



APRIL 2024

IST APS

ISAE 3402 TYPE 2 ERKLÆRING

CVR 25545079

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

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

www.beierholm.dk



Erklæringsopbygning

Kapitel 1:

Ledelseserklæring.

Kapitel 2:

Beskrivelse af kontrolmiljøet 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

IST ApS behandler personoplysninger på vegne af kunder i henhold til databehandlersaftale i tilknytning til it-driften af IST SaaS løsninger.

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 2023 - 31. marts 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 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 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 2023 - 31. marts 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 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 2023 - 31. marts 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. april 2023 - 31. marts 2024.
- (C) Der er etableret og opretholdt passende tekniske og organisatoriske sikringsforanstaltninger med henblik på at opfylde aftalerne med de dataansvarlige og god databehandlerskik.
- (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 IST ApS' standardaftale samt tilhørende databehandleraftale. Kriterierne for dette grundlag var:
- (i) Politik for informationssikkerhed
 - (ii) Informationssikkerhedshåndbog

Roskilde, den 2. april 2024



Anne Brink Pedersen, Adm. direktør

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



Janne Veng, Data Security Manager

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

Indledning

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

Omfanget af beskrivelsen er en afdækning af de tekniske og organisatoriske sikringsforanstaltninger, som er implementeret i forbindelse med driften af IST SaaS løsninger. Produktrammen for denne beskrivelse er følgende SaaS løsninger:

- IST Dagtilbud Børn
- IST Dagtilbud Personale
- IST Dagtilbud Admin (herunder SFO Admin)
- IST Elevadministration
- IST Tjenestetid
- IST Ungdomsskole (Lara)
- IST Pladsanvisningen
- IST Personkreds
- IST Studie+

Beskrivelse af IST ApS

IST ApS er en del af den svenskejede koncern IST Group AB, som blev grundlagt i 1982. IST ApS beskæftiger cirka 100 medarbejdere, som er fordelt på to kontoret i hhv. Roskilde og Midtlyn.


I 2013 opkøbte IST Group AB den danske virksomhed Tabulex ApS, som blev stiftet i 1998, og i 2017 ekspanderede IST ApS med købet af virksomheden UDDATA til også at omfatte ungdomsuddannelser.

IST ApS udvikler primært administrative it-løsninger som software-as-a-service (SaaS) til offentlige og private uddannelsesinstitutioner, herunder dagtilbud, grundskole, ungdomsuddannelser og FGU, herunder bl.a. løsninger til elevadministration, skemalægning og medarbejdernes arbejdstid. Med løsningerne fra IST ApS er det nemt for brugerne at samle alt til administrationen af dagtilbuddet eller skolen ét sted.

Leverancerne omfatter drift, service og support, konsulenttydelser og kurser. Systemerne udvikles løbende, herunder også tilpasning af funktionalitet, således at systemerne lever op til gældende lovgivning og reguleringer. Alle vores systemer udvikles, drives og forvaltes af dygtige medarbejdere med base i Danmark og i samarbejde med vores kollegaer i IST Group AB. IST Group AB har ansatte i Sverige, Norge, Tyskland og Danmark.

Ca. halvdelen af medarbejderne i IST ApS har en baggrund fra uddannelsesverdenen. Det giver os en god indsigt i brugernes udfordringer og behov og et godt grundlag for at yde god og brugbar support til brugerne.

Udviklingen af løsningerne sker i tæt samarbejde med brugerne, domæneeksperter og udviklere med stor viden om forvaltningsområdet.



IST ApS leverer løsninger til stort set alle 98 kommuner i Danmark, samt mange uddannelsesinstitutioner, og er den førende leverandør på markedet.

IST ApS arbejder med fastlagte processer og er certificeret i ISO9001 – kvalitetsledelsessystem, hvilket sammen med vores sikkerhedsarbejde, baseret på ISO27001 & 27002, sikrer ensartethed og minimering af fejl.

Forretningsstrategi/ it-sikkerhedsstrategi

Det er IST ApS' strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, så selskabet ikke påføres uacceptable risici.

Som leverandør til offentlige og private uddannelsesinstitutioner arbejder IST ApS med informationssikkerhed på et forretningsstrategisk niveau. Dette grundet de mange personoplysninger, som håndteres i vores systemer. IST ApS' målsætning er at være kundernes professionelle samarbejdspartner, der forsvarligt håndterer data, som de betror til os.

Det er IST ApS' holdning, at vi skal sikre overholdelse af gældende lovgivning og gøre, hvad der er teknisk og økonomisk muligt, for at sikre databehandlingens fortrolighed, integritet og tilgængelighed på et højt niveau. Informationssikkerheden er i højsædet på alle niveauer af organisationen. Alle medarbejdere skal være vidende om vigtigheden af dette fokus og selv være medvirkende til løbende at forbedre arbejdet omkring sikkerhed.

Vores målsætning for informationssikkerheden er, at IST ApS gennemfører alle nødvendige aktiviteter for at sikre:

- Tilgængelighed: At opnå en høj tilgængelighed med høje opetid og minimeret risiko for nedbrud.
- Integritet: At opnå en pålidelig og korrekt funktion af informationssystemerne med minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.
- Fortrolighed: At sikre fortrolig databehandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.

Det er IST ApS' mål at opretholde et informationssikkerhedsniveau, der som minimum:

- Følger gældende lovgivning, herunder GDPR.
- Følger god brancheskik.
- Lever op til kundens ønsker, krav og forventninger til en professionel leverandør.

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, samt Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger nr. 502 af 23/05/2018 udgør den lovgivningsmæssige ramme for behandling af personoplysninger i it-services.

Kunden kan supplere med yderligere instrukser formaliseret i en databehandleraftale, som indgås mellem kunden (dataansvarlige) og IST ApS (databehandler). IST ApS' ansvar er at foretage de nødvendige tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger behandles på en sikker og forsvarlig måde.

For at sikre en ensartet leverance, som lever op til branchens bedste standarder, har vi valgt at underlægge driften af SaaS løsninger en revisionsproces med det formål at leve op til kravene i en ISAE3402 erklæring. Revisionsprocessen gentages årligt, og resulterer i en revisionserklæring, der offentliggøres på

vores hjemmeside www.ist.dk. Erklæringen kan bidrage til kundens (dataansvarlig) kontrol af, hvorvidt IST ApS lever op til instruksen i den indgåede databehandleraftale.

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

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed

- Kommunikationssikkerhed
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse med lov- og kontraktkrav

De implementerede sikringsforanstaltninger hos IST ApS fremgår af bilag 1 til denne beskrivelse.


IST ApS' organisation og organisering af it-sikkerheden

IST ApS er en del af koncernen IST Group AB, bestående af selvstændige virksomheder i hhv. Sverige, Norge, Tyskland og Danmark.

IST ApS er organiseret efter følgende struktur.



Support & Consulting består af 38 medarbejdere, der varetager kontakt med brugere i form af support, konsulentbistand, kurser. Yderligere har de kontakt med myndigheder, samarbejdspartnere, laver test af vores løsninger m.m.



Development & Operations består af 45 medarbejdere, med kompetencer indenfor de udviklingsteknologier, vi benytter. De står for udvikling og vedligeholdelse af de it-services, som vi tilbyder vores kunder. Den grundlæggende it-drift til SaaS løsninger varetages af koncernens egne medarbejdere. Vores dygtige medarbejdere sikrer størst mulig tilgængelighed og driftsstabilitet.

Sales & Marketing består af 4 medarbejdere, der varetager kommunikation og kontakten med kunder i forbindelse med salg, organiserer produktdemoer, deltager på messer, afgiver tilbud, ordrer, databehandleraftaler og giver feedback til *Solution Management* om, hvad der rører sig i markedet.

Solution Management består af 5 medarbejdere, der arbejder med hvad, der rører sig i vores markeder, udvikler nye ideer til produkter og services, udarbejder business cases og konkurrentanalyser.

CEO, Administrerende Direktør udvikler strategier og mål, og er en del af Koncernledelsen i IST Group AB. CEO varetager HR funktionen.

IST ApS arbejder med en struktureret metode og er ISO9001 certificeret for at sikre, at alle processer og politikker er beskrevet i vores kvalitetsstyringssystem og ISMS. Dette for at sikre uafhængighed af enkeltpersoner. Incidents eller afvigelser af it-sikkerhedsrelateret karakter behandles på månedlige møder på baggrund af faste procedurer for håndtering af afvigelser.

Forankringen af it-sikkerhedsarbejdet i virksomheden er sikret med ansvaret i ledelsen og informations-sikkerhedskonsulenten. Ledergruppen og informationssikkerhedskonsulenten arbejder sammen om at højne opmærksomheden på regler og procedurer blandt medarbejderne.

Risikostyring i IST ApS

Det er IST ApS' 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. Endvidere er det en del af IST ApS' politik, at vores systemer skal have passende foranstaltninger, der beskytter systemet mod brud på fortrolighed, integritet og tilgængelighed.


Som led i ovenstående it-sikkerhedsstrategi arbejder IST ApS med standard ISO27001+2:2017 for it-sikkerhed som primær referenceramme for it-sikkerheden. Arbejdsprocessen omkring it-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at IST ApS til hver en tid er i overensstemmelse med vores kunders krav.

IST ApS har indarbejdet faste procedurer for risikovurdering af forretningen, samt for den registrerede i vores systemer. Det sikres dermed, at de risici, som er forbundet med de services, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når der ændres i eksisterende systemer eller implementeres nye systemer, som vurderes for relevante i forbindelse med at genvurdere vores generelle risikovurdering. Risikovurderingen er en del af ledergruppens ansvar.

Håndtering af it-sikkerhed

Ledelsen hos IST ApS 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 IST ApS' struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

IST ApS' 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. Der følges bestemte procedurer, som sikrer sporbarhed, forebyggende og korrigerende handlinger, samt underretning af kunderne.



Alle servere og netværksenheder er dokumenteret i IST Groups dokumentationssystem. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewalls, routere, switche og lignende) ligger gemt i vores dokumentationssystem.

It-sikkerhedspolitikken er udarbejdet, så IST ApS har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af såvel politikker, procedurer som den operationelle drift.

På det generelle it-sikkerhedsområde har IST ApS implementeret de nødvendige procedurer og kontroller i forhold til de enkelte områder inden for ISO27001+2:2017, der er defineret i bilag 1, som viser sikkerhedsstrukturen og de kontrolmål, der er implementeret hos IST ApS.

HR, medarbejdere og uddannelse

Medarbejdernes domæneviden og kompetencer er en vigtig forudsætning for IST ApS' forretning. Det er vigtigt at vedligeholde og udbygge de kompetencer, vi råder over, så vi er i stand til at imødekomme udfordringerne i en omskiftelig branche. Vi afsætter hvert år penge til efter/videreuddannelse af vores medarbejdere, og der holdes flere årlige kompetencesamtaler, hvor der er fokus på mål, samt medarbejdernes ønsker til faglig udvikling.

Vi arbejder med faste procedurer for bl.a. rekruttering, ansættelse og fratrædelser. Nye medarbejdere gennemgår et introduktionsforløb til alle afdelinger i virksomheden. Forløbet omfatter en introduktion i informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på IST ApS' rolle som databehandler. IST ApS indhenter ved ansættelse underskrift fra medarbejderen på en erklæring, hvori medarbejderen tilslutter sig virksomhedens regler for omgang med kundedata, og at medarbejderen er blevet gjort bekendt med hvilket lovgrundlag, der er gældende.


IST ApS' medarbejdere har i begrænset omfang mulighed for at arbejde fra andre faciliteter end virksomhedens kontorer. Virksomheden har udarbejdet en procedure, der beskriver regler og gode råd til fjernarbejdsplads. Vi har etableret tekniske foranstaltninger, der sikrer en krypteret opkobling til kontorfaciliteter fra fjernarbejdspladser. Adgang til backend-systemer og driftsmiljøer er teknisk begrænset. Endelig er medarbejderen informeret om, at en eventuel fjernarbejdsplads også kan være omfattet af ekstern inspektion.

Alle medarbejdere har en fortrolighedsklausul i deres ansættelseskontrakter. Som en del af vores fratrædelsesprocedure indgår en exit-samtale med nærmeste leder, hvor vi minder om, at fortrolighedsklausulen fortsat er gældende efter endt ansættelse. Ved brug af eksterne konsulenter, benytter vi en NDA-ska-belon.

For at sikre en kontinuerlig tilgang til informationssikkerhedskulturen har IST ApS en plan for awareness-kampagner. Planen beskriver, hvilke emneområder, der skal arbejdes med i løbet af et år. Planen revurderes årligt af informationssikkerhedsgruppen.

Fysisk sikkerhed

IST ApS har samarbejdet med Interxion siden 2008. Samarbejdet betyder, at vi har overladt de grundlæggende datacenteropgaver til en leverandør, der er ekspert i opbygning og drift af datacentre. Interxion er ansvarlig for fysisk sikring, brand-, og vanddetektion og -bekæmpelse, strøm og køling. Interxions datacenter giver flere lag sikkerhed og opfylder anerkendte internationale standarder for informationssikkerhed vedr. managementsystemer og business continuity management.



At være i stand til at tilbyde stabile og sikre it-services til vores kunder er naturligvis et centralt krav. Fordi Interxion er carrier-neutral, har IST ApS det bredeste udvalg af ISP-udbydere. Datacenteret er hjemsted for Danish Internet Exchange (DIX), og giver os den bedst mulige quality of service for internetforbundne datalinjer.

IST ApS' driftsmiljø er ejet af IST Group AB, som IST ApS er ejet af. Driftsmiljøet vedligeholdes af eget driftspersonale. Vi har en 10 kvm stor privat celle, der er fysisk adskilt fra andre kunder hos Interxion. Alle adgange til cellen sker via personlige adgangskort og registreres i et centralt system.

Strøm og køling

Der er etableret redundant power setup med to uafhængige plugsets (Feed A) og (Feed B). Hertil et (A+B Feed) via ATS (Powerswitch) for udstyr, der kun har ét strømudtag. Strømforsyningen til datacenteret har flere niveauer af sikring ved tab af bystrøm. Der er etableret fuldskala batteri-backup til begge strøm feeds. Hvis batterikapaciteten når et kritisk niveau, vil et antal dieselgeneratorer overtage strømproduktionen, der er i stand til at levere fuld kapacitet. Generatorerne er sat i et redundant setup med ekstra kapacitet, således at fejl i en generator ikke medfører mangel på redundans. Datacenteret har lokal dieselkapacitet til at køre mindst 24 timer, og der er forsyningsaftaler med olieselskab om 24/7/365 leverance af dieselolie. Der foretages jævnlige tests af de enkelte komponenter i batteri og dieselgeneratorer, ligesom der én gang årligt foretages en fuldskala test af hele setuppet.

Sikring mod vand

Datacenteret er bygget med forhøjet gulvniveau, og der er etableret intelligent water leak detection systemer, der lokaliserer en eventuelt vandlæk. Bygningen er indrettet med sikring mod, at kondensvand kan dryppe på hardwaren. Dette gælder også i tilfælde af, at brandbekæmpelses anlægget aktiveres. Ved hjælp af målere og termostater holdes en konstant temperatur og luftfugtighed i datacenteret.

Brandsikring

Der er etableret automatiseret og overvåget brandbekæmpelsessystem, der via sensorer måler varme og fugtighed. Anlægget er energenbaseret, og alle energenflasker overvåges for, om de holder det anbefalede tryk. Hertil er der jævnlig fysisk kontrol og periodisk udskiftning af flasker v. udløbsdato.

Fysisk sikring

Interxion har et omfattende sikkerheds-setup bestående af vagtpersonel i 24/7/365 rundring, og teknisk overvågning af perimeter, bygninger og gangarealer inden i centeret. Fysisk adgang foregår via vagtcentralen og kun med godkendt adgangskort. Identiteten af personer med adgang foregår via irisscanning eller fingeraftryk. Alle indgange til centeret er videoovervåget, og sluserne har vægtkontrol, der sikrer, at to personer ikke kan komme ind på samme tid.

Offsite lokation

Vi har etableret en sekundær backuplokation, der ligger mere end 15 km væk fra den primære lokation. Den sekundære lokation driftes ligeledes af Interxion og er opbygget efter samme principper som den primære driftslokation. Det er blandt andet hertil, at offsite backups overføres.

Kontrol med Interxion

IST ApS fører løbende kontrol med, om Interxion, som leverandør til kritiske dele af vores driftsmiljø, lever op til kvalitetskrav samt overholdelse af kravene fra SLA i tilknytning til deres ydelser. Interxion leverer årligt en SOC2 auditorrapport, som er resultatet af deres omfattende eksterne revision. IST ApS evaluerer rapporten og sammenholder den med egne observationer. Herefter vurderer vi, om leverandøren lever op til de aftalte serviceydelser, og hvorvidt der er grund til at tage aspekter op med dem.



Datalinjer og netværkssikkerhed

Dataforbindelsen til driftsmiljøet består af to uafhængige ISP'er 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 driftspersonale, 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 aktiv/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).

Firewallen har en indbygget "Load balancer", der benyttes til at sikre fordelingen af den samlede trafik til flere servere.

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

Hardware setup

Hardware i driftsmiljøet er opbygget med et antal fysiske servere (Hypervisor), hvori flere virtuelle servere driftes. Hertil er der dedikeret storage systemer (SAN), som sammen med Hypervisor sikrer High Availability og skalerbarhed.

De virtuelle miljøer består af 31 fysiske servere fordelt over flere clustre. Alle clustre har ledige ressourcer, så 1 eller flere noder kan fejle, uden at det har indflydelse på de kørende services, og som samtidig giver mulighed for opdatering af firmware og software, uden at det giver driftsforstyrrelse.

Diskkapacitet håndteres af en central netværksbaseret løsning (SAN). SAN'et tilgås via fuld redundant switching mellem hypervisorne. Den samlede diskkapacitet er delt op i logiske "diske", kaldet LUN. Hver LUN replikeres. Alle diske er krypteret, og hvis diske fjernes fra SAN'et, bliver krypteringsnøglen permanent slettet efter få sekunder.


Drift af SaaS løsninger

Faste driftsopgaver udføres med faste intervaller. Disse opgaver styres i IST ApS' driftsafdeling, som varetager kontrolleret vedligehold og drift af samtlige servere. Opgaven er beskrevet i tilhørende checklister.

Registrering af it-udstyr i produktion (aktiver)

IST ApS registrerer it-udstyr og services i virksomhedens CMDB (Configuration Management Database). Formålet er, at vi altid har en opdateret database med relevant data omhandlende det it-udstyr, der er nødvendigt for, at vi kan levere it-services til kunder.

It-udstyr med en ip-adresse, der enten direkte eller indirekte indgår i produktionsmiljøer og/eller kontormiljøer, skal registreres og holdes opdateret i CMDB'en. Dette er eksempelvis: Netværksudstyr, Servere (Fysiske/virtuelle), Printere, PC'er, Mobile Enheder, Applikationer, Styresystemer, Services og Databaser.



I CMDB'en registreres nødvendige detaljer om aktivet og det omkringliggende it-miljø. Detaljeringsgraden afhænger af aktivtypen. Der registreres, hvilket netværk enheden er tilkøbet, IP- adresse, ansvarlig person/team, rolle (produktion, test/staging mv.), relationer til databaser, applikationer og andre services.

Driftsovervågning – NOC

Driftsmiljøet overvåges 24/7/365 via en automatiseret service. Der overvåges ressourcer for servere (Cpu, ram, disk, netværk) og tilgængelighed. Overvågningen omfatter også relevante it-services eksempelvis backups, tilgængelighed for kundevedt systemer og systemer til internt brug.

Den primære overvågning foregår internt i driftsmiljøet, men for også at dække den eksterne tilgængelighed har vi etableret en offsite overvågning. Ved fejl rapporteres til NOC, hvorefter fejlen bliver undersøgt. Er der tale om kritiske fejl i servere eller services, adviseres den vagthavende driftsmedarbejder direkte.

Driftens NOC er til internt brug i IST ApS, og er således ikke tilgængelig for kunder. Kunder, der oplever driftsproblemer, skal kontakt os via de supportkanaler, der er aftalt i kontrakter og Generelle vilkår.

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

Logning

Logning er et værdifuldt værktøj til overvågning, fejlhåndtering og efterforskning. Da logs indeholder mange forskellige informationer, har vi adgangsstyring til logs afhængigt af, hvilke opgaver den enkelte medarbejder må udføre. IST ApS arbejder med logning på flere niveauer: Applikationslogs – der håndterer specifikke operationer i applikationer, Sikkerhedslogs – der logger, hvornår brugere logger ind i applikationer, logning af, hvilke brugere der tilgår information af følsom og fortrolig karakter i vores applikationer og Syslog – overvågningslogning.

Backup

Formålet med backup er at sikre, at kundens data i IST ApS' hostingcenter kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid. Der tages backup på forskellige niveauer som virtuelle servere, konfigurationer og data. Dette sikrer, at vi har flere muligheder for at sætte ind ved behov for reetablering.

Der tages backup af relevante databaser og konfigurationer, med henblik på at muliggøre reetablering i en given nødsituation. Der er forskellige krav til frekvens af backups afhængigt af it-systemets kritikalitet.

Backuppolitikken for kundedatabaser beskriver, at der skal tages daglige backups, minimum én i døgnet. For mindst én af disse backups foretages der ugentligt en reetableringstest, der tester backuppens integritet. Hver backup gemmes på dedikerede backupservere placeret i driftsmiljøet. Desuden flyttes backups til en fysisk adskilt lokation.

Alle backups krypteres med AES-256 krypteringsnøgle, og transport af data mellem primær site og offsite foregår med krypterede datalinjer.

Daglige backups af kundedatabaser opbevares i 30 dage. Herefter opbevares den sidste backup i hver måned. Backups, der er ældre end 6 måneder, slettes permanent.



Patch management / ændringshåndtering

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

Vedligehold af Windows operativsystemer og tilhørende backend-systemer fra Microsoft, håndteres af Microsofts indbyggede WSUS (Windows Server Update Services), hvor sikkerheds- og kritiske patches installeres automatisk med faste intervaller.

Efter installation af operativsystemer følges en procedure, der sikrer, at det kun er relevante services og applikationer, der er tilgængelige på serveren. Umiddelbart inden en server sættes i produktion, følges en "Hardening"-proces, der sikrer, at de anbefalede sikkerhedsindstillinger er sat korrekt på serveren.

Styring af it-sikkerhedshændelser

Sikkerhedshændelser og svagheder i IST ApS' systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt. Der er etableret procedurer for hændelsesstyring og afvigerapportering, herunder sikkerhedsbrud. Procedurene sikrer, at der arbejdes systematisk, foretages nødvendig dataindsamling og dokumentation, således at der efterfølgende er et godt grundlag at evaluere ud fra. Afvigerapporteringen er en del af vores Kvalitetsstyringssystem, og det er ledelsen, der er ansvarlig for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Brugerstyring/ adgangssikkerhed

Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.

Tildeling af adgang til driftsmiljø skal ske i overensstemmelse med forretningsbetingede formål og informationernes klassifikation. Både fysisk og logisk adgang er baseret på principperne "need-to-know" og "least privilege", hvor der tildeles adgang til de informationer, som man har behov for, for at kunne udføre sine opgaver/sit job eller rolle.


Anmodning om adgang til interne it-systemer og produktionsmiljøer følger en fastlagt procedure, der sikrer en adskillelse i anmodning, godkendelse, verifikation og implementering. Adgangsstyringen dokumenteres i et centralt system.

Krav til password: Alle brugere oprettet i IST ApS' centrale brugerdatabase skal skifte password hver 90. dag. Passwordet skal være på mindst 8 tegn, skal indeholde tal eller specialtegn, samt skal indeholde både store og små bogstaver.

Beredskabsstyring

IST ApS' forretning er i stor grad baseret på den grundliggende it-infrastruktur, hvorfra it-services udbydes til kunderne. It-beredskabsplanen skal således ses som en samlet Business Continuity Plan (BCP) eller Forretningskontinuitetsplan.

Ved alvorlige fejl informeres den it-sikkerhedsansvarlige og ledelsen i IST ApS. Den aktuelle beredskabsplan beskriver, hvorledes der skal informeres, fejlsøges og fejlrettes. For at gøre planerne så operationelle som muligt er der etableret procedurer for beredskabsstyring på flere niveauer. En overordnet BCP beskriver definitioner af beredskabsfaser, kritikalitet, eskalerings-, og kommunikationsprocedure. Planen beskriver håndteringen af to af de værst tænkelige scenarier: Nedbrud i datalinjer og totalt datacenter-nedbrud.



BCP-planen suppleres af et antal reetableringsplaner for kundevedtde it-services samt kritiske interne systemer. For at sikre tilgængeligheden til reetableringsplanerne er disse lagret på flere forskellige medier og i hardcopy.

I løbet af kontrolperioden er der gennemført relevante afprøvninger af beredskabsplanen. Hertil skal der foregå en årlig kvalitetssikring af alle reetableringsplaner, hvorefter enkelte systemer vil blive udvalgt til en skrivebordstest.

Udviklingsmiljøet

Når IST ApS udvikler software (kunderettede it-services) bruges der dedikerede testmiljøer, hvorfra softwaren kan afvikles til udvikling og test. Disse miljøer er andre miljøer end dem, som kundernes software afvikles på.

Eventuelle fejl i data og systemintegrationer er således afgrænset til kun at have indflydelse på integriteten af testdata. Testdata er fiktive data oprettet i systemet til formålet (= ikke kundedata). Under de afsluttende testfaser kan der være behov for at teste med data, der ligner live-miljøernes.

Test- og udviklingsmiljøer afvikles fra produktionsmiljøet i et selvstændigt IP-segment. Tilgængeligheden til miljøerne er begrænset, så disse kun kan tilgås fra de udgående adresser for IST's kontorer. Dette er styret via specifikke grupper i vores firewall, som også styrer, hvilke protokoller og porte systemerne kan tilgås med.

Der er fastlagte procedurer for udvikling, test og godkendelse i virksomhedens Kvalitetsstyringsystem.

Væsentlige ændringer i forhold til it-sikkerhed

Vi arbejder i IST ApS konstant med et fokus på at forbedre processer og procedurer for at højne it-sikkerheden.

Vores arbejde med risikovurderinger og den enkelte medarbejders rolle i forbindelse med it-sikkerheden er konstant i udvikling. Ligeledes er der kommet et øget fokus på vores samarbejde på tværs af koncernens kontorer i Sverige, Norge og Tyskland.

For kontrolperioden har der været fokus på forbedring af processerne omkring løbende risikovurdering.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver det generelle kontrolmiljø for IST ApS' SaaS løsninger, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

IST ApS er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgang til SaaS løsninger. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

IST anvender til datatransmission TLS-kryptering jf. Datatilsynets retningslinjer for transmission over åbne netværk i forbindelse med web-tjenester. Kunden er derudover selv ansvarlig for datatransmissionen til SaaS løsningerne, og det er kundens ansvar at skabe den nødvendige datatransmission til IST ApS' datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.



BILAG 1:

IST ApS har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27001+2:2017

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
-

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, jævnfør databehandleraftale med kunder, i hele perioden 1. april 2023 - 31. marts 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 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 2023 - 31. marts 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. april 2023 - 31. marts 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. april 2023 - 31. marts 2024.

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.



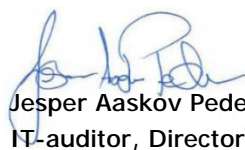
Søborg, den 3. april 2024

Beierholm

Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68



Kim Larsen
Statsautoriseret revisor



Jesper Aaskov Pedersen
IT-auditor, Director

KAPITEL 4:

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 2023 - 31. marts 2024.

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 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>

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.

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>	Ingen bemærkninger.
<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>	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 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.

KONTROLMÅL 7:

Medarbejdersikkerhed

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

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 opdeling med udgangspunkt i den forretningsmæssige 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>



<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>

KONTROLMÅL 10:

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 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. 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
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. IST ApS logger, når brugerne logger af og på systemerne. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har: <ul style="list-style-type: none">forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, og gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påsat, 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 overvågnings-skærm, der er monteret i projekt- og driftsafdelingen. Kritiske alarmer afgives også pr. mail og sms.	Vi har: <ul style="list-style-type: none">forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.påsat, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for samtlige medarbejdere.påsat, at der afgives alarmer pr. mail og sms ved opståede fejl.gennemgået statusrapporter.	Ingen bemærkninger.



<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>	<ul style="list-style-type: none"> • påset, at der er etableret en driftsvagt, samt at denne tjekker rapporter dagligt. 	
--	--	--

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
<p>Ændringer til driftsmiljøet følger de fastlagte procedurer.</p>	<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>	<p>Ingen bemærkninger.</p>
<p>Ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgange og processer.</p>	<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 	<p>Ingen bemærkninger.</p>

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.

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.

IST ApS' kontrolaktivitet	Beierholms udførte test	Resultat af test
Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.	<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>	Ingen bemærkninger.

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 afprøvnings- 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 på-</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 sikre redundans i forhold produktionsmiljøet • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen. 	<p>Ingen bemærkninger.</p>