhedspolitikken. Dette er nødvendigt, da det er Perspektiva IT ApS' vigtigste opgave at beskytte kunders data og organisationsudstyr, hvilket dermed også beskytter forretningen. Strategien bliver årligt evalueret, ligesom den fremtidige strategi bliver defineret, så Perspektiva IT ApS fortsætter med at udvikle forretningen og styrker markedspositionen.

Mobilt udstyr og fjernarbejdspladser

I IT-sikkerhedspolitikken er der udarbejdet et reglement for brug af mobilt udstyr og fjernarbejdspladser, som alle medarbejdere skal overholde. Dette reglement bliver gennemgået for alle nye medarbejdere i forbindelse med ansættelse hos Perspektiva IT ApS'.

Det er udelukkende tilladt at benytte krypterede og sikkerhedsgodkendte enheder. 2 faktor godkendelse skal aktiveres på samtlige tjenester, hvor det er muligt.

Personalesikkerhed

Medarbejdersikkerhed stiller krav om tiltag til at reducere risikoen for menneskelige fejl samt misbrug og lignende. Der er udarbejdet en fast procedure for medarbejdersikkerhed før, under, og efter ansættelse i Perspektiva IT.

Før ansættelsen
Der er en fast procedure for behandling af ansøgningerne, som sikrer at alt udleveret dokumentation fra ansøger bliver behandlet i henhold til lovningen. Ansættelsesvilkår, -betingelser samt vilkår for ansættelse er beskrevet i ansættelseskontrakten hos den enkelte medarbejder. Samtidig udleveres og gennemgås IT-sikkerhedspolitikken ved en af de første arbejdsdage. Det er medarbejderens ansvar at holde sig opdateret på ændringer i IT-sikkerhedspolitikken. Ændringer adviseres af ledelsen.

Under ansættelsen
Alle medarbejderdata bliver opbevaret under hele ansættelsesperioden på et netværksdrev, som har opsat begrænset adgang. Der foreligger en fast procedure for at sikre alle medarbejderoplysninger bliver indsamlet og opbevaret korrekt.

Ledelsesansvar
Hver medarbejder har en direkte leder, som sørger for at medarbejderens opgaver og systemadgange er tilsvarende medarbejderens kompetencer og ansættelsesgrundlag. Ligeledes har den nærmeste leder ansvaret for medarbejderens trivsel og at medarbejderen får den nødvendige information i dagligdagen.

Bevidsthed om, uddannelse og træning i informationssikkerhed
Der foreligger en fast procedure for uddannelse og træning i informationssikkerhed. Dertil bliver alle medarbejdere løbende underrettet og opdateret inden for emnet.

Styring af aktiver

Informationssikkerhedspolitikken omfatter alle aktiver, som understøtter Perspektiva IT ApS' forretningsområder og organisation. Disse omfatter data, systemer, fysiske aktiver samt tekniske forsyninger, der understøtter it-anvendelsen. Al udleveret udstyr bliver dokumenteret, så der er styr på hvilket udstyr den enkelte medarbejder har fået udleveret. Der er opsat overvågning på udleveret udstyr, således der kan udføres kontroller, som sikrer at IT-sikkerhedspolitikken bliver overholdt. Der er en fast procedure i forbindelse med udlevering af koder og adgangskort til Perspektiva IT ApS' hovedkontor samt datacenter.

Fortegnelse over aktiver
Ledelsen har adgang til en fortegnelse over udleverede aktiver til den enkelte medarbejder

Ejerskab over aktiver
Ledelsen har adgang til en liste for ejerskab af aktiver.

Accepteret brug af aktiver
Retningslinjerne for accepteret brug af aktiver står beskrevet i IT-Sikkerhedspolitikken.

Adgangsstyring

Adgangsstyring stiller krav til sikring af adgang til systemer og data. Systemer og data, herunder teknisk basisprogrammel, er sikret mod uberettiget eller utilsigtet adgang. Tildelingen af adgangsrettigheder m.v. sker ud fra et arbejdsbetinget behov og under hensyntagen til en effektiv funktionsadskillelse.

Adgangsstyring bliver håndteret via Perspektiva IT ApS domæne, som sikrer at alle medarbejdere overholder IT-sikkerhedspolitikken i forhold til adgangskode til domænet. Desuden registreres medarbejdernes log-in såvel lokalt som på fjernadgang.

Politik for adgangsstyring
Der er en fast procedure for adgangsstyring jf. IT-sikkerhedspolitikken. Denne procedure bliver revurderet løbende samt i forbindelse med ændringer i medarbejderstaben

Administration af brugeradgange
Der er udarbejdet en fast procedure til adgangsstyring. Hvis der er et ønske om udvidet adgang skal dette godkendes af den nærmeste leder. Det er et begrænset antal medarbejdere, som har adgang til tildeling af rettigheder.

Tildeling af brugeradgang
Tildeling af brugeradgang til Perspektiva IT ApS' systemer godkendes af ledelsen. Der er et begrænset antal medarbejdere, som kan tildele adgange.

Styring af privilegerede adgangsrettigheder
Privilegerede adgangsrettigheder godkendes af ledelsen og tildeles medarbejdere på system niveau således adgangen begrænses til netop medarbejderens arbejdsbehov.

Styring af hemmelig autentifikationsinformation om brugere
Perspektiva IT ApS' IT-sikkerhedspolitik foreskriver, at medarbejdernes kodeord er personlige og ikke må deles med andre.

Gennemgang af brugernes adgangsrettigheder
Perspektiva IT ApS gennemfører periodisk opfølgning på tildelte rettigheder og den fortsatte relevans, så risikoen for misbrug eller fejl minimeres, og så retningslinjer og lovgivning (jf. fx databeskyttelsesforordningen) efterleves.

Inddragelse eller justering af adgangsrettigheder
Brugerens adgangsrettigheder revideres løbende og justeres eller inddrages hvis nødvendigt.

Brug af hemmelig autentifikationsinformation
Perspektiva IT ApS' IT-sikkerhedspolitik foreskriver, at medarbejdernes kodeord er personlige og ikke må deles med andre. Der er opsat en GPO, som sikrer at de foreskrevne retningslinjer overholdes.

Fysisk sikring og miljøsikring

Fysisk sikkerhed og miljøsikring omfatter krav og sikkerhedsforanstaltninger til beskyttelse af bygninger, forsyninger og tekniske installationer, der er relevante for Perspektiva IT ApS'.

Der skelnes i dette kapitel mellem Perspektiva IT ApS' lokaler på Højvang 5, 4300 Holbæk og lokalerne hos hosting underleverandøren Penta Infra, Smedeland 32, 2600 Glostrup.

For Penta Infra henvises der generelt til Erklæring ISAE3402, som udarbejdes årligt af Penta Infra.

Fysisk adgangskontrol
Hovedkontoret har tyverialarm som skal afkobles inden indgang og hoveddøren åbnes direkte til kontorlokalet så ingen kan entrere uden det bemærkes.

Adgang til hosting center har kun autoriseret personale. Disse skal udover nøglebrik samt personlig kode også iris scannes inden adgang til hosting centeret.

Driftssikkerhed

Styring af drift omfatter krav til stabilitet, overvågning og sikkerhed i forbindelse med afvikling af it-produktion. Der er etableret dokumentation af driftsprocesser, driftsafvikling, udstyr og systemer i tilstrækkeligt omfang til, at det muliggør en effektiv driftsafvikling samt en hurtig og effektiv afhjælpning af eventuelle driftsproblemer.

Der kører dagligt en scanning på PC-enhederne, som er tilknyttet medarbejdere i Perspektiva IT. Scanningen producerer en liste med software som er installeret på enhederne. Listen gennemgås for uautoriserede programmer med faste intervaller.

Dokumenterede driftsprocedurer
Der foreligger faste driftsprocedurer for hostingcenteret. Alle ændringer er dokumenteret og godkendt af IT Driftschef. Derudover er der overvågning på alt essentielt udstyr i hosting og der sendes en alarm, hvis der skulle forekomme uønskede hændelser.

Ændringsstyring
Perspektiva IT følger principperne for ændringsstyring i ITIL. Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.

Der skal indhentes godkendelse fra drift chefen, før ændringen gennemføres. Systemdokumentation skal opdateres ved hver ændring. Forældet systemdokumentation skal arkiveres eller destrueres.

Kapacitetsstyring
IT-systemernes belastning og dimensionering overvåges løbende for at sikre, at nødvendig kapacitet er til rådighed. Belastningen og kapaciteten overvåges således, at opgradering og tilpasning kan planlægges samt finde sted løbende.

Kontroller mod malware
Perspektiva IT ApS' opfatter malware som en af de største trusler mod forretningen. Derfor opretholdes strenge kontroller omkring installation af anti-malware systemer på enheder samt daglig overvågning og alarmering ved detekterede sikkerhedshændelser. Der er etableret en avanceret perimeter sikring med intelligente firewall enheder som automatisk henter informationer om nye sårbarheder og blokerer disse. Perspektiva IT ApS' har udarbejdet procedure omkring håndtering af malware udbrud.

Backup
Der foretages backup med frekvenser på timebasis, dagligt, ugentlig, månedligt og årligt afhængig af behov. Backup foretages lokalt samt til anden lokation og arkiveres i en sky baseret tjeneste.

Backup testes og verificeres ved restore tests med jævne mellemrum. Genopretningsplan ved systemfejl, datakorruption eller malware angreb er etableret og afprøves årligt. For kunder med specifikke krav til backuppolitik aftales og designes denne individuelt.

Backup overvåges af Perspektiva IT's support og hændelser håndteres og fejl udbedres.

Logning og overvågning

Hændelseslogning
Logs er så vidt muligt personhenførbare således at Perspektiva IT ApS' sikrer, at det altid kan spores hvilken medarbejder, som har tilgået kritisk udstyr og systemer. For særligt kritiske systemer logges også ændringer til konfigurationer. Der foretages løbende en kontrol af hændelseslogning.

Beskyttelse af logoplysninger
Logoplysninger er låst og kan ikke redigeres.

Administrator- og operatørlogs
Logning af administrator adgange sker i forbindelse med den almindelige logning.

Softwareinstallation på driftssystemer
Patching af operativsystemer sker automatiseret i forud definerede service vinduer. Der patches hver måned. Alle kritiske og sikkerheds- opdateringer bliver installeret inden 2 måneder fra de bliver frigivet.

3. parts programmer (Java, Adobe Reader etc.) opdateres i samme interval såfremt der foreligger nye versioner med sikkerheds rettelser.

Sårbarhedsstyring

Styring af tekniske sårbarheder
Perspektiva IT ApS' ledelse godkender idriftsættelsen af nye it-systemer, nye versioner og opdateringer af eksisterende it-systemer, samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

Der abonneres på sikkerheds e-mails med adviseringer omkring sårbarheder. Disse kan resultere i straks opdateringer i form af ekstra ordinære servicevinduer.

Leverandørforhold

Omfatter informationssikkerhedskravene til at styre risici forbundet med leverandører og outsourcingspartnere.

Der er indgået en aftale med alle leverandører, som bliver revideret hvis der forekommer større ændringer hos enten leverandøren eller Perspektiva IT ApS'.

Overvågning og gennemgang af leverandørydelser
Der rekvireres årligt en revisor erklæring fra alle Perspektiva IT ApS' leverandører, som leverer en driftskritisk ydelse for Perspektiva IT ApS'.

Styring af ændringer af leverandørydelser
Hvis der sker ændringer i Perspektiva IT ApS' politikker eller procedurer, vurderes det om der er sket ændringer i leverandørforholdet, som skal tilføjes til risikovurderingen. På samme måde foregår det, hvis leverandørerne ændrer i deres politikker, procedurer og ydelser

Styring af informationssikkerhedsbrud

Information security incident management omfatter krav til kontroller, der skal sikre overblik over indtrufne it-sikkerhedshændelser samt en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

Ansvar og procedurer
Ansvaret omkring sikkerhedsbrud er entydigt defineret i IT-Sikkerhedspolitikken og gælder for alle typer sikkerhedsbrud. Det er ledelsens ansvar at sikre udarbejdelsen af nødvendige procedurer og få disse implementeret på tilfredsstillende vis. Procedurerne indeholder nødvendige foranstaltning og processer, som skal udføres eller tages i anvendelse ifm. et evt. sikkerhedsbrud.

Rapportering af informationssikkerhedshændelser
Rapportering af hændelser følger af retningslinjer i IT-Sikkerhedspolitikken analogt til GDPR-hændelser.

Som udgangspunkt er det den enkelte medarbejder i virksomheden, der i første omgang har pligt til at reagere på en hændelse, og dermed sikre den videre rapportering til den risikoansvarlige.

Rapportering af informationssikkerhedssvagheder
Medarbejdere og eksterne samarbejdspartnere er forpligtet til at anmelde sikkerhedshændelser til nærmeste leder jf. de indgåede kontrakter, aftaler samt IT-sikkerhedspolitikken. Det skal sikre, at der kan reageres hurtigst muligt på eventuelle hændelser.

Vurdering af og beslutning om informationssikkerhedshændelser
Det er i risikogruppen at evt. sikkerhedshændelser vurderes og evalueres og evt. klassificeres som et sikkerhedsbrud. Vurdering af evt. hændelser sker ved indsamling af relevant information inden eller samtidigt med afhjælpning af fejl/risiko.

Håndtering af informationssikkerhedsbrud
Medarbejdere er instrueret i, at der umiddelbart i forbindelse med evt. hændelser eller incidents generelt er en skærpet opmærksomhed på sikring samt logføring af forløbet. Således sikres grundlag for en efterfølgende analyse og sikring af udbedring efter en hændelse. Ledelsen skal altid informeres. Ved større hændelser aktiveres Perspektiva IT ApS' beredskabsplan.

Erfaring fra informationssikkerhedsbrud

Ved incidents- eller sikkerhedshændelser evalueres efterfølgende på forløbet. De grundlæggende logs fra forløbet anvendes til sikring af mulige forbedringer eller skærpelse af sikkerheden, så fremtidige lignende sikkerhedshændelser kan minimeres.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Omfatter krav til beredskabsstyring, herunder udarbejdelse og test af beredskabsplaner.

Planlægning af informationssikkerhedskontinuitet
Der er udarbejdet en IT-beredskabsplan i tilfælde af sikkerhedsbrud. Alle involverede parter er informeret om deres rolle, hvis der skulle forekomme en hændelse som kræver at beredskabsplanen aktiveres. Beredskabsplanen godkendes af ledelsen og testes årligt.

Implementering af informationssikkerhedskontinuitet
Beredskabsplanen er udleveret til de medarbejdere, som indgår i IT-beredskabet, så de involverede medarbejdere altid har IT-beredskabsplanen til rådighed.

Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten
Der foretages årlig skrivebordstest af IT-beredskabsplanen, som verificeres, gennemgås og evalueres.

Redundans

Tilgængelighed af informationsbehandlingsfaciliteter
Der er overvågning og redundans på alt driftskritisk udstyr i hostingcenteret.

Komplementerende kontroller

Perspektiva IT ApS' kunder er, medmindre andet er aftalt, ansvarlige for:

- rettidigt at håndtere anmodninger om brugeroprettelser og bruger nedlæggelser.
- at der foretages periodisk gennemgang af kundens egne brugere.
- at der opretholdes sporbarhed i tredjeparts software som kunden selv administrerer
- at udstyr, som ikke er en driftsaftale på med Perspektiva IT ApS, bliver opdateret.
- at have en fungerende og tilstrækkelig internetforbindelse samt evt. opsætning og test af alternative internetforbindelser, hvis den primære internetforbindelse skulle fejle.
- at ajourføre liste over sammenhæng mellem brugerkonti og ansatte/maskiner.
- at udarbejde en beredskabsplan til håndtering af egen virksomhed i tilfælde af større uheld eller katastrofer

Sektion 4: Kontrolmål, udførte kontroller, test og resultater heraf

Formål og omfang

Beskrivelse og resultat af vores tests af kontroller fremgår af efterfølgende skema. I det omfang vi ved vores test har konstateret afvigelser i design, implementering eller operationel effektivitet af de testede kontroller, har vi anført disse under resultat af test.

Denne erklæring er udarbejdet efter partielmetoden og Perspektiva IT ApS' kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos Perspektiva IT ApS' underleverandør Penta Infra ApS og Microsoft.

Kontroller, som er specifikke for de enkelte kundeløsninger, eller som er udført af Perspektiva IT ApS' kunder, er ikke omfattet af vores erklæring.

Udførte test

Metoder anvendt til test af kontrollers funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Perspektiva IT ApS. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af kontrollens udførelse.
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 operationelt effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover foretages der stikprøvevis test af kontrollernes operationelle effektivitet i revisionsperioden.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Resultater af test

I nedenstående oversigt har vi opsummeret tests udført af Grant Thornton som grundlag for vurdering af de generelle it-kontroller hos Perspektiva IT ApS.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed
Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	*Perspektiva IT ApS' kontrol*	*Grant Thorntons test*	*Resultat af test*
5.1.1	*Politikker for informationssikkerhed* Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.	Vi har inspiceret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter. Vi har inspiceret, at informationssikkerhedspolitikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.
5.1.2	*Gennemgang af politikker for informationssikkerhed* Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken. Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

A.6.2 Mobilt udstyr og fjernarbejdspladser
Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	Perspektiva IT ApS' kontrol	Grant Thorntons test	Resultat af test
6.2.1	*Politik for mobilt udstyr* Der er etableret en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.	Vi har inspiceret politik for mobilt udstyr. Vi har inspiceret, at relevante medarbejdere er blevet informeret omkring politikken for mobilt udstyr. Vi har inspiceret, at der er defineret tekniske kontroller til sikring af mobilt udstyr.	Ingen afvigelser konstateret.
6.2.2	*Fjernarbejdspladser* Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.	Vi har inspiceret politik for sikring af fjernarbejdspladser. Vi har inspiceret underliggende sikkerhedsforanstaltninger til beskyttelse af fjernarbejdspladser.	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen
Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

Nr.	Perspektiva IT ApS' kontrol	Grant Thorntons test	Resultat af test
7.1.1	*Screening* Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse se med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.	Vi har inspiceret procedure for screening af nye medarbejdere. Vi har stikprøvevis inspiceret dokumentation for at der bliver indhentet screeningsdokumentation på nye medarbejdere i perioden.	Ingen afvigelser konstateret.

A.7.1 Før ansættelsen Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.			
7.1.2	*Ansættelsesvilkår og -betingelser* Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har inspiceret procedure for ansættelse af nye medarbejdere. Vi har stikprøvevis inspiceret dokumentation for at nye medarbejdere er blevet orienteret omkring deres roller samt ansvar ved informationssikkerhed.	Ingen afvigelser konstateret.

A.7.2 Under ansættelsen Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
7.2.1	*Ledelsesansvar* Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har inspiceret informationssikkerhedspolitikken vedrørende fastsættelse af krav til medarbejdere og kontrahenter. Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde informationssikkerhedspolitikken i ansættelseskontrakterne med medarbejderne.	Ingen afvigelser konstateret.
7.2.2	*Bevidsthed om, uddannelse og træning i informationssikkerhed* Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter vil ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, idet omfang det er relevant for deres jobfunktion.	Vi har inspiceret procedurer til sikring af tilstrækkelig uddannelse og træning i informationssikkerhed (awarenesstræning). Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejderne.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

A.8.1 Ansvar for aktiver
Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	*Perspektiva IT ApS' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.1.1	*Fortegnelse over aktiver* Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Vi har inspiceret fortegnelser over aktiver.	Ingen afvigelser konstateret.
8.1.2	*Ejerskab af aktiver* Der udpeges en ejer i organisationen for hvert aktiv.	Vi har inspiceret oversigt over ejerskab til aktiver.	Ingen afvigelser konstateret.
8.1.3	*Accepteret brug af aktiver* Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, dokumenteres og implementeres.	Vi har inspiceret reglerne for accepteret brug af aktiver.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

A.9.1 Forretningsmæssige krav til adgangsstyring
Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	*Perspektiva IT ApS' kontrol*	*Grant Thorntons test*	*Resultat af test*
9.1.1	*Politik for adgangsstyring* En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.	Vi har inspiceret politikken for adgangsstyring. Vi har inspiceret at politikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.

A.9.2 Administration af brugeradgang Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
9.2.1	*Brugerregistrering-og afmelding* Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling og afmelding af adgangsrettigheder.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgangsrettigheder. Vi har stikprøvevis inspiceret, at brugernes adgangsrettigheder er godkendt. Vi har inspiceret, at fratrådte brugeres adgangsrettigheder er nedlagt.	Ingen afvigelser konstateret.
9.2.2	*Tildeling af brugeradgang* Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har stikprøvevis inspiceret, at tildelte brugeradgange er blevet tildelt efter proceduren for adgangsstyring og kontrol. Vi har forespurgt om der har været brugere der har skiftet funktion i perioden.	Ingen afvigelser konstateret.
9.2.3	*Styring af privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder. Vi har inspiceret et udtræk af privilegerede brugere og forespurgt om adgangsrettigheder er tildelt baseret på et arbejdsbetinget behov. Vi har inspiceret at privilegerede brugeradgange er personhenførbare. Vi har inspiceret, at der periodisk foretages gennemgang af privilegerede adgangsrettigheder.	Ingen afvigelser konstateret.
9.2.4	*Styring af hemmelig autentifikationsinformation om brugere* Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces.	Vi har inspiceret proceduren vedrørende tildeling af passwords til platforme. Vi har inspiceret dokumentation for at password politikken er implementeret i anvendte systemer til styring af hemmelig autentifikationsinformation om brugere.	Ingen afvigelser konstateret.

Nr.	Perspektiva IT ApS' kontrol	Grant Thorntons test	Resultat af test
9.2.5	*Gennemgang af brugeradgangsrettigheder* Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har inspiceret procedure for regelmæssig gennemgang og evaluering af adgangsrettigheder. Vi har inspiceret, at der foretages gennemgang og evaluering af adgangsrettigheder to gange årligt.	Ingen afvigelser konstateret.
9.2.6	*Inddragelse eller justering af adgangsrettigheder* Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Vi har inspiceret procedurerne for inddragelse og justering af adgangsrettigheder. Vi har stikprøvevis inspiceret at fratrådte medarbejdere har fået deres adgangsrettigheder inddraget rettidigt.	Ingen afvigelser konstateret.

A.9.3 Brugernes ansvar Kontrolmål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.			
Nr.	**Perspektiva IT ApS' kontrol**	**Grant Thorntons test**	**Resultat af test**
9.3.1	*Brug af hemmelig autentifikationsinformation* Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.	Vi har inspiceret retningslinjer for brug af fortrolige passwords. Vi har inspiceret, at den implementerede passwordpolitik følger fastlagte retningslinjer.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

A.11.1 Sikre områder
Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	*Perspektiva IT ApS' kontrol*	*Grant Thorntons test*	*Resultat af test*
11.1.2	*Fysisk adgangskontrol* Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har inspiceret adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til kontoret. Vi har inspiceret at der er opsat alarmsystemer til fysisk adgangskontrol.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

A.12.1 Driftsprocedurer og ansvarsområder
Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	*Perspektiva IT ApS' kontrol*	*Grant Thorntons test*	*Resultat af test*
12.1.1	*Dokumenterede driftsprocedurer* Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem.	Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret og vedligeholdt. Vi har inspiceret, at driftsdokumentation er opdateret og tilgængelig for medarbejdere, som har behov for dem.	Ingen afvigelser konstateret.
12.1.2	*Ændringsstyring* Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret proceduren vedrørende ændringer til informationsbehandlingsudstyr og – systemer. Vi har stikprøvevis inspiceret dokumentation for at implementerede ændringer er håndteret i overensstemmelse med proceduren herfor.	Ingen afvigelser konstateret.
12.1.3	*Kapacitetsstyring* Anvendelsen af ressourcer overvåges og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.	Vi har inspiceret proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav. Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring.	Ingen afvigelser konstateret.

A 12.2 Malwarebeskyttelse Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.2.1	*Kontroller mod malware* Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har inspiceret retningslinjer for kontroller mod malware. Vi har inspiceret, at der er implementeret kontroller mod malware.	Ingen afvigelser konstateret.

A.12.3 Backup Kontrolmål: At beskytte mod tab af data.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.3.1	*Backup af information* Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har inspiceret dokumentation for at proceduren for backup er gennemgået og opdateret i perioden. Vi har stikprøvevis inspiceret, at der tages daglig backup jf. proceduren. Vi har inspiceret dokumentation for at der er udført en restoretest.	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning Kontrolmål: At registrere hændelser og tilvejebringe bevis.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.4.1	*Hændelseslogning* Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Vi har forespurgt til logning af brugeraktivitet. Vi har inspiceret at logningskonfigurationerne indeholder brugeraktivitet, undtagelser, fejl og hændelser.	Ingen afvigelser konstateret.

12.4.2	*Beskyttelse af log-oplysninger* Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har forespurgt til procedurer for sikring af logoplysninger. Vi har inspiceret at logningsinformationer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	*Administrator- og operatørlog* Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt.	Vi har inspiceret procedurer vedrørende logning af aktiviteter udført af systemadministratorer og -operatører. Vi har stikprøvevis inspiceret at systemadministratorers og -operatørers handlinger logges på servere og databasesystemer.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware Kontrolmål: At sikre integriteten af driftssystemer.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.5.1	*Softwareinstallation på driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret proceduren for patching og opgradering af systemer og at den er gennemgået og opdateret i perioden. Vi har inspiceret dokumentation for at relevante systemer er opdateret og patchet efter bestemte krav i proceduren herfor.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.6.1	*Styring af tekniske sårbarheder* Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder. Vi har stikprøvevis inspiceret at servere, databasesystemer og netværkskomponenter er patchet rettidigt.	Ingen afvigelser konstateret.

A.15 Leverandørforhold

15.2 Styring af leverandørydelser
Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

Nr.	Perspektiva IT ApS' kontrol	Grant Thorntons test	Resultat af test
15.2.1	*Overvågning og gennemgang af leverandørydelser* Leverandørydelser overvåges og gennemgås.	Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører i perioden.	Ingen afvigelser konstateret.
15.2.2	*Styring af ændringer af leverandørydelser* Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, - procedurer og -kontroller, styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, - systemer og -processer er, og til en revurdering af risici.	Vi har forespurgt til styring af ændringer hos leverandører og inspiceret dokumentation for håndteringen.	Vi er blevet oplyst, at der ikke har været væsentlige ændringer til leverandørydelser i perioden. Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

A.16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	Perspektiva IT ApS' kontrol	Grant Thorntons test	Resultat af test
16.1.1	*Ansvar og procedurer* Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har inspiceret proceduren for håndtering af sikkerhedshændelser og -brud.	Ingen afvigelser konstateret.

A.16.1 Styring af informationssikkerhedsbrud og forbedringer Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.			
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret retningslinjer for rapportering af informationssikkerhedshændelser. Vi har stikprøvevis inspiceret, at informationssikkerhedshændelser er rapporteret ad passende ledelseskanaler.	Ingen afvigelser konstateret.
16.1.3	*Rapportering af informationssikkerhedssvagheder* Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester.	Vi har inspiceret retningslinjer for rapportering af informationssikkerhedssvagheder. Vi har stikprøvevis inspiceret, at medarbejdere har rapporteret svagheder eller mistanke om svagheder i informationssystemer og -tjenester.	Ingen afvigelser konstateret.
16.1.4	*Vurdering af og beslutning om informations- sikkerhedshændelser* Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	Vi har inspiceret procedure for vurdering af informationssikkerhedshændelser. Vi har stikprøvevis inspiceret, at informationssikkerhedshændelser har været håndteret i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
16.1.5	*Håndtering af informationssikkerhedsbrud* Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer.	Vi har inspiceret proceduren for håndtering af informationssikkerhedsbrud. Vi har forespurgt om der har været informationssikkerhedsbrud i perioden.	Ingen afvigelser konstateret.
16.1.6	*Erfaring fra informationssikkerhedsbrud* Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.	Vi har forespurgt til hvordan erfaringer fra informationssikkerhedsbrud håndteres. Vi har stikprøvevis inspiceret, at erfaringer fra informationssikkerhedsbrud bliver håndteret.	Ingen afvigelser konstateret.

A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

A.17.1 Informationssikkerhedskontinuitet
Kontrolmål: At sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Nr.	*Perspektiva IT ApS' kontrol*	*Grant Thorntons test*	*Resultat af test*
17.1.1	*Planlægning af informationssikkerhedskontinuitet* Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.	Vi har inspiceret at beredskabsplanen er godkendt af ledelsen. Vi har inspiceret at beredskabsplanen er udarbejdet ud fra en risikovurdering.	Ingen afvigelser konstateret.
17.1.2	*Implementering af informationssikkerhedskontinuitet* Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.	Vi har inspiceret at beredskabsplanen vedligeholdes og opdateres efter behov. Vi har inspiceret dokumentation for at beredskabsplanen er tilgængelig for relevante medarbejdere.	Ingen afvigelser konstateret.
17.1.3	*Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten* Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har inspiceret dokumentation for at der er udført tests af beredskabsplanens risikoområder i perioden.	Ingen afvigelser konstateret.

A.17.2 Redundans Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.			
Nr.	***Perspektiva IT ApS' kontrol***	***Grant Thorntons test***	***Resultat af test***
17.2.1	*Tilgængelighed af informationsbehandlingsfaciliteter* Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	Vi har inspiceret etablering af redundans til sikring af tilgængelighed af driftssystemer.	Ingen afvigelser konstateret.

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."

Martin Krogh Nielsen
PERSPEKTIVA IT ApS CVR: 29616892
Underskriver 1
Serienummer: 52370409-3370-406c-aa92-a6135aaa42da
IP: 5.103.xxx.xxx
2024-08-30 06:43:05 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2024-08-30 06:44:42 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serienummer: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 213.83.xxx.xxx
2024-08-30 06:45:47 UTC