BEIERHOLM
VI SKABER BALANCE

JANUAR 2025

INVENTIO.IT A/S

ISAE 3402 TYPE 2 ERKLÆRING

CVR 26112001

Uafhængig revisors erklæring om kontrolmiljøet i tilknytning til it-driften for ERP Online Services.

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

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

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:

Ledelseserklæring.

Kapitel 2:

Beskrivelse af kontrolmiljøet i tilknytning til it-driften af ERP Online Services.

Kapitel 3:

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

Kapitel 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, tests og resultater heraf.

KAPITEL 1:

Ledelseserklæring

Inventio.IT A/S behandler personoplysninger på vegne af kunder i henhold til databehandleraftale om it-driften af ERP Online Services.

Medfølgende beskrivelse er udarbejdet til brug for kunder og deres revisorer, der har anvendt Inventio.IT A/S' ERP Online Services, 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.

Inventio.IT A/S bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2 (inkl. bilag 1), giver en retvisende beskrivelse af Inventio.IT A/S' kontrolmiljø i tilknytning til it-driften af ERP Online Services i hele perioden 1. januar 2024 - 31. december 2024. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

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

- De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
- De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og 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 afgrænsning af it-driften af ERP Online Services 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 ved it-driften af ERP Online Services foretaget i hele perioden 1. januar 2024 - 31. december 2024.

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

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

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. januar 2024 - 31. december 2024.

(C) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere 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 Inventio.IT A/S' standardaftale samt tilhørende databehandleraftale. Kriterierne for dette grundlag var:

(i) Inventio.IT - Service Level Agreement
(ii) Inventio.IT – Databehandleraftale

Brøndby, den 9. januar 2025

Michael Steen Sørensen	**Kenneth Kornbeck Lindeblad**
Adm. Direktør	It-sikkerhedskoordinator/ Marketingchef

Inventio.IT A/S, Vallensbæksvej 45, DK-2605 Brøndby, CVR 26112001

KAPITEL 2:

Beskrivelse af kontrolmiljøet i tilknytning til it-driften af ERP Online Services

Indledning

Formålet med nærværende beskrivelse er at levere information til Inventio.IT 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 kontrolbeskrivelse afdækningen af de tekniske og organisatoriske sikringsforanstaltninger, som er implementeret i forbindelse med Inventio.IT A/S' it-drift af ERP Online Services.

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.

Omfang for denne beskrivelse

Inventio.IT A/S er leverandør af online services inden for ERP, og kerneaktiviteten i Inventio.IT er ERP Online Services, som omfatter udvikling og leverance af standardiserede online-løsninger til Microsoft Dynamics produktserie. Overvågning og support er på Inventio.ITs egen platform, som er placeret i Inventio.ITs datacenter.

Inventio.IT har leverandøransvaret 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 denne kerneaktivitet, der danner grundlag for nærværende beskrivelse.

Beskrivelse af Inventio.IT A/S

Inventio.IT A/S er grundlagt i 2001 og er en sund dansk virksomhed med stabil vækst og overskud. I 2019 blev Inventio.IT en del af den svenske børsnoterede Dustin Group.

Vores forcer er standardiserede abonnementsbaserede ERP-løsninger til Microsoft Dynamics, men vi udvikler også skræddersyede løsninger (Extensions) til kunder, som har behov for det. Tryghed og tillid er nøgleord, når man skal vælge samarbejdspartner, derfor lægger vi hos Inventio.IT vægt på at have en organisation, hvor alle medarbejdere er kompetente, erfarne, troværdige og med stort engagement i hver enkelt kunde.

Vi er ca. 60 medarbejdere, og med vores afdelinger på Sjælland og i Jylland dækker vi hele landet. Vi fokuserer på små og mellemstore virksomheder, da vi her gør bedst brug af alle vores kompetencer. Vi servicerer også vores internationale kunders datter- og søsterselskaber i bl.a. Skandinavien, Europa, Afrika og Nordamerika.

Forretningsstrategi/ it-sikkerhedsstrategi

Inventio.ITs strategi er fortsat at udnytte vores ekspertise inden for hosting af ERP-systemer og til at videreudvikle online services, der kan sælges via en abonnementsbaseret model i store volumener.

Vores fremtidsorienterede løsninger til Microsoft Dynamics 365 hjælper små og mellemstore virksomheder, som ønsker at udnytte mulighederne med ERP i skyen ved at migrere fra en forældet platform med begrænsede muligheder og til at begynde at automatisere og optimere nemt og billigt.

Vi adskiller os fra den traditionelle ERP-leverandør, da vi tilbyder priseffektive online services (SMART apps), som dækker behovet for at komme hurtigt og nemt i gang med standardisering og effektivisering af forretningsdrift, typiske processer og samarbejde internt i virksomheden og eksternt med kunder.

Med vores online services til ERP (SMART apps og online platform) er vi allerede førende inden for volumensalg af Microsoft-ERP-systemer. Ved hjælp af vores ekspertise inden for ERP og hosting, skal denne markedsposition udbygges. Både med videreudvikling af nuværende produkter og tilføjelse af nye.

Hostede ERP-løsninger

Inventio.IT tilbyder følgende ERP Online Services:

- ➢ ERP-online
  (BConline, NAVonline, C5online)
- ➢ SMART apps

Inventio.IT arbejder med it-sikkerhed på et forretningsstrategisk niveau og arbejder derfor løbende med at sikre et højt service- og kvalitetsniveau. Såvel Inventio.ITs egen ledelse som Dustin Group, der er Inventio.ITs ejer, prioriterer gennem selskabets sikkerhedspolitik, at it-sikkerhed skal være og er en vigtig del af selskabets virksomhedskultur.

Inventio.IT har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27001+2, 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
- Kryptografi
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhed
- Informationssikkerhedsaspekter ved nød-, beredskabs – og reetableringsstyring
- Overensstemmelse med lov- og kontraktkrav

De implementerede kontrolmål og sikringsforanstaltninger hos Inventio.IT fremgår af bilag 1 til denne beskrivelse.

Inventio.IT A/S' organisation og organisering af it-sikkerheden

Inventio.ITs formelle ansvar for it-sikkerhedspolitik og procedurer er placeret hos CSO/Adm. direktør. It-sikkerhedspolitikken godkendes af virksomhedens bestyrelse.

Hos Inventio.IT eksisterer der en klart opdelt organisation, hvad ansvar angår, og Inventio.IT har udførlige ansvars- og rollebeskrivelser på alle niveauer, lige fra ledelsesniveau til de enkelte driftsmedarbejdere.

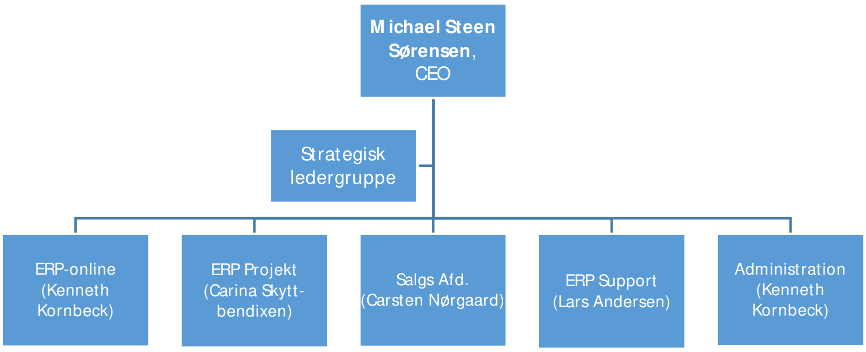
Alle medarbejdere holdes løbende opdateret med ændringer i it-sikkerhedspolitikken. Koordinering af udmelding og undervisning planlægges af it-sikkerhedskoordinatoren.

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

Inventio.ITs organisation er opdelt i 5 afdelinger – ERP-online, ERP support, ERP projekt, Salg, og Administration.

I og med at de fleste krav til it-sikkerhed vedrører ERP-online, varetager Kenneth Kornbeck Lindeblad rollen som it-sikkerhedskoordinator på tværs af alle afdelingerne.

Derfor lægger vi hos os vægt på at have en organisation, hvor alle medarbejdere er kompetente, erfarne, troværdige og med stort engagement i hver enkelt kunde.



Vi har fokus på den enkelte virksomheds forretningsmæssige mål og behov, og vi sætter en ære i at overholde tidsfrister, budgetter, funktionalitet og kvalitet.

Vi har en flad organisation, hvor der ikke er langt fra beslutning til handling, og hvor medarbejdere er beskæftiget både med udvikling og med at servicere vores kunder.

Vi har ry for: ”én gang kunde hos Inventio.IT - altid kunde hos Inventio.IT”. Noget tilsvarende gælder vores medarbejdere, hvoraf mange har været med, siden vi startede i 2001. Dette skaber gode relationer mellem os og kunderne. Vi sætter en ære i at have tilfredse medarbejdere, som løbende holdes opdateret med kurser o.l. Vi har i dag flere Microsoft-certificeringer og er Microsoft Gold Partner.

Risikostyring i Inventio.IT A/S

Det er Inventio.ITs 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. Inventio.IT gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering.

Inventio.IT har indarbejdet faste procedurer for risikovurdering af forretningen og specielt ERP-online. Vi sikrer dermed, at de risici, som er forbundet med de services og ydelser, 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 vurderes relevante i forbindelse med at revurdere vores generelle risikovurdering. Ansvaret for risikovurderingen ligger hos den adm. direktør.

Som led i ovenstående it-sikkerhedsstrategi arbejder Inventio.IT med den internationale standard for it-sikkerhed - ISO27001+2 – som primær referenceramme for it-sikkerheden. Arbejdsprocessen omkring it-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at Inventio.IT til hver en tid er i overensstemmelse med kundernes krav og behov.

Håndtering af it-sikkerhed

Ledelsen hos Inventio.IT 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 Inventio.ITs struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

Inventio.ITs 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.

Inventio.ITs 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.

Alle servere og netværksenheder er dokumenteret i Inventio.ITs dokumentationssystem. Her logges alle ændringer af vores system.

Sikkerhedspolitikken sætter de grundlæggende politikker for Inventio.ITs infrastruktur, og omhandler ikke forhold vedrørende specifikke produkter, ydelser eller brugere.

Sikkerhedspolitikken er udarbejdet sådan, at Inventio.IT 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.

På it-sikkerhedsområdet har Inventio.IT implementeret de nødvendige procedurer og kontroller i forhold til de enkelte områder inden for ISO27001+2, som er defineret i bilag 1, som viser sikkerhedsstrukturen og de kontrolmål, som er implementeret hos Inventio.IT.

HR, medarbejdere og uddannelse

Alle hos Inventio.IT skal leve op til den rolle, som er tildelt dem, samt følge vores procedurer jf. vores it-sikkerhedspolitik. Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold tilpasses og håndteres. Hos Inventio.IT har det topprioritet, at man passer på kunders data, virksomhedens udstyr og dermed forretningen.

Rolle- og ansvarsbeskrivelsen, herunder opgaver og ansvar i forhold til sikkerheden, er defineret i de udarbejdede rollebeskrivelser, medarbejdernes ansættelseskontrakter, samt i it-sikkerhedspolitikken.

Generelle vilkår for ansættelse omfatter, at medarbejderen til enhver tid er underlagt den gældende it-sikkerhedspolitik.

Inventio.IT betragter medarbejderne som vigtige aktiver, og anvender en struktureret proces i forhold til medarbejdernes kvalifikationer, uddannelse og certificeringer. Der afholdes løbende - dog minimum årligt - kurser, foredrag samt andre relevante aktiviteter til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med sikkerhed og bevidstgøres om evt. nye trusler.

Alle udførende konsulenter har kompetencer inden for de områder, de beskæftiger sig med. Det dokumenteres ved hjælp af relevante certificeringer og intern uddannelse.

Inventio.IT 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. Inventio.IT sikrer via løbende produkttræning og kursusdeltagelse opretholdelsen af denne høje certificeringsstatus.

Fysisk sikkerhed og miljøsikring

Hardware der vedrører ERP-online, er placeret i Interxions datacentre på forskellige lokaliteter. Datacentrene har redundans på alle væsentlige infrastrukturkomponenter, som strøm, UPS, nødgeneratorer, netværk samt internetforbindelse.

Interxion – det primære datacenter - er placeret på indhegnet grund. Hoveddøren er altid låst og kan kun låses op af medarbejdere med adgangskort.

Alene autoriserede personer får adgang til lokalerne via den etablerede procedure, og der følges periodisk - minimum årligt - op på, hvilke personer der har denne adgang. Kun ganske få udvalgte personer fra Inventio.IT og MMT har adgang til Interxion.

Serverne er fysisk placeret i et aflåst lokale, som har monteret køling og brandslukning mv. Serverrummet indeholder centralt netværksudstyr, og er således sikret på samme vis som servere. Strømforsyning til datacenterdrift er UPS- og generatorbeskyttet.

Der udføres et løbende kontroltilsyn med it-sikkerheden placeret hos Interxion (underleverandør).

Eksterne personer (leverandører eller kunder) får kun adgang til lokalet i følgeskab med en autoriseret medarbejder.

Ingen uvedkommende vil kunne gå uhindret omkring i Inventio.ITs kontorer, da yderdøre altid er er aflåste og som minimum kræver nøglekort.

Brugerstyring/ adgangssikkerhed

Der er etableret politik for adgangstildeling. Politikken er en del af Inventio.ITs it-sikkerhedspolitik.

Kunders brugere oprettes alene på baggrund af skriftlig bestilling/accept fra kunden, og ligeledes tildeles revisoradgang til slutkunder kun efter accept fra slutkunden.

Inventio.ITs egne brugere oprettes alene på baggrund af skriftlig autorisation fra ledelsen. Brugere tildeles som udgangspunkt det laveste sæt rettigheder, som er påkrævet for at udføre de tildelte arbejdsopgaver. It-sikkerhedspolitik foreskriver, at medarbejdernes kodeord er personlige, og det alene er brugeren selv, der må kende kodeordet.

- Krav til password - Password skal være på et minimum af tal eller bogstaver.
- Der benyttes 2-faktor log-on.

For at sikre højeste sikkerhed er det kun ganske få medarbejdere hos Inventio.IT og MMT, der har fået tildelt adgang til back-end systemer vedr. ERP-online.

Hvis en ny bruger skal havde adgang kræver det godkendelse fra min. 2 personer fra ERP-online afdelingen.

Kryptografi

Kryptering er en vigtig sikkerhedsforanstaltning, der bruges til at beskytte data under transport eller opbevaring. At bruge sikre krypteringsalgoritmer er afgørende for at opretholde høj sikkerhed i forbindelse med kommunikation og opbevaring af data. Vi bruger sædvanligvis TLS (Transport Layer Security) version 1.2 eller nyere.

- Sikre netværkstrafik mellem brugerens klient (browser) og Inventio.IT's tjenester. HTTPS-trafik bliver filtreret gennem en firewall og dirigeret videre til centrale "load balancers".
- VPN (Virtual Private Network) tunneller bliver brugt til at sikre netværkstrafik mellem kunder, tredjeparter og Inventio.IT's netværk.
- SFTP (Secure File transport Protocol) bliver brugt ved udveksling af filer mellem kunder, tredjeparter og Inventio.IT.
- Sikker mail, standardindstillinger er sat op til at bruge kryptering ved sending/modtagelse af e-mail via SMTP.
- Backup af filer og databaser bliver udført lokalt og er sikret ved at bruge TLS-kryptering.
- Lagringsdiske (SAN) bruger kryptering på diske, som er aktivt registreret i SAN-clusteret. Når en disk bliver fjernet, bliver krypteringen automatisk slettet efter kort tid.

Udviklingsmiljø

Når Inventio.IT A/S udvikler apps, bruges der dedikerede sandkasse- og testmiljøer, hvorfra softwaren kan afvikles til udvikling og test. Disse miljøer er andre miljøer end dem, som driften afvikles på.
Der er fastlagte procedurer for udvikling, test og godkendelse. Kodeændringer er separeret fra standardapplikationen.

Change management

Formålet med change management er at sikre, at ændringer testes og afprøves, inden ændringer sættes i drift. Alle ændringer er automatisk logget, og der benyttes versionsstyring.

Hvis der sker hændelser, som kan påvirke driften, vil overvågningssystemet automatisk alarmere vagtberedskabet, og der forefindes en indarbejdet procedure for eskalation, sluttende med at den adm. direktør involveres.

Drift af ERP Online Services

Driften af ERP-online varetages af Inventio.IT, i tæt samarbejde med MMT.

Overvågning

Der er etableret automatisk overvågning af servere, storagesystemer, netværk, m.v. og der er 1. line supportpersonale på vagt 24/7/365. Inventio.IT følger løbende tilsyn med denne kontrol.

Endvidere fortager Inventio.IT overvågning på applikationsniveau for at sikre optimal performance på systemerne.

Hvis en kritisk fejl konstateres, afsendes alarm både visuelt på en overvågningsskærm og på SMS. Opstår en situation, hvor der konstateres en fejl på en komponent, der ikke er en del den automatiske overvågning, tages der skridt til, at den fremover registreres i systemet.

Hostingcenteret hos Interxion overvåges med hensyn til strømafbrydelser, temperatur, brand, vand, luftfugtighed, og hele hostingcenteret er i øvrigt kameraovervåget.

Backup/ Restore

Formålet med backup og restore er at sikre, at kundens data i Inventio.ITs ERP Platform kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid.

Inventio.IT sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis og efter de aftaler, der eksisterer med Inventio.ITs kunder.

Der er etablereret en testplan for verificering af, hvorvidt sikkerhedskopieringen fungerer, samt en test af, hvordan systemer og data praktisk kan reetableres. Der føres en log over disse tests, så der kan følges op på, om der foreligger forbedringsmuligheder for procedurer og processer.

Der fortages daglig sikkerhedskopiering af hele ERP-onlineplatformen og de omkringliggende systemer samt af kundernes databaser.

Der er udarbejdet faste procedurer og beskrivelser for opsætning og vedligehold.

Hver nat overføres en fuld kopi af data fra Inventio.ITs centrale systemer til det sekundære datacenter ved hjælp af backup-systemet. Dermed er backup-data fysisk separeret fra driftssystemer.

Opgaver vedr. backup varetages af både MMT og Inventio.IT. Inventio.IT følger løbende tilsyn med denne kontrol.

Såfremt en kunde ønsker en restore fra backup, eller udlæsning af BAK fil, faktureres dette efter medgået tid.

Patch management / ændringshåndtering

Formålet med patch management er at sikre, at alle relevante opdateringer som patches, fixes og service packs fra leverandører implementeres. Dette sker for at sikre systemerne mod nedetid og uautoriseret adgang, og for at implementeringen sker på en kontrolleret måde.

Alle Windows-servere er opdelt i forskellige opdateringsgrupper. Nogle servere opdateres automatisk med det samme. Andre servere opdateres kort tid efter, hvis den første opdatering er succesfuld. Kritiske servere opdateres manuelt for at højne driftsstabiliteten.

Der er 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.

Opgaver vedr. patch management / ændringshåndtering varetages af MMT i tæt dialog med Inventio.IT, som samtidig følger løbende tilsyn med denne kontrol.

Kommunikationssikkerhed

Internetleverandøren til driftscenteret er Telia. Der er lagt to 2GB linjer, med separate føringsveje, til datacentret i Ballerup og to 1GB linjer, med separate føringsveje, til datacentret i Valby. Derudover er der en 6GB linje mellem de to datacentre, og begge datacentre kan fungere som primær adgang til alle systemer.

Der er redundante firewalls/routere i begge datacentre. Fire styk i Ballerup og to styk i Valby. Alle firewalls er beskyttet mod DDOS ved hjælp af policies.

Vi er beskyttet mod ransomware med antivirus og spamfilter.

Opgaver vedr. kommunikationssikkerhed varetages af MMT i tæt dialog med Inventio.IT, som samtidig følger løbende tilsyn med denne kontrol.

Styring af it-sikkerhedshændelser

Sikkerhedshændelser opdaget fra henholdsvis egne observationer, alarmering fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, bliver viderebragt til ERP Online med samtidig orientering af ledelsen i Inventio.IT.

Sikkerhedshændelser og svagheder i Inventio.ITs systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

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

Ledelsen har ansvaret for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Opgaver vedr. styring af it-sikkerhedshændelser varetages af MMT i tæt samarbejde med Inventio.IT. Inventio.IT udfører løbende tilsyn med denne kontrol.

Beredskabsstyring

Både Inventio.IT og MMT har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer. Beredskabsplanen omfatter it-systemer og processer på alle niveauer. Beredskabsplanen er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen.

I udformningen af beredskabsplaner og review heraf, vurderes disse løbende i forhold til Inventio.ITs gældende it-sikkerhedspolitik.

Via medlemskabet af DCC (Danish Cloud Community) er Inventio.IT forpligtet til, inden for 3 dage, at kunne retablere enhver enhed i datacenteret. Dette sikres ved, at man har afvejet risici, klassificeret enheder i driftsapparatet og har procedurer, der sikrer, at beredskabsplanlægningen kan foretage udskiftning af driftsplatformen, så de leverede ydelser vil retableres rettidigt.

Der foretages løbende disaster recovery test af beredskabet. Efter endt udførelse analyseres resultatet, og på den baggrund opdateres de relevante elementer, procedurer og planer.

Overensstemmelse med rollen som databehandler

Det er ledelsen hos Inventio.IT, 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
- Service Level Agreement
- Standardkontrakt eller andre relevante kilder

Inventio.IT er forpligtet til at inddrage juridiske eksperter efter behov for at sikre et passende niveau i forhold til overholdelsen af lovgivningen. Desuden gennemgår ledelsen regelmæssigt alle sikkerhedspolitikker, evt. med inddragelse af relevante interessenter. It-sikkerhedsrammen revideres regelmæssigt af en uvildig, ekstern part, og revisionsrapporten deles ved efterspørgsel med alle Inventio.ITs kunder.

EU Databeskyttelsesforordningen (GDPR)

Inventio.ITs it-services understøtter kundernes arbejdsprocesser i forbindelse med ERP Online Services. Inventio.IT ejer ikke data, som kunderne indsamler, men udvikler og driver de it-services, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er Inventio.IT databehandler, og kunden er dataansvarlig.

Inventio.IT samarbejder med juridiske eksperter med henblik på at sikre, at alle relevante juridiske krav er identificeret og imødekommet. Inventio.IT 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 Inventio.IT med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.

Ifølge GDPR sikrer en passende overensstemmelse med ISO 27001+2-standarderne et passende informationssikkerhedsniveau.

Databeskyttelsesrådgiver (DPO)

Inventio.IT har vurderet, at det ikke er nødvendigt at have en DPO.

Privatliv og beskyttelse af personoplysninger

Som nævnt er Inventio.IT databehandler for sine kunder, i og med, at kunderne tilbydes en it-service, hvortil de kan overføre og behandle data og anvende data til videre bearbejdning indenfor deres respektive it-opgaver. Inventio.IT er ikke ansvarlig for data, som kunderne uploader til deres Inventio.IT it-service. Med udgangspunkt i kategorier og fortrolighed af data, som kunden overlader til behandling, skal Inventio.IT iværksætte alle nødvendige sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Nedenfor beskrives Inventio.ITs procedurer for, hvordan Inventio.IT som databehandler opererer under instruks fra de dataansvarlige.

Databehandleraftaler

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

Som databehandler pålægges Inventio.IT A/S et særligt ansvar defineret i Databeskyttelsesforordningen, udmøntet som krav i en databehandleraftale. Inventio.IT A/S 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 Databeskyttelsesforordningen - GDPR).
- Stille ekspertise til rådighed for kunden for at sikre efterlevelse af Artikel 32 – 34 i GDPR.
    - Artikel 32 – behandlingssikkerhed
    - Artikel 33 – Anmeldelse af brud på persondatasikkerheden
    - Artikel 34 – Underretning om brud på persondatasikkerheden til 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 Inventio.IT med persondata på baggrund af kundernes instrukser, der beskriver en formålsafgrænsning for, hvad data må benyttes til. Inventio.IT er således ansvarlig for, at data indsamlet med ét formål ikke behandles i strid med dette.

Hjemmelen for behandling af persondata i Inventio.ITs udbudte ERP Online Services, skal søges i den dataansvarliges overholdelse af retlig forpligtigelse eller opfyldelse af kontraktligt forhold.

Adgang til kundedata

Inventio.IT tilbyder ERP Online Services, der driftes af Inventio.ITs driftsafdeling. Generelt har medarbejdere i Inventio.IT ikke adgang til kundedata, medmindre specifikke arbejdsopgaver taler herfor.

Inventio.IT 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.
- Omfattende introduktionsforløb med fokus på regler for omgang med kundedata og opfølgning via awarenes-kampagner.
- Procedure for tildeling, revision og kontrol af adgange til kundedata.
- Regler for behandling af kundedata i Inventio.ITs ISMS.

Inventio.IT logger og overvåger adgangen til kundernes data for at sikre, at ingen uautoriserede personer får adgang, eller tildelte adgange misbruges.

Væsentlige ændringer i forhold til it-sikkerhed

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

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver den generelle ramme for Inventio.ITs ERP Online Services, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Inventio.IT er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til Inventio.ITs ERP Online Services. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål. I forbindelse med håndteringen af password-sikkerheden er revisionen udført ud fra et generelt perspektiv.

For nogle brugervirksomheder kan sikkerheden omkring password-opbygningen ligge under rammen, såfremt ledelsen hos kunden har ønsket det. Ansvaret for afstemning af kontrolmiljøet for password-sikkerheden ligger hos den enkelte brugervirksomhed, og hos dem som anvender denne erklæring.

Kunderne er ansvarlige for datatransmission til Inventio.ITs ERP Online Services, og det er kundernes ansvar at skabe den nødvendige datatransmission til Inventio.ITs datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Inventio.ITs beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af Inventio.ITs ERP Online Services. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

BILAG 1:

Inventio.IT har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27001 og 2

0. Risikoanalyse og -håndtering

0.0. Vurdering af sikkerhedsrisici
0.1. Risikohåndtering

5. Informationssikkerhedspolitik

5.1. Retningslinjer for styring af informationssikkerhed

6. Organisering af informationssikkerhed

6.1. Intern organisering
6.2. Mobilt udstyr og fjernarbejdspladser

7. Medarbejdersikkerhed

7.1. Før ansættelsen
7.2. Under ansættelsen
7.3. Ansættelsesforholdets ophør eller ændring

8. Styring af aktiver

8.1. Ansvar for aktiver

9. Adgangsstyring

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

10. Kryptografi

10.1. Kryptografiske kontroller

12. Driftssikkerhed

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

13. Kommunikationssikkerhed

13.1. Styring af netværkssikkerhed

14. (Anskaffelse), udvikling og vedligeholdelse af systemer

14.1. Sikkerhedskrav til it-systemet
14.2. Sikkerhed i udviklings- og hjælpeprocesser

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 Inventio.IT A/S' ERP Online Services og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Inventio.IT A/S' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af kontrolmiljøet i tilknytning til it-driften af ERP Online Services, jævnfør databehandleraftale med kunder, i hele perioden 1. januar 2024 - 31. december 2024, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. Erklæringen dækker ikke kontroller eller tilsyn med underleverandører. Disse underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Erklæringen dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. virksomhedsbeskrivelsen kapitel 2, afsnittet om komplementerende kontroller.

Inventio.IT A/S' ansvar

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

Beierholms uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om Inventio.IT 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 Inventio.IT 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 Inventio.IT A/S

Inventio.IT 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 Inventio.IT 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 Inventio.IT A/S' kontrolmiljø i tilknytning til it-driften af ERP Online Services, således som det var udformet og implementeret i hele perioden 1. januar 2024 - 31. december 2024, i alle væsentlige henseender er retvisende, og

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

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

Beskrivelse af testede 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 Inventio.IT 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 kontrolmiljøet er passende, og om kravene i databeskyttelsesforordningen er overholdt.

Søborg, den 9. januar 2025

Beierholm
Godkendt Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT auditor, Director

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, tests og resultater heraf

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

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

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som Inventio.IT 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. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel til passende personale hos Inventio.IT 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.

KONTROLMÅL - INDLEDNING:

Risikovurdering og – håndtering

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

Inventio.IT 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 den i beskrivelsen definerede it-drift af ERP Online Services. 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 it-driften af ERP Online Services arbejdes med en løbende vurdering af den risiko, der opstår som følge af de forretningsmæssige forhold. Vi har kontrolleret, at risikovurderingen er forankret ned igennem virksomhedens organisation. Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.	Ingen bemærkninger.

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.

Inventio.IT 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 godkendte af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes med planlagte intervaller.	Vi har indhentet og revideret Inventio.IT 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 Inventio.IT A/S' intranet.	Ingen bemærkninger.

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.

Inventio.IT 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 it-driften af ERP Online Services. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder.	Ingen bemærkninger.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og håndteringen af sikkerhedsforholdene er passende.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevist inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos Inventio.IT A/S har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, således at området er afdækket i forhold til risikovurderingen for området.	Ingen bemærkninger.

KONTROLMÅL 7:

Medarbejdersikkerhed

Der 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.

Inventio.IT 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 Inventio.IT 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 bekendte med deres tavshedspligt via en underskrevet ansættelseskontrakt og via Inventio.IT 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 it-driften af ERP Online Services er bekendt med deres tavshedspligt. Vi har stikprøvevis gennemgået centrale medarbejderes stillingsbeskrivelser og ansættelseskontrakter, og efterfølgende testet den enkelte medarbejders kendskab til arbejdsmæssige roller og tilhørende sikkerhedsansvar. Revision har påset, at Inventio.IT A/S' personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos Inventio.IT A/S.	Ingen bemærkninger.

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 it-driften af ERP Online Services får et passende beskyttelsesniveau.

Inventio.IT 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 it-driften af ERP Online Services.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til Inventio.IT A/S' it-drift af ERP Online Services. Gennem observation og kontrol har vi kontrolleret relationer over til de centrale knowhow-systemer for it-driften af ERP Online. Vi har ved observationer og forespørgsler kontrolleret, at Inventio.IT A/S overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Ingen bemærkninger.

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.

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for Inventio.IT A/S' adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i Inventio.IT A/S. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. Inventio.IT A/S' retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger Inventio.IT A/S' retningslinjer, og at autorisationer tildeles i henhold til aftale.	Ingen bemærkninger.
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 formaliserede forretningsgange for tildeling og afbrydelse af brugeradgang. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende autorisationssystemer i relation til adgangsstyring i Inventio.IT. • at den formaliserede forretningsgang for tildeling og afbrydelse af brugeradgang er implementeret i Inventio.IT A/S' systemer, og at der foretages løbende opfølgning på registrerede brugere.	Ingen bemærkninger.
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 almindelige og udvidede rettigheder hver 12. måned.	Ingen bemærkninger.

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 Inventio.IT A/S. Vi har ved stikprøvevis inspektion påset, • at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login. • at standardpassword ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standardpassword.	Ingen bemærkninger.
Adgange til operativsystemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde, krav om kompleksitet, maksimal løbetid og et password kan ikke kan genbruges. Herudover er opsat krav om 2-faktor logon. Endvidere bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i Inventio.IT 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 • maksimal levetid for password • minimum historik for password • lockout efter fejlede login-forsøg • 2-faktor logon	Ingen bemærkninger.

KONTROLMÅL 10:

Kryptografi

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

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

KONTROLMÅL 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.

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

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.

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

Kontrolmål: Backup

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

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

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.

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

Kontrolmål: Styring af driftssoftware

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

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

KONTROLMÅL 13:

Kommunikationssikkerhed

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

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og 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 er etableret forbindelser for datakommunikation mod internettet via mere end én ISP-leverandør. • Stikprøvevist gennemgået dokumentationen fra leverandørerne i forhold til skriftligt aftalegrundlag samt løbende afregning af ydelser hos ISP-leverandørerne.	Ingen bemærkninger.
Der skal være etableret passende forretningsgange for håndtering af trusler målrettet angreb fra internettet (cyberangreb). I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.	Det er kontrolleret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for håndtering af cyber-angreb. • at der er udarbejdet og implementeret planer for håndtering af truslen. • at planerne har et tværorganisatorisk samarbejde mellem interne grupper.	Ingen bemærkninger.

KONTROLMÅL 14:

(Anskaffelse), udvikling og vedligeholdelse af systemer

Sikre, at ERP Online Services er håndteret med en passende it-sikkerhed, herunder en passende funktionsadskillelse mellem produktionsmiljøet og udviklingsmiljø.

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Inventio.IT A/S har tilrettelagt systemudvikling og vedligeholdelsesaktiviteter baseret på egenudviklet projektmodel. Udviklingsorganisationen er opbygget med en central styregruppe, som har ansvaret for udformning af passende forretningsgange samt tilhørende ledelseskontroller. Udviklingsgruppen for en bestemt løsning i ERP Online Services skal godkende alle ændringerne i denne løsning, inden ændringerne idriftsættes. Softwareudvikling skal være placeret på selvstændige testmiljøer.	Vi har: • forespurgt ledelsen om, der er udarbejdet en overordnet kvalitetsstyringsmodel for håndteringen af softwareudvikling. • i forbindelse med revisionen er det kontrolleret, at der findes procedurer og forretningsgange for udrulning af software-ændringer. Brugerstyringen sikrer, at der er en passende kontrol i forbindelse med håndteringen af den logiske adgangskontrol. Vi har stikprøvevist kontrolleret, at alle brugeraktiviteter bliver registeret og logget i central database. Logdatabasen bliver regelmæssigt gennemgået af den it-sikkerhedsansvarlige. Vi har kontrolleret, at der findes procedurer for adskillelse mellem produktionsmiljøet og miljøet for udvikling og vedligeholdelse. I forbindelse med vores revision har vi kontrolleret, at der findes adskilte testmiljøer til brug for softwareudviklingen. Stikprøvevist er det testet, at produktions-miljøet for softwareudvikling sker fra et selvstændigt IP-segment.	Ingen bemærkninger.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevist inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Ingen bemærkninger.
Ved ændringer, der påvirker driftsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt i samarbejde mellem driftschefen og den ansvarlige for it-sikkerheden. Der anvendes udelukkende godkendte leverandører.	Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere. Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører. Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.	Ingen bemærkninger.
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.	Ingen bemærkninger.

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.

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

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.

Inventio.IT 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 ERP Online Services i Inventio.IT 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 Inventio.IT A/S' interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Ingen bemærkninger.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Principper for behandling af personoplysninger:

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

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme i form af standardkontrakter, Service Level Agreement samt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, og at procedurerne indeholder krav til lovlig behandling af personoplysninger.	Ingen bemærkninger.
Der udføres alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har kontrolleret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har kontrolleret, ved en stikprøve på et passende antal behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen bemærkninger.
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 i strid med lovgivningen.	Ingen bemærkninger.

Databehandling:

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

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

Den databehandlendes 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.

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
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 4 underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger.
Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere skal dette godkendes af den dataansvarlige.	Vi har kontrolleret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen bemærkninger.
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 4 underdatabehandleraftaler, at aftalerne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen bemærkninger.

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

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.

Inventio.IT A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
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 den registrerede.	Vi har kontrolleret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen bemærkninger.

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.

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

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.

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

PENNEO

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

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

Jesper Aaskov Pedersen
IT auditor, Director
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: 55a3ea90-967e-4a5c-b854-37be4db4517b
IP: 212.98.xxx.xxx
2025-01-09 12:51:38 UTC

Kenneth Kornbeck Lindeblad
It-sikkerhedskoordinator/ Marketingchef
På vegne af: Inventio.IT A/S
Serienummer: 150486e1-69c1-4395-9422-c2306e6a3a76
IP: 83.140.xxx.xxx
2025-01-09 12:51:55 UTC

Michael Steen Sørensen
Adm. Direktør
På vegne af: Inventio.IT A/S
Serienummer: 41ee698a-f792-4e50-962c-04040c96a55d
IP: 45.148.xxx.xxx
2025-01-09 13:31:55 UTC

Kim Holm Larsen
Beierholm Godkendt Revisionspartnerselskab CVR: 32895468
Statsautoriseret revisor
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2025-01-09 13:34:39 UTC