BEIERHOLM
VI SKABER BALANCE

JANUAR 2025

ECIT SOLUTIONS A/S

ISAE 3402 TYPE 2 ERKLÆRING

CVR 28843151

Uafhængig revisors erklæring om kontrolmiljøet for it-driften i tilknytning til hostingaktiviteter.

Herudover er der angivet et afsnit i beskrivelsen vedrørende rollen som databehandler i henhold til Databeskyttelsesforordningen.

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

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af kontrolmiljøet for it-driften i tilknytning til hostingaktiviteter.

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

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

KAPITEL 1:

Ledelseserklæring

ECIT Solutions A/S behandler personoplysninger på vegne af de dataansvarlige i henhold til databehandleraftaler vedrørende it-driften i tilknytning til hostingaktiviteter.

Medfølgende beskrivelse er udarbejdet til brug for kunder og deres revisorer, der har anvendt hostingaktiviteter fra ECIT Solutions A/S, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne dvs. de dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt databeskyttelsesforordningen er overholdt.

ECIT Solutions A/S bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2 (inkl. bilag 1), giver en retvisende beskrivelse af kontrolmiljøet for it-driften i tilknytning til hostingaktiviteter i hele perioden 1. januar 2024 - 31. december 2024. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
- De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette eller begrænse behandling af personoplysninger
- De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med kunden dvs. den dataansvarlige
- De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
- De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
- De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede
- De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
- Kontroller, som vi med henvisning til hostingaktiviteternes afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de anvendte forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

(ii) Indeholder relevante oplysninger om ændringer vedrørende it-driften for ECIT Solutions A/S' hostingaktiviteter foretaget i hele perioden 1. januar 2024 - 31. december 2024.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller 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 kontroller, som den enkelte kunde måtte anse som vigtigt efter deres særlige forhold.

(B) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. januar 2024 - 31. december 2024. Kriterierne for dette udsagn er, 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 forhindrer 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 hele perioden 1. januar 2024 - 31. december 2024.

(C) Der er etableret og opretholdt passende tekniske og organisatoriske sikringsforanstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen.

(D) Den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2 (inkl. bilag 1), er udarbejdet med baggrund i overholdelse af ECIT Solutions A/S' standardaftale samt tilhørende databehandleraftale. Kriterierne for dette grundlag var:

(i) Informationssikkerhedspolitik for ECIT Solutions
(ii) IT-sikkerhedsregler/ håndbog for ECIT Solutions (rammen efter ISO 27002)

Viby J, den 8. januar 2025

Kim Bahir Andersen, Managing Director **Rolf Ljungberg, Director of Operations**
ECIT Solutions A/S, Rudolfgårdsvej 1B, DK-8260 Viby J, CVR 28843151

KAPITEL 2:

Beskrivelse af kontrolmiljøet for it-driften i tilknytning til hostingaktiviteter

Indledning

Formålet med nærværende beskrivelse er at levere information til ECIT Solutions A/S' kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Omfanget af denne beskrivelse er en afdækning af de tekniske og organisatoriske sikkerhedsforanstaltninger, som er implementeret i forbindelse med it-driften af hosting-aktiviteter.

Som supplement til nedenstående beskrivelse er der tilføjet et selvstændigt afsnit (Overensstemmelse med rollen som databehandler) med beskrivelse af centrale krav i forbindelse med rollen som databehandler, kombineret med generelle krav fra databehandleraftaler.

Beskrivelse af ECIT Solutions A/S

ECIT Solutions blev etableret i 1996 af tidligere administrerende direktør Mikkel Walde. I dag beskæftiger virksomheden over 70 medarbejdere.

ECIT Solutions primære ydelse er serverhosting, hvilket leveres til et bredt udvalg af større og mindre virksomheder. Alle ydelser er baseret på de leverancer, der udgår fra eget datacenter. Datacenteret blev bygget i 2017 - og er skabt på baggrund af den nyeste viden inden for datacenterteknologi og IT-sikkerhed.

Med egne servere, transformerstation og generatorer fysisk placeret i eget datacenter - og fuldt ejerskab over alle kunde-dedikerede forbindelser ud af huset - har ECIT Solutions således fuld kontrol over alle dele af serviceleverancen. Det betyder, at løsninger altid kan skræddersyes til den enkelte kundes behov. Der tilbydes ydelser helt fra web- og maildrift op til komplekse løsninger af forretningskritisk IT for virksomheder, der kræver oppetid året rundt.

Til hver enkelt kunde sammensættes den mest optimale kombination af virtuelle og fysiske servere, for at tilbyde den bedst mulige service. Det er også muligt at tilføje en lokal server hos kunderne til spejling af data.

Datacenteret er sikret efter bedste evne på baggrund af den nyeste teknologi inden for elektronisk adgangskontrol, videoovervågning, temperaturalarmer, røg/brandsensorer, klimastyring og UPS.

Datacenteret er modulært opbygget således der løbende kan tilføjes ekstra servere, CPU'er eller storagekapacitet, alt afhængigt af behov, hvilket sikrer kunderne en fleksibel og funktionel leverance.

ECIT Solutions har mere end 25 års erfaring med IT-drift for primært små og mellemstore virksomheder.

Da alle leverancer udgår direkte fra ECIT Solutions, sættes der stor fokus på at holde hver enkelt medarbejder opdateret og specialiseret indenfor deres eget arbejdsområde. Der lægges også vægt på det mere generelle niveau, så hver enkelt medarbejder kan bistå kunder såvel som kollegaer efter bedste evne. Det gør, at kunden i større grad oplever, at der ikke er behov for kontakt med hele virksomheden, og at de i stedet kan kommunikere med den samme medarbejder, som har en bedre indsigt i den unikke problemstilling.

ECIT Solutions har som mission at sikre sine kunder et højt niveau af tryghed og driftsstabilitet for hele deres IT-infrastruktur. For at opnå dette benyttes et redundant setup, hvilket gør, at der kan tilbydes maksimal oppetid, sikker backup, dynamiske diske samt agile servere. De virksomheder, der har valgt

ECIT Solutions som IT-partner, kan derfor fokusere på deres kerneydelse, uden at skulle bekymre sig om deres IT-drift.

Hos ECIT Solutions beskæftiger vi os udelukkende med IT-drift/hosting for virksomheder og organisationer, og vores kundereferencer er opbygget igennem mange år med langvarige og dedikerede kundeforløb.

ECIT Solutions er AAA-rated, hvilket sikrer vores kunder, at vi som IT-leverandør har en sund økonomi. Vi har desuden over en længere periode arbejdet målrettet med IT-sikkerhed og EU's databeskyttelsesforordning.

Omfang for denne beskrivelse

ECIT Solutions A/S er leverandør af services inden for IT, hvoraf kerneaktiviteten er professionel leverance af hosting- og driftsydelser. Overvågning og support er fleksibel, idet dette kan foregå på kunders egne platforme placeret i vores datacenter - eller på løsninger, der afvikles på vores infrastruktur, som kunder lejer sig ind på.

ECIT Solutions har ansvaret for at etablere og opretholde passende procedurer og kontroller med henblik på at finde og forebygge fejl, for således at overholde de i aftalerne stillede krav. Det er netop vores kerneaktivitet - hosting og driftsydelser samt vedligeholdelse - der danner grundlag for denne beskrivelse.

Forretningsstrategi/ IT-sikkerhedsstrategi

Et af de strategiske mål for os i ECIT Solutions er at indbygge de nødvendige sikkerhedsmæssige implementeringer i vores forretning, så selskabet ikke påføres uacceptable risici til ulempe for hverken os selv eller vores kunder.

ECIT Solutions har tre overordnede strategiske pejlemærker:

- Hos ECIT Solutions bestræber vi os på at holde os opdaterede inden for den nyeste viden for moderne informationsteknologi. Dette sker med henblik på at kunne udøve den bedst mulige service, og dermed hjælpe og vejlede vores kunder.
- Hos ECIT Solutions er vores primære fokus at opbygge, administrere og vejlede i drift og vedligeholdelse af blandt andet IT-systemer, netværksløsninger og cloud-løsninger.
- ECIT Solutions har som arbejdsplads fokus på medarbejdertrivsel. Dette gøres blandt andet ved at prioritere muligheder for yderligere uddannelse og specialisering af den enkelte medarbejder. Ved kontinuerligt at give medarbejderne mulighed for at dygtiggøre sig, sikres der et kontinuerligt højt niveau inden for hver medarbejders respektive område.

ECIT Solutions ønsker at være kundernes uvildige og rådgivende partner inden for IT-sikkerhed, hvilket er hvorfor IT-sikkerhed prioriteres på et forretningsstrategisk højt niveau.

Der arbejdes løbende med at sikre det høje service- og kvalitetsniveau inden for området. Ledelsen prioriterer gennem selskabets IT-sikkerhedspolitik, at IT-sikkerhed fortsat skal være en vigtig del af selskabets arbejdskultur.

ECIT Solutions har omkring IT-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27001+2:2017, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

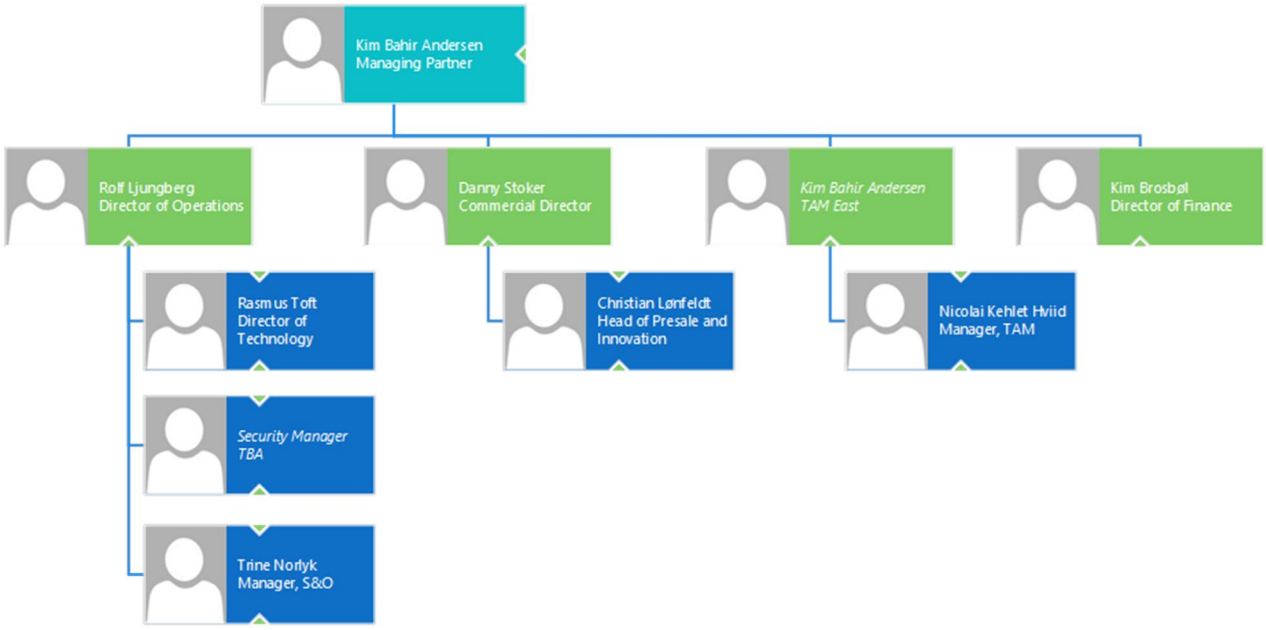
- Informationssikkerhedspolitik
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Leverandørforhold
- Styring af informationssikkerhed
- Informationssikkerhedsaspekter ved nød-, beredskabs– og reetableringsstyring
- Overensstemmelse med lov- og kontraktkrav

De implementerede kontrolmål og sikringsforanstaltninger hos ECIT Solutions A/S fremgår af bilag 1 til denne beskrivelse.

ECIT Solutions A/S' organisation og organisering af IT-sikkerheden

For ECIT Solutions ligger det overordnede ansvar hos CEO Danny Stoker. Organisationsansvaret er uddelegeret til COO Rolf Ljungberg, og ansvaret for IT-sikkerhed er uddelegeret til Security Manager Nikolaj Olssen.

Ved brug af eksterne samarbejdspartnere udarbejdes samarbejdsaftale, inden arbejde påbegyndes.



Figur 1 - Organisationsdiagram

Risikostyring i ECIT Solutions A/S

Det er ECIT Solutions' politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift. ECIT Solutions gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres hvert år to risiko- og trusselsvurderinger.

ECIT Solutions har indarbejdet faste procedurer for risikovurdering af forretningskritiske processer og datacenterdrift. Der sikres dermed, at de risici, som er forbundet med de services, der stilles til rådighed, er minimerede til et acceptabelt niveau. Risikovurderingerne foretages periodisk, samt når der ændres i eksisterende systemer eller implementeres nye systemer.

Ansvaret for risikovurderingen ligger hos COO og skal efterfølgende forankres og godkendes hos virksomhedens øvrige ledelse.

Som led i ovenstående IT-sikkerhedsstrategi arbejder ECIT Solutions med de danske og internationale standarder for it-sikkerhed – ISO27001+2:2017 – som primær referenceramme for IT-sikkerheden. Arbejdsprocessen omkring IT-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at ECIT Solutions til enhver tid er i overensstemmelse med de lovpligtige krav.

Håndtering af IT-sikkerhed

Det daglige ansvar for IT-sikkerheden ved ECIT Solutions ligger hos Security Manager. Gennem den centrale IT-sikkerhedspolitik har ledelsen beskrevet ECIT Solutions' struktur for IT-sikkerhed. IT-sikkerhedspolitikken skal som minimum revideres én gang årligt.

ECIT Solutions' kvalitetsstyringssystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker IT-drift til samtlige kunder. Til at sikre dette er det nødvendigt, at der er indført politikker og procedurer til at sikre, at samtlige services og leverancer er af samme ensartede og gennemsigtige kvalitet.

ECIT Solutions' IT-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved en eventuel fejl eller sikkerhedsbrist i driftsmiljøet udbedres det hurtigst muligt afhængigt af kritikaliteten.

IT-sikkerhedsudvalgets behandling af rapporterede informationssikkerhedshændelser indbefatter såvel en kommunikationsplan, en vurdering af om hændelsen kan ske andre steder samt en videregivelse af erfaringer til relevante medarbejdere.

Alle servere og netværksenheder er dokumenteret i ECIT Solutions' dokumentationssystem. Her logges alle ændringer af systemerne. Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) er ligeledes dokumenteret i systemet.

Sikkerhedspolitikken sætter de grundlæggende politikker for ECIT Solutions' infrastruktur. Politikken omfatter ikke forhold vedrørende specifikke produkter, ydelser eller brugere.

Sikkerhedspolitikken er udarbejdet, så ECIT Solutions har ét fælles overordnet regelsæt. Dermed opnåes et stabilt driftsmiljø og et højt sikkerhedsniveau. Der foretages løbende forbedringer af både politikker, procedurer og den operationelle drift.

Kontroller og sikringsforanstaltninger

I det følgende behandler vi:

- HR, medarbejdere og uddannelse
- Styring af aktiver
- Brugerstyring/ adgangssikkerhed
- Fysisk sikkerhed og miljøsikring
- Malwarebeskyttelse
- Backup
- Logning og overvågning
- Patch management / ændringshåndtering
- Cyberkriminalitet
- Styring af it-sikkerhedshændelser
- Leverandørforhold
- Beredskabsstyring
- Overensstemmelse med rollen som databehandler

HR, medarbejdere og uddannelse

ECIT Solutions har opnået Gold Partner for drift af **Datacenter** & **Cloud Platform** og **SMV Cloud Solutions** hos Microsoft.

Alle udførende konsulenter har kompetencer inden for de områder, de beskæftiger sig med. Det dokumenteres ved hjælp af relevante certificeringer fra teknologiudbyderne. ECIT Solutions er som nævnt certificeret Microsoft partner, og kravene til at opretholde denne status er høje.

ECIT Solutions skal leve op til en række krav fra Microsoft, herunder specifikke krav om at et bestemt antal konsulenter har bestået bestemte produktcertificeringer, som løbende skal fornyes. ECIT Solutions sikrer via løbende produkttræning og kursusdeltagelse at opretholde denne høje certificeringsstatus.

Styring af aktiver

ECIT Solutions styrer aktiver ved hjælp af defineret ejerskab og beskrevne arbejdsgange for accepteret brug af aktiver.

- Data klassificeres jævnfør procedurer for tildeling af sikkerhedsniveauer, data og ansatte.
- Aktiver, der fjernes, sikres at være fri for nogen form for data ved hjælp af ECIT Solutions procedure for destruktion af datamedier. Proceduren sikrer tilintetgørelse af data på datamedier, når disse ikke længere skal anvendes.

Brugerstyring/ adgangssikkerhed

Adgang til de forskellige systemer, der anvendes som led i drift og serviceydelser, bestemmes og tildeles på baggrund af funktioner og stillingsbetegnelser for hver enkelt medarbejder. Der udføres jævnligt kontrol på disse rettigheder.

- Adgang til alle tjenester, der er eksternt tilgængelige, kræver login med 2-trins-validering.
- Krav for godkendte adgangskoder følger best-practice anbefalinger fra Microsoft, og genbrug af tidligere adgangskoder tillades som udgangspunkt ikke for nogen medarbejder- eller service-konti.
- Alle medarbejdermaskiner låses automatisk efter få minutter ved inaktivitet.
- Forbindelser til kundens driftsmiljø sker igennem et administrationspunkt (Remote Desktop Manager), der adskiller kunden fra øvrige netværk. Det er et ekstra sikkerhedslag.

Fysisk sikkerhed og miljøsikring

- Adgangsforhold
- Alle adgange til bygningen er beskyttet af et chipkort, og al aktivitet logges. Hosting-miljøet er delt op i 2 selvstændige rum. Adgang til hosting-miljøerne er kameraovervåget samt forsynet med branddøre med kortlås.
- Selve strømforsyningen er sikret ved redundant N+1 UPS nødstrømsenheder. Hvis bystrømmen forsvinder fra elnettet i mere end 60 sekunder, starter vores eget redundante N+1 generatoranlæg automatisk op og leverer strøm til datacenteret.

Malwarebeskyttelse

Installation af AV indgår i generelle server deployment-procedurer for at sikre en ensartet installation på servere, så servere altid bliver installeret med samme høje sikkerhedsniveau.

Opdatering af virusdefinitioner sker automatisk via *Hosted Manager*. Support-manageren kontrollerer ugentligt end-points for out-of-date definitioner og håndterer de enheder, det måtte være relevant at gøre noget ved.

Opfølgning i forhold til skadevoldende software: Der er som minimum en månedlig opfølgning på meta-information indsamlet af antivirus. Ligeledes vil der ske en vurdering, hvis noget kræver speciel opmærksomhed.

Backup

Formålet med backup er at sikre, at kundens data i ECIT Solutions' datacenter kan genskabes, så kunderne undgår unødvendig nedetid.

Der tages backup af al data i datacenteret. Backupdata kopieres dagligt til anden lokalitet, hvorved en disaster recovery-backup bibeholdes på den anden lokalitet.

ECIT Solutions foretager periodisk kontrol af restore-processen for tilfældigt udvalgte kundeservere.

ECIT Solutions har efter aftale ansvar for backup. Backuprutinen følger GFS-metoden, hvilken er den alment kendte standard for branchen.

Logning og overvågning

Som en integreret del af løsningen fra ECIT Solutions leveres overvågning med i vores løsninger. Via vores ECIT Solutions Operations Center overvåges performance-data fra servere og andre enheder.

Afhængigt af, hvilken enhed som overvåges, kan man se en række forskellige statistikker og live-data fra de underliggende systemer, som f.eks. CPU, RAM, virtuelle/fysiske disks, status, antivirus-status og meget mere. Udover at trække disse data ad-hoc, kan man opsætte og schedulere forskellige rapporter, som kan bruges til historik, afrapportering m.v

Log-oplysninger er vigtigt bevismateriale til opklaring af et eventuelt sikkerhedsbrud.

ECIT Solutions tilbyder udvidet sikkerhedsovervågning, hvor logs gemmes centralt til analyse. Data gemmes i Azure. Præcis lokation afhænger af, hvilken lokation man vælger i Azure. ECIT benytter som udgangspunkt altid EU-West (Holland), med mindre kunden har specifikke krav.

Patch management / ændringshåndtering

Formålet med patch management er at sikre, at alle relevante opdateringer som sikkerhedspatches fra leverandører implementeres for at sikre systemerne mod nedetid og uautoriseret adgang, og at implementeringen sker på en kontrolleret måde. Servere opdateres automatisk i aftalte servicevinduer. Opdateringer installeres 1 gang månedligt.

ECIT Solutions har udarbejdet en fall-back-plan i forbindelse med patch management. Formålet med fall-back-planen er at sikre, at systemerne kan komme tilbage i normal drift, hvis opdateringen ikke virker efter hensigten.

Cyberkriminalitet

For at beskytte vores hosting-kunder mod cyberkriminalitet, har vi indført følgende systemer:
Alle indgående mails skal igennem filtre, hvor de scannes og verificeres af 2 uafhængige antivirus/malware producenter. Hvis der er tvivl, lægges mailen i karantæne.

Alle internet-vendte servere benytter anti-malware software, der foretager analyse af netværkstrafik, med det formål at identificere og standse ondsindet adfærd og identificere mistænkeligt adfærd, i form af cyberangreb eller anden mistænkelig adfærd. Sikkerhedsafdelingen i ECIT Solutions overvåger konstant systemer og reagerer på mistænkelig adfærd. Skulle der opstå en sikkerhedshændelse på en server, vil denne server blive isoleret fra netværket automatisk, hvorefter der foretages incident response på ramte servere/systemer

På de månedlige møder i IT-sikkerhedsudvalget gennemgås alle IT-sikkerhedshændelser siden sidste møde samt stikprøver på malware logs, for at de nødvendige tiltag kan tages til at begrænse nye angrebstendenser.

Styring af IT-sikkerhedshændelser

Sikkerhedshændelser og svagheder i ECIT Solutions' systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt. Medarbejdere modtager løbende web-træning, der bl.a. uddanner dem i håndtering af IT-sikkerhedshændelser.

Alle medarbejdere i ECIT Solutions er bekendt med procedurerapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af ECIT Solutions' drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til ledelsen.

Procedure for fremskaffelsen og håndteringen af kriminaltekniske beviser sker på en sådan måde, at der ikke kan rejses tvivl om bevisernes ægthed og gyldighed. Ledelsen har ansvaret for at definere og koordinere en struktureret styringsproces, der sikrer en passende reaktion på sikkerhedshændelser.

Leverandørforhold

I tilfælde, hvor en leverandør har direkte adgang til systemer og/eller bygningen, foreligger der en underskrevet NDA (fortrolighedserklæring). Ligeledes vedligeholder Chief Information Security Officer en leverandøroversigt.

Beredskabsstyring

ECIT Solutions har en beredskabsplan, som beskriver i hovedtræk, hvordan man skal håndtere en disaster situation. Planen indeholder overordnet en punktopstilling, hvoraf det fremgår, hvilke systemer og i hvilken rækkefølge man skal genetablere driften.

Ved alvorlige fejl følges politikken for major incidents, der sikrer intern kommunikation og kundekommunikation.

Der er udarbejdet en plan for, hvad der skal ske i tilfælde af totalskade på et af serverrummene, herunder hvilke leverandører der skal involveres for at skaffe hardware. Når nødvendig hardware er på plads, vil systemerne kunne gendannes fra backupserver.

Overensstemmelse med rollen som databehandler

Det er ledelsen hos ECIT Solutions, der er ansvarlig for at sikre, at alle relevante juridiske og kontraktuelle krav er identificeret og korrekt overholdt. Relevante krav kan fx være:

- EU's Databeskyttelsesforordning
- Dansk lov om Databeskyttelse
- Databehandleraftaler
- ECIT Solutions A/S' Service Level Agreement
- ECIT Solutions A/S' standardkontrakt eller andre relevante kilder

Tilstedeværelsen af alle nødvendige aftaler, en it-sikkerhedshåndbog samt andre relevante dokumenter sikrer overholdelsen af relevante juridiske og kontraktuelle krav.

ECIT Solutions er forpligtet til at inddrage juridiske eksperter efter behov for at sikre et passende niveau i forhold til overholdelsen af lovgivningen.

Desuden gennemgår IT-Sikkerhedsafdelingen regelmæssigt alle IT-sikkerhedspolitikker, evt. med inddragelse af relevante interessenter. ISMS revideres regelmæssigt af en uvildig, ekstern part, og revisionsrapporten deles med alle via ECIT Solutions' platforme.

Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er ECIT Solutions databehandler, og kunden er dataansvarlig.

ECIT Solutions har også sørget for at have relevante kontrakter med alle nøgleinteressenter (herunder kunder, samarbejdspartnere, nøgleleverandører osv.) med henblik på at sikre overholdelse af loven. Desuden samarbejder ECIT Solutions med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.

Databeskyttelsesrådgiver (DPO)
ECIT Solutions DPO er Bastian Lentz
Kontakt: privacy@ecitsolutions.dk

Privatliv og beskyttelse af personoplysninger
Som nævnt er ECIT Solutions databehandler for sine kunder, i og med, at kunderne tilbydes en databehandling, hvortil de kan overføre og behandle data og anvende dette til videre bearbejdning indenfor deres respektive opgaver. Med udgangspunkt i kategorier og fortrolighed af data, som kunden overlader til behandling, skal ECIT Solutions iværksætte alle nødvendige sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Nedenfor beskrives ECIT Solutions' procedurer for, hvordan ECIT Solutions som databehandler opererer under instruks fra de dataansvarlige.

Databehandleraftaler
ECIT Solutions indgår databehandleraftaler med alle sine kunder. Databehandleraftalen er en fastlagt procedure ved kontraktindgåelse, og der benyttes enten ECIT Solutions' egen skabelon eller kundens skabelon. Disse aftaler beskriver ECIT Solutions' rolle og ansvar som databehandler.

Som databehandler pålægges ECIT Solutions et særligt ansvar defineret i Databeskyttelsesforordningen, udmøntet som krav i en databehandleraftale. ECIT Solutions skal blandt andet:

- Føre fortegnelse over, hvilke kategorier af persondata der behandles i de respektive IT-services.
- Beskrive de tekniske og organisatoriske sikkerhedsforanstaltninger, som er iværksat med henblik på at værne om persondata.
- Bidrage til at opfylde kundens forpligtelser vedr. den registreredes rettigheder (jf. kapitel 3 i EU's Databeskyttelsesforordning).
- Stille ekspertise til rådighed for kunden for at sikre efterlevelse af Artikel 32 – 34 i EU's Databeskyttelsesforordning.
    - Artikel 32 – behandlingssikkerhed
    - Artikel 33 – Anmeldelse af brud på persondatasikkerheden
    - Artikel 34 – Underretning om brud på persondatasikkerheden for de registrerede
- Iagttage kundens krav vedr. overførsel af persondata uden for EØS.
- Registrere navn og kontaktinformation på leverandører, der er underdatabehandlere.
- Sikre, at krav vedr. persondatabehandling fra kunden matcher krav til en underdatabehandler.

Formålsbestemthed og hjemmel
Som databehandler arbejder ECIT Solutions med persondata på baggrund af instrukser fra kunderne. ECIT Solutions er således ansvarlig for, at data ikke behandles i strid med instruksen.

Hjemmelen for behandling af persondata hos ECIT Solutions skal søges i den dataansvarliges overholdelse af retlig forpligtigelse eller opfyldelse af kontraktligt forhold.

Adgang til kundedata
ECIT Solutions tilbyder databehandling, der afvikles på ECIT Solutions' egen IT-platform. ECIT Solutions påtager sig derigennem det fulde ansvar for behandling af kunders data. Medarbejdere i ECIT Solutions har kun adgang til kundedata, hvis specifikke arbejdsopgaver taler herfor.

ECIT Solutions har indført principper for medarbejderes adgang til og arbejde med kunders data:

- Det er kun betroede medarbejdere, der har adgang til kundedata, og kun ud fra et arbejdsbetinget behov.
- En gang årlig skal alle medarbejdere gennemgå selskabsregler for databehandling i henhold til IT-sikkerhedshåndbog/ politikken.
- Procedure for tildeling og revision og kontrol af adgange til kundedata.
- Rammer og regler for databehandling af kundedata er defineret i selskabets IT-sikkerhedspolitik.

Væsentlige ændringer i forhold til IT-sikkerhed

For erklæringsperioden har der ikke været væsentlige it-sikkerhedsmæssige ændringer.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver den generelle ramme for ECIT Solutions' hostingaktiviteter, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvaret for de forretningssystemer og brugersystemer, som drives på ECIT Solutions' hostingaktiviteter, er kundernes eget.

ECIT Solutions er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til ECIT Solutions' hostingaktiviteter. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål. I forbindelse med håndteringen af passwordsikkerheden er revisionen udført ud fra et generelt perspektiv. For nogle brugervirksomheder kan sikkerheden omkring passwordopbygningen ligge under rammen, såfremt ledelsen hos kunden har ønsket det. Ansvaret for afstemning af kontrolmiljøet for passwordsikkerheden ligger hos den enkelte brugervirksomhed og hos dem, som anvender denne erklæring.

Hvis kunden foretrækker at ligge under rammen for ISMS' krav, dokumenteres dette i en sikkerhedsafvigelse.

Kunderne er ansvarlige for datatransmission til ECIT Solutions' hostingaktiviteter, og det er kundernes ansvar at skabe den nødvendige datatransmission til ECIT Solutions' datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

ECIT Solutions' beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af ECIT Solutions' hostingaktiviteter. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

BILAG 1:

ECIT Solutions A/S har arbejdet med følgende kontrolmål og sikringsforanstaltninger fra ISO27001+2

0. Risikoanalyse og -håndtering
- 0.1. Vurdering af sikkerhedsrisici
- 0.2. Risikohåndtering

5. Informationssikkerhedspolitik
- 5.1. Retningslinjer for styring af informationssikkerhed

6. Organisering af informationssikkerhed
- 6.1. Intern organisering
- 6.2. Mobilt udstyr og fjernarbejdspladser

7. Medarbejdersikkerhed
- 7.1. Før ansættelsen
- 7.2. Under ansættelsen
- 7.3. Ansættelsesforholdets ophør eller ændring

8. Styring af aktiver
- 8.1. Ansvar for aktiver
- 8.3. Mediehåndtering

9. Adgangsstyring
- 9.1. Forretningsmæssige krav til adgangsstyring
- 9.2. Administration af brugeradgang
- 9.3. Brugernes ansvar

10. Kryptografi
- 10.1. Kryptografiske kontroller

11. Fysisk sikkerhed og miljøsikring
- 11.1. Sikre områder
- 11.2. Udstyr

12. Driftssikkerhed
- 12.1. Driftsprocedurer og ansvarsområder
- 12.2. Malwarebeskyttelse
- 12.3. Backup
- 12.4. Logning og overvågning
- 12.5. Styring af driftssoftware

13. Kommunikationssikkerhed
- 13.1. Styring af netværkssikkerhed

15. Leverandørforhold
- 15.1. Informationssikkerhed i leverandørforhold
- 15.2. Styring af leverandørydelser

16. Styring af informationssikkerhedsbrud
- 16.1. Styring af informationssikkerhedsbrud og forbedringer

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- 17.1. Informationssikkerhedskontinuitet

18. Overensstemmelse
- 18.1. Overensstemmelse med lov- og kontraktkrav

KAPITEL 3:

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

Til kunder af ECIT Solutions A/S' hostingaktiviteter og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om ECIT Solutions A/S' beskrivelse i kapitel 2 inkl. bilag 1, som er en beskrivelse af kontrolmiljøet i tilknytning til it-driften af hostingaktiviteter i perioden 1. januar 2024 - 31. december 2024, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter helhedsmetoden.

Erklæringen dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. beskrivelsen kapitel 2 (inkl. bilag 1), afsnittet om komplementerende kontroller.

ECIT Solutions A/S' ansvar

ECIT Solutions A/S er ansvarlig for udarbejdelsen af beskrivelsen i Kapitel 2 og tilhørende udtalelse i Kapitel 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om ECIT Solutions A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB. Denne standard kræver, at vi overholder etiske krav samt planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt. En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelse, udformning og funktionalitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad

af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som ECIT Solutions A/S har specificeret og beskrevet i kapitel 2 (inkl. bilag 1).

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

Begrænsninger i kontroller hos ECIT Solutions A/S

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

Konklusion

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

a) at beskrivelsen af ECIT Solutions A/S' kontrolmiljø for it-driften i tilknytning til hostingaktiviteter, således som det var udformet og implementeret i hele perioden 1. januar 2024 - 31. december 2024, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. januar 2024 - 31. december 2024, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. januar 2024 - 31. december 2024.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt ECIT Solutions A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, som kunderne som dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt i databeskyttelsesforordningen er overholdt.

Søborg, den 8. januar 2025

Beierholm
Godkendt Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT auditor, Director

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, tests og resultater heraf

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

Hvad angår periode har vi i vores test forholdt os til, om ECIT Solutions A/S har levet op til kontrolmålene i perioden 1. januar 2024 - 31. december 2024.

Under det grå felt er tre kolonner:

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

De udførte tests

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

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

INDLEDENDE KONTROLMÅL:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i it-driften af hostingaktiviteter. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Gennem en risikovurdering er der sket identificering og prioritering af risici. Udgangspunkt for vurderingen er de i beskrivelsen definerede hostingaktiviteter. Resultatet bidrager til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for hostingaktiviteter arbejdes med en løbende vurdering af den risiko, som opstår som følge af de forretningsmæssige forhold og deres udvikling. Vi har kontrolleret, at risikovurderingen er forankret ned igennem virksomhedens organisation. Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.	Ingen kommentarer.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes iht. planlagte intervaller.	Vi har indhentet og revideret ECIT Solutions A/S' seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrolleret, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen kontrolleret, at de underliggende støttepolitikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og at den er gjort tilgængelig for medarbejderne via ECIT Solutions A/S' intranet.	Ingen kommentarer.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikringsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.

Virksomheden skal sikre, at fjernarbejdspladser og brugen af mobilt udstyr får et passende beskyttelsesniveau.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisationen i forhold til hostingaktiviteter. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder.	Ingen kommentarer.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og håndteringen af sikkerhedsforholdene er passende.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevist inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos ECIT Solutions A/S har vi gennemgået, hvorvidt der er implementeret passende sikringsforanstaltninger, så at området er afdækket i forhold til risikovurderingen for området.	Ingen kommentarer.

KONTROLMÅL 7:

Medarbejdersikkerhed

Det skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Via fastlagte arbejdsprocesser og procedurer er det sikret, at alle nye medarbejdere får oplyst deres særlige ansvar og rolle i forbindelse med ansættelse i ECIT Solutions A/S, herunder de fastlagte rammer for deres arbejde og den omkringliggende it-sikkerhed. Eventuelle sikkerhedsansvar er fastlagt og nærmere beskrevet gennem stillingsbeskrivelse og i form af vilkår i ansættelseskontrakten. Medarbejderne er bekendt med deres tavshedspligt via en underskrevet ansættelseskontrakt og via ECIT Solutions A/S' personalepolitik.	Vi har kontrolleret, at de af ledelsen udarbejdede forretningsgange og procedurer i forbindelse med ansættelse og ansættelsesophør er overholdt. Gennem stikprøver har vi testet, om ovenstående forretningsgange og procedurer er overholdt både i forhold til ansættelse og ansættelsesophør. Ved interview har vi kontrolleret, at væsentlige medarbejdere for hostingaktiviteter er bekendt med deres tavshedspligt. Vi har gennemgået centrale medarbejderes stillingsbeskrivelser og ansættelseskontrakter, og efterfølgende testet den enkelte medarbejders kendskab til arbejdsmæssige roller og tilhørende sikkerhedsansvar. Revisionen har påset, at ECIT Solutions A/S' personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos ECIT Solutions A/S.	Ingen kommentarer.

KONTROLMÅL 8:

Styring af aktiver

Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig "ejer". Virksomheden skal sikre, at informationsaktiver i forhold til hostingaktiviteter får et passende beskyttelsesniveau.

Der skal være betryggende kontroller, som sikrer, at datamedier bliver bortskaffet på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver. Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af hostingaktiviteter.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af ECIT Solutions A/S' hostingaktiviteter. Gennem observation og kontrol har vi kontrolleret relationer over til de centrale knowhow-systemer for driften af hosting aktiviteter. Vi har ved observationer og forespørgsler kontrolleret, at ECIT Solutions A/S overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Ingen kommentarer.
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.	Vi har: • forespurgt ledelsen om, hvilke procedurer/ kontrolaktiviteter der udføres vedr. destruktion af databærende medier. • stikprøvevist gennemgået procedurerne for destruktion af databærende medier.	Ingen kommentarer.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for ECIT Solutions A/S' adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i ECIT Solutions A/S. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. ECIT Solutions A/S' retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger ECIT Solutions A/S' retningslinjer, og at autorisationer tildeles i henhold til aftale.	Ingen kommentarer.
Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåges.	Vi har forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i ECIT Solutions A/S. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende autorisationssystemer i relation til adgangsstyring i ECIT Solutions A/S. • at den formaliserede forretningsgang for tildeling og afbrydelse af brugeradgang er implementeret i ECIT Solutions A/S' systemer, og at der foretages løbende opfølgning på registrerede brugere.	Ingen kommentarer.
Interne brugeres adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang.	Vi har ved stikprøvevis inspektion påset, at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne, herunder: • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med udvidede rettigheder hver 3. måned. • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med almindelige rettigheder hver 6. måned.	Ingen kommentarer.

Tildeling af adgangskoder styres gennem en formaliseret og kontrolleret proces, som bl.a. sikrer, at der sker skift af standardpassword.	Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i ECIT Solutions A/S. Vi har ved stikprøvevis inspektion påset, • at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login. • at standardpassword ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standardpassword.	Ingen kommentarer.
Adgange til operativsystemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde, krav til kompleksitet, maksimal løbetid, ligesom password-opsætninger medfører, at de seneste passwords ikke kan genbruges. Desuden bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i ECIT Solutions A/S. Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for: • minimum længde for password • minimum krav til kompleksitet • maksimal levetid for password • minimum historik for password • lockout efter fejlede login-forsøg	Ingen kommentarer.

KONTROLMÅL 10:

Kryptografi

Der skal være korrekt og effektiv brug af kryptografi for at beskytte informations fortrolighed, autenticitet og/ eller integritet.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
ECIT Solutions A/S har implementeret en krypteringspolitik for kryptering af persondata, der definerer styrken og protokollen for kryptering. Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at der anvendes kryptering ved transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden.	Ingen bemærkninger.

KONTROLMÅL 11:

Fysisk sikkerhed og miljøsikring

Der skal være beskyttelse af virksomhedens lokaler og informationsaktiver mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser. Der skal opbygges sikkerhedstiltag, som sikrer, at der undgås tab af, skader på eller kompromittering af virksomhedens informationsaktiver, desuden sikrer, at der undgås forstyrrelser af virksomhedens forretningsaktiviteter og endelig sikrer nødvendige forsyninger som el, vand og ventilation samt kabelinstallationer.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret en sikker fysisk afgrænsning, som beskytter de områder, hvorfra hostingaktiviteter driftes. De sikre områder er beskyttet med adgangskontrol, så kun autoriserede personer kan få adgang. Der er etableret overvågning af områder til af- og pålæsning samt øvrige områder, hvortil offentligheden har adgang.	Jf. serviceleverandørens beskrivelse er den fysiske adgangssikkerhed bl.a. gennemgået og kontrolleret med udgangspunkt i de af ledelsen fastsatte krav. Vi har gennemgået og kontrolleret de fysiske adgange til begge datcentre, som bl.a. sikres via et chipkort, som sikrer begrænset adgang til ECIT Solutions A/S' datacentre. Via besøg, interview og observation er det kontrolleret, at adgangen til begge ECIT Solutions A/S' datacentre er i overensstemmelse med ovenstående forretningsgange omkring adgangsbegrænsning. Vi har stikprøvevist gennemgået procedurer for fysisk sikkerhed vedrørende sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt at personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse. Vi har stikprøvevist gennemgået medarbejdere med adgang til sikre områder og påset, at de er oprettet i henhold til de fastlagte procedurer.	Ingen kommentarer.
Udstyr, som er placeret i datacenter, beskyttes mod fysiske trusler såsom brand, vandskade, strømafbrydelse, tyveri eller hærværk. Datacellerne er sikret mod forsyningssvigt af elektricitet, vand, varme og ventilation. Der er installeret udstyr til overvågning af indeklima, såsom luftfugtighed.	Vi har gennemgået og kontrolleret, at ECIT Solutions A/S' datacentre overholder de af ledelsen fastsatte krav. Revisionen har kontrolleret overholdelsen af de nødvendige sikringsforanstaltninger jf. ISO 27002 afsnit 11 i forholdene til beskyttelse mod skader forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.	Ingen kommentarer.

Kabler til brug for datakommunikation og elforsyning er beskyttet imod uautoriserede indgreb. Udstyret til brug for hostingaktiviteter vedligeholdes efter forskrifterne for at sikre dets tilgængelighed og pålidelighed.	Konkret har vi: • påset tilstedeværelse af brandbekæmpelsessystemer og køling i datacentre. • at UPS og dieselgenerator løbende vedligeholdes og testes. • observeret under besøg i datacenter, at der foretages monitering af UPS og dieselgenerator. • påset tilstedeværelse af udstyr til overvågning af indeklima i datacentre. • påset sikring af kabler for datakommunikation og elforsyning. • stikprøvevist gennemgået dokumentationen for at vedligeholdelse af udstyr til beskyttelse mod fysiske trusler sker løbende.	

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Driftsprocedurer og ansvarsområder

En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er dokumenteret driftsafviklingsprocedurer for forretningskritiske systemer, og de er tilgængelige for personale med et arbejdsbetinget behov. Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse.	Vi har: • forespurgt ledelsen, om alle relevante driftsprocedurer er dokumenteret. • i forbindelse med revisionen af de enkelte driftsområder stikprøvevist kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. • foretaget inspektion af brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Ingen kommentarer.
Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud. Der foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har: • forespurgt ledelsen, om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået, at ressourceforbruget i driftsmiljøet bliver overvåget og tilpasset i forhold til det forventede og nødvendige kapacitetsbehov.	Ingen kommentarer.

Kontrolmål: Malwarebeskyttelse

At beskytte mod skadevoldende programmer, som eksempelvis virus, orme, trojanske heste og logiske bomber.
Der skal træffes foranstaltninger til at forhindre og konstatere angreb af skadevoldende programmer.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret både forebyggende, opklarende og udbedrende sikrings- og kontrolforanstaltninger, herunder den nødvendige uddannelses- og oplysningsindsats for virksomhedens brugere af informationssystemer mod skadevoldende programmer.	Vi har: • forespurgt og inspiceret de procedurer/ kontrolaktiviteter, der udføres i tilfælde af virusangreb eller –udbrud. • forespurgt og inspiceret de aktiviteter, som skal gøre medarbejdere opmærksomme på forholdsregler ved virusangreb eller -udbrud. • Kontrolleret, at servere har installeret antivirusprogrammer, inspiceret signaturfiler, der dokumenterer, at de er opdateret.	Ingen kommentarer.

Kontrolmål: Backup

At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foretages sikkerhedskopiering af alle virksomhedens væsentlige informationsaktiver, herunder eksempelvis parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede. • stikprøvevist gennemgået backuplog til bekræftelse af, at backup er gennemført succesfuldt, og at tilfælde af mislykket backup håndteres rettidigt. • gennemgået fysisk sikkerhed (bl.a. adgangsbegrænsning) for intern opbevaringslokation til bekræftelse af, at backup opbevares betryggende.	Ingen kommentarer.

Kontrolmål: Logning og overvågning

At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges, og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. ECIT Solutions A/S logger, når brugerne logger af og på systemerne. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres, og gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger udført af brugere med udvidede rettigheder bliver logget. • stikprøvevist kontrolleret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer.	Ingen kommentarer.
Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår. Om muligt overvåges for, om en fejl er ved at opstå, for at kunne handle proaktivt. Alarmer sker igennem en overvågningsskærm, der er monteret i projekt- og driftsafdelingen. Kritiske alarmer afgives også pr. mail og sms. Der indmeldes statusrapporter pr. mail fra forskellige systemer. Nogle dagligt – andre når der opstår en hændelse i systemet. Driftsvagten har til ansvar dagligt at kontrollere disse mails.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • påset, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for samtlige medarbejdere. • påset, at der afgives alarmer pr. mail og sms ved opståede fejl. • gennemgået statusrapporter. • påset, at der er etableret en driftsvagt, samt at denne tjekker rapporter dagligt.	Ingen kommentarer.

Kontrolmål: Styring af driftssoftware

At sikre, at der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i ECIT Solutions A/S. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til ECIT Solutions A/S' produktionsmiljøer. • at ændringer til driftsmiljøer i ECIT Solutions A/S følger de gældende retningslinjer, herunder at registreringer og dokumentation af ændringsanmodninger foretages korrekt. Vi har stikprøvevist inspiceret, at styresystemerne er opdateret efter gældende procedurer, samt at status herpå registreres.	Ingen kommentarer.
Ændringer i styresystemer og driftsmiljøer følger formaliserede forretningsgange og processer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i ECIT Solutions A/S. Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til produktionsmiljøerne, herunder at krav til patch management kontroller sikrer: • at der sker registrering og beskrivelse af ændringsanmodninger • at alle ændringer er underlagt formel godkendelse inden idriftsætning • at ændringer er underlagt formelle konsekvensvurderinger • at der beskrives fall-back-planer • at der sker identifikation af systemer, der påvirkes af ændringer • at der sker en dokumenteret test af ændringer inden idriftsætning • at dokumentationen opdateres, så den i al væsentlighed afspejler de påførte ændringer • at procedurer er underlagt styring og koordination i et "change board"	Ingen kommentarer.

KONTROLMÅL 13:

Kommunikationssikkerhed

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

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og transmitteret data. Produktionsmiljøet skal være sikret mod forsyningssvigt i forhold til redundans til netværksforbindelse til internettet. Netværkstrafikken/ adgange fra produktionsmiljøet ud til omverdenen kan opnås ved hjælp af flere forsyningsindgange eller adgang fra mere end ét forsyningsselskab.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • Der er etableret passende procedurer for styring af netværksudstyr. • Der er funktionsadskillelse mellem brugerfunktioner. • Der er etableret passende procedurer og løbende opfølgning på logs og overvågning. • Styring af virksomhedens netværk er koordineret for at sikre en optimal udnyttelse af ressourcer og et sammenhængende sikkerhedsniveau. • Påset, at der etableret forbindelser for datakommunikation mod internettet via mere end én ISP-leverandør. • Stikprøvevist gennemgået dokumentationen fra leverandørerne i forhold til skriftligt aftalegrundlag samt løbende afregning af ydelser hos ISP-leverandørerne.	Ingen kommentarer.
Der skal være etableret passende forretningsgange for håndtering af trusler i form af angreb fra internettet (cyber-angreb). I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.	Det er kontrolleret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for håndtering af cyber-angreb. • at der er udarbejdet og implementeret planer for håndtering af truslen. • at planerne har et tværorganisatorisk samarbejde mellem interne grupper.	Ingen kommentarer.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevist inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Ingen kommentarer.
Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende godkendte leverandører.	Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere. Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører. Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.	Ingen kommentarer.
Der skal udføres regelmæssig overvågning, herunder føres tilsyn med eksterne samarbejdspartnere.	Vi har påset, at findes passende processer og procedurer for løbende overvågning af eksterne leverandører. Vi har kontrolleret, at der udføres løbende tilsyn gennem uafhængig revisors rapporter eller anden form certificeringer.	Ingen kommentarer.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

At opnå at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.	Vi har forespurgt ledelsen, om der er etableret procedurer for rapportering af sikkerhedshændelser. Vi har kontrolleret, at der er udarbejdet procedurer og forretningsgange for rapportering og behandling af sikkerhedshændelser, samt at rapporteringen tilgår de rette steder i organisationen jf. retningslinjer. Vi har kontrolleret, at ansvaret for håndteringen af kritiske hændelser er klart placeret, og at de tilhørende forretningsgange sikrer, at der sker en hurtig, effektiv og metodisk håndtering af brud på sikkerheden.	Ingen kommentarer.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse.	Vi har forespurgt ledelsen, om der er udarbejdet beredskabsstyring for hostingaktiviteter i ECIT Solutions A/S. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring. • at der er udarbejdet og implementeret beredskabsplaner. • at planerne har en tværorganisatorisk beredskabsstyring. • at planerne indeholder passende strategi og procedurer for kommunikation med ECIT Solutions A/S' interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Ingen kommentarer.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Principper for behandling af personoplysninger:

Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med aftalen for behandling af personoplysninger.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme i form af standardkontrakter, Service Level Agreement samt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, og at procedurerne indeholder krav til lovlig behandling af personoplysninger.	Ingen kommentarer.
Der udføres alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har kontrolleret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har kontrolleret, ved en stikprøve på et passende antal behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen kommentarer.
Ledelsen underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har kontrolleret, at ledelsen sikrer, at behandling bliver gennemgået, og at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har kontrolleret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har kontrolleret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet at være i strid med lovgivningen.	Ingen kommentarer.

Databehandling:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har kontrolleret, at procedurerne er opdateret.	Ingen kommentarer.
Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har kontrolleret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har kontrolleret, ved en passende stikprøvepopulation på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen kommentarer.
Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har kontrolleret, at procedurerne er opdateret. Vi har kontrolleret via stikprøver, om der i forbindelse med databehandlinger findes underliggende dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen kommentarer.

Databehandlerens ansvar:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen kommentarer.
Databehandleren anvender til behandling af personoplysninger alene underdatabehandlere, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på 3 underdatabehandler fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen kommentarer.
Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere skal dette godkendes af den dataansvarlige.	Vi har kontrolleret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen kommentarer.
Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har kontrolleret, at der foreligger underskrevne underdatabehandleraftaler med alle de anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på 3 underdatabehandleraftale, at disse aftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen kommentarer.

Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af databehandlingen	Vi har kontrolleret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen kommentarer.

Bistå den dataansvarlige:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen kommentarer.
Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til de registrerede.	Vi har kontrolleret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen kommentarer.

Fortegnelse over behandlingsaktiviteter:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over den behandling af personoplysninger, som er under databehandlerens ansvar.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der skal foreligge en fortegnelse over behandlingsaktiviteterne for hosting kombineret med en tilhørende dataansvarlig.	Vi har kontrolleret dokumentationen for, at der foreligger en fortegnelse over behandlingsaktiviteterne for hosting sammenstillet med en dataansvarlig.	Ingen kommentarer.
Der foretages løbende – og mindst en gang årligt – vurdering af, hvorvidt fortegnelsen er opdateret og korrekt.	Vi har kontrolleret dokumentationen for, at fortegnelsen over behandlingsaktiviteterne for den enkelte dataansvarlige er opdateret og korrekt.	Ingen kommentarer.

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

ECIT Solutions A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som opdateres mindst en gang årligt, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for håndtering af brud på persondatasikkerheden, herunder at rettidig kommunikation til den dataansvarlige er beskrevet.	Ingen kommentarer.
Databehandleren sikrer registrering af alle brud på persondatasikkerheden.	Vi har kontrolleret dokumentationen for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Ingen kommentarer.
Ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har kontrolleret dokumentationen for, at ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Ingen kommentarer.

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."

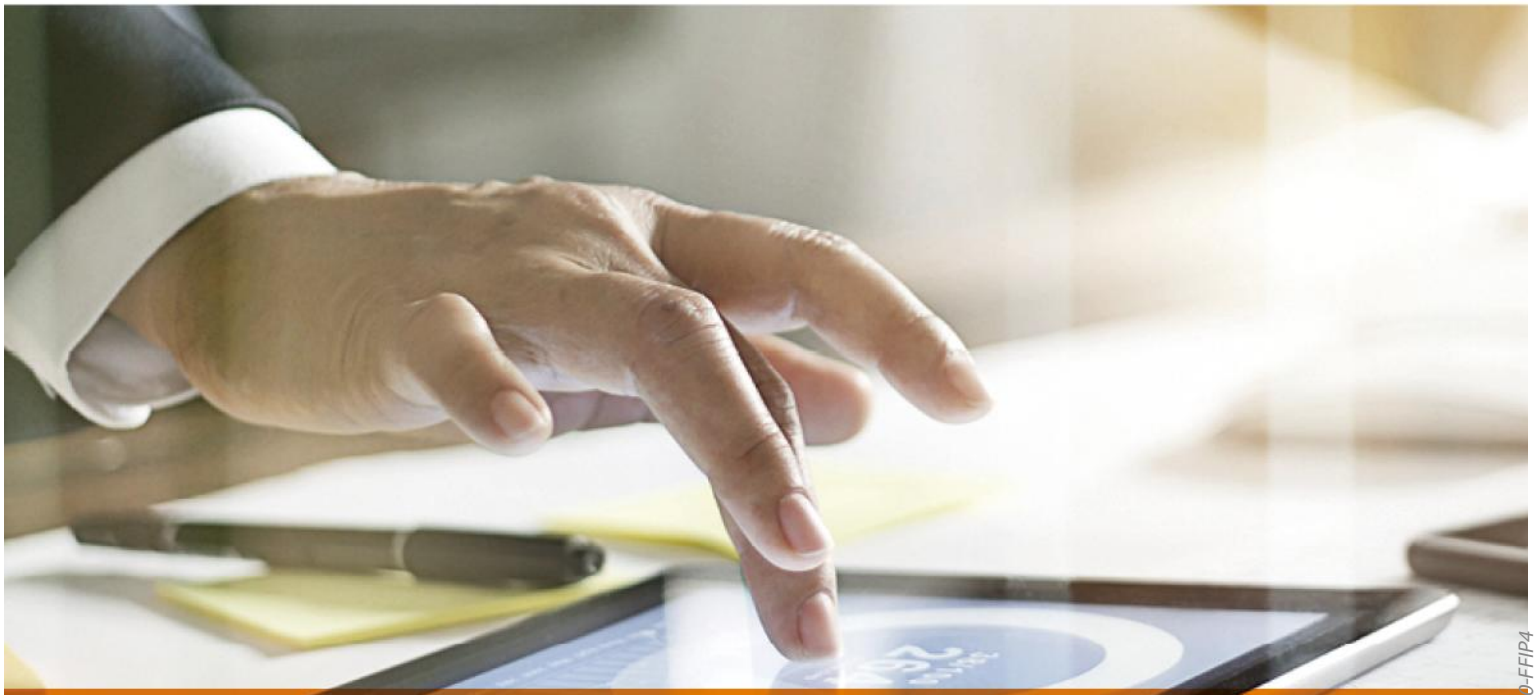
Jesper Aaskov Pedersen
IT auditor, Director
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: 55a3ea90-967e-4a5c-b854-37be4db4517b
IP: 212.98.xxx.xxx
2025-01-08 16:31:42 UTC

Rolf Wulff Ljungberg
Director of Operations
På vegne af: ECIT Solutions A/S
Serienummer: ac3ac967-fe1c-4712-8d30-6eb2a93dd905
IP: 80.208.xxx.xxx
2025-01-08 20:13:56 UTC

Kim Bahir Andersen
Managing Director
På vegne af: ECIT Solutions A/S
Serienummer: f0014b70-b15b-4e04-9368-4381c27345ad
IP: 82.163.xxx.xxx
2025-01-09 09:23:18 UTC

Kim Holm Larsen
Beierholm Godkendt Revisionspartnerselskab CVR: 32895468
Statsautoriseret revisor
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2025-01-09 10:15:35 UTC

BEIERHOLM



JANUARY 2025

ECI T SOLUTI ONS A/ S

ISAE 3402 TYPE II ASSURANCE REPORT

CVR 28843151

Independent auditor's Report on the control environment related to the IT operation of hosting activities.

In addition, a paragraph has been added to the description about the role as data processor in accordance with the General Data Protection Regulation.

Beierholm
Godkendt Revisionspartnerselskab
Copenhagen
Knud Højgaards Vej 9
DK-2860 Søborg
Denmark
CVR no. DK 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Structure of the Assurance Report

Chapter 1:
Letter of Representation.

Chapter 2:
Description of the control environment for the IT operation of hosting activities.

Chapter 3:
Independent auditor's assurance report on the description of controls, their design, and operating effectiveness.

Chapter 4:
Auditor's description of control objectives, security measures, tests, and findings.

CHAPTER 1:

Letter of Representation

ECIT Solutions A/S processes personal data on behalf of Data Controllers according to Data Processor Agreements regarding IT operation of hosting activities.

The accompanying description has been prepared for the use of customers and their auditors, who have used ECIT Solutions A/S' hosting activities, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers i.e. the Data Controllers themselves, when assessing, whether the demands to the control environment as well as requirements laid down in the General Data Protection Regulation are complied with.

ECIT Solutions A/S hereby confirms that

(A) The accompanying description, Chapter 2 (incl. Appendix 1) gives a true and fair description of ECIT Solutions A/S' control environment in relation to IT operations of hosting activities throughout the period 1 January 2024 - 31 December 2024. The criteria for this assertion are that the following description:

(i) Gives an account of how the controls were designed and implemented, including:

- The types of services delivered, including the type of personal data processed
- The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase, and limit the processing of personal data
- The processes utilized to secure that the performed data processing was conducted according to contract, directions or agreements with the customer i.e. the Data Controller
- The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality
- The processes securing that - at the Data Controller's discretion - all personal data is erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation
- The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal data security breaches
- The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed
- Control procedures, which we assume – with reference to the limitations of the hosting activities – have been implemented by the Data Controllers and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description
- Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data

(ii) Includes relevant information about changes in ECIT Solutions A/S' IT operation of hosting activities performed throughout the period 1 January 2024 - 31 December 2024.

(iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of

the control system that each individual customer may consider important in their own particular environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 January 2024 - 31 December 2024. The criteria for this assertion are that:

(i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified

(ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives, and

(iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 January 2024 - 31 December 2024.

(C) Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, compliance with generally accepted data processor standards and relevant demands to Data Processors according to the General Data Processing Regulation.

(D) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2 (incl. Appendix 1) have been prepared based on compliance with ECIT Solutions A/S' standard agreement as well as related Data Processing Agreement. The criteria for this basis are:

(i) Information Security Policy for ECIT Solutions
(ii) IT Security Rules/Handbook for ECIT Solutions (Framework according to ISO 27002)

Viby J, den 8. January 2025

Kim Bahir Andersen, Managing Director **Rolf Ljungberg, Director of Operations**
ECIT Solutions A/S, Rudolfgårdsvej 1B, DK-8260 Viby J, CVR 28843151

CHAPTER 2:

Description of the control environment in relation to the IT operation of hosting activities

Introduction

The purpose of this description is to provide ECIT Solutions A/S' customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organisations.

The scope of this description is coverage of the technical and organisational security measures implemented in connection with the IT operation of hosting activities.

As a supplement to the description below is added an independent paragraph (Compliance with the role as data processor), including a description of essential requirements in connection with the role as data processor combined with general requirements from data processor agreements.

Description of ECIT Solutions A/S

ECIT Solutions was established in 1996 by former CEO Mikkel Walde. Today the company employes more than 70 employees.

Our primary service is server hosting, and it is provided to a broad range of larger and smaller businesses. All services are based on deliveries originating from our own data centre. The data centre was built in 2017 – and was created based on the latest knowledge within data centre technology and IT security.

With our own servers, transformer station, and generators physically placed in own data centre – and full ownership of all customer-dedicated connections out of the building – ECIT Solutions has thus total control over all parts of the service delivery. It means that solutions can always be customized to the individual customer's demands. We offer services from simple web operations and e-mail operations to complex solutions regarding business-critical IT for businesses demanding uptime all year round.

We put together the optimal combination of virtual and physical servers to offer the best service possible for each customer. It is also possible to add a local server at the customers to mirror data.

The data centre is secured to the best of our knowledge based on the latest technology in electronic access control, video monitoring, temperature alarm, smoke/fire sensors, climate control, and UPS.

The data centre's composition is modular making it possible- on an ongoing basis - to add extra servers, CPUs, or storage capacity, depending on the demands, and all this ensures a flexible and functional delivery for the customers.

ECIT Solutions has more than 25 years of experience with IT operation primarily for small and medium-sized businesses.

As all deliveries are sent directly from ECIT Solutions, sharp focus is always on keeping each employee updated and specialized within their own field of work. Emphasis is also on the general level, making it possible for every employee to support customers as well as colleagues to the best of their knowledge. In this way, the customer has the experience that it is not necessary to contact the entire company, but that instead the customer can continue to communicate with the same employee, who has a deeper insight into the unique demands of the customer in question.

ECIT Solutions has as our mission to ensure a high level of safety and stability of operations for our customers' entire IT infrastructure. To accomplish this objective, we use a redundant setup, enabling us to offer maximum uptime, secure backup, dynamical disks, as well as agile servers. The companies, who have chosen ECIT Solutions as their IT partner, can in this way focus on their own core services without having to worry about their IT operations.

At ECIT Solution we solely work with IT operations/ hosting for companies and organisations, and our customer references have been built over the course of many years with long and dedicated cooperation with the customers.

ECIT Solutions is AAA-rated, and for our customers this ensures that we- as their IT provider - have sound finances. Furthermore, we have for a long time worked determinedly with IT security and EU's General Data Protection Regulation.

Scope of this description

ECIT Solutions A/S is supplier of services within IT, and the core activity is providing hosting and operation services. Monitoring and support are flexible services, as these can be performed on the customers' own platforms placed in our data centre – or on solutions executed on our infrastructure where the customers hire some space.

ECIT Solutions is responsible for establishing and maintaining suitable procedures and controls for the purpose of finding and preventing errors, and in this way comply with the demands laid down in the agreements. It is exactly this core activity – hosting and operation as well as maintenance – that forms the basis for this description.

Business strategy/ IT-security strategy

One of the strategic objectives for us at ECIT Solutions is to incorporate the necessary security implementations in our business, ensuring that the company is not inflicted by unacceptable risks to the disadvantage of ourselves or our customers.

ECIT Solutions has 3 general strategic points of orientation:

- At ECIT Solutions, we aim to keep ourselves updated in relation to the latest knowledge within modern information technology. We do this with a view to provide the best service possible, and in this way assist and guide our customers.
- At ECIT Solutions, our primary focus is to build, administer and guide in relation to operations and maintenance of, inter alia, IT systems, network solutions, and cloud solutions.
- As a workplace, ECIT Solutions has focus on the wellbeing of our employees. This is carried out, inter alia, by giving priority to the possibility of further education and specializing for the individual employee. By continuously giving the employees the possibility of requiring new skills, we ensure a continual high level within each employee's area of knowledge.

ECIT Solutions wants to be our customers' impartial and consultative partner regarding IT-security, and this is why IT-security is given a high level of priority in relation to business-strategy.

We work continuously to ensure the high level of service and quality within the area. Via the company's IT-security policy, Management makes it their priority to ensure that IT-security will continue to be an important part of the company's work culture.

ECIT Solutions has chosen to base our IT security strategy on ISO27001+2:2017, and has in this way used the ISO methodology for implementation of relevant security measures within the following areas:

- Information security policies
- Organisation of information security
- Human ressources security
- Asset management
- Access control
- Physical and environmental security
- Operations security
- Communication security
- Supplier relationships
- Information security management
- Information security aspects of business continuity management
- Compliance with legal and contractual requirements

The implemented control objectives and security measures at ECIT Solutions A/S are displayed in Appendix 1 to this description.

ECIT Solutions A/S' organisation and organising of IT-security

At ECIT Solutions, the general responsibility is placed at CEO Danny Stoker. The organisational responsibility is delegated to COO Rolf Ljungberg, and the responsibility for IT-security is delegated to Security Manager Nikolaj Olssen.

When using external business partners, a cooperation agreement is prepared before the work commences.

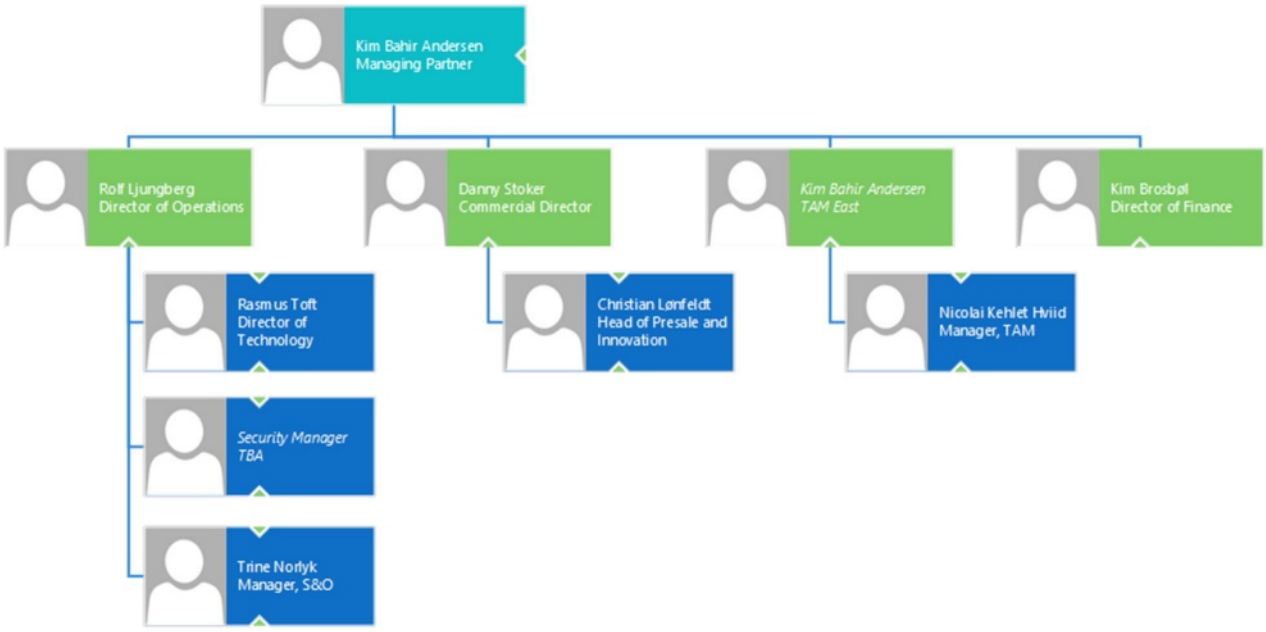


Figure 1 – Organisational chart

Risk management at ECIT Solutions A/S

It is ECIT Solutions' policy that the risks related to the company's activities must be covered or limited to such an extent that the company will be able to continue normal operations. ECIT Solutions performs risk management and internal controls within several areas and at different levels. Every year, two risk and threat assessments are performed.

ECIT Solutions has implemented set procedures for risk assessment of the business-critical processes and the operation of the data centre. In this way, we ensure that the risk connected to the services we provide are minimized to an acceptable level. Risk assessment is conducted at intervals, and when we make changes to existing systems or implement new systems.

The responsibility for the risk assessment is placed at the COO and must subsequently be deployed and approved by the other members of the company's Management.

As part of the IT-security strategy mentioned above, ECIT Solutions work with Danish and international standards for IT-security – ISO27001+2:2017 – as the primary reference framework for IT-security. The work process regarding IT security is a continual and dynamic process, ensuring that ECIT Solutions always complies with legal requirements.

IT-security management

The Security Manager at ECIT Solutions has the day-to-day responsibility for IT security. In the central IT security policy, Management has described ECIT Solutions' IT security structure. The IT security policy must be revised at least once a year.

ECIT Solutions' quality assurance system has been defined based on the overall objective about delivering stable and secure IT operations to all customers. To ensure this objective, it is necessary that we have introduced policies and procedures to secure that all our services and deliveries are of the same uniform and transparent quality.

ECIT Solutions' IT security policy has been prepared with reference to the above, and the policy applies to all employees and all deliveries. In the event of errors and security flaws in our operating environment, the error/security flaw will be remedied as soon as possible depending on the criticality.

The IT-security Committee's processing of reported information security incidents includes a communication plan, an assessment of the likelihood of the incident occurring elsewhere, as well as giving the experiences to relevant employees.

All servers and network devices are documented in ECIT Solutions' documentation system. Here all changes to the systems are logged. Configuration files to network units (firewalls, routers, switches etc.) are also documented in the system.

The security policy lays down the general policies for the infrastructure of ECIT Solutions. The policy does not deal with issues regarding specific products, services, or users.

The security policy has been prepared to provide ECIT Solutions with one single overall set of rules. In this way, we achieve a stable operating environment and a high security level. We are making regular improvements to policies, procedures, and operations.

Controls and security measures

In the following section we deal with:

- HR, employees, and training
- Asset management
- User management/ access security
- Physical and environmental security
- Protection from malware
- Backup
- Logging and monitoring
- Patch management/ change management
- Cybercrime
- IT-security incident management
- Supplier relationships
- Business continuity management
- Compliance with the role as data processor

HR, employees, and training

ECIT Solutions has obtained certification from Microsoft as Gold Partner for operation of **Data Centre** & **Cloud Platform**, and **Small and Midmarket Cloud Solutions**.

All consultants have competences with their areas of work. This is documented by means of relevant certifications from the technology providers. As mentioned, ECIT Solutions is a certified Microsoft Partner, and the requirements to maintain this status are high.

ECIT Solutions must meet a series of requirements from Microsoft, including specific demands that a certain number of consultants have passed certain product certifications, and they must be renewed on an ongoing basis. ECIT Solutions ensures this high status of certification via continuous product training and the consultants' participation in courses.

Asset management

ECIT Solutions manages assets using defined ownership and described work routines for acceptable use of assets.

- Data is classified, see procedures for granting security level, data, and employees.
- We ensure that removed assets contain no data by using ECIT Solutions' procedure for destruction of data media. The procedure ensures the destruction of data found on data media, when these media are no longer in use.

User management/ access security

Access to the different systems used as part of operations and services, are defined and granted based on the functions and job titles of each employee. Control in relation to these access rights is performed on a regular basis.

- Access to all services with external access requires two-factor validation.
- The requirements to approved passwords comply with best-practice recommendations from Microsoft, and as a rule, re-use of previous passwords is not allowed for any employee or service account.
- All devices used by employees are locked after a few minutes of inactivity.
- Connection to the customer's operation environment takes place via an administration point (Remote Desktop Manager), which segregates the customer from the other part of the network. This is an extra level of security.

Physical and environmental security

- Entry conditions
- All entries to the building are protected by chip card, and all activities are logged. The hosting environment is divided into 2 independent rooms. Entries to the hosting environments have camera surveillance and fire doors with keycard lock.
- The power supply is secured by redundant N+1 UPS back-up power unit. If the public power supply disappears from the electricity network for more than 60 seconds our own redundant N+1 generator will start up automatically and supply power to the data centre.

Protection from malware

Installation of AV is included in the general server deployment procedure to ensure a uniform installation on servers and always an installation with the same high level of security.

Updating the virus definitions takes place automatically via *Hosted Manager*. Every week, the Support Manager controls the endpoints for out-of-date definitions and deals with units it might be relevant to investigate.

Follow-up regarding malicious software: There is as a minimum a monthly follow-up on metainformation collected by antivirus. Likewise, an assessment will be made if some issue requires special attention.

Backup

The purpose of backup is to ensure that the customer's data in ECIT Solutions' data centre can be restored to avoid unnecessary downtime for the customers.

Backup copy is taken of all data in the data centre. Backup data is every day copied to another location, and in this way a disaster recovery backup is maintained at the other location.

At regular interval, ECIT Solutions performs control of the restore process for a random sample of customer servers.

According to agreement, ECIT Solutions is responsible for backup. The backup procedure adheres to the GFS method, which is the generally known standard for the industry.

Logging and monitoring

As an integrated part of the services from ECIT Solutions, monitoring is included in our solutions. Performance data from servers and other units is monitored via our ECIT Solutions Operations Centre.

Depending on the monitored unit in question, it is possible to watch several different statistics and live data from the underlying systems, e.g. CPU, RAM, virtual/physical discs, status, antivirus status, and many more. Apart from retrieving data ad hoc, it is possible to set up and schedule various reports to use for history, reporting etc.

Logging information is important as evidence in solving any security breaches.

ECIT Solutions offers enhanced security monitoring including storing logs at a central place for analysis. Data is stored in Azure. The exact location depends on the location chosen in Azure. As a rule, ECIT Solutions always uses EU-West (the Netherlands), unless the customer has specific demands.

Patch management / change management

The purpose of patch management is to ensure that all relevant updates such as security patches from suppliers are implemented to protect systems against downtime and unauthorized access as well as ensure that the implementation is done in a controlled manner. Servers are updated automatically during agreed service windows. Updates are installed once a month.

ECIT Solutions has prepared a fall-back plan regarding patch management. The purpose of the fall-back plan is securing that systems return to normal operations, if the update does not work as desired.

Cybercrime

To protect our hosting customers against cybercrime, we have introduced the following systems:
All incoming e-mails must pass through filters, where they are scanned and verified by 2 independent antivirus/anti-malware producers. In case of doubt, the e-mail is placed in quarantine.

All servers connected to the internet use anti-malware software, which performs an analysis of network traffic to identify and stop malicious behavior and identify suspicious behavior in the form of cyber-attack or other suspicious behavior. The Security Department at ECIT Solutions monitors the systems constantly and reacts in case of suspicious behavior. In the event a security incident occurs on a server, this server will be isolated from the network automatically, and subsequently, incident response will be performed on the affected servers/systems.

In the monthly meetings of the IT security committee, all IT security incidents that occurred since the previous meeting as well as samples of malware logs are scrutinized to ensure that all necessary initiatives can be taken to limit new tendencies of attack.

Managing IT-security incidents

Security incidents and weaknesses in ECIT Solutions' systems must be reported in such a way that it is possible to make timely corrections. On an ongoing basis, the employees receive web-training, which, inter alia, is training them to deal with IT-security incidents.

All employees at ECIT Solutions are familiar with the procedures for reporting different types of incidents and weaknesses, which can influence ECIT Solutions operational security. Security incidents and weaknesses must be reported as quickly as possible to Management.

The procedure for obtaining and handling forensic evidence is conducted in such a way that no doubts can be raised about the authenticity and validity of the evidence. Management is responsible for defining and coordinating a structured steering process ensuring an appropriate response to security incidents.

Supplier relationships

In cases, when a supplier has direct access to systems and/or entry to the premises, there is a signed NDA (declaration of secrecy). Likewise, the Chief Information Security Officer keeps and maintains a list of suppliers.

Business continuity management

ECIT Solutions has a business continuity plan, which describes in outline how to manage a disaster. The plan includes a general bullet list describing the systems and the order of activating the system to re-establish the operation.

In the event of major errors, the policy for major incidents must be followed to secure internal communication and communication with customers.

A plan has been prepared in the event of a total loss of one of the server rooms, including which suppliers to involve for acquiring hardware. When the necessary hardware is installed, it will be possible to restore the systems from the backup server.

Compliance with the role as data processor

Continia's Management is responsible for identifying and ensuring compliance with all relevant legal and contractual requirements. Relevant requirement might be, e.g.:

- The EU General Data Protection Regulation
- The Danish Data Protection Act
- Data Processor Agreements
- ECIT Solutions A/S' Service Level Agreement
- ECIT Solutions A/S' standard contract or other relevant sources

The existence of all necessary agreements, a comprehensive ISMS (management system for managing information security), as well as other relevant documents, ensure compliance with all relevant legal and contractual requirements.

ECIT Solutions is obliged to involve legal experts as needed to ensure an appropriate level of compliance with law and regulations.

Furthermore, ECIT Solutions IT-Security Department reviews all our IT-security policies on a regular basis, involving any relevant stakeholders. ISMS is regularly audited by an independent, external party, and on request the audit report is shared with everybody via ECIT Solutions' platforms.

According to the EU General Data Protection Regulation and Danish additional regulation (The Danish Data Protection Act), ECIT Solutions is the Data Processor, and the customer is the Data Controller.

ECIT Solutions has also ensured relevant contracts with all key stakeholders (including customers, business partners, key suppliers etc.) to ensure compliance with law and regulations. In addition, ECIT Solutions works together with the customers to ensure that the customers are aware of and comply with the relevant GDPR rules.

Data Protection Officer (DPO)
ECIT Solutions' DPO is Bastian Lentz
Contact: privacy@ecitsolutions.dk

Privacy and protection of personal data
As mentioned above, ECIT Solutions is the customers' Data Processor, given that the customers are offered an IT service to which they can transfer and process data and utilize it for further processing within their respective assignments. Based on the categories and confidentiality of the data the customers have entrusted to ECIT Solutions for processing, ECIT Solutions must put all necessary security measures required into practice to ensure an appropriate level of security.

Below is described ECIT Solutions' procedures of how ECIT Solutions operates as Data Processor according to directions from the Data Controllers.

Data Protection Agreements
ECIT Solutions has Data Processor Agreements (DPA) in place with all our customers. The Data processor Agreement is a set procedure when entering a contract, and either ECIT Solutions' own template is used or the customer's template. These contracts outline ECIT Solutions' role and responsibilities as Data Processor.

As Data Processor ECIT Solutions is subject to a special responsibility defined in the General Data Protection Regulation and implemented as requirements in a Data Processor Agreement. ECIT Solutions must, inter alia:

- Keep record of the types of personal data processed in the respective IT services.
- Describe the technical and organisational security measures implemented to safeguard personal data.
- Contribute to the customer's obligations regarding the Data Subject's rights (see Chapter 3 in the EU General Data Protection Regulation)
- Provide expertise for the customer to ensure compliance with Article 32 – 34 of the General Data Protection Regulation:
  - Article 32 – Processing security
  - Article 33 – Reporting breaches of personal data security
  - Article 34 – Providing information about breaches of personal data security to the Data Subjects
- Comply with the customer's demands about transfer of any personal data outside of the EEA
- Register name and contact information of suppliers, who are sub-processors.
- Secure that requirements from the customer in relation to processing of personal data match the requirements to a sub-processor.

Decision of purpose and legal basis
As data processor, ECIT Solutions works with personal data based on the customers' directions. In this way, it is the responsibility of ECIT Solutions that data is not processes contrary to the directions.

The legal basis for processing personal data at ECIT Solution is found in the data controller's compliance with legal obligations or in performance of obligations under a contract.

Access to the data in customer instances
ECIT Solutions offers data processing operated on ECIT Solutions' own IT-platform. In this way, ECIT Solutions takes on the full responsibility for processing the customers' data. ECIT Solutions' employees only have access to customer instances, if specific tasks speak in favour of doing so.

ECIT Solutions has laid down principles for employees' access to and processing customers' data.

- Only trusted employees have access to customer data and only when there is a work-related need.
- Once a year all employees must review company rules about data processing in relation to the IT-security handbook/ policy.
- Procedure for granting, review, and control of access to customer data.
- Framework and rules for processing customer data is defined in the company's IT-Security policy.

Important changes in relation to IT security

During the period covered by the report, there have been no significant changes in relation to IT security.

Customers' responsibilities (complementary controls at the customer)

This chapter describes the general framework for ECIT Solutions' hosting activities. This means that no account has been made for the agreements of individual customers.

The customers themselves are responsible for the business systems and user systems operated on ECIT Solutions' hosting activities.

ECIT Solutions is not responsible for access rights, including granting, changing, and revoking rights, in relation to the individual customer's users and their access to ECIT Solutions' hosting activities. The customers themselves are obliged to secure the necessary controls in relation to this control objective. Regarding the handling of password security, the audit is performed based on a general perspective. For some users the security in relation to construction of passwords might be below the framework, if this was what the customer's Management wanted. The responsibility for reconciliation of the control environment is placed at the individual user company and at those who use this report.

If the customer prefers to stay below the framework of the demands of the ISMS, this issue is documented in a security deviation.

The customers are responsible for the data transmission to ECIT Solutions' hosting activities, and it is the customers' responsibility to establish the necessary data transmission to ECIT Solutions' data centre. The customers themselves must secure the necessary controls in relation to this control objective.

ECIT Solutions' business continuity management is built around a general emergency plan describing the approach and actions in the event re-establishing ECIT Solutions' hosting activities is needed. Specific business continuity plans for the individual customer can be prepared if required in relation to risks in the event of disruption of business processes.

APPENDIX 1:

ECIT Solutions A/S applies the following control objectives and security measures from ISO27001+2

0. Risk assessment and management
- 0.1. Assessment of security risks
- 0.2. Risk management

5. Information security policies
- 5.1. Management directions for information security

6. Organisation of information security
- 6.1. Internal organisation
- 6.2. Mobile devices and teleworking

7. Human ressource security
- 7.1. Prior to employment
- 7.2. During employment
- 7.3. Termination or change of employment

8. Asset management
- 8.1. Responsibility for asssets
- 8.3. Handling of media

9. Access control
- 9.1. Business requirements of access control
- 9.2. User access management
- 9.3. Users' responsibility

10. Cryptography
- 10.1. Cryptographical controls

11. Physical and environmental security
- 11.1. Secure areas
- 11.2. Equipment

12. Operations security
- 12.1. Operational procedures and responsibilities
- 12.2. Protection from malware
- 12.3. Backup (not covered by the report)
- 12.4. Logging and monitoring
- 12.5. Operational software management

13. Communication security
- 13.1. Network security management

15. Supplier relationships
- 15.1. Information security in supplier relationships
- 15.2. Supplier service delivery management

16. Information security incident management
- 16.1. Management of information security incidents and improvements

17. Information security aspects of business continuity management
- 17.1. Information security continuity
- 17.2. Redundancies

18. Compliance
- 18.1. Compliance with legal and contractual requirements

CHAPTER 3:

Independent auditor's assurance report on the description of controls, their design and operating effectiveness

For the customers of ECIT Solutions A/S' hosting activities and their auditors

Scope

We have been engaged to report on ECIT Solutions A/S' description in Chapter 2 (incl. Appendix 1), which is a description of the control environment in connection with the IT operations of Hosting activities, see Data Processor Agreements with customers, throughout the period 1 January 2024 - 31 December 2024, as well as on the design and function of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

The report is based on the overall approach.

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section: Complementary controls at the customer.

ECIT Solutions A/S' responsibility

ECIT Solutions A/S is responsible for the preparation of the description in Chapter 2 and accompanying assertion in Chapter 1, including the completeness, accuracy, and method of presentation of the description and assertion; for providing the services covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality, and professional conduct.

We apply ISQM 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on ECIT Solutions A/S's description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed and operate effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and about the design and operating effectiveness of controls. The procedures selected depend on the judgement of the service organisation's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively.

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by ECIT Solutions A/S in Chapter 2 (including Appendix 1).

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at ECIT Solutions A/S

ECIT Solutions A/S's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment. Moreover, because of their nature, controls at ECIT Solutions A/S may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisation may become inadequate or fail.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description fairly presents ECIT Solutions A/S' control environment in relation to the IT operations of hosting activities, such as it was designed and implemented throughout the period 1 January 2024 - 31 December 2024 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 January 2024 - 31 December 2024; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period 1 January 2024 - 31 December 2024.

Description of tests of controls

The specific controls tested, and the nature, timing, and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for ECIT Solutions A/S' customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the customers as Data Controllers have performed themselves, when assessing whether the control environment is appropriate, and there is compliance with the requirements of General Data Protection Regulation.

Søborg, 8 January 2025

Beierholm
Godkendt Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Jesper Aaskov Pedersen
IT-auditor, Director

CHAPTER 4:

Auditor's description of control objectives, security measures, tests, and findings

We have structured our engagement in accordance with ISAE 3402 – Assurance Reports on Controls at a Service Organisation. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27001 and 27002.

With respect to the period, we have tested whether ECIT Solutions A/S has complied with the control objectives throughout the period 1 January 2024 - 31 December 2024.

Below the grey field are three columns:

- The first column tells the activities ECIT Solutions A/S, according to their documentation, has put into practice in order to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to assess, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at ECIT Solutions A/S. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.

CONTROL OBJECTIVE - INTRODUCTION:

Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of Hosting activities. The findings are to contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Through a risk assessment, risks have been identified and prioritised. The hosting activities defined in the description are used as basis for the assessment. The findings contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.	We have requested and obtained the relevant material in connection with the audit of risk management. We have checked that regular risk assessments are carried out for The hosting activities in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organisation. We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.	No comments.

CONTROL OBJECTIVE 5:

Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies, and overall action plan. The information security policy is maintained, taking the current risk assessment into consideration.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
There is a written strategy covering, among other things, Management's security objectives, policies, and overall action plan. The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organisation. The policy is available for all relevant employees. The policy is re-evaluated according to planned intervals.	We have obtained and audited ECIT Solutions A/S' latest IT security policy. During our audit, we checked that maintenance of the IT security policy is conducted on a regular basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented. We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on ECIT Solutions A/S' intranet.	No comments.

CONTROL OBJECTIVE 6:

Organisation of Information Security

Management of the IT security must be established in the company. Organisational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

Management must ensure a suitable level of protection for teleworking and the use of mobile devises.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Organisational responsibility for IT security has been placed, documented, and implemented. The IT security has been coordinated across the company's organisation.	Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented. We have checked that the IT security is deployed across the organisation in relation to Hosting activities. By conducting interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.	No comments.
Risks in relation to use of mobile devices and teleworking have been identified, and security issues in relation customers are managed.	We checked that formal policies exist in connection with the use of mobile devices and teleworking. On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices. Regarding the use of teleworking at ECIT Solutions A/S, we have checked whether appropriate security measures have been implemented thus this area is covered in relation to the risk assessment of the area.	No comments.

CONTROL OBJECTIVE 7:

Human Resource Security

It must be ensured that all new employees are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at ECIT Solutions A/S. This includes the framework laid down for the work and the IT security involved. Security responsibilities, if any, are determined and described in job descriptions and in the form of terms and conditions in the employment contract. The employees are familiar with their professional secrecy based on a signed employment contract and through ECIT Solutions A/S' HR policy.	We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to. Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment. Through interviews, we have checked that employees of significance to Hosting activities are familiar with their professional secrecy. We have on a test basis examined the job descriptions and employment contracts of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility. We have ensured that ECIT Solutions A/S' HR policy is easily accessible and has a section on terms for professional secrecy with respect to information obtained in connection with work conducted at ECIT Solutions A/S.	No comments.

CONTROL OBJECTIVE 8:

Asset Management

Necessary protection of the company's information assets must be ensured and maintained, all the company's physical and functional assets related to information must be indentified, and a responsible owner appointed. The company must ensure that information assets related to Hosting activities have an appropriate level of protection.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
All information assets have been identified and an updated list of all significant assets has been established. An "owner" of all significant assets is appointed in connection with the operation of Hosting activities.	We have examined and checked the company's central IT register for significant IT entities in connection with the operation of ECIT Solutions A/S' Hosting activities. Through observations and control, we checked relations to central knowhow systems for the operation of Hosting activities. By observations and enquiries, we have checked that ECIT Solutions A/S complies with all material security measures for the area in accordance with the security standard.	No comments.

CONTROL OBJECTIVE 9:

Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be secured, and unauthorised access must be prevented.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Documentation and updated directions exist for ECIT Solutions A/S' access control.	We have: • asked Management, whether access control procedures have been established at ECIT Solutions A/S. • verified on a test basis that access control procedures exist and have been implemented; see ECIT Solutions A/S' directions. • by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with ECIT Solutions A/S' directions, and authorisations are granted according to agreement.	No comments.
A formal procedure exists for granting and discontinuing user access. Granting and application of extended access rights are limited and monitored.	We have asked Management, whether a formal procedure exists for granting and discontinuing user access. We have by inspection on a test basis verified: • that adequate authorisation systems are used in relation to access control at ECIT Solutions A/S. • that the formalised business procedures for granting and discontinuing user access have been implemented in ECIT Solutions A/S' systems, and registered users are subject to regular follow-up.	No comments.
Internal users' access rights are reviewed regularly according to a formalised business procedure.	By inspection on test basis, we have verified that a formalised business procedure exists for follow-up on authorisation control according to the directions, including: • that formal management follow-up is performed on registered users with ordinary rights and extended rights every 12 months.	No comments.

The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.	We have asked Management whether procedures granting access code have been established at ECIT Solutions A/S. By inspection on a test basis, we have verified • that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login. • that standard passwords are changed in connection with implementation of systems software, etc. • if this is not possible, that procedures ensure that standard passwords are changed manually.	No comments.
Access to operating systems and networks are protected by passwords. Quality requirements have been specified for passwords, which must have a minimum length, requirements as to complexity, maximum duration, and likewise password setup means that passwords cannot be reused. In addition, 2-factor logon is a requirement. Furthermore, the user will be barred, in the event of repeated unsuccessful attempts to login.	We have asked Management whether procedures ensuring quality passwords in ECIT Solutions A/S are established. By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for: • minimum length of password • maximum life of password • minimum history of password • lockout after unsuccessful login attempts • 2-factor logon	No comments.

CONTROL OBJECTIVE 10:

Cryptography

There must be correct and efficient use of cryptography to protect information confidentiality, authenticity, and/or integrity.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
For encrypting personal data ECIT Solutions A/S has implemented an encrypting policy defining the strength and protocol of encrypting. Encryption is used when transmitting confidential and sensitive personal data via internet and e-mail.	Inspected the existence of formalized procedures ensuring that transmission of sensitive and confidential information via the internet is protected by strong encryption based on an approved algorithm. Inspected that encryption is applied when sensitive and confidential personal data is transmitted via internet or using e-mail. Inspected that technological solutions for encryption have been accessible and activated throughout the entire reporting period.	No comments.

CONTROL OBJECTIVE 11:

Physical and environmental security

There must be protection of the company's premises and information assets against unauthorised physical entry and against physical damage and disruption. Security steps must be taken to prevent loss of, damage on, or compromise of the company's information assets and to prevent disruption of the company's business activities, and finally to secure necessary supplies like power, water, and ventilation as well as cable installations.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Secure physical demarcation is established to protect the areas where hosting activities are operated. The secure areas are protected by entry control, only allowing entry for authorized persons. Monitoring is established of areas for loading and unloading, as well as of other areas with public access.	According to the service provider's description, the physical entry security is scrutinized and controlled based on the requirements decided by management. We have investigated and controlled the physical access to both data centres. They are secured, inter alia, by a chip card that ensures limited entry to ECIT Solutions A/S' data centres. Via visits, interviews, and observation we have controlled that the entry to both ECIT Solutions A/S' data centres comply with the above procedures regarding restricted admission. By applying sampling, we have investigated the procedures for physical security regarding secure areas to assess whether entry to these areas requires documented approval from Management, as well to assess whether persons without approval to secure areas must register and be accompanied by an employee with appropriate approval. By applying sampling, we have investigated employees with entry to secure areas and checked that their entry is granted according to the established procedures.	No comments.
Equipment placed in data centre is protected against physical threats like fire, water damage, power failure, theft, or vandalism. The data cells are secured against supply failure of power, water, heating, and ventilation. Equipment is installed to monitor indoor environment, such as air humidity. Cables for data communication and power supply are protected	We have investigated and controlled that ECIT Solutions A/S' data centres comply with the requirements established by Management. The audit has controlled the compliance with the necessary security measures, see ISO 27002, section 11 in conditions for protection against damage caused by physical conditions like e.g. fire, water damage, power failure, theft, or vandalism. Specifically, we have: • Verified the presence of fire fighting systems and cooling in data centres.	No comments.

against unauthorised interference. Equipment to be used in relation to hosting activities is maintained according to regulations to ensure availability and reliability.	• Verified that UPS and diesel generator are maintained and tested on an ongoing basis. • Observed during visit to data centre that UPS and diesel generator are monitored. • Verified the presence of equipment for monitoring the indoor environment in data centre. • Verified securing of cables for data communication and power supply. • By applying sampling, investigated documentation for ongoing maintenance of equipment for protection against physical threats.	

CONTROL OBJECTIVE 12:

Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs. Management has implemented policies and procedures to ensure satisfactory segregation of duties.	We have: • Asked Management whether all relevant operation procedures are documented. • In connection with our audit of the individual areas of operation verified on a test basis that documented procedures exist and that there is concordance between the documentation and the procedures actually performed. • Inspected users with administrative rights in order to verify that access is justified by work-related needs and does not compromise the segregation of duties.	No comments.
Management of operational environment is established in order to minimise the risk of technology related crashes. Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.	We have: Asked Management about the procedures and control activities performed. On a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.	No comments.

Control objective: Protection from malware To protect from malicious software, such as virus, worms, Trojan horses, and logic bombs. Precautions must be taken to prevent and detect attacks from malicious software.		
ECIT Solutions A/S' control procedures	Auditor's test of control procedures	Test findings
Preventive, detecting and remedial security and control measures have been established, including the required training and provision of information for the company's users of information systems against malicious software.	We have: • enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks. • enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks. • verified that anti-virus software has been installed on servers and inspected signature files documenting that they are updated.	No comments.

Control objective: Backup To ensure the required accessibility to the company's information assets. Set procedures must be established for backup and for regular testing of the applicability of the copies.		
ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Backup is made of all the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions.	We have: • asked Management about the procedures/ control activities performed. • examined backup procedures on a test basis to confirm that these are formally documented. • examined backup log on a test basis to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis. • examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored.	No comments.

Control objective: Logging and monitoring To reveal unauthorised actions. Business-critical IT systems must be monitored, and security events must be registered. Logging must ensure that unwanted incidences are detected.		
ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis. ECIT Solutions A/S logs when internal users log off and on the systems. Only in the event of suspected or identified abuse of the systems, users are actively monitored.	We have: • asked Management about the procedures/ control activities performed and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged. • checked on a test basis that logs from critical systems are subject to sufficient follow-up.	No comments.
A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur in order to react proactively. Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS. Status reports are sent by email from different systems. Some daily – others when incidents occur in the system. The operator on duty is responsible for checking these emails daily.	We have: • asked Management about the procedures/ control activities performed. • ensured that a monitoring tool is used and that this is available to all employees. • ensured that alerts are sent by email and SMS, if errors occur. • examined status reports. • ensured that an operator on duty is established and that this operator on duty checks reports on a daily basis.	No comments.

Control objective: Managing operations software

Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Changes in the operation environment comply with established procedures.	We have asked Management, whether procedures for patch management are established in ECIT Solutions A/S. By inspection on test basis, we have verified that • adequate procedures are applied, when controlled implementation of changes to the production environment of ECIT Solutions A/S is performed. • changes to ECIT Solutions A/S' operation environment comply with directions in force, including correct registration and documentation of applications about changes. On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.	No comments.
Changes in existing user systems and operation environments comply with formalised procedures and processes.	We have asked Management, whether procedures for patch management are established in ECIT Solutions A/S. By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that • applications for change are registered and described. • all changes are subject to formal impact assessments before implementation. • All changes are subject to formal impact assessments • fall-back plans are described • systems affected by changes are identified. • Documented test of changes is performed before they are put into operation • documentation is updated reflecting the implemented changes in all material respects. • procedures are subject to managing & coordination by a "Change Board"	No comments.

CONTROL OBJECTIVE 13:

Communications Security

To ensure protection of information in networks and ensure protection of support of information processing facilities.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Networks must be protected against threats in order to secure network-based systems and the transmitted data. Production environment must be secured against failing supply in relation to redundancy to network connection to the internet. Network traffic/access from production environment to the outside world is available by means of multiple supply entries or access from more than one supplier.	It has been checked that necessary protection against unauthorised access is implemented, including: • Appropriate procedures for managing network equipment are established. • Segregation of user functions is established. • Appropriate logging and monitoring procedures as well as follow-up are established. • Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level. • Ensured that connections for data communication with the internet are established via more than one ISP supplier. • On a sample basis gone through documentation from the suppliers about written basis for contract, as well as regular settlement of accounts for services rendered by the ISP suppliers.	No comments.
Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented. In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.	We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented. By inspection on a test basis, we have ensured: • that appropriate framework for managing cyber-attacks is devised. • that plans for managing the threat are devised and implemented. • that the plans include cross-organisational collaboration between internal groups.	No comments.

CONTROL OBJECTIVE 15:

Supplier Relationships

External business partners are obliged to comply with the company's established framework for IT security level.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Risks related to external business partners are identified, and security in third-party agreements are managed.	We have verified that in connection with the use of external business partners there are formal cooperation agreements. On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.	No comments.
In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected through collaboration between the Operations Manager and the IT Security Manager. Solely approved suppliers are used.	We have asked Management about relevant procedures applied in connection with selecting external partners. We have ensured that appropriate procedures for managing cooperation with external partners are established. We have tested that key suppliers have updated and approved contracts.	No comments.
Monitoring must be conducted on a regular basis, including supervision of external business partners.	We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers.	No comments.

CONTROL OBJECTIVE 16:

Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Security incidents are reported to Management as soon as possible, and the handling is performed in a consistent and efficient way.	We have asked Management whether procedures are established for reporting security incidents. We have verified that procedures and routines are devised for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organisation; see Directions. We have verified that the responsibility for the handling of critical incidents is clearly delegated, and that the related routines ensure that security breaches are handled expediently, efficiently, and methodically.	No comments.

CONTROL OBJECTIVE 17:

Information Security Aspects of Business Continuity Management

Business continuity management is to counteract interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements and to determine the prioritisation of tests and maintenance.	We have asked Management whether business continuity management has been devised for Hosting activities at ECIT Solutions A/S. By inspection on a test basis, we have verified • that appropriate framework for preparation of business continuity management has been established • that contingency plans are prepared and implemented • that the plans include business continuity management across the organisation • that the plans include appropriate strategy and procedures for communication with the stakeholders of ECIT Solutions A/S. • that contingency plans are tested on a regular basis • that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.	No comments.

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

Principles for processing personal data:

There is compliance with procedures and controls ensuring that collecting, processing, and storing of personal data are performed in accordance with the agreements for processing personal data.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
A uniform framework is established in the form of standard contracts, Service Level Agreements, as well as Data Processor Agreements or the like, containing an outline of the basis for processing personal data.	We have controlled the existence of updated procedures in writing for processing personal data, and that the procedures include requirements to legal processing of personal data.	No comments.
Only the kind of processing of personal data included in directions from Data Controller is performed.	We have controlled that Management ensures that processing of personal data is solely performed in accordance with directions. We have checked, using a sample consisting of a suitable number of processing that processing is performed according to directions.	No comments.
Management immediately informs the Data Controller, if Directions in the Data Processor's view is contrary to the General Data Protection Regulation or data protection provisions according to other EU legislation or the national legislation of the member states.	We have controlled that Management ensures that processing is reviewed and the existence of formalised procedures securing that processing of personal data is not performed against the EU General Data Protection Regulation or other legislation. We have controlled the existence of procedures for informing the Data Controller in cases when processing of personal data is deemed to be against legislation. We have controlled that the Data Controller was informed in cases when processing of personal data was deemed to be against legislation.	No comments.

Data Processing:

There is compliance with procedures and controls ensuring that personal data can be erased or returned if an agreement is entered with the Data Controller.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing with requirements about storing and erasing of personal data in accordance with the agreement with the Data Controller. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures for storing and erasing of personal data in accordance with the agreement with the Data Controller. We have checked that the procedures are updated.	No comments.
According to the agreement with the Data Controller, when processing of personal data is finished, data are • Returned to the Data Controller, and/or • Erased, when erasing is not against other legislation.	We have controlled that there are formalised procedures for handling the Data Controllers' data when processing of personal data is finished. We have controlled by random check using a suitable population of finished data processing cases that conducting the agreed erasing or returning of data is documented.	No comments.
There are procedures in writing including demands that personal data is only stored in accordance with the agreement with the Data Controller. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures ensuring that storing and processing of personal data are solely undertaken according to the Data Processor Agreements. We have checked that the procedures are updated. We have controlled on sample basis, whether documentation exists that data processing is conducted in accordance with the Data Processor Agreement.	No comments.

The Data Processor's responsibility:

There is compliance with procedures and controls ensuring that solely approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of Data Subjects and the processing of personal data, the Data Processor ensures adequate security of processing.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing including demands to the Data Processor in relation to use of sub-processors, including demands about Sub-processor Agreements and Directions. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures regarding the use of sub-processors, including demands about Sub-processor Agreements and Directions. Inspected that procedures are updated.	No comments.
For processing personal data, the Data Processor solely uses Sub-processors, who are specifically or generally approved by the Data Controller.	Inspected that the Data Processor has a complete and updated list of the sub-processors used. Inspected using a sample of 4 Sub-processor from the Data Processor's list that it is documented that the Sub-processor's data processing is included in the Data Processor Agreements – or in other ways approved by the Data Collector.	No comments.
When changing the generally approved sub-processors used, the Data Controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the Data Processor. When changing the specially approved sub-processors used, this must be approved by the Data Controller.	We have controlled that formalized procedures are in place for informing the Data Controller when changing the sub-processors used. Inspected documentation that the Data Controller was informed when changing the sub-processors used throughout the assurance period.	No comments.
The Data Processor has placed the same data protection obligations on the sub-processors as the obligations included in the Data Processor Agreement or similar document with the Data Controller.	We have controlled the existence of signed Sub-processor Agreements with all sub-processors used and included in the Data Processor's list. Inspected using a sample of 4 Sub-processor Agreement that the agreements include the same demands and obligations as stated in the Data Processor Agreements between the Data Controllers and the Data Processor.	No comments.

The Data Processor has a list of approved sub-processors including the following information: • Name • CVR.no. • Address • Outline of the processing	We have controlled that the Data Processor has a total and updated list of approved sub-processors used. Inspected that the list as a minimum includes the required information about each sub-processor.	No comments.

Assisting the Data Controller:

Procedures and controls are complied with to ensure that the Data Processor can assist the Data Controller in handing out, correcting, deleting, or restricting processing of personal data as well as providing information about the processing of personal data to the Data Subjects.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have controlled that formalised procedures are in place for the Data Processor's assistance to the Data Controller in relation to the rights of Data Subjects. Inspected that procedures are up to date.	No comments.
The Data Processor has established procedures in so far as this was agreed that enable timely assistance to the Data Controller in handing out, correcting, deleting, or restricting processing as well as providing information about the processing of personal data to Data Subjects.	We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for: • Handing out data; • Correcting data; • Deleting data; • Restricting the processing of personal data; • Providing information about the processing of personal data to Data Subjects. Inspected documentation that the systems and databases used support the performance of the said relevant detailed procedures.	No comments.

Records of processing activities:

There is compliance with procedures and controls ensuring that the Data Processor keeps records of processing personal data for which the Data Processor is responsible.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
There are records of the processing activities for each activity in Hosting activities in combination with the relevant Data Controller.	We have controlled documentation displaying the existence of records for processing activities for each activity in Hosting activities combined with the relevant Data Controller.	No comments.
Assessment is made on an ongoing basis – and at least once a year – that the records are updated and correct.	We have controlled the documentation disclosing that the records of the processing activities for each Data Controller are updated and correct.	No comments.

Reporting breaches of personal data security to the Supervisory Authority (the Danish Data Protection Agency):

There is compliance with procedures and controls ensuring that any security breaches are managed in accordance with the entered Data Processor Agreement.

ECIT Solutions A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing - updated at least once a year – describing how to manage personal data security breaches including timely communication to the Data Controller.	We have controlled the existence of updated procedures in writing regarding managing personal data security breaches, including description of timely communication to the Data Controller.	No comments.
Data Processor ensures recording of all personal data security breaches.	We have controlled documentation disclosing that all personal data security breaches are recorded at the Data Processor.	No comments.
Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	We have controlled documentation displaying that Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	No comments.

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."

Jesper Aaskov Pedersen
IT auditor, Director
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: 55a3ea90-967e-4a5c-b854-37be4db4517b
IP: 212.98.xxx.xxx
2025-01-31 16:29:14 UTC

Mit ID

Kim Holm Larsen
Beierholm Godkendt Revisionspartnerselskab CVR: 32895468
State-authorized Public Accountant
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2025-01-31 17:29:33 UTC

Mit ID

Kim Bahir Andersen
Managing Director
På vegne af: ECIT Solutions A/S
Serienummer: f0014b70-b15b-4e04-9368-4381c27345ad
IP: 188.180.xxx.xxx
2025-02-02 09:33:30 UTC

Mit ID

Rolf Wulff Ljungberg
Director of Operations
På vegne af: ECIT Solutions A/S
Serienummer: ac3ac967-fe1c-4712-8d30-6eb2a93dd905
IP: 82.163.xxx.xxx
2025-02-03 08:41:41 UTC

Mit ID