AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. FEBRUAR 2024 TIL 31. JANUAR 2025 OM BESKRIVELSEN AF DRIFT OG HOSTINGMILJØET OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

IT Confidence A/S

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. FEBRUAR 2024 TIL 31. JANUAR 2025 OM BESKRIVELSEN AF DRIFT OG HOSTINGMILJØET OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Til: Ledelsen i IT Confidence A/S
IT Confidence A/S' kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om den af IT Confidence A/S (serviceleverandøren) for hele perioden fra 1. februar 2024 til 31. januar 2025 udarbejdede beskrivelse i sektion 3 af drift og hostingmiljøet og de tilhørende kontroller, og om udformningen og den operationelle effektivitet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandørens ansvar

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

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed kontroller hos en serviceorganisation. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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

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

Begrænsninger i kontroller hos en serviceleverandør

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

Konklusion

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

a. at beskrivelsen af drift og hostingmiljøet og de tilhørende kontroller, således som de var udformet og implementeret fra 1. februar 2024 til 31. januar 2025, i alle væsentlige henseender er retvisende, og

b. at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet fra 1. februar 2024 til 31. januar 2025, og

c. at de testede kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt fra 1. februar 2024 til 31. januar 2025.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

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

København, den 1. april 2025

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. IT CONFIDENCE A/S' UDTALELSE

IT Confidence A/S udfører drift og hosting af it-løsninger med udgangspunkt i kundernes behov.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt drift og hostingmiljøet, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, når de opnår en forståelse af kunders informationssystemer, som er relevante for regnskabsaflæggelsen.

IT Confidence A/S anvender serviceunderleverandør. Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

IT Confidence A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af drift og hostingmiljøet og de tilhørende kontroller fra 1. februar 2024 til 31. januar 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for drift og hostingmiljøet, og hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant.
    - Relevante kontrolmål og kontroller udformet til at nå disse mål.
    - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner
2. Indeholder relevante oplysninger om ændringer i serviceleverandørens drift og hostingmiljøet foretaget fra 1. februar 2024 til 31. januar 2025.
3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af drift og hostingmiljøet og de tilhørende kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved drift og hostingmiljøet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

IT Confidence A/S bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt fra 1. februar 2024 til 31. januar 2025. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.
2. De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.
3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. februar 2024 til 31. januar 2025.

Kongens Lyngby, den 1. april 2025

IT Confidence A/S

Erik Schulz
Administrerende direktør

3. IT CONFIDENCE A/S' BESKRIVELSE AF DRIFT OG HOSTINGMILJØET

Denne beskrivelse er udarbejdet med henblik at give oplysninger til aktuelle samt potentielle kunder og deres revisorer. Beskrivelsen indeholder oplysninger om kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402.

IT Confidence's serviceydelser
IT Confidence A/S (herefter ITC) har siden begyndelsen af 2020 arbejdet professionelt med leverance af konkurrencedygtige IT-løsninger med udgangspunkt i kundernes behov.

ITC er vokset i takt med tilgangen af nye kunder, og er vokset støt og roligt siden begyndelsen. I dag er ITC en velkonsolideret virksomhed med mange nye kunder. I takt med kundetilgangen har ITC etableret et datacenter med henblik på at levere konkurrencedygtige hosting- og serviceydelser.

ITC's Datacenter leverer følgende ydelser:

- Hostede Virtuelle Servere
- Hostede Netværk
- Remote backup

Denne kontrolbeskrivelse omhandler ovenstående serviceydelser.
Foruden ovenstående ydelser leverer ITC også assistance på følgende områder.

- Generel IT-support
- IT-konsulentbistand indenfor IT-infrastruktur
- Drift af lokale server, enheder og netværksudstyr
- Rådgivning på flere niveauer.

A.4 – Risikovurdering og håndtering
I ITC forstår vi, at der en risiko ved alle ændringer i og omkring vores datacenter. Derfor opvejes altid de potentielle skader en opgave/ændring kan forvolde, samt hvor sandsynlig at skaden indtræffer. Risiko er vurdereret ud fra skade omfang samt sandsynlighed. ITC's risikovurdering bliver årligt gennemgået og der bliver truffet de nødvendige tekniske og organisatoriske foranstaltninger i form af kontroller og procedurer, som passer til de identificerede risici i vurderingen. Ansvaret for risikovurderingen ligger hos ledelsen.

A.5 – Informationssikkerhedspolitik
ITC har udarbejdet politikker for virksomhedens informations- og IT-sikkerhed. Disse politikker indeholder regler og retningslinjer for omgangen med bl.a. leverandører, kunder, brugere, medarbejdere, teknologi, netværk, fysisk og digital adgang til data, drift, sikkerhedshændelser mm. Informations- og IT-sikkerhedspolitikkerne er godkendt af ledelsen og gennemgås én gang årligt, samt i tilfælde af væsentlige ændringer. Dokumentation, kontroller og procedurer understøtter informationssikkerhedspolitikken.

A.6 – Organisering af informationssikkerhed
ITC har udarbejdet politikker for organisering af informationssikkerheden, som revideres minimum én gang årligt. Der er desuden lavet en ansvarsfordeling af informationssikkerheden for specifikke områder i informationspolitikken.

Sikkerhedsudvalget har konkrete ansvarsområder og har til opgave at sørge for, at sikkerhedskrav og -regler overholdes, gennemgå risikovurdering og IT- og informationssikkerhedspolitikker, samt beredskabssituationer. Desuden sørger udvalget for, at relevante informationer og aftaler videregives og udarbejdes med medarbejdere, kunder og leverandører.

Funktionsadskillelse
ITC funktionsadskiller med det formål at beskytte og opdele kundens data, så der kun gives adgang til relevante personer med konkret arbejdsrelateret behov. Sletning af persondata er i projektudvikling underlagt ændringsstyring, hvor ITC som Databehandler, er underlagt underretningspligt overfor den Dataansvarlige. Organisatorisk er ITC opdelt i forskellige områder så som drift, support, udvikling og administration, hvor medarbejdere tildeles rettigheder, som matcher deres arbejdsområde. Funktionsadskillelse sikres for kritiske systemer og data ved tildeling af brugerrettigheder efter et arbejdsbetinget behov. ITC har implementeret procedurer for administration af brugeradgange og brugerroller. Det er desuden fastlagt i rotationsplan at gennemgå brugerrettigheder i virksomheden. Funktionsadskillelse implementeres blandt andet ved anvendelse af Active Directory (AD), kildekodesystem, kundefaktureringssystemet og Office365 igennem hovedsageligt rollebaseret rettighedsstyring, hvor hver enhed, gruppe eller rolle har unikke rettigheder, begrænsninger og adgange, som står mål med medarbejderens funktioner og behov. ITC følger med i IT-sikkerhedsrelaterede aktiviteter i branchen gennem brancheorganisation og IT-relaterede nyhedskanaler. Samtidig modtager nøglemedarbejdere sikkerhedsvarsler på e-mail ved opdagede sikkerhedsbrud i anvendte standard-systemer.

På projektplan
Informationssikkerheden er en integreret del af projektudviklingen, uanset projekttype. I den forbindelse udarbejdes der også risikovurderinger i forhold til sikkerheden, hvor potentielle sikkerhedsrisici identificeres for nye projekter. Det er projektchefernes og projektledernes ansvar, at ITC som databehandler, overholder informationssikkerheden på projektstyringsplan. Indgåelse af databehandleraftaler med kunder er en del af informationssikkerheden.

Mobilt udstyr og fjernarbejdspladser
ITC har udarbejdet politikker og sikkerhedsforanstaltninger vedr. brugen af mobilt udstyr og arbejde ude af huset. Data tilgås via fællesdrevet, som er beskyttet med unik brugeradgang. Personalet skal følge personalehåndbogen og IT-håndbogens retningslinjer for omgang med udstyr.

A.7 – Personalesikkerhed

Før ansættelse
Ny ansættelser foretages både på egen hånd og i samarbejde med rekrutteringsbureauer. Ud over personernes tekniske kundskaber, vurderes endvidere personens serviceniveau, integritet og pålidelighed. Personens CV-gennemgås i detaljer og eventuelle referencer kontaktes. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.

Under ansættelse
Medarbejderes kundskaber vurderes løbende i forhold til deres respektive ansvarsområder og opgaver. Uddannelse tilbydes jf. beskrivelsen i ITCs Personalehåndbog. I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. Heri er den pågældendes stillingsbeskrivelse ligeledes klart defineret. På ugentlige møder samles der op på den forgangene uge samt nyt tiltag eller vigtige sikkerhedsemner.

Ophør og ændring i ansættelse
Når en medarbejder stopper i ITC bliver alle redskaber, herunder mobil og bærbar returneret til ITC og alle adgange til ITC og eventuelle kundesystemer, bliver lukket ned. En overleveringssamtale sikrer at al nødvendig viden, som den pågældende måtte ligge inden med, bliver videregivet og dokumenteret. Medarbejdere er underlagt deres tavshedspligt også efter ophør af deres ansættelseskontrakt

A.8 – Styring af aktiver

Ansvar for aktiver
ITC har udarbejdet fortegnelser over både fysiske aktiver samt væsentlige softwareaktiver. Dette for at kunne spore og håndtere aktivernes sikkerhed og drift. Ejeren af aktiverne fremgår af fortegnelserne. Ejeren er ansvarlig for den daglige drift og vedligeholdelse af systemerne.

ITC har udformet og implementeret regler og retningslinjer for acceptabel håndtering og brug af aktiver, fx arbejdsstationer. Der er desuden fastlagt procedurer for sikker udlevering og tilbagelevering af udstyr. Mediehåndtering ITC har retningslinjer og politikker for brug, bortskaffelse og tilbagelevering af aktiver, fremmedudstyr, styring af bærbare medier og for bortskaffelse af medier.

A.9 - Adgangsstyring

Forretningsmæssige krav til adgangsstyring

ITC har politikker for adgangsstyring til systemer og data, som revideres årligt. De fysiske omgivelser på kontoret er begrænsede med ADK (adgangskontrol). Det samme gør sig gældende for serverlokationen, hvor kun autoriseret personale har adgang. Adgang til systemer og data tildeles alene brugere med et arbejdsrelateret behov. Der er hertil udarbejdet procedurer for oprettelse og håndtering af brugeradgange.

Brugerens ansvar

Der er fastlagt politikker og konkrete regler for medarbejdernes ansvar i forbindelse med håndtering af logininformation og adgangskoder. Det er kun medarbejdere med arbejdsrelaterede behov, som har adgang til det interne netværk.

Styring af hemmelig autentifikationsinformation

Den hemmelige autentifikationsinformation for system- og servicebrugere opbevares som en del af Active Directory (AD), og andre vigtige adgangskoder opbevares i beskyttet form i et dedikeret adgangskodesystem. Her er det kun brugere med særligt arbejdsbetinget behov, som har adgang til koderne. Adgang til adgangskodesystemet tildeles af den IT-ansvarlige. Tildeling af rettigheder til adgangskodesystem gennemgås mindst én gang årligt.

Administration af brugeradgang, brugerrettigheder og styring af system- og applikationsadgang

Ledelsen eller systemejer autoriserer tildeling af adgange. Brugerne er påkrævet at skifte adgangskode ved første log-on i de systemer, som understøtter denne funktion, ellers har ITC fastlagt adgangskodepolitikker. Der er implementeret faste procedurer for oprettelse af brugere, tildeling af brugeradgange, opsætning af brugerrettigheder og sletning af brugere. Adgang til systemerne er baseret på Windows-login (AD), hvor der anvendes personlige adgangskoder, som medarbejderen selv vælger i overensstemmelse med adgangskoderreglerne. Efter Windows-login er der adgang til interne systemer, som styres og overvåges i AD. Mindst hvert halve år skifter medarbejderne deres login med ny adgangskode, hvilket AD påtvinger. Når arbejdsstationer forlades, er der sikret anvendelse af skærmlås. Ved ophør af et ansættelsesforhold deaktiveres brugeren i alle tildelte systemer.

Styring af privilegerede adgangsrettigheder

Tildeling af privilegerede adgangsrettigheder sker ud fra et arbejdsbetinget behov, hvor ansøgning om adgang skal godkendes af den ansvarlige ledelse for medarbejderens område. Privilegerede adgangsrettigheder gives til en unik brugerkonto, så brugerens handlinger kan identificeres. Desuden registreres tildelingen af rettigheder via ticketsystem. Adgange gennemgås én gang årligt af systemejer.

Sikkert log-on

Der er retningslinjer for personalet i forhold til sikkert log-on. Det er eksempelvis en integreret del af operativsystemet AD, at log-on kræves og udskiftes jævnligt. Ved flere fejlede log-on forsøg låses brugerkonto automatisk ved systemer, som understøtter denne funktion. Ved låsning af konto, der ikke kan tilskrives brugeren, registreres dette i hændelseslog. Her låses kontoen op, og adgangskode udskiftes. Log-on-forsøg logges centralt i de enkelte systemer.

Adgangsrettigheder - eksternt samarbejde

Det fremgår i databehandleraftalen, hvilke brugerrettigheder der gør sig gældende for samarbejdet med kunden. En procedure understøtter administrationen af medarbejderes, underdatabehandleres og leverandørers adgang til personoplysninger. Leverandører og underdatabehandlere har ikke direkte adgangsrettigheder til data. Der er udarbejdet databehandleraftaler/fortrolighedserklæringer med de parter, som kan få adgang til persondata. Dette afhænger af dataklassificering.

Begrænset adgang til informationer
Adgang til systemer og filsystem er bestemt af arbejdsbetinget behov. Tildeling af adgang autoriseres af virksomhedens ledelse og/eller systemejer, hvor ansøgeren søger om adgang til pågældende system. Adgangsrettigheder gennemgås minimum én gang årligt.

Brug af privilegerede systemprogrammer - centrale systemer
Anvendelse af privilegerede systemprogrammer på servere kræver administrative rettigheder, hvilket i de fleste tilfælde er den IT-ansvarlige og systemadministratorer. Det er derfor kun medarbejdere med arbejdsbetinget behov, der har adgang til privilegerede systemprogrammer. Anvendelse af privilegerede systemprogrammer på servere logges og overvåges.

Håndtering af kildekoder
Kildekoder håndteres i et system for kodestyring og versionsstyring. Her er adgang begrænset til arbejdsrelaterede behov og baserer sig på bruger/gruppe-styring.

A.10 – Kryptografi
Vi har en formel politik for anvendelse af kryptografi til beskyttelse af data og forbindelser, samt administrering af krypteringsnøgler. Vi foretager kryptering i den grad det giver mening i forhold til den pågældende tjeneste og/eller enhed. Beslutningen træffes af den øverste ledelse.

Sikker bortskaffelse eller genbrug af udstyr
Ved bortskaffelse, reparation eller genbrug af IT-udstyr sikres det, at udstyret er forsvarligt renset for alle data. Når IT-udstyr bortskaffes eller på anden måde udskiftes, slettes alle data på en sådan måde, så de ikke kan gendannes. Der er udarbejdet procedure for dette.

A.12 – Driftsikkerhed
Politik for driftssikkerhed er fastlagt og revideres årligt.
ITC håndterer selv driften og backup på egne servere. Ekstern backup håndteres af backupleverandør. Logning af interne servere håndteres internt, hvorimod eksterne servere og backup i andre EU-lande håndteres og logges af ekstern leverandør. ITC sikre at indhente relevante IT-revisionserklæringer fra virksomhedens underleverandører, årligt.

Driftsprocedurer
Procedurebeskrivelser eller arbejdsinstrukser understøtter arbejdet med rutinemæssige opgaver og systemer. Der foretages desuden logning og overvågning af driftssystemer. I forbindelse med driften udføres der løbende overvågning og opfølgning af log, fejlmeddelelser og alarmer, som sikrer, at afvikling af driften og eventuelle rettelser af fejl sker rettidigt og med så få gener for brugerne som muligt. Overvågningen foretages af IT-afdelingen, der kan tage stilling til eventuelle problemer og involvere de rigtige parter. Alle systemhændelser registreres og gemmes i 6 mdr., dog afhængig af systemets logningsmuligheder. Der er udarbejdet instruktioner til genetablering af driftskritiske systemer, hvilket er en væsentlig del af beredskabssituationer.

Ændringsstyring
Alle ændringer udgør en risiko. ITC vurderer derfor, hvad der kan gå galt ved implementering af en ændring og hvad sandsynligheden er for at det vil ske. ITC foretager løbende risikovurderinger af de ydelser ITC leverer. Derudover foretages kontrol af alle ændringer jf. ITC Change Management politik. Formålet med ITC Change Management politik er at kontrollere og sikre at ændringer foretages med et minimum af afbrydelser i driften. ITC Change Management politik gør ITC i stand til at følge ændringer, godkendelser og eventuelle problemer og hændelser i forbindelse med implementerede ændringer. Ændringer skal godkendes af et Change Advisory Board, der varierer alt efter hvilken ændring, der forespørges på.

Kapacitetsstyring
Kapaciteten i ITC's datacenter udvides løbende efterhånden, som eksisterende kunders behov stiger og nye kunder kommer til. Således foretages løbende gennemgang af kapacitet og optimeringsmuligheder af konsulent-teamet samtidig med at ITC's interne overvågningssystem advarer om grænseværdier, der er ved at blive overskredet.

Malwarebeskyttelse
Alle enheder tilsluttet ITCs netværk er som udgangspunkt beskyttet mod malware. Der er på alle enheder muligt installeret et antivirusprogram. Antivirusprogrammer opdateres automatisk med signaturfiler og virusdefinitioner. Ved adgang til ITCs netværk via fjernopkobling kontrolleres antivirusprogrammer for at tjekke, om de er opdaterede og aktive.

Backup
ITC foretager sikkerhedskopiering af kritiske servere og data. Der foretages daglig sikkerhedskopiering af data på alle driftsservere. Omfang og frekvens for sikkerhedskopiering er fastsat ud fra en risikovurdering og beskrevet i informationssikkerhedspolitikker og systemdokumentation. Systemejer er ansvarlig for implementering af passende sikkerhedskopiering. Sikkerhedskopiering sker til en ekstern leverandør. Data i sikkerhedskopier er krypteret under opbevaring og transmission mellem kilde og backup-system. Status for sikkerhedskopiering kontrolleres dagligt og dokumenteres i ITCs driftsdokumentation. ITC har etableret procedurer for systematisk test af sikkerhedskopiering.

Logning og overvågning
Konsulentafdelingen er ansvarlig for at logge hændelser i kritiske systemer. Logning sker via interne systemværktøjer, men ekstern overvågning af internetbaserede services kan også foretages, hvis dette er aftalt med kunden. Kun autoriseret personale har adgang til hændelseslogning og overvågningsinformation. Administratorlogs overvåges og gennemgås periodisk - både i form af stikprøver, samt årlig gennemgang fastlagt i rotationsplan. Alle serverure synkroniseres, så hændelser, dokumentation og kontroller foretages entydigt. Procedurer for hændelseslogninger og overvågning er etableret og følges

Styring af software på driftssystemer
Installation af software fortages kun af ITCs konsulenter med de fornødne rettigheder til det pågældende system. Kundespecifikke programmer som ønskes afviklet fra vores datacenter bliver evalueret i forhold til ITCs sikkerhedspolitik. Opdatering af software herunder sikkerhedsopdateringer, foretages efter instrukser fra system-ejer og den tekniske direktør i tilfælde af opdatering af host-systemer.

Styring af tekniske sårbarheder
ITC holder sig opdateret omkring sårbarheder via fora, sociale medier, nyhedsbreve og Microsoft. Eventuelle risici bliver omdelt i organisationen på den til enhver lejlighed hurtigste facon (mobil, SMS, opkald, e-mail, Teams mv.) og nødvendige tiltag foretages omgående. ITC anvender værktøjer til scanning for sårbarheder i netværket og på servere. Der udføres port-scanninger mod servere samt test af kendte sårbarheder på servere. Af andre tekniske foranstaltninger foretages der løbende sikkerhedstests af virksomhedens drift, og risikovurderinger udarbejdes på standardopsætninger, herunder servere, arbejdsstationer, andre enheder inkl. kontrolleret software og applikationer.

A.13 - Kommunikationssikkerhed
Der er udarbejdet politikker for netværkssikkerhed og informationsoverførsel, som revideres årligt.

Netværkssikkerhed
Adgang til netværksenheders konfiguration er kun tildelt medarbejdere med et arbejdsbetinget behov, hvilket er den IT-ansvarlige og systemteknikerne. Al indkommende trafik er som standard blokeret, og der åbnes kun for porte, hvor der er behov for kommunikation. ITC opdeler netværk i WAN, LAN og DMZ, hvor bindeleddet er de kombinerede firewalls og routere. I det trådløse netværk er der to forskellige netværk. Et til internt brug og et gæstenetværk til separat brug med begrænset adgang til netværket. Det trådløse netværk benytter sikker godkendelse og kryptering af data. Der er etableret firewall-løsninger, der beskytter mod forbindelser til

usikre netværk. Der etableres udelukkende forbindelser fra internettet til godkendte services på servere i DMZ. Der sker løbende overvågning af netværket for at spore, udbedre og undgå sikkerhedsbrister. Overvågningen er fastlagt i rotationsplan.

Informationsudveksling
Der er udarbejdet politikker for information via elektroniske meddelelser (e-mail). Ekstern adgang til systemer og databaser sker gennem sikret firewall, samt eksterne kommunikationsforbindelser er krypterede. ITC har en oversigt over hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk og det er indført i fast rotationsplan at opdatere denne oversigt. Selvom det er tilladt, at medarbejderen bruger sin e-mail til privat brug, forbeholder ITC sig retten til at skaffe sig adgang til data/mails på kontoen, hvis dette sker af forretnings-, drifts-eller sikkerhedsmæssige hensyn.

A.15 - Leverandørforhold

Der er fastlagt politikker for håndtering af leverandører, som gennemgås årligt. Der indgås databehandleraftaler med leverandører, hvor behandling af persondata er en del af aftalen. Disse aftaler inkluderer information om sikkerhedsforanstaltninger, der skal følges både for databehandlerens og leverandørens side. Der er udarbejdet procedure for indgåelse af databehandleraftale samt tilsyn med leverandører. I indgåelse af aftale med ny leverandør laver ITC en screening af leverandøren, og det sikres, at der er indgået databehandleraftaler med leverandøren, eller at leverandøren kan fremvise dokumentation for uafhængig IT-revision, hvis det anses som nødvendigt. I forbindelse med det årlige interne review gennemgås leverandøraftaler med forretningskritiske leverandører. ITCs ledelse godkender ændringer af leverandørydelser, som er forretningskritiske.

A.16 – Styring af informationssikkerhedsbrud

I tilfælde af brud på sikkerheden, følger ITC deres beskrivende og formaliseret procedurer og dokumentation. Dette er let tilgængeligt for alle medarbejder, samt let forståeligt.

Rapportering af sikkerhedshændelser og svagheder
Medarbejdere har pligt til at indrapportere sikkerhedshændelser og -svagheder til ledelsen eller IT-ansvarlige. Herefter er det ledelsens og den IT-ansvarliges ansvar at viderebringe information vedr. sikkerhedsbruddet. Den IT-ansvarlige sørger for hændelseslog, hvilket der er udarbejdet procedurer for til de relevante systemer. Alle informationssikkerhedshændelser, svagheder og brud registreres i hændelsesloggen. Informationssikkerhedshændelser vurderes i forhold til potentielle risici for, om hændelsen kan ske igen. Her bestemmes den fremtidige håndtering af hændelsen. Dette gøres som en del af hændelsesdokumentationen. Ved alvorlige sikkerhedshændelser afholdes retrospektmøder for at minimere risikoen for gentagelser. ITCs ledelse gennemgår årligt hændelsesloggen og iværksætter forbedringer af informationssikkerheden.

Procedurer
For at efterleve informationssikkerheden følges formaliserede procedurer og handlingsplaner for sikkerhedshændelser. Disse planer dækker både, hvordan hændelsen skal håndteres i situationen samt efterfølgende. Ligeledes fremgår det, hvem der skal informeres om hændelsen, fx kunden og/eller Datatilsynet

A.17 - Informationsaspekter ved nød-, beredskabs- og retableringsstyring

Der er på baggrund af risikovurdering etableret en plan for informationssikkerhedskontinuitet i form af en beredskabsplan. ITC har udarbejdet en praktisk og fyldestgørende beredskabsplan, som indeholder informationer, handlingsplaner og reetableringsplaner for forskellige typer hændelser. Beredskabsplanen holdes løbende opdateret for at være tidssvarende og effektiv. Planen skrivebordstestes og revurderes årligt. Beredskabsplanen testes hvert 3. år. Al personale har adgang til beredskabsplanerne.

Beredskabsplanen omfatter:

- Skadebegrænsende tiltag
- Etablering af nødløsninger

- Genetablering af permanent løsning

Der er etableret handlingsplaner for følgende scenarier:

- Oversvømmelse, brand/vandskade, indbrud/ødelæggelse af udstyr, fysisk terror/indtrængen
- Kortvarigt strømsvigt
- Langvarigt strømsvigt eller internetsvigt
- Medarbejdere i ITC begår ulovlige handlinger/ødelæggelse
- Interne servere og systemer
- Eksterne services
- Virus- eller hackerangreb

Beredskabsplanen er tilgængelig for al personale og er lagret elektronisk på fælles drev samt i fysisk udgave hos administrationen.

ÆNDRINGER I PERIODEN FRA 1. FEBRUAR 2024 TIL 31. JANAUR 2025

IT Confidence har foretaget følgende væsentlige ændringer i drift og hostingmiljøet og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden fra 1. februar 2024 til 31. januar 2025:

- IT Confidence har udskiftet deres datacenter i løbet af erklæringsperioden.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

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

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

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

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt fra 1. februar 2024 til 31. januar 2025.

Udførte testhandlinger

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

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

For de ydelser, som Cibicom A/S leverer inden for hosting, har vi modtaget ISAE 3402 vedrørende serviceunderleverandørens kontroller.

For de ydelser, som Adeo Datacenter ApS leverer inden for hosting, har vi modtaget ISAE 3402 vedrørende serviceunderleverandørens kontroller.

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

Resultat af test

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

En afvigelse foreligger, når:

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

A.4: Risikovurdering og -håndtering

Kontrolmål

- *Formålet er at sikre, at virksomheden periodisk foretager en analyse og vurdering af IT-risikobilledet.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering - ITC gennemfører løbende risikovurdering af informationssikkerheden. Risikovurderingen gennemføres mindst én gang årligt. - For alle identificerede risici, er der truffet passende tekniske og organisatoriske foranstaltninger i form af kontroller eller procedurer. - Ved væsentlige ændringer i ITCs systemer, organisation eller ændring i trusselsbilledet gennemføres der en fornyet risikovurdering af selskabets informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at risikovurderingen er gennemgået i revisionsperioden og observeret, at denne er blevet gennemgået den 16. maj 2024. Vi har inspiceret, at IT Confidence har gennemført en risikovurdering af informationssikkerheden med passende tekniske og organisatoriske foranstaltninger. Vi har inspiceret, at IT Confidence minimum én gang årligt, gennemgår risikovurderingen eller ved organisatoriske ændringer eller ved ændringer i trusselbilledet.	Ingen afvigelser konstateret.

A.5: Informationssikkerhedspolitikker

Kontrolmål

- *At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for informationssikkerhed - Ledelsen har udformet og implementeret politikker for informationssikkerhed. Sikkerhedspolitikken er godkendt af ledelsen. - Informationssikkerhedspolitikker gennemgås og revideres årligt som en del af ITCs årshjul eller ved væsentlige ændringer i system, organisation eller trusselsbillede. - Sikkerhedspolitikken er gjort tilgængelig for medarbejdere.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har implementeret IT Sikkerhedspolitik for informationssikkerheden, hvoraf fremgår gyldighed, samt ledelsen har godkendt IT Sikkerhedspolitikken. Vi har inspiceret, at gennemgang af sikkerhedspolitikken er foretaget den 6. maj 2024. Vi har inspiceret, at It-sikkerhedspolitikken er tilgængelige på fællesdrev.	Ingen afvigelser konstateret.

A.6: Organisation af informationssikkerhed

Kontrolmål

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed I organisationen.*
- *At sikre fjernarbejdspladser og brugen af mobilt udstyr.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Roller og ansvarsområder for informationssikkerhed ▶ De organisatoriske ansvarsområder for informationssikkerhed, herunder ansvar, beføjelser, ramme og roller, er defineret, og ansvarlige med de nødvendige kompetencer er udpeget. ▶ ITC har udpeget sikkerhedsudvalg med ansvar for at sikre overholdelse af relevante regler og sikkerhedskrav. ▶ Sikkerhedsudvalget informerer medarbejdere, kunder og leverandører om relevante aftaler og informationer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har dokumenteret organisatoriske ansvarsområder, herunder ansvar, beføjelser, ramme og roller, og de nødvendige kompetencer er udpeget. Vi har inspiceret, at IT Confidence har udpeget et sikkerhedsudvalg.	Vi har konstateret at IT Confidences sikkerhedsudvalg ikke har informeret medarbejdere, kunder og leverandører om relevante aftaler og informationer i erklæringsperioden. Ingen yderligere afvigelser er konstateret.
Funktionsadskillelse ▶ Funktionsadskillelse sikres for kritiske systemer og data ved tildeling af brugerrettigheder efter et arbejdsbetinget behov. ▶ Funktionsadskillelse sikres ved hjælp af rollebaseret rettighedsstyring.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har implementeret funktionsadskillelse for adgang til kritiske systemer og data, efter et arbejdsbetinget behov. Vi har inspiceret, at IT Confidence har funktionsadskillelse ved hjælp af rollebaseret rettighedsstyring.	Ingen afvigelser konstateret.
Projektstyring ▶ Alle projekter risikovurderes som del af projektudviklingsprocessen. Risikovurderingen dokumenteres i projektdokumentation.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret politikker for risikovurdering i forbindelse med projektudviklingsprocessen. Vi har inspiceret at IT Confidence har udarbejdet en risikovurdering i forbindelse med projektudviklingsprocessen.	Ingen afvigelser konstateret.

A.6: Organisation af informationssikkerhed

Kontrolmål

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed I organisationen.*
- *At sikre fjernarbejdspladser og brugen af mobilt udstyr.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Mobilt udstyr og fjernarbejdspladser. - ITC har udformet og implementeret politikker for anvendelse af mobilt udstyr. - Politikker er gjort tilgængelige for medarbejdere i personalehåndbog og it-håndbog. - Alle mobile enheder er beskyttet med adgangskode.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret politikker for anvendelse af mobilt udstyr. Vi har inspiceret at It-sikkerhedspolitikken er tilgængelig for medarbejderne. Vi har inspiceret, at alle mobile enheder, Windows arbejdsstationer og smartphones, er beskyttet med adgangskode.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for personalesikkerhed ▶ Politik for personalesikkerhed er fastlagt og dokumenteret. ▶ Politikker for personalesikkerhed er godkendt af virksomhedens ledelse. ▶ Politikken revideres minimum én gang årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har fastlagt og dokumenteret politikker for personalesikkerhed. Vi har inspiceret, at IT Confidence ledelse har godkendt politikker for personalesikkerhed. Vi har inspiceret, at politikken er gennemgået i revisionsperioden.	Ingen afvigelser konstateret.
Før ansættelse ▶ ITC har implementeret faste procedurer for ansættelse af medarbejder ▶ Kandidater bliver før ansættelse screenet og vurderet i forhold til kompetence. ▶ Generelle vilkår for ansættelse fremgår af ansættelseskontrakt, herunder fortrolighed og betingelser for ansættelsesophør. ▶ Alle medarbejdere underskriver ansættelseskontrakt og fortrolighedserklæring ved ansættelse.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har implementeret procedure for ansættelse af nye medarbejdere. Vi har inspiceret, at IT Confidence har procedure for ansøgere bliver screenet og vurderet i forhold til kompetence. Vi har stikprøvevis inspiceret at kandidater før ansættelsen er screenet og vurderet i forhold til kompetence. Vi har inspiceret, at IT Confidence har ansættelsekontrakt med vilkår for fortrolighed og betingelse for ansættelsesophør. Vi har stikprøvevis inspiceret underskrevet ansættelseskontrakt på en medarbejder og observeret, at denne indeholder krav om fortrolighed.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*

Under ansættelse ▶ Medarbejdere informeres ved ansættelse om retningslinjer og informationssikkerhedsmateriale. ▶ ITC har implementeret faste procedurer for oprettelse af brugere og tildeling af adgang til systemer og data. ▶ Alle ansatte er forpligtet til at gennemlæse personale- og it-håndbog. ▶ Medarbejdere er undervist i informationssikkerhed, politikker, procedurer og håndtering af persondata der er relevante for deres funktion og rolle. ▶ Medarbejdere er informeret om ansvar og sanktioner ved overtrædelse af virksomhedens sikkerhedsregler.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence informerer medarbejdere ved ansættelse om retningslinjer og informationssikkerhedsmateriale. Vi har inspiceret, at IT Confidence har procedure for oprettelse og tildeling af adgange til systemer og data. Vi har stikprøvevis inspiceret at der tildeles adgang til systemer og data i overensstemmelse med IT Confidences procedure. Vi har inspiceret, at IT Confidence medarbejdere er undervist i informationssikkerhed, politikker, procedurer og håndtering af persondata. Vi har inspiceret, at medarbejdere bliver informeret om ansvar og sanktioner ved overtrædelse af IT Confidences sikkerhedsregler.	Ingen afvigelser konstateret.
Ansættelsesforholdets ophør eller ændring ▶ ITC har implementeret faste procedurer for ansættelsesophør. ▶ Alle brugeradgange slettes ved fratrædelse. ▶ I forbindelse med ansættelsesophør informeres medarbejderen om, at tavshedserklæring er gældende efter ansættelsesforholdets ophør.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har en procedure for ansættelsesophør. Vi har inspiceret, at IT Confidence har procedure for sletning af adgange i forbindelse med en fratrædelse. Vi har stikprøvevis inspiceret at fratrådte medarbejderes brugeradgange slettes i forbindelse med fratrædelsen. Vi har stikprøvevis inspiceret ansættelseskontrakt for medarbejder, der er ansat i erklæringsperioden og har observeret, at der er	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*

	angivet at tavshedspligt også er gældende efter ansættelsesforholdets ophør.	

A.8: Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.*
- *At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.*
- *At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Ansvar for aktiver ▶ Forretningskritiske fysiske aktiver og softwareaktiver er identificeret og dokumenteret. Dokumentationen vedligeholdes løbende. ▶ Alle informationsaktiver er registreret i fortegnelse over aktiver, oplysninger om ejerskab og fysisk placering fremgår af fortegnelsen. ▶ For alle systemer er der udpeget en systemejer, der er ansvarlig for daglig drift og vedligeholdelse. ▶ ITC har fastlagt retningslinjer for accepteret brug og håndtering af aktiver. ▶ Alle medarbejdere er informeret om retningslinjer for accepteret brug og håndtering af aktiver. ▶ ITC har implementeret procedurer for udlevering og tilbagelevering af udstyr.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har identificeret fysiske- og software aktiver og dokumenteret disse. Vi har inspiceret, at fortegnelse indeholder information om ejerskab og fysisk placering af aktiver. Vi har inspiceret, at der for alle systemer er udpeget en systemejer, der er ansvarlig for daglig drift og vedligeholdelse. Vi har inspiceret, at IT Confidence har retningslinjer for accepteret brug og håndtering af aktiver. Vi har inspiceret, at IT Confidence har informeret alle medarbejdere om retningslinjer for accepteret brug af aktiver. Vi har inspiceret, at IT Confidence har procedure for udlevering og tilbagelevering af udstyr. Vi har stikprøvevis inspiceret, at medarbejder har kvitteret for udlevering af udstyr. Vi har stikprøvevis inspiceret at fratrådte medarbejder har tilbageleveret deres udstyr.	Ingen afvigelser konstateret.
Mediehåndtering ▶ Alle diske og medier destrueres, når de tages ud af drift. ▶ Alle diske og medier slettes og formateres før genanvendelse.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for destruktion af diske og medier.	Vi har konstateret, at der er etableret en procedure for destruktion af diske og medier. Vi har ikke kunne udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har være destruktion af diske og medie.

A.8: Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.*
- *At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.*
- *At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ ITC har udformet standard procedure for konfiguration og udlevering af arbejdsstation til medarbejdere. ▶ Alle bærbare PC'ere er beskyttet med adgangskoder og Bitlocker.	Vi har inspiceret, at IT Confidence har procedure for sletning og formatering af diske og medier. Vi har inspiceret, at IT Confidence har procedure for konfiguration og udlevering af arbejdsstation til medarbejdere. Vi har inspiceret, at alle arbejdsstationer er beskyttet med adgangskoder og Bitlocker.	Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.*
- *At forhindre uautoriseret adgang til systemer og applikationer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Administration af brugeradgang, brugerrettigheder og styring af system- og applikationsadgang ▶ Alle loginforsøg logges og registreres. ▶ Ved ophør af ansættelsesforhold deaktiveres brugeren i alle systemer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for, at loginforsøg logges og registreres. Vi har inspiceret, at IT Confidence har procedure for deaktivering af brugeren i alle systemer ved fratrædelse. Vi har stikprøvevis inspiceret at fratrådte medarbejderes brugeradgange til systemerne deaktiveres i forbindelse med fratrædelsen.	Ingen afvigelser konstateret.
Brugerens ansvar ▶ Der er fastlagt politikker og konkrete regler for brugeren i forbindelse med brug af hemmelig autentifikationsinformation.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for politikker og regler for anvendelse af hemmelig autentifikationsinformation.	Ingen afvigelser konstateret.
Begrænset adgang til informationer ▶ Adgang til systemer og filsystem er bestemt af arbejdsbetinget behov. Tildeling af adgang autoriseres af virksomhedens ledelse og/eller systemejer og gennemgås minimum én gang årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for adgang til systemer og filsystem, ud fra et arbejdsbetinget behov. Vi har inspiceret, at der er gennemført periodisk gennemgang af brugeres adgange til systemer og informationer.	Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.*
- *At forhindre uautoriseret adgang til systemer og applikationer.*

Procedurer for sikkert log-on ▶ Adgangskoder lever op til de til enhver tid gældende anbefalinger om sikre password, som beskrevet i it-håndbogen. ▶ Retningslinjer for anvendelse af log-on oplysninger til systemer er udformet, og medarbejdere er informeret om disse. ▶ Ved flere fejlede log-on forsøg låses brugerkonto automatisk ved systemer, som understøtter denne funktion.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for sikre password. Vi har inspiceret, at IT Confidence har procedure for anvendelse af log-on oplysninger til systemer, og medarbejderne er informeret herom. Vi har inspiceret, at ved flere fejlede log-on forsøg, låses brugerkontoen automatisk i 10 minutter.	Vi har konstateret at IT Confidences procedure for sikre password ikke stemmer overens med de opsatte passwordkrav. Ingen yderligere afvigelser konstateret.
Styring af privilegerede adgangsrettigheder ▶ Tildeling af privilegerede adgangsrettigheder sker ud fra et arbejdsbetinget behov. ▶ Tildeling af privilegerede adgangsrettigheder godkendes af ledelsen. ▶ Privilegerede adgangsrettigheder sker på en særlig bruger-id. ▶ Tildelt privilegerede adgangsrettigheder gennemgås og revideres en gang årligt af systemejer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har en procedure for tildeling af privilegerede adgangsrettigheder, hvor ledelsen godkender tildelingen. Vi har stikprøvevis inspiceret, at privilegerede rettigheder er tildelt efter et arbejdsbetinget behov. Vi har inspiceret, at IT Confidence har en procedure for periodisk gennemgang af medarbejders adgange. Vi har inspiceret, at adgange er gennemgået i revisionsperioden.	Vi har konstateret at IT Confidence har tildelt privilegerede adgangsrettigheder til et almindeligt bruger-id. Ingen yderligere afvigelser er konstateret.

A.10: Kryptografi

Kontrolmål

- *At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for kryptografi ▶ Politik for anvendelse af kryptografi er fastlagt og dokumenteret.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for kryptografi og at denne er dokumenteret i It-Sikkerhedspolitikken.	Ingen afvigelser konstateret.
Beskyttelse og kryptering af information ▶ Ved overførsel af data i forbindelse med backup er dette sikret med kryptering i transmission. ▶ Alle forbindelser imellem servere og klienter foregår med en krypteret forbindelse. ▶ Al data på backup-lokationer er krypteret.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for kryptering i forbindelse med dataoverførelse til backup, samt alle data på backup-lokationer er krypteret. Vi har inspiceret, at alle forbindelser mellem servere og klienter er krypteret.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sikre områder ▶ Kontoret har adgangskontrol og tyverialarm. ▶ Gæster modtages og eskorteres i sikre områder af medarbejder. ▶ Kun medarbejdere med arbejdsbetinget behov er tildelt adgang til faciliteret, der administrerer persondata. ▶ ITC har udformet og implementeret politik for ryddeligt skrivebord og blank skærm. Alle medarbejdere er informeret om politikker.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har observeret, at IT Confidence har adgangskontrol og tyverialarm. Vi har inspiceret, at IT Confidence har procedure for modtagelse og eskortering af gæster. Vi har inspiceret, at IT Confidence kun tildeler adgang til faciliteter der administrerer persondata til medarbejdere med arbejdsbetinget behov. Vi har inspiceret, at IT Confidence har en procedure ryddeligt skrivebord. Vi har inspiceret, at IT Confidence har procedure for klassificeret materiale ikke ligger fremme på skrivebordene, ryddeligt skrivebord og blank skærm.	Ingen afvigelser konstateret.
Sikker bortskaffelse eller genbrug af udstyr ▶ Ved bortskaffelse, reparation eller genbrug af it-udstyr fjernes alle data. ▶ ITC har implementeret procedure for sletning og bortskaffelse af it-udstyr. ▶ Data slettes, så det ikke er muligt at gendanne.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har en procedure for sletning af data, bortskaffelse, reparation og genbrug af it-udstyr.	Vi har konstateret, at der er etableret en procedure for bortskaffelse eller genbrug af udstyr. Vi har ikke kunne udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har være bortskaffelse eller genbrug af udstyr. Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for ryddeligt skrivebord og blank skærm ▶ PC låses automatisk med skærmlås, når arbejdspladsen forlades, eller PC står urørt i kort tid. ▶ Medarbejdere er gjort bekendt med politikker for ryddeligt skrivebord.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret at IT Confidence har opsat regler for automatiks skærmlås på PC'er. Vi har inspiceret, at IT Confidence har en procedure for skærmlås af arbejdsstation og ryddelige skriveborde, og at medarbejdere er bekendt med politikken.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*
- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*
- *At beskytte mod tab af data.*
- *At registrere hændelser og tilvejebringe bevis.*
- *At sikre integriteten af driftssystemer.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At minimere virkningen af auditaktiviteter på driftssystemer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik driftssikkerhed ▶ Politik for driftssikkerhed er fastlagt og dokumenteret. ▶ Politik for driftssikkerhed revideres årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence i IT sikkerhedspolitikken har en politik for driftssikkerhed. Vi har inspiceret at politikken for driftssikkerhed er blevet gennemgået i maj 2024.	Ingen afvigelser konstateret.
Ændringsstyring ▶ En procedure for ændringsstyring sikrer ensartet håndtering af ændringer. ▶ Alle ændringer i forbindelse med den centrale hosting platform foregår med afsæt i driftsprocedure. ▶ Ændringer i kundens løsninger foregår med afsæt i gældende driftsprocedure.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for ensartet håndtering af ændringsstyring, herunder ændringer i forbindelse med den centrale hosting platform. Vi har stikprøvevis inspiceret ændringer i kundernes løsninger og observeret, at IT Confidence følger gældende procedure for ændringer.	Ingen afvigelser konstateret.
Kapacitetsstyring ▶ Der foretages løbende overvågning af ydelse og kapacitet i driftsmiljø. ▶ Der iværksættes forbyggende kapacitetstilpasning på baggrund af kapacitetsovervågning.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence foretager løbende overvågning af ydelse og kapacitet.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*
- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*
- *At beskytte mod tab af data.*
- *At registrere hændelser og tilvejebringe bevis.*
- *At sikre integriteten af driftssystemer.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At minimere virkningen af auditaktiviteter på driftssystemer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret at IT Confidence har opsat grænseværdier og observeret, at der iværksættes forbyggende kapacitetstilpasning, hvis kapaciteten overstiger grænseværdierne.	
Malwarebeskyttelse - Servere og arbejdsstationer tilsluttet ITCs netværk er beskyttet mod Malware. - Ved tilkobling til ITCs netværk, kontrolleres opdatering og status på antivirusprogrammer. - Antivirus software opdateres automatisk. - Procedure for håndtering af malware udbrud er beskrevet og implementeret.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har installeret beskyttelse mod malware, samt at systemerne overvåges. Vi har stikprøvevis udvalgt servere hos IT Confidence og inspiceret, at disse er beskyttet mod malware. Vi har inspiceret, at IT Confidence har compliance krav til tilkoblet udstyr til netværket. Vi har inspiceret, at antivirus software automatisk opdateres. Vi har inspiceret, at IT Confidence har beskrevet og implementeret beredskabsplan for håndtering af malware udbrud.	Ingen afvigelser konstateret.
Backup - Der foretages dagligt backup af kritiske servere og data i driftsmiljø. - Systemejer er ansvarlig for implementering af sikkerhedskopiering.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*
- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*
- *At beskytte mod tab af data.*
- *At registrere hændelser og tilvejebringe bevis.*
- *At sikre integriteten af driftssystemer.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At minimere virkningen af auditaktiviteter på driftssystemer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Status for sikkerhedskopiering kontrolleres dagligt og dokumenteres i driftsdokumentation. ▶ Der foretages løbende systematisk test af sikkerheds-kopi.	Vi har inspiceret, at IT Confidence har politik for backup af servere og data i driftsmiljøet. Vi har inspiceret, at der er foretaget backup af servere og data. Vi har inspiceret, at der er udpeget en systemejer for sikkerhedsko-piering. Vi har inspiceret, at status for sikkerhedskopiering kontrolleres dag-ligt samt der er ved fejl oprettes en Ticket til behandling. Vi har inspiceret, at der foretages løbende test af sikkerhedskopie-ring og det kontrolleres for fejl.	
Kapacitetslogning og -overvågning ▶ Der føres hændelseslogning og overvågning af kritiske systemer. ▶ Kapaciteten i forbindelse med alle servere med kritiske informationer overvåges i hændelsesloggen. ▶ Der er udarbejdet politikker og procedurer for logning. ▶ Kun medarbejdere med arbejdsbetinget behov har ad-gang til logning. ▶ Systemtid er synkroniseret ved hjælp af NTP. ▶ Administratorlogs overvåges og gennemgås periodisk, både i form af stikprøver og fast gennemgang.	Vi har udført forespørgsel hos passende personale hos servicelevе-randøren. Vi har inspiceret, at IT Confidence fører hændelseslogning og over-vågning af kritiske systemer. Vi har inspiceret, at IT Confidence overvåger kapaciteten. Vi har inspiceret, at IT Confidence har politikker og procedurer for logning. Vi har inspiceret, at IT Confidence har opsat synkroniseret system-tid ved hjælp af NTP. Vi har på forespørgsel fået oplyst, at IT Confidence har udført perio-disk gennemgang af administratorlogs.	Ingen afvigelser er konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*
- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*
- *At beskytte mod tab af data.*
- *At registrere hændelser og tilvejebringe bevis.*
- *At sikre integriteten af driftssystemer.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At minimere virkningen af auditaktiviteter på driftssystemer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Styring af driftssoftware ▶ ITC har implementeret politikker for installation af software på servere og arbejdsstationer. ▶ Softwareinstallation på driftssystemer er underlagt procedure for ændringsstyring. ▶ Sikkerhedsopdateringer installeres, når disse er gjort tilgængelige hos systemleverandøren.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har politik for installation af software på servere og arbejdsstationer. Vi har inspiceret, at IT Confidence har en procedure for ændringsstyring og at driftssystemer er underlagt ændringsstyring. VI har inspiceret, at IT Confidence installerer sikkerhedsrettelser når de er tilgængelige.	Ingen afvigelser konstateret.
Sårbarhedsstyring. ▶ Der er udarbejdet procedure for identifikation og håndtering af tekniske sårbarheder. ▶ Der gennemføres løbende sårbarhedstjek.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har udført sårbarhedstjek. Vi har observeret, at der ikke er identificeret kritiske sårbarheder på netværket.	Ingen afvigelser er konstateret.

A.13: Kommunikationssikkerhed

Kontrolmål

- *At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.*
- *At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for kommunikationssikkerhed ▶ Politik for kommunikationssikkerhed er fastlagt og dokumenteret. ▶ Politik for kommunikationssikkerhed revideres årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence politik for kommunikationssikkerhed er dokumenteret i IT Sikkerhedspolitik, samt IT Sikkerhedspolitikken revideres årligt.	Ingen afvigelser konstateret.
Netværkssikkerhed ▶ Adgang til netværksenheders konfiguration er kun tildelt medarbejdere med et arbejdsbetinget behov. ▶ Al indkommende trafik er som standard blokeret, og der åbnes kun for porte, hvor der er behov for kommunikation. ▶ Netværket er opdelt i WAN, LAN og DMZ. ▶ Kommunikation mellem Internet, LAN og DMZ styres af firewall. ▶ Der foretages periodisk gennemgang og review af firewall konfiguration. ▶ Trådløse netværk er opdelt i internt og gæstenetværk. ▶ Gæstenetværk er separat LAN netværk for gæster uden adgang til interne netværk og servere. ▶ Trådløse netværk benytter sikker godkendelse og kryptering af data. ▶ Der foretages overvågning af netværket for at spore, udbedre og undgå sikkerhedsbrister.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. VI har inspiceret, at adgange til netværksenheders konfiguration, kun er tildelt medarbejdere med et arbejdsbetinget behov. Vi har inspiceret, at al indkommende trafik som standard er blokeret, og der åbnes kun for porte, hvor der er behov for kommunikation. Vi har inspiceret, at netværket er opdelt i WAN, LAN og DMZ, samt styres af Firewall. Vi har inspiceret, at der foretages periodisk gennemgang og review af firewallkonfigurationen. Vi har inspiceret, at det trådløse netværk er opdelt i internt og gæste netværk, og gæstenetværket er et separat LAN netværk for gæster uden adgang til interne netværk og servere. Vi har inspiceret, at kommunikationen overvåges for at spore, udbedre og undgå sikkerhedsbrister.	Ingen afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.*
- *At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for leverandørforhold ▶ Der er fastlagt politikker for håndtering af leverandører. ▶ Politikkerne gennemgås én gang årligt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har politikker for håndtering af leverandører. Vi har inspiceret at politikker for leverandørforhold er blevet gennemgået.	Ingen afvigelser konstateret.
Informationssikkerhed i leverandørforhold ▶ Der foreligger aftaler med serviceleverandører. ▶ Informationssikkerhedskrav til serviceleverandører er fastlagt i aftale. ▶ Procedure for vurdering og gennemførelse af tilsyn med leverandører er beskrevet og dokumenteret. ▶ Der gennemføres tilsyn med serviceleverandører mindst én gang årligt. ▶ I forbindelse med det årlige interne review gennemgås serviceleverandøraftaler med forretningskritiske serviceunderleverandører. ▶ Ved indgåelse af aftale med serviceunderleverandører foretages der en vurdering af denne i forhold til informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har indgået aftale med serviceleverandør, og at informationssikkerhedskrav til serviceleverandøren er fastlagt i aftalen. Vi har inspiceret, at IT Confidence gennemfører tilsyn med leverandøren ved indhentning af ISAE 3402 revisorerklæring. Vi har inspiceret at IT Confidence har indhentet ISAE 3402 erklæringen fra Cibicom A/S. Vi har inspiceret at IT Confidence har indhentet ISAE 3402 erklæringen fra ADEO, som er udarbejdet af Algade Revision. Vi vurderer ikke, at erklæringen der er udstedt, lever op til de gældende standarder. Vi har desuden konstateret, at revisorerklæringen ikke er dækkende for perioden. Vi er på forespørgsel oplyst, at IT Confidence ikke har lavet kompenserende tilsyn med serviceleverandøren.	Vi har konstateret, at der ikke foreligger en revisorerklæring fra ADEO, som er dækkende for revisionsperioden. Vi har konstateret, at IT Confidence ikke har udført formaliseret dokumenteret tilsyn med ADEO som serviceleverandør. Ingen yderligere afvigelser er konstateret.

A.15: Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.*
- *At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret årshjul og observeret, at aftale med serviceleverandøren, gennemgås en gang årligt, og der samtidig udføres en vurdering af leverandørens informationssikkerhed.	

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

- *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og –svagheder.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Rapportering af sikkerhedshændelser ▶ Medarbejdere indrapporterer alle informationssikkerhedshændelser, svagheder og brud til ledelsen. ▶ Alle informationssikkerhedshændelser, svagheder og brud registreres af it-ansvarlige i hændelseslog i samarbejde med ledelsen. ▶ Informationssikkerhedshændelser vurderes i forhold til risici for gentagelse af hændelsen. ▶ ITCs ledelse og it-ansvarlige gennemgår kvartårligt hændelsesloggen og iværksætter forbedringer af informationssikkerheden.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har procedure for indrapportering af informationssikkerhedshændelser, svagheder og brud til ledelsen og hele virksomheden.	Vi har konstateret, at der er etableret en procedure for indrapportering af informationssikkerhedshændelser. Vi har ikke kunne udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har være informationssikkerhedshændelser. Ingen afvigelser konstateret.

A.17: Informationssikkerhedsaspekter ved nød–, beredskabs- og retableringsstyring

Kontrolmål

- *Informationssikkerhedskontinuiteten skal være forankret I organisationens ledelsessystemer for nød-, beredskabs- og retableringsstyring.*
- *At sikre tilgængelighed af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Planlægning af informationssikkerhedskontinuitet ▶ Der er på baggrund af risikovurdering etableret en plan for informationssikkerhedskontinuitet i form af beredskabsplan.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at IT Confidence har opbygget plan for informationssikkerhedskontinuitet i form af beredskabsplan.	Ingen afvigelser konstateret.
Implementering af informationssikkerhedskontinuitet ▶ Beredskabsplanen er tilgængelig for al personale. Både skriftlig og elektronisk. ▶ Roller og ansvar i forbindelse med aktivering af beredskab er kommunikereret til relevante personer; herunder information om placering af nødvendige informationer. ▶ Der er, som en del af beredskabsplanen, udarbejdet procedure og arbejdsbeskrivelser for reetablering af driftskritiske systemer. ▶ Beredskabsplanen er lagret elektronisk på fælles drev og fysisk hos administrationen.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret, at Beredskabsplanen er tilgængelig for al personale elektronisk. Vi har inspiceret, at roller og ansvar er defineret i beredskabsplanen, og er kommunikeret ud til relevante personer, med henvisning til, al personale har underskrevet læsning af IT Sikkerhedspolitikken. Vi har inspiceret, at der i beredskabsplanen er udarbejdet procedure og arbejdsbeskrivelser for reetablering af forretningskritiske systemer.	Vi har konstateret at IT Confidence ikke har opbevaret deres beredskabsplan fysisk, så denne er tilgængelig for al personale. Ingen yderligere afvigelser er konstateret.
Revidering og afprøvning for sikkerhedskontinuitet ▶ Beredskabsplaner revideres og skrivebordstestes én gang årligt ved implementering af nye systemer eller ændringer i risikovurderingen. Beredskabsplanerne testes fuldt ud en gang hvert 3. år.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har inspiceret at der i erklæringsperioden er udført en skrivebordstest for beredskabsplanen og observeret, at IT Confidence har dokumenteret testens forløb og resultat.	Ingen afvigelser konstateret.

▶ Beredskabsplaner afprøves efter en fastlagt rotationsplan. Afprøvning af beredskabsplaner er planlagt i årshjul.	Vi har inspiceret at IT Confidence har testet deres beredskabsplan i erklæringsperioden. Vi har på forespørgsel fået oplyst, at beredskabsplanen testes igen om 3 år, medmindre der implementeres nye systemer eller ændringer i risikovurderingen.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

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."

Erik Hugo Schultz
Administrerende direktør
Serienummer: 5decdd88-197c-4340-86de-800643a0d8e0
IP: 92.241.xxx.xxx
2025-04-01 11:21:38 UTC

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2025-04-01 11:26:53 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 62.66.xxx.xxx
2025-04-01 18:26:53 UTC