



APRIL 2026

IST APS

ISAE 3402 TYPE 2 ERKLÆRING

CVR 25545079

Uafhængig revisors erklæring om kontrolmiljøet i tilknytning til it-driften for IST SaaS løsninger.

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 IST SaaS løsninger.

Kapitel 3:

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

Kapitel 4:

Kontrolmål, kontrolaktivitet, tests og resultater heraf.

Ledelseserklæring

Medfølgende beskrivelse er udarbejdet til brug for kunder og deres revisorer, der har anvendt IST SaaS løsninger, 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 er overholdt.

IST ApS bekræfter, at:

- (A) Den medfølgende beskrivelse, kapitel 2 (inkl. bilag 1), giver en retvisende beskrivelse af IST ApS' kontrolmiljø i tilknytning til it-driften af IST SaaS løsninger i hele perioden 1. april 2025 - 31. marts 2026. 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 med IST SaaS løsninger
 - Relevante kontrolmål og kontroller designet og implementeret til at nå disse mål
 - Kontroller, som vi med henvisning til IST SaaS løsningers afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
 - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger
 - (ii) Indeholder relevante oplysninger om ændringer i it-driften af IST SaaS løsninger foretaget i perioden 1. april 2025 - 31. marts 2026.
 - (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 vigtig 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. april 2025 - 31. marts 2026. 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. april 2025 - 31. marts 2026.
- (C) 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 IST ApS' standardaftale samt tilhørende databehandlertale.

Roskilde, den 17. april 2026

Kristian Madsen,
Head of Business Region Danmark

Pernille Frederiksen,
Informationsikkerhedskonsulent

IST ApS, Gammel Marbjergvej 9, 4000 Roskilde, CVR 25545079

Beskrivelse af kontrolmiljøet i tilknytning til it-driften af IST SaaS løsninger

Indledning

Formålet med denne beskrivelse er at give IST ApS' kunder og deres revisorer indsigt i de kontroller og sikkerhedsforanstaltninger, der er etableret i forbindelse med driften af IST ApS' SaaS-løsninger. Beskrivelsen er udarbejdet med henblik på at understøtte kravene i ISAE 3402, som er den internationale standard for erklæringer om kontroller hos serviceleverandører.

Beskrivelsen omfatter de væsentligste tekniske og organisatoriske sikkerhedsforanstaltninger, der er implementeret i forbindelse med drift, vedligeholdelse og udvikling af virksomhedens SaaS-løsninger.

Produktrammen for denne beskrivelse omfatter følgende løsninger:

- IST Dagtilbud Børn
- IST Dagtilbud Personale
- IST Dagtilbud Admin
- IST Elevadministration
- IST Tjenestetid
- IST Pladsanvisningen
- IST Personkreds
- IST Studie+
- IST SPS Flow

Beskrivelse af IST ApS

IST ApS er en del af den svenske koncern IST Group AB, som blev grundlagt i 1982. Virksomheden beskæftiger omkring 105 medarbejdere fordelt på kontorer i Roskilde og på Midtfn.

I 2013 opkøbte IST Group AB den danske virksomhed Tabulex ApS, og i 2017 udvidede IST ApS forretningen yderligere gennem opkøbet af UDDATA, hvilket betød, at virksomheden også begyndte at levere løsninger til ungdomsuddannelser.

IST ApS udvikler og leverer administrative it-løsninger som Software-as-a-Service (SaaS) til offentlige og private uddannelsesinstitutioner, herunder dagtilbud, grundskoler og ungdomsuddannelser. Løsningerne understøtter blandt andet elevadministration, planlægning og håndtering af medarbejdernes arbejdstid.

Virksomheden leverer desuden drift, support, konsulentydelse og kurser i relation til de leverede systemer. Systemerne udvikles og vedligeholdes løbende, blandt andet for at sikre, at funktionalitet og data-behandling lever op til gældende lovgivning og regulering.

IST ApS leverer løsninger til størstedelen af de danske kommuner samt en række uddannelsesinstitutioner og er blandt de førende leverandører af administrative it-systemer til uddannelsessektoren i Danmark.

Virksomheden arbejder efter dokumenterede processer og er certificeret i ISO 9001. Arbejdet med informationssikkerhed tager udgangspunkt i principperne i ISO 27001 og ISO 27002.

IST ApS' SaaS-plattform drives i et centralt driftsmiljø, hvor både infrastruktur, applikationer og databaser administreres og overvåges af virksomhedens driftsorganisation.



Periodens ændringer

I den seneste revisionsperiode har IST ApS haft fokus på videreudvikling og konsolidering af virksomhedens centrale produkter.

Dette omfatter blandt andet fortsat udvikling af løsningen Vikar+ samt implementering og udrulning af virksomhedens fraværløsning. Disse initiativer bidrager til at styrke virksomhedens produktportefølje og understøtte den langsigtede udvikling af virksomhedens løsninger.

For at sikre fortsat relevans inden for efter- og voksenuddannelsesområdet har IST ApS udvidet systemgodkendelsen for Studie+ til også at omfatte AVU, hvilket betyder, at løsningen nu kan understøtte hele ungdoms- og voksenuddannelsesområdet.

Derudover har virksomheden arbejdet med implementering af løsningen SPS Flow som en integreret del af den samlede produktportefølje.

Forretningsstrategi og it-sikkerhedsstrategi

IST ApS' strategi er at sikre, at virksomhedens drift og leverancer understøttes af et højt niveau af informationssikkerhed. Informationssikkerhed er derfor integreret i virksomhedens forretningsprocesser og organisatoriske styring.

Som leverandør af it-løsninger til uddannelsessektoren håndterer IST ApS betydelige mængder personoplysninger. Det er derfor et centralt mål for virksomheden at sikre, at data behandles forsvarligt og i overensstemmelse med gældende lovgivning.

Informationssikkerhedsarbejdet i IST ApS tager udgangspunkt i følgende grundlæggende principper:

Tilgængelighed

Systemer og data skal være tilgængelige for autoriserede brugere, når der er behov for det.

Integritet

Data skal være korrekte og beskyttet mod uautoriseret ændring eller sletning.

Fortrolighed

Adgang til data skal være begrænset til autoriserede brugere.

IST ApS arbejder for at sikre, at virksomhedens sikkerhedsniveau som minimum:

- overholder gældende lovgivning, herunder GDPR
- følger anerkendt branchestandard
- lever op til kundernes krav til en professionel leverandør


Arbejdet med informationssikkerhed er forankret i et Information Security Management System (ISMS) baseret på ISO 27001, som understøtter virksomhedens processer for risikostyring, sikkerhedspolitikker og kontroller.

IST ApS' organisation og organisering af it-sikkerheden

IST ApS indgår i koncernen IST Group AB, som har aktiviteter i Sverige, Tyskland, Norge og Danmark.

Den overordnede ledelse i IST ApS varetages af virksomhedens CEO/Adm. Direktør, som også indgår i koncernledelsen i IST Group AB.

Organisationen er opdelt i flere forretningsområder, herunder:



Customer Success. Består af 28 medarbejdere, som håndterer support, konsulentytelser og kontakt med brugere og kunder.

Development & AI. Består af 44 medarbejdere, som står for udvikling og vedligeholdelse af virksomhedens it-systemer.

Sales & Marketing. Består af 7 medarbejdere, som varetager salg, kommunikation og kontraktforhold.

Informationssikkerhed koordineres af en informationssikkerhedskonsulent, som arbejder tværgående i organisationen.

Risikostyring

IST ApS arbejder systematisk med identifikation og håndtering af risici i relation til drift og informationsikkerhed.

Formålet med risikostyringen er at sikre, at de risici, der er forbundet med virksomhedens aktiviteter, reduceres til et acceptabelt niveau.

Risikovurderinger gennemføres blandt andet:

- periodisk som led i den løbende sikkerhedsstyring
- ved væsentlige ændringer i systemer eller infrastruktur
- ved implementering af nye systemer eller services

Resultaterne dokumenteres i et centralt risikoregister, og relevante risikobegrænsende tiltag implementeres i driftsmiljøet.

Håndtering af it-sikkerhed

Ledelsen i IST ApS har det overordnede ansvar for virksomhedens informationssikkerhed og for at sikre, at de fastlagte sikkerhedspolitikker og procedurer efterleves.

Virksomhedens centrale it-sikkerhedspolitik fastlægger de overordnede principper for informationssikkerhed og beskriver organisationens struktur for styring af sikkerhed.

Politikken gennemgås og opdateres minimum én gang årligt.


It-sikkerhedspolitikken suppleres af mere detaljerede procedurer, der beskriver håndtering af sikkerhed i forbindelse med drift, udvikling og support.

Servere og netværksenheder er dokumenteret i virksomhedens dokumentationssystem, hvor konfigurationer og ændringer registreres for at sikre sporbarhed.

HR, medarbejdere og kompetencer

Medarbejdernes kompetencer og domæneviden udgør en væsentlig forudsætning for virksomhedens evne til at levere stabile og sikre it-services til kunderne. Virksomheden arbejder derfor systematisk med at sikre, at medarbejderne har de nødvendige faglige og sikkerhedsmæssige kompetencer til at varetage deres arbejdsopgaver.

IST ApS har etableret dokumenterede procedurer for rekruttering, ansættelse og fratrædelse af medarbejdere. I forbindelse med ansættelse gennemgår nye medarbejdere et introduktionsforløb, som blandt andet omfatter virksomhedens organisation, arbejdsprocesser og grundlæggende principper for informa-



tionssikkerhed og databeskyttelse. Introduktionsforløbet indeholder også en gennemgang af virksomhedens it-sikkerhedsregler, herunder god it-adfærd, håndtering af personoplysninger samt virksomhedens rolle som databehandler.

Som led i ansættelsesprocessen underskriver medarbejdere en erklæring om fortrolig behandling af kundedata og virksomhedens informationer. Fortrolighedsforpligtelsen er en del af medarbejderens ansættelseskontrakt og gælder også efter ansættelsesforholdets ophør.

IST ApS afholder løbende medarbejdersamtaler og kompetenceudviklingsaktiviteter med henblik på at sikre, at medarbejdernes faglige kompetencer vedligeholdes og udvikles i takt med virksomhedens behov og udviklingen i branchen.

Medarbejdere kan i begrænset omfang arbejde fra andre lokationer end virksomhedens kontorer. For sådanne situationer er der etableret retningslinjer for fjernarbejde, herunder krav til sikker adgang til virksomhedens systemer. Adgang til interne systemer fra eksterne lokationer sker via krypterede forbindelser, og adgangen til backend-systemer og driftsmiljøer er begrænset til autoriserede medarbejdere.

Ved fratrædelse af medarbejdere gennemføres en formaliseret proces, hvor relevante systemadgange lukkes, og udleveret udstyr tilbageleveres. I forbindelse med fratrædelsessamtalen orienteres medarbejderen om, at fortrolighedsforpligtelsen fortsat er gældende efter ansættelsens ophør.

Fysisk sikkerhed

IST ApS' driftsmiljø er placeret i et datacenter hos Digital Realty, som leverer faciliteter og infrastruktur til hosting af virksomhedens it-systemer. Ved at anvende en specialiseret datacenterleverandør sikres, at de fysiske rammer omkring driften lever op til anerkendte standarder for sikkerhed og drift.

Digital Realty er ansvarlig for den fysiske sikring af datacenteret, herunder adgangskontrol, overvågning, strømforsyning, køling samt systemer til brand- og vanddetektion. Datacenteret er opbygget med flere lag af fysisk sikkerhed, der tilsammen skal reducere risikoen for uautoriseret adgang eller driftsforstyrrelser.

IST ApS anvender to geografisk adskilte datacentre, hvor det sekundære datacenter anvendes til backup og beredskabsformål.

IST ApS råder over et separat serverområde i datacenteret, som er fysisk adskilt fra andre kunders installationer. Adgang til området sker via personlige adgangskort og registreres i datacenterets adgangssystem.

Datacenteret overvåges løbende af sikkerhedspersonale, og adgang til bygningen sker via kontrollerede adgangspunkter. Identifikation af personer med adgang til datacenteret sker blandt andet ved brug af biometriske metoder.

Strøm og køling

Datacenteret er etableret med redundant strømforsyning for at sikre høj tilgængelighed for de systemer, der hostes i miljøet. Strømforsyningen leveres via flere uafhængige strømfeeds, hvilket reducerer risikoen for nedetid i tilfælde af fejl i den primære strømforsyning.

Ved bortfald af ekstern strømforsyning overtages strømforsyningen først af batteribackup-systemer og efterfølgende af dieselgeneratorer, der kan levere strøm til datacenteret i en længere periode. Generatorerne er etableret i redundant konfiguration, så fejl i en enkelt generator ikke medfører tab af redundans.

Datacenterets kølesystemer overvåges løbende for at sikre stabile temperatur- og fugtighedsforhold i servermiljøet.

Sikring mod vand og brand

Datacenteret er udstyret med systemer til detektion af vandlækager og overvågning af luftfugtighed. Serverområderne er etableret med hævet gulv og overvågningssystemer, som kan registrere eventuelle vandlækager i datacenteret.

Branddetektion og brandslukning varetages af automatiserede systemer, der kontinuerligt overvåger temperatur og røgudvikling. Brandslukningssystemet er baseret på gasbaseret slukning, som kan slukke en brand uden at beskadige elektronisk udstyr.

Offsite lokation

Som en del af virksomhedens beredskabs- og backupstrategi anvender IST ApS en sekundær lokation placeret i betydelig geografisk afstand fra den primære datacenterlokation.

Den sekundære lokation drives ligeledes af Digital Realty og anvendes blandt andet til opbevaring af off-site-backups. Placeringen af backupdata på en separat lokation reducerer risikoen for datatab i tilfælde af større hændelser, der påvirker den primære driftslokation.

Kontrol med datacenterleverandør

IST ApS fører løbende kontrol med den eksterne datacenterleverandør for at sikre, at leverandøren lever op til de aftalte service- og sikkerhedskrav.

Datacenterne er etableret i overensstemmelse med Tier 3-standarder for datacenterinfrastruktur og er certificeret efter ISO 27001 samt ISO 22301. Digital Realty udarbejder årligt en SOC 2 revisionsrapport, som dokumenterer de kontroller, der er etableret i datacenteret. Rapporten gennemgås af IST ApS som led i virksomhedens leverandøropfølgning. Resultatet af gennemgangen indgår i vurderingen af, om leverandøren fortsat lever op til de aftalte serviceforpligtelser.

Netværk og datalinjer

Dataforbindelsen til driftsmiljøet består af to uafhængige linjer med opgraderbar 1gbs kapacitet. I setuppet indgår én primær og én sekundær datalinje, hvor BGP automatisk afgør, hvilken det er bedst at benytte. Bryder den primære linje ned, routes trafikken automatisk via den sekundære. Når den primære er reetableret, routes trafikken igen via denne.

Vores samarbejde med ISP'en omfatter Ddos beskyttelse med automitigering indenfor kort tid. Mitigeringsstrategien er lagt i samarbejde med IST Group AB's driftsteknikere, og tilpasset vores normale trafikmønstre. Ved et Ddos angreb overstiges tærskelværdierne, og automitigeringen træder til.


Driftsmiljøets perimetersikkerhed består af to veldimensionerede firewalls, der er sat i et aktivt/passivt cluster. Forbindelsen gennem firewallen sikres via en gensidig overvågning i de to firewalls, der selv afgør, hvilken der er aktiv, og hvilken der er passiv.

Firewallen er regelbaseret og har som udgangspunkt en "deny all" trafikregel. Herpå er der udarbejdet et regelsæt, der tillader specifikke protokoller mod en given servergruppering (Eks: https -> Webservere).

Trafikken passerer gennem redundante firewalls og videresendes herefter til en dedikeret load balancer, som fordeler trafikken mellem de relevante applikationsservere.

Endelig fortager firewallen inspektion af datapakker (IDS). Automatiseret scanning og blokering af trafik baseres på sårbarhedssituationen og holdes dagligt opdateret.

Driftsmiljøet er tilkoblet internettet via to redundante forbindelser leveret af en internetudbyder. Forbindelserne er etableret som en primær og sekundær linje, hvor redundans håndteres via VRRP og BGP, så trafikken automatisk kan omdirigeres i tilfælde af udfald. Forbindelserne er etableret med kapacitet på op



til 1 Gbit/s og er konfigureret således, at trafikken automatisk kan omdirigeres mellem forbindelserne i tilfælde af udfald.

Trafikstyring mellem forbindelserne håndteres via BGP, som sikrer automatisk failover mellem forbindelserne. Hvis den primære forbindelse ikke er tilgængelig, vil trafikken automatisk blive dirigeret via den sekundære forbindelse.

Som en del af samarbejdet med internetudbyderen anvendes DDoS-beskyttelse, som kan identificere og mitigere trafikmønstre, der indikerer et distribueret denial-of-service-angreb.

Perimetersikkerheden i driftsmiljøet varetages af redundante firewalls konfigureret i et high-availability setup. Firewallkonfigurationen følger princippet om, at al trafik som udgangspunkt er blokeret, hvorefter specifikke trafiktyper tillades via definerede regler.

Firewallen anvendes desuden til belastningsfordeling mellem servere samt til inspektion af netværkstrafik med henblik på at identificere og blokere uautoriseret eller skadelig trafik.

Hardware setup

Driftsmiljøets hardwareinfrastruktur er opbygget omkring et antal fysiske servere (hypervisorer), hvorpå der afvikles flere virtuelle servere. Til understøttelse af den virtuelle infrastruktur anvendes dedikerede storage-systemer (SAN), som sammen med hypervisorplatformen bidrager til høj tilgængelighed og skalerbarhed i driftsmiljøet.

Det virtuelle miljø består af fysiske servere organiseret i flere clustre. Clustrene er dimensioneret med tilstrækkelige ressourcer til, at en eller flere noder kan udfalde uden at påvirke de kørende services. Denne arkitektur muliggør samtidig gennemførelse af opdateringer af firmware og software uden planlagte driftsafbrydelser.

Diskkapacitet håndteres via en central netværksbaseret storage-løsning (SAN). Adgangen til SAN'et sker gennem fuldt redundante netværksforbindelser mellem hypervisorerne. Den samlede storagekapacitet er opdelt i logiske enheder (LUN'er), som replikeres for at understøtte datatilgængelighed og redundans.

Alle diske er krypteret. Hvis en disk fjernes fra SAN-løsningen, slettes den tilhørende krypteringsnøgle automatisk efter kort tid, hvilket sikrer, at data ikke længere kan tilgås.

Drift af SaaS løsninger


Faste driftsopgaver udføres med fastlagte intervaller som en del af den løbende drift og vedligeholdelse af IST ApS' it-infrastruktur. Opgaverne administreres og udføres af virksomhedens driftsafdeling, som er ansvarlig for den kontrollerede drift og vedligeholdelse af servermiljøet.

De enkelte driftsopgaver er dokumenteret i tilhørende procedurer og checklister, som beskriver opgavernes indhold, frekvens og udførelse. Dette understøtter en ensartet og systematisk gennemførelse af driftsopgaverne.

Registrering af it-udstyr i produktion (aktiver)

IST ApS registrerer virksomhedens it-aktiver og tilhørende services i en central CMDB (Configuration Management Database). Formålet med CMDB'en er at sikre et opdateret overblik over de it-aktiver, der understøtter leverancen af virksomhedens it-services til kunder.

It-udstyr med en tilknyttet IP-adresse, som direkte eller indirekte indgår i produktions- eller kontormiljøer, skal registreres og vedligeholdes i CMDB'en. Dette omfatter blandt andet netværksudstyr, fysiske og virtuelle servere, printere, pc'er, mobile enheder, applikationer, styresystemer, services og databaser.



For hvert registreret aktiv dokumenteres relevante oplysninger om aktivet og dets tilknytning til det omkringliggende it-miljø. Detaljeringsgraden afhænger af aktivtypen. De registrerede oplysninger kan f.eks. omfatte tilknyttet netværk, IP-adresse, ansvarlig person eller team, aktivets rolle (f.eks. produktion eller test/staging) samt relationer til databaser, applikationer og øvrige services.

CMDB'en anvendes som grundlag for styring og vedligeholdelse af virksomhedens it-infrastruktur.

Driftsovervågning

Driftsmiljøet hos IST ApS overvåges kontinuerligt 24/7/365 ved hjælp af automatiserede overvågningsværktøjer. Overvågningen omfatter blandt andet serverressourcer såsom CPU, RAM, diskforbrug og netværkskapacitet samt generel systemtilgængelighed.

Overvågningen inkluderer desuden relevante it-services, herunder backupfunktioner, tilgængelighed af kundevedtatte systemer samt udvalgte interne systemer, der understøtter driften.

Den primære overvågning foretages internt i driftsmiljøet. For også at sikre overvågning af eksternt tilgængelighed er der etableret en supplerende offsite-overvågning. Ved registrering af fejl eller driftsforstyrrelser genereres en alarm til virksomhedens Network Operations Center (NOC), hvor hændelsen analyseres og håndteres. Ved kritiske fejl i servere eller services adviseres den vagthavende driftsmedarbejder direkte med henblik på hurtig håndtering.

NOC-funktionen anvendes internt i IST ApS og er ikke tilgængelig for kunder. Kunder, der oplever driftsrelaterede problemer, skal kontakte IST ApS via de supportkanaler, der er fastlagt i kundens kontraktgrundlag og de generelle vilkår.

Driftsstatus kommunikerer via IST ApS' hjemmeside: <https://www.ist.com/dk/drift>

Logning

Logning anvendes som et centralt værktøj til overvågning, fejlhåndtering og efterfølgende analyse af hændelser. Da logdata kan indeholde forskellige typer informationer, er adgangen til logs begrænset og styres i overensstemmelse med medarbejdernes arbejdsopgaver og ansvarsområder.

IST ApS anvender logning på flere niveauer for at understøtte driftsovervågning og sikkerhedsmæssig opfølgning. Dette omfatter blandt andet:


- Applikationslogs, som registrerer specifikke operationer og hændelser i virksomhedens applikationer.
- Sikkerhedslogs, som registrerer brugeraktiviteter, herunder login til applikationer samt adgang til informationer af følsom eller fortrolig karakter.
- Syslog, som anvendes til central overvågning og registrering af systemrelaterede hændelser i infrastrukturen.

Logningen understøtter virksomhedens arbejde med driftsovervågning, hændeshåndtering og sikkerhedsopfølgning.

Backup

Formålet med backup er at sikre, at kundedata i IST ApS' hostingmiljø kan genskabes korrekt og inden for en rimelig tidsramme i tilfælde af driftsforstyrrelser eller datatab. Backup etableres på flere niveauer, herunder virtuelle servere, systemkonfigurationer og databaser, hvilket understøtter flere muligheder for reetablering afhængigt af hændelsens karakter.

Der foretages backup af relevante databaser og systemkonfigurationer med henblik på at muliggøre reetablering i tilfælde af en nødsituation. Frekvensen af backup fastsættes på baggrund af systemets kritikalitet og de forretningsmæssige krav til tilgængelighed og databeskyttelse.



I henhold til virksomhedens backuppolitik for kundedatabaser foretages der daglige backups, minimum én gang i døgnet. For mindst én af disse backups gennemføres der ugentligt en reetableringstest med henblik på at verificere backupens integritet og anvendelighed. Backups lagres på dedikerede backupservere i driftsmiljøet og kopieres desuden til en fysisk adskilt lokation for at reducere risikoen for datatab.

Alle backups krypteres ved anvendelse af AES-256-kryptering. Overførsel af backupdata mellem primært driftsmiljø og offsite-lokation sker via krypterede datalinjer.

Daglige backups af kundedatabaser opbevares i 30 dage. Derudover opbevares månedlige backups i op til tre måneder, halvårlige backups i seks måneder samt årlige backups i op til tolv måneder i overensstemmelse med virksomhedens backuppolitik.

Patch management og ændringshåndtering

Formålet med patch management er at sikre, at relevante opdateringer fra leverandører – herunder patches, sikkerhedsopdateringer og service packs – implementeres rettidigt for at reducere risikoen for driftsforstyrrelser, sårbarheder og uautoriseret adgang til systemerne.

Implementeringen af opdateringer sker efter fastlagte procedurer, der understøtter en kontrolleret og systematisk håndtering af ændringer i driftsmiljøet.

Vedligeholdelse og opdatering af Windows-operativsystemer samt tilhørende backend-systemer administreres via Windows Server Update Services (WSUS). Via denne løsning distribueres sikkerhedsopdateringer og kritiske patches til relevante systemer med faste intervaller.

Ved etablering af nye servere følges en standardiseret installationsprocedure, der sikrer, at kun nødvendige services og applikationer aktiveres. Inden en server sættes i produktion, gennemføres en hardeningproces, hvor serverens sikkerhedsindstillinger konfigureres i overensstemmelse med anbefalede sikkerhedsstandarder. Formålet er at reducere systemets angrebsflade og sikre et ensartet sikkerhedsniveau i infrastrukturen.

Styring af it-sikkerhedshændelser

Sikkerhedshændelser og identificerede svagheder i IST ApS' systemer registreres og håndteres i henhold til virksomhedens fastlagte procedurer for hændelseshåndtering.

Formålet med hændelseshåndteringen er at sikre, at sikkerhedshændelser identificeres, analyseres og håndteres rettidigt, samt at der iværksættes relevante korrigerende og forebyggende tiltag.

Virksomheden har etableret procedurer for registrering og rapportering af hændelser, herunder sikkerhedsbrud og driftsrelaterede afvigelser. Procedurene understøtter en systematisk håndtering af hændelser og sikrer, at relevante oplysninger indsamles og dokumenteres, så hændelser efterfølgende kan analyseres og evalueres.

Registrering af afvigelser indgår som en del af virksomhedens kvalitetsstyringssystem, hvor hændelser dokumenteres og følges op af ledelsen. Ledelsen er ansvarlig for at koordinere den overordnede proces for håndtering af sikkerhedshændelser og sikre, at der gennemføres relevante forbedringstiltag.

Adgangsstyring og brugersikkerhed

Den logiske adgangsstyring i IST ApS har til formål at sikre, at kun autoriserede brugere har adgang til virksomhedens systemer og informationer.

Tildeling af adgang til driftsmiljøer sker på baggrund af et dokumenteret forretningsmæssigt behov og under hensyntagen til informationernes klassifikation.

Adgang til systemer administreres i overensstemmelse med principperne need-to-know og least privilege, hvilket betyder, at brugere alene tildeles adgang til de systemer og informationer, der er nødvendige for at udføre deres arbejdsopgaver.

Anmodning om adgang til interne systemer og produktionsmiljøer følger en fastlagt proces, der sikrer funktionsadskillelse mellem anmodning, godkendelse og implementering af adgang. Administration og dokumentation af adgangsrettigheder registreres i et centralt system til styring af adgang.

Adgang til interne systemer og driftsmiljøer fra eksterne lokationer sker via krypterede forbindelser og kontrolleret adgangsstyring.

Beredskabsstyring og forretningskontinuitet

IST ApS' leverance af SaaS-løsninger er i væsentlig grad afhængig af den underliggende it-infrastruktur. Virksomheden har derfor etableret en Business Continuity Plan (BCP), som beskriver de overordnede rammer for håndtering af væsentlige driftsforstyrrelser.

Beredskabsplanen beskriver procedurer for håndtering af hændelser, herunder kommunikation, fejlsøgning, eskalation og reetablering af systemer.

Den overordnede BCP indeholder blandt andet definitioner af beredskabsfaser, vurdering af systemers kritikalitet samt procedurer for eskalation og kommunikation.

Planen omfatter også håndtering af væsentlige hændelsesscenerier, herunder nedbrud i datalinjer og total nedetid i datacentret.

BCP'en suppleres af særskilte reetableringsplaner for kundevedtente it-services og kritiske interne systemer. For at sikre tilgængelighed til planerne opbevares de på flere forskellige medier, herunder også i fysisk form.

I løbet af kontrolperioden gennemføres relevante afprøvninger af beredskabsplanen. Derudover gennemføres årligt en kvalitetssikring af reetableringsplanerne, hvor udvalgte systemer testes gennem såkaldte skrivebordstests med henblik på at verificere planernes anvendelighed.

Udviklingsmiljø

Udvikling og test af IST ApS' software foregår i dedikerede udviklings- og testmiljøer, som er adskilt fra de produktionsmiljøer, hvor kundernes systemer afvikles.

Denne adskillelse sikrer, at fejl eller ændringer i forbindelse med udviklings- og testaktiviteter ikke påvirker de systemer, der anvendes i produktion.

Testdata i udviklingsmiljøerne består som udgangspunkt af fiktive data oprettet til testformål og indeholder ikke kundedata. I forbindelse med afsluttende testfaser kan der i visse tilfælde være behov for at anvende data, der strukturelt svarer til data i produktionsmiljøet.

Udviklings- og testmiljøer er netværksmæssigt adskilt fra produktionsmiljøet og placeret i separate netværkssegmenter. Adgangen til disse miljøer er begrænset og kan kun ske fra de udgående IP-adresser tilknyttet IST ApS' kontorlokationer.

Adgangsstyringen håndhæves via konfigurerede sikkerhedsregler i virksomhedens firewall, som regulerer hvilke protokoller og porte systemerne kan tilgås via.

Processer for udvikling, test og godkendelse af ændringer er dokumenteret i virksomhedens kvalitetsstyringssystem.



Væsentlige ændringer i forhold til it-sikkerhed

IST ApS arbejder kontinuerligt med at udvikle og forbedre virksomhedens processer og procedurer for informationsikkerhed.

Dette omfatter blandt andet løbende evaluering af eksisterende kontroller, opdatering af sikkerhedspolitikker og implementering af forbedringstiltag i den operationelle drift.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Denne beskrivelse omfatter det generelle kontrolmiljø for IST ApS' SaaS-løsninger og tager ikke højde for kundespecifikke konfigurationer eller individuelle kundefaftaler.

IST ApS er ikke ansvarlig for administration af adgangsrettigheder for den enkelte kundes brugere, herunder tildeling, ændring og nedlæggelse af brugeradgange til SaaS-løsningerne. Ansvar for styring og vedligeholdelse af brugeradgange påhviler kunden.

Kunden er derfor ansvarlig for at etablere og opretholde relevante kontroller, der understøtter opfyldelsen af dette kontrolmål.

IST ApS anvender flere former for kryptering til beskyttelse af data i transit og ved lagring. Dette omfatter blandt andet HTTPS/TLS til webtrafik, VPN-forbindelser (IPSec/OpenVPN) til sikre netværksforbindelser, SFTP til filoverførsel samt kryptering af data på storage-systemer og backupmedier.

Kunden er derudover ansvarlig for etablering og drift af forbindelsen til IST ApS' datacenter samt for at implementere relevante kontroller i relation til dette.

IST ApS har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27001+2

0. Risikoanalyse og -håndtering

- 0.0. Vurdering af sikkerhedsrisici
 - 0.1. Risikohåndtering
-

5. Informationssikkerhedspolitikker

- 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 ansættelse
 - 7.2. Under ansættelsen
 - 7.3. Ansættelsesforholds ophør eller ændring
-

8. Styring af aktiver

- 8.1. Ansvar for aktiver
 - 8.3. Mediehåndtering
-

9. Adgangsstyring

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

10. Kryptografi

- 10.1. Kryptografiske kontroller
-

11. Fysisk sikkerhed og miljøsikring

** Kontorlokaler**

- 11.1. Sikre områder
- 11.2. Udstyr

12. Driftssikkerhed

- 12.1. Driftsprocedurer og ansvarsområder
 - 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. It-sikkerhed 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
-

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

Til kunder af IST SaaS løsninger og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om IST ApS' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af kontrolmiljøet i tilknytning til it-driften af IST SaaS løsninger i hele perioden 1. april 2025 - 31. marts 2026, 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 tilknyttet anvendelsen af eksterne samarbejdspartnere. Brugen af underleverandører er nærmere oplyst i databehandleraftaler med kunderne.

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

IST ApS' ansvar

IST ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn, 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.

Beierholms ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om IST ApS' 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 kontrollerens 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 IST ApS 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 IST ApS

IST ApS' 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 vigtigt efter deres særlige forhold.

Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på datasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler 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 IST ApS' kontrolmiljø i tilknytning til it-driften af IST SaaS løsninger, således som det var udformet og implementeret i hele perioden 1. april 2025 - 31. marts 2026, 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. april 2025 - 31. marts 2026, 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. april 2025 - 31. marts 2026.

Beskrivelse af de 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 IST ApS' 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.

Søborg, den 17. april 2026

Beierholm

Godkendt Revisionspartnerselskab
CVR 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Kontrolmål, kontrolaktivitet, 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, version 2017.

Hvad angår periode har vi i vores test forholdt os til, om IST ApS har levet op til kontrolmålene i perioden 1. april 2025 - 31. marts 2026.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som IST ApS 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 er implementeret, og om de overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel til passende personale hos IST ApS. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genduføre kontrollen	Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Risikovurdering og – håndtering

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

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Gennem en risikovurdering er der sket identificering og prioritering af risici. Udgangspunkt for vurderingen er de i beskrivelsen definerede IST SaaS løsninger.</p> <p>Resultatet bidrager til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.</p>	<p>Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen.</p> <p>Vi har kontrolleret, at der for IST SaaS løsninger arbejdes med en løbende vurdering af den risiko, som opstår som følge af de forretningsmæssige forhold. Vi har kontrolleret, at risikovurderingen er forankret ned igennem virksomhedens organisation.</p> <p>Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.</p>	<p>Ingen bemærkninger.</p>

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Der er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan.</p> <p>It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation.</p> <p>Politikken revurderes efter planlagte intervaller.</p> <p>Politikken er tilgængelig for alle relevante medarbejdere.</p>	<p>Vi har indhentet og revideret IST ApS' seneste it-sikkerhedspolitik.</p> <p>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.</p> <p>Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og at den er gjort tilgængelig for medarbejderne via IST ApS' intranet.</p>	<p>Ingen bemærkninger.</p>
<p>Alle medarbejdere skal mindst 1 gang årligt have modtaget en gennemgang af de for dem relevante sikkerhedspolitikker og tilhørende retningslinjer.</p> <p>Ledelsen skal hvert år indhente en skriftlig sikkerhedserklæring fra hver medarbejder. Sikkerhedserklæringen skal bekræfte medarbejderens deltagelse i undervisningen om it-sikkerhed samt forståelse for og tilslutning til virksomhedens politikker og retningslinjer.</p>	<p>Vi har kontrolleret det seneste undervisningsmateriale i forhold til uddannelse og vejledning af IST ApS' medarbejdere i gældende politikker og retningslinjer vedrørende it-sikkerhed.</p> <p>Vi har stikprøvevist inspiceret, at medarbejderne har afgivet sikkerhedserklæringen om modtagelse af undervisningen og om forståelse af og tilslutning til virksomhedens regler og retningslinjer vedr. it-sikkerhed.</p>	<p>Ingen bemærkninger.</p>

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 sikkerhedsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.

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

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret.</p> <p>It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer.</p>	<p>Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret.</p> <p>Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisationen i forhold til IST SaaS løsninger.</p> <p>Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder.</p>	Ingen bemærkninger.
<p>Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til anvendelsen er håndteret.</p>	<p>Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser.</p> <p>Vi har stikprøvevist inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr.</p> <p>Ifm. anvendelsen af fjernarbejdspladser hos IST ApS har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, sådan at området er afdækket i forhold til risikovurderingen for området.</p>	Ingen bemærkninger.

Medarbejdersikkerhed

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

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

Styring af aktiver

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

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

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver.</p> <p>Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af IST SaaS løsninger.</p>	<p>Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af IST ApS' SaaS løsninger. Gennem observation og kontrol har vi kontrolleret relationer over til de centrale knowhow-systemer for driften af IST SaaS løsninger.</p> <p>Vi har ved observationer og forespørgsler kontrolleret, at IST ApS overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.</p>	Ingen bemærkninger.
<p>Informationer og data i relation til IST SaaS løsninger er opdelt med udgangspunkt i den forretningsmæssig værdi, følsomhed og behovet for fortrolighed.</p>	<p>Vi har kontrolleret, at der findes en passende opdeling af aktiver og tilhørende procedurer/forretningsgange ifm. IST ApS' drift af SaaS løsninger. I denne forbindelse har vi kontrolleret, om de interne procedurer og arbejdsgange mht. ejerskab af applikationer og data er overholdt.</p> <p>Vi har kontrolleret, at kontrakter, SLA og databehandleraftaler anvendes som et centralt værktøj til at sikre definitionen, adskillelsen og afgrænsningen mellem IST ApS' ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data.</p> <p>Derved påhviler der typisk kunden et eget ansvar med at sikre, at der er et passende beskyttelsesniveau på egne informationer og data.</p>	Ingen bemærkninger.
<p>Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.</p>	<p>Vi har:</p> <ul style="list-style-type: none"> forespurgt ledelsen om hvilke procedurer/kontrolaktiviteter, der udføres vedrørende destruktion af databærende medier. stikprøvevist gennemgået procedurerne for destruktion af databærende medier. 	Ingen bemærkninger.

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Der foreligger dokumenterede og ajourførte retningslinjer for IST ApS' adgangsstyring.</p>	<p>Vi har:</p> <ul style="list-style-type: none"> forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i IST ApS. stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. IST ApS' retningslinjer. gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger IST ApS' retningslinjer, og at autorisationer tildeles i henhold til aftale. 	<p>Ingen bemærkninger.</p>
<p>Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang.</p> <p>Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåges.</p>	<p>Vi har forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i IST ApS.</p> <p>Vi har ved stikprøvevis inspektion påset,</p> <ul style="list-style-type: none"> at der anvendes passende autorisationssystemer i relation til adgangsstyring i IST ApS. at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgang er implementeret i IST ApS' systemer, og at der foretages løbende opfølgning på registrerede brugere. 	<p>Ingen bemærkninger.</p>
<p>Interne brugeres adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang.</p>	<p>Vi har ved stikprøvevis inspektion påset, at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne, herunder:</p> <ul style="list-style-type: none"> at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med udvidede rettigheder hver 3. måned at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med almindelige rettigheder hver 6. måned. 	<p>Ingen bemærkninger.</p>

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Tildeling af adgangskoder styres gennem en formaliseret og kontrolleret proces, som bl.a. sikrer, at der sker skift af standardpassword.</p>	<p>Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i IST ApS.</p> <p>Vi har ved stikprøvevis inspektion påset,</p> <ul style="list-style-type: none"> • 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. 	<p>Ingen bemærkninger.</p>
<p>Adgange til operativsystemer og netværk er beskyttet med password.</p> <p>Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde, krav om kompleksitet og maksimal løbetid, lige som password-opsætninger medfører, at password ikke kan genbruges. Et password kan højst skiftes én gang på samme dag.</p> <p>Endvidere bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.</p>	<p>Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i IST ApS.</p> <p>Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for:</p> <ul style="list-style-type: none"> • minimum længde for password • maksimal levetid for password • minimum historik for password • minimum levetid for password • lockout efter fejlede loginforsøg • password skal være komplekst 	<p>Ingen bemærkninger.</p>

Kryptografi

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

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

Fysisk sikkerhed og miljøsikring

Der skal være beskyttelse af kontorbygningen mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Der er etableret en sikker fysisk afgrænsning, som beskytter adgange til kontorbygningen.</p> <p>De sikre områder er beskyttet med adgangskontrol, så kun autoriserede personer kan få adgang.</p> <p>Der er etableret overvågning af indgangsdøre, hvorfra der er adgang til kontorbygningen.</p>	<p>Jf. beskrivelse er den fysiske adgangssikkerhed til kontorbygningen bl.a. gennemgået og kontrolleret med udgangspunkt i de af ledelsen fastsatte krav.</p> <p>Vi har gennemgået og kontrolleret de fysiske adgange til kontorbygningen, som bl.a. sikres via et chipkort, som sikrer begrænset adgang til IST ApS' kontorbygning.</p> <p>Via interview og observation er det kontrolleret, at adgangen til kontorbygningen er i overensstemmelse med ovenstående forretningsgange omkring adgangsbegrænsning.</p> <p>Vi har stikprøvet gennemgået procedurer for fysisk sikkerhed vedrørende sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt at personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse.</p> <p>Vi har stikprøvet gennemgået medarbejdere med adgang til sikre områder og påset, at de er oprettet i henhold til de fastlagte procedurer.</p>	<p>Ingen bemærkninger.</p>

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Der er dokumenteret driftsafviklingsprocedurer for forretningskritiske systemer, og de er tilgængelige for personale med et arbejdsbetinget behov.</p> <p>Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse.</p>	<p>Vi har:</p> <ul style="list-style-type: none"> 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. 	<p>Ingen bemærkninger.</p>
<p>Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud.</p> <p>Der foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.</p>	<p>Vi har:</p> <ul style="list-style-type: none"> 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. 	<p>Ingen bemærkninger.</p>

Kontrolmål: Backup

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

IST ApS' kontrolaktivitet	Beierholms udførte test	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: <ul style="list-style-type: none">forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede.stikprøvevist gennemgået backup-log, for 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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt.</p> <p>IST ApS logger, når brugerne logger af og på systemerne.</p> <p>Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.</p>	<p>Vi har:</p> <ul style="list-style-type: none">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.
<p>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.</p> <p>Alarmer sker igennem en overvågnings-skærm, der er monteret i projekt- og driftsafdelingen. Kritiske alarmer afgives også pr. mail og sms.</p> <p>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.</p>	<p>Vi har:</p> <ul style="list-style-type: none">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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	<p>Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i IST ApS.</p> <p>Vi har ved stikprøvevis inspektion påset,</p> <ul style="list-style-type: none">• at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til IST ApS' produktionsmiljøer.• at ændringer til produktionsmiljøet i IST ApS følger de gældende retningslinjer, herunder at registreringer og dokumentation af ændringsanmodninger foretages korrekt. <p>Vi har stikprøvevist inspiceret, at styresystemerne er opdateret efter gældende procedurer, samt at status herpå registreres.</p>	Ingen bemærkninger.
Ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgange og processer.	<p>Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i IST ApS.</p> <p>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:</p> <ul style="list-style-type: none">• at der sker registrering og beskrivelse af ændringsanmodninger• at ændringer er underlagt formelle konsekvensvurderinger• at der beskrives fall-back planer• at der sker identifikation af systemer, der påvirkes af ændringer• at dokumentationen opdateres, så den i al væsentlighed afspejler de påførte ændringer• at procedurer er underlagt styring og koordination i et "change board".• At alle ændringer er underlagt formel godkendelse inden idriftsætning	Ingen bemærkninger.

Kommunikationssikkerhed

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

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og transmitteret data.</p>	<p>Det er kontrolleret, at der er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder:</p> <ul style="list-style-type: none"> • 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. 	<p>Ingen bemærkninger.</p>
<p>Der skal være etableret passende forretningsgange for håndtering af trusler i form af angreb fra internettet (cyber-angreb).</p> <p>I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.</p>	<p>Det er kontrolleret, at der er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb.</p> <p>Vi har ved stikprøvevis inspektion påset:</p> <ul style="list-style-type: none"> • 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. 	<p>Ingen bemærkninger.</p>

(Anskaffelse), udvikling og vedligeholdelse af systemer

Sikre, at IST SaaS løsninger er håndteret med en passende it-sikkerhed, herunder en passende funktionsadskillelse mellem produktionsmiljøet og udviklingsmiljø.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>IST ApS har tilrettelagt systemudvikling og vedligeholdelsesaktiviteter baseret på en projektmodel.</p> <p>Udviklingsorganisationen er opbygget med en central styregruppe, som har ansvaret for udformning af passende forretningsgange samt tilhørende ledelseskontroller.</p> <p>Alle ændringer, som skal idriftsættes i produktionsmiljøet, skal være godkendt af udviklingsgruppen for de enkelte IST SaaS løsninger.</p>	<p>Vi har:</p> <ul style="list-style-type: none"> 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 ændringer til IST SaaS løsninger. <p>Brugerstyringen sikrer, at der er en passende kontrol i forbindelse med håndteringen af den logiske adgangskontrol. Vi har kontrolleret, at medlemmer af de forskellige brugergrupper udfører periodevis kontrol.</p>	<p>Ingen bemærkninger.</p>
<p>Udvikling af IST SaaS løsninger skal være placeret på selvstændige testmiljøer.</p>	<p>Vi har kontrolleret, at der for softwareudviklingen findes procedurer for adskillelse mellem produktionsmiljøet og miljøet for udvikling og vedligeholdelse.</p> <p>I forbindelse med vores revision har vi kontrolleret, at der er adskilte testmiljøer og produktionsmiljøer for softwareudviklingen.</p> <p>Stikprøvevis er det testet, at produktionsmiljøet for softwareudvikling sker fra et selvstændigt IP-segment.</p>	<p>Ingen bemærkninger.</p>
<p>§19-logning – IST SaaS løsninger skal være tilsluttet IST's interne procedurer for reglerne for login, herunder krav til overholdelse af rammerne til indhold og format.</p> <p>Oplysninger vedrørende login skal opbevares i op til 6 måneder.</p>	<p>Vi har stikprøvevist kontrolleret, at brugeraktiviteter i forbindelse med login til IST SaaS løsninger bliver registeret og logget i central database.</p> <p>Kontroller har påvist, at login informationer bliver slettet efter 6 måneders opbevaring.</p>	<p>Ingen bemærkninger.</p>

Leverandørforhold

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

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand håndteres.	<p>Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere.</p> <p>Vi har stikprøvevist inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.</p>	Ingen bemærkninger.
Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende godkendte leverandører.	<p>Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere.</p> <p>Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører.</p> <p>Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.</p>	Ingen bemærkninger.
Der skal udføres regelmæssig overvågning, herunder føres tilsyn med eksterne samarbejdspartnere.	<p>Vi har påset, at findes passende processer og procedurer for løbende overvågning af eksterne leverandører.</p> <p>Vi har kontrolleret, at der udføres løbende tilsyn gennem uafhængig revisors rapporter.</p>	Ingen bemærkninger.
Ved brug af eksterne parter f.eks. konsulenter eller andre eksterne medarbejdere, der får adgang til fortrolige informationer, skal der være indhentet NDA, før samarbejdet kan påbegyndes.	<p>Vi har påset, at findes en standard for fortroligheds- og hemmeligholdelsesaftaler.</p> <p>Vi har kontrolleret, at der anvendes NDA i forbindelse med brug af eksterne medarbejdere.</p>	Ingen bemærkninger.

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.</p>	<p>Vi har forespurgt ledelsen, om der er etableret procedurer for rapportering af sikkerhedshændelser.</p> <p>Vi har kontrolleret, at der er udarbejdet procedurer og forretningsgange for rapportering og behandling af sikkerhedshændelser, samt at rapporteringen tilgår rette steder i organisationen jf. retningslinjer.</p> <p>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.</p>	<p>Ingen bemærkninger.</p>

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
<p>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.</p>	<p>Vi har forespurgt ledelsen, om der er udarbejdet beredskabsstyring for IST SaaS løsninger i IST ApS. Vi har ved stikprøvevis inspektion påset,</p> <ul style="list-style-type: none"> • 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 IST ApS' interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at planen sikrer redundans i forhold til produktionsmiljøet • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen. 	<p>Ingen bemærkninger.</p>

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.”

Pernille Louise Brøns Frederiksen

Informationssikkerhedskonsulent

På vegne af: IST ApS

Serienummer: 28c4d74a-76ff-4298-9eb0-cc77229d219a

IP: 91.143.xxx.xxx

2026-04-17 06:59:51 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

2026-04-17 08:16:40 UTC



Kaj Kristian Grün Hovmand Madsen

Head of Business Region Danmark

På vegne af: IST ApS

Serienummer: 9fc232f7-32f8-4e7b-99ce-57c7786eba9b

IP: 104.28.xxx.xxx

2026-04-21 09:32:24 UTC



Penneo dokumentnøgle: 7TLYL-9Y8G2-3VGQ9-DOGYG-EK9K3-M497W

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.