BEIERHOLM
VI SKABER BALANCE

JANUAR 2020

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

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

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

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

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

KAPITEL 1:

Ledelseserklæring

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

Medfølgende beskrivelse er udarbejdet til brug for kunder, 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 2019 - 31. december 2019. 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 2019 - 31. december 2019.

(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 2019 - 31. december 2019. 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 2019 - 31. december 2019.**

(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 Hosting**
(ii) **IT-sikkerhedsregler/ håndbog for ECIT Solutions Hosting (rammen efter ISO 27002-2017)**

Viby J, den 10. januar 2020

Mikkel Walde, CEO

Rolf Ljungberg, COO

ECIT Solutions A/S, Rudolfgårdsvej 1 B, DK-8260 Viby J, CVR 28843151

KAPITEL 2:

Beskrivelse af kontrolmiljøet for it-drift-ten 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 databehandling.

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 1998 af nuværende CEO Mikkel Walde. I dag beskæftiger virksomheden 43 medarbejdere inden for hosting.

ECIT Solutions leverer hostingaktiviteter til et bredt udvalg af større og mindre virksomheder. Alle leverancer udgår fra eget hostingcenter, som blev bygget i 2017 - og er skabt på baggrund af den nyeste viden inden for datacenter-teknologi og IT-sikkerhed. Med egne servere, transformerstation og generatorer fysisk placeret i eget hostingcenter - og fuldt ejerskab over alle kunde-dedikerede forbindelser ud af huset - har ECIT Solutions således fuld kontrol over alle delene af serviceleverancen. Det betyder, at løsninger altid kan skræddersyes til den enkelte kundes behov. Der tilbydes ydelser fra web- og mail-drift til komplekse løsninger af forretningskritisk IT for virksomheder, der kræver drift 24/7 året rundt.

Til hver enkelt kunde sammensættes det bedste serversetup ved valg mellem virtuelle og fysiske servere og evt. lokal server hos kunden til spejling af data. Virksomheden får desuden optimal sikring af servere og data, da vores datacenter er bygget på den nyeste teknologi inden for elektronisk adgangskontrol, videoovervågning, temperaturalarmer, røg/brandsensorer, klimastyring, UPS - og fordi vi har eget generatoranlæg, som producerer strøm. Datacenteret er modulært opbygget således, at der løbende kan tilføjes ekstra servere, CPU samt storage-kapacitet - på den måde får vores kunder en fleksibel leverance, som justeres i takt med kundens ændrede behov.

**ECIT Solutions har 21 års erfaring med IT-drift for mindre og mellemstore virksomheder.
Da alle leverancer udgår fra ECIT Solutions er medarbejderne opdaterede og specialiserede både i dybde og bredde. Det gør, at kunden kun skal henvende sig ét sted, hvis der opstår problemer eller behov for justeringer i den nuværende løsning - uanset om kunden ønsker on-premise, private cloud eller en hybrid cloud-løsning med integration til offentlig cloud f.eks. Office 365.**

ECIT Solutions har som mission at sikre kunden tryghed og høj driftsstabilitet i hele IT-infrastrukturen - derfor benyttes redundant infrastruktur til sikring af maksimal oppetid, sikker backup, dynamisk diskplads og agile servere, så leverancen til kunden bliver af højeste kvalitet uden at gå på kompromis med hverken sikkerhed eller fleksibilitet. På den måde kan virksomheder, der har valgt ECIT Solutions som IT-partner, koncentrere sig om deres kerneforretning uden bekymringer omkring deres IT-drift.

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

er AAA-rated, der sikrer, at virksomheden har en IT-leverandør, der har den fornødne robuste økonomi. Vi har desuden over en længere periode arbejdet målrettet med IT-sikkerhed og EU's nye persondata-forordning.

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 nærværende beskrivelse.

Forretningsstrategi/ IT-sikkerhedsstrategi

Det strategiske formål i ECIT Solutions er at indbygge den nødvendige sikkerhed i vores forretning, så selskabet ikke påføres uacceptable risici til ulempe for os og - ikke mindst - vores kunder.

ECIT Solutions har tre overordnede strategiske pejlepunkter:

- ECIT Solutions holder sig opdateret på den nyeste viden inden for moderne informationsteknologi med henblik på at hjælpe og vejlede virksomheder til en optimal brug af dette.
- ECIT Solutionss primære fokus er at arbejde med administrative systemer, netværksløsninger og internet/intranetløsninger
- ECIT Solutions er en god arbejdsplads for en stabil og veluddannet medarbejderstyrke, som har kontinuerlig mulighed for specialisering og udvidelse af eget kompetenceområde.

ECIT Solutions ønsker at være kundens uvildige, rådgivende partner inden for IT-sikkerhed, og prioriterer IT-sikkerhed på et forretningsstrategisk niveau - derfor arbejdes der løbende med at sikre et højt service- og kvalitetsniveau inden for dette område. Ledelsen prioriterer gennem selskabets sikkerhedspolitik, at IT-sikkerhed skal være og er en vigtig del af selskabets virksomhedskultur.

ECIT Solutions har omkring IT-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27002:2017, 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

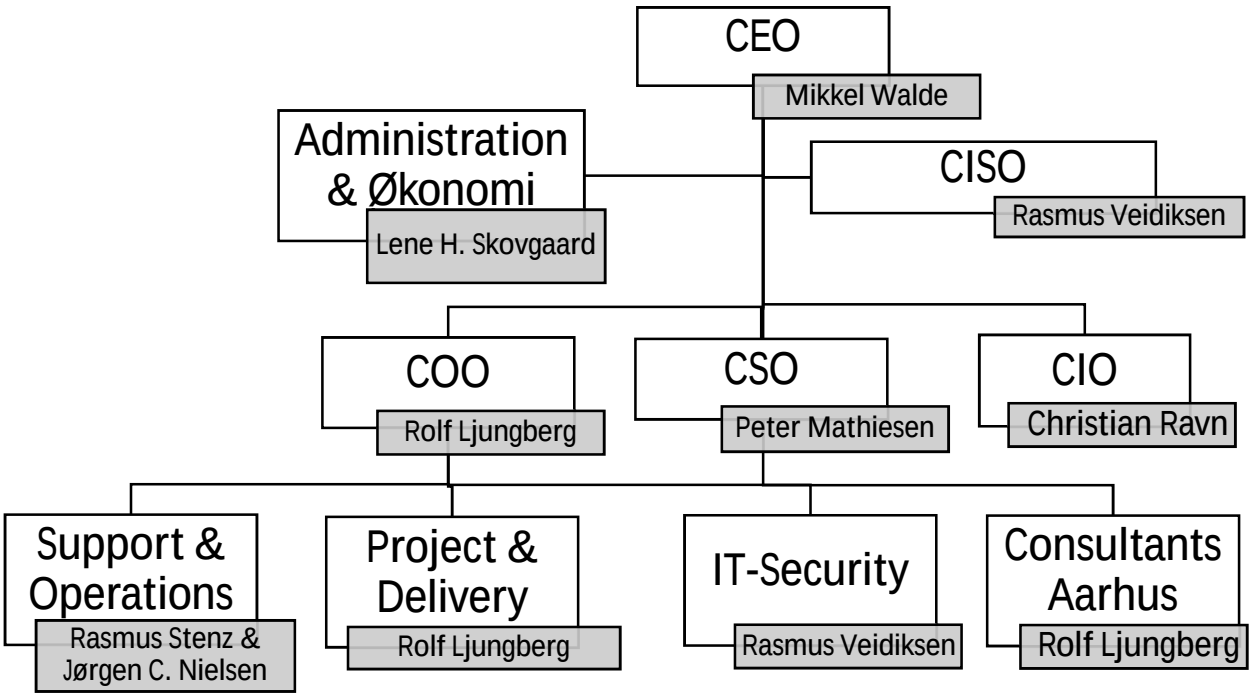
De implementerede kontrolmål og sikringsforanstaltninger hos ECIT Solutions A/S fremgår af bilag 1 til denne beskrivelse.

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

Overordnet ansvarlig er CEO, der har uddelegeret ansvaret for it-sikkerheden til Chief Information Security Officer.

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

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 2 årlige risiko- og trusselsvurderinger.

ECIT Solutions har indarbejdet faste procedurer for risikovurdering af forretningen og specielt hostingcentret. Vi sikrer dermed, at de risici, som er forbundet med de services, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderer relevante i forbindelse med at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderingen ligger hos direktør Mikkel Walde og skal efterfølgende forankres og godkendes hos virksomhedens øvrige ledelse.

Som led i ovenstående IT-sikkerhedsstrategi arbejder ECIT Solutions med de danske/internationale standarder for it-sikkerhed – ISO27002:2017 – som primær referenceramme for IT-sikkerheden. Arbejdsprocessen omkring IT-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at ECIT Solutions til hver en tid er i overensstemmelse med sine kunders krav og behov.

Håndtering af IT-sikkerhed

Chief Information Security Officer (CISO) hos ECIT Solutions har det daglige ansvar for IT-sikkerhed, og derved sikres det, at de overordnede krav og rammer for IT-sikkerhed er overholdt. 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 kunderne. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

ECIT Solutions' IT-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedshullet omgående.

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

Alle servere og netværksenheder er dokumenteret i ECIT Solutions' dokumentationssystem. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) ligger gemt i vores dokumentationssystem.

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

Sikkerhedspolitikken er udarbejdet, så ECIT Solutions har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager 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 Datacenter, Cloud Platform og SMV Cloud Solutions Silver Partner status hos Microsoft, hvilket kompetencemæssigt placerer os i den høje ende af IT-virksomheder.

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.

- Klassifikation af information
  Data klassificeres jævnfør procedurer for tildeling af sikkerhedsniveauer, data og ansatte.
- Styring af flytbare medier
  Kundedata overføres kun til hardwarekrypterede eksterne harddiske, der overholder Military Grade FIPS PUB 197 Validated Encryption Algorithm.
- Bortskaffelse af medier
  Aktiver, der fjernes, sikres at være fri for nogen form for data ved hjælp af ECIT Solutionss procedure for destruktion af datamedier. Proceduren sikrer tilintetgørelse af data på datamedier, når disse ikke længere skal anvendes.

Brugerstyring / adgangssikkerhed

Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne. For at sikre funktionsadskillelse benyttes stillingsbetegnelser. Der er forskel i rettigheder og funktioner mellem medarbejderne ud fra de pågældendes stillingsbetegnelser.

- Adgang til alle tjenester, der er eksternt tilgængelige, kræver login med 2-trins-validering.
- Krav til password - alle brugere oprettet i ECIT Solutions' centrale brugerdatabase skal have passwords på mindst 12 tal eller bogstaver, og de seneste 24 passwords kan ikke bruges igen.
- Krav om pauseskærm - pauseskærm er aktiveret for alle vores brugere, for at beskytte dem mod uautoriseret adgang.
- Forbindelser til kundens driftsmiljø sker igennem et administrationspunkt (jumphost), 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 alle adgange logges. Hostingmiljøet er delt op i 2 selvstændige rum. Adgang til hostinglokaler er kameraovervåget samt forsynet med branddøre med kortlås.
- Strømsikring
  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 kontoret.

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 endpoints for out-of-date definitioner og håndterer de enheder, det måtte være relevante 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' hostingcenter kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid.

Der tages backup af alle data i hostingcenteret. Backupdata kopieres dagligt til anden lokalitet, hvorved en disaster-backup bibeholdes på den anden lokalitet. ECIT Solutions kontroller periodisk kundernes backup ved at gennemgå logs på serveren.

ECIT Solutions har ansvaret for backup af virksomhedens servere og data. Der foretages dagligt snapshot-backup, som lagres i 30 eller 90 dage.

Logning og overvågning

Som en integreret del af løsninger fra ECIT Solutions leveres overvågning med i vores løsninger. Via vores ECIT Solutions Operations Center (MOC) 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 Hosting tilbyder central log-opbevaring, der sikrer, at firmaets log-filer opbevares i ECIT Solutions' eget danske datacenter i Aarhus.

ECIT Solutions' centrale log-infrastruktur gør det muligt at vælge hvilke oplysninger, der skal bevares, og i hvor lang tid. Med central log-opbevaring er der bedre mulighed for at efterforske en sikkerhedshændelse.

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 hostingkunder mod cyberkriminalitet, har vi indført følgende systemer:
Alle indgående mails skal igennem filtre, hvor de scannes og checkes af 2 uafhængige antivirus/malware producenter. Hvis der er tvivl, lægges mailen i karantæne.

Al internettrafik scannes og checkes med Host Intrusion Protection System. Dette indbefatter bl.a. både antivirus og Intrusion Prevention Service (IPS) for at sikre, at de data, der hentes og sendes, overhol-

der gældende standard og ikke er fyldt med ondsindet data. Hvis der findes mistænkeligt indhold, droppes datapakken, ellers lukkes brugerens internetadgang i 10 min. Det samme sker, hvis eksterne forsøger at portscanne vores firewalls. Her bliver deres ip-adresse også blokeret i 10 min.

For at de nødvendige tiltag kan tages til at begrænse nye angrebs tendenser. Så gennemgås alle IT-sikkerhedshændelser siden sidste møde og stikprøver fra malware logs på de månedlige IT-sikkerheds-udvalgsmøder.

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 ledelsesproces, 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.

Ved totalskade på et af serverrummene er der udarbejdet en plan for, hvad der skal ske, herunder indkøb af servere og harddiske til ECIT Solutions SAN. Herefter 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-Sikkerhedsafdeling regelmæssigt alle IT-sikkerhedspolitikker, evt. med inddragelse af relevante interessenter. ISMS revideres regelmæssigt af en uvildig, ekstern part, og revisionsrapporten deles med alle via på 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 har vurderet, at det ikke er nødvendigt at have en DPO.

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' 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 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

MultiHouse og M-Data er i 2019 fusioneret og har dannet ECIT Solutions. Dette har foranlediget et større arbejde med at identificere sikkerhedsniveauet og overenstemme disse. Dette projekt vil strække sig ind i 2020 hvorefter begge afdelinger vil benytte sig af de samme teknologier og procedurer samt have et fuld implementeret ISMS der dækker begge afdelinger, dette vil være implementeret på tværs af virksomhederne senest slut 2020.

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 ansvar.

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 ISO27002:2017

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
- 8.2. Klassifikation af information
- 8.3. Mediehåndtering

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

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
- 12.6. Sårbarhedsstyring

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
- 17.2. Redundans

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 driften af hostingaktiviteter i perioden 1. januar 2019 - 31. december 2019, 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 og tilhørende udsagn i kapitel 2 (inkl. bilag 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 ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om 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 2019 - 31. december 2019, 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 2019 - 31. december 2019, 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 2019 - 31. december 2019.

Beskrivelse af test 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 i databeskyttelsesforordningen er overholdt.

Søborg, den 10. januar 2020

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT auditor, Manager

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med ISAE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27002:2017.

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 2019 - 31. december 2019.

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 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og håndteretingen 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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 hostingaktiviteter. Vi har ved observationer og forespørgsler kontrolleret, at ECIT Solutions A/S overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationer og data i relation til hostingaktiviteter og den efterfølgende drift af hostingcenter er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed.	Vi har kontrolleret, at der er passende opdeling og tilhørende procedurer/forretningsgange ifm. beskyttelse omkring ejerskab mellem applikationer og data samt øvrige enheder i forhold til ECIT Solutions A/S' drift af hostingaktiviteter. Vi har kontrolleret, at kontrakter og SLA anvendes som et centralt værktøj til at sikre definition, adskillelse og afgrænsning mellem ECIT Solutions A/S' ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data. Derved påhviler der typisk kunden et eget ansvar med at sikre, at der er et passende beskyttelsesniveau på egne informationer og data.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.	Vi har: · forespurgt ledelsen om, hvilke procedurer/ kontrolaktiviteter der udføres. · stikprøvevist gennemgået procedurerne for destruktion af databærende medier til bekræftelse af, at de er formelt dokumenterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**
Adgange til operativsystemer og netværk er beskyttet med password. **Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (12 tegn), krav til kompleksitet, maksimal løbetid (max 90 dage), ligesom password-opsætninger medfører, at password ikke kan genbruges (husker de seneste 24 versioner).** **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**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**

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, samt sikrer, at der undgås forstyrrelser af virksomhedens forretningsaktiviteter. Beskyttelsesforanstaltningerne skal også omfatte destruktion af forældet eller beskadiget udstyr samt sikre 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 datacentre, som bl.a. sikres via et nøglesystem kombineret med personlig kode, 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Udstyr, som er placeret i datacenter, beskyttes mod fysiske trusler såsom brand, vandskade, strømafbrydelse, tyveri eller hærværk. Datacenteret 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 27002:2017 afsnit 11 i forholdene til beskyttelse mod skader forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.** **Det udstyr, der benyttes uden for datacentrene, beskyttes efter samme retningslinjer, som gælder for udstyr inden i datacenter, under hensyntagen til de særlige risici ved ekstern anvendelse.** **Alt udstyr med lagringsmedier kontrolleres for at sikre, at kritiske/følsomme informationer og licensbelagte systemer er fjernet eller overskrevet, når udstyret bortskaffes eller genbruges.**	**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.** · **gennemgået og kontrolleret de af ledelsen udarbejdede procedurer til bortskaffelse af udstyr tilknyttet driften af hostingaktiviteter.**	

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Styring af driftssoftware samt sårbarhedsstyring

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 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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"	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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 de transmitterede 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 anerkendte 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser

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 aftale.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 1underdatabehandler. fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 1 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**

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.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**
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.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren sikrer registrering af alle brud på persondatasikkerheden.	Vi har kontrolleret dokumentationen for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.