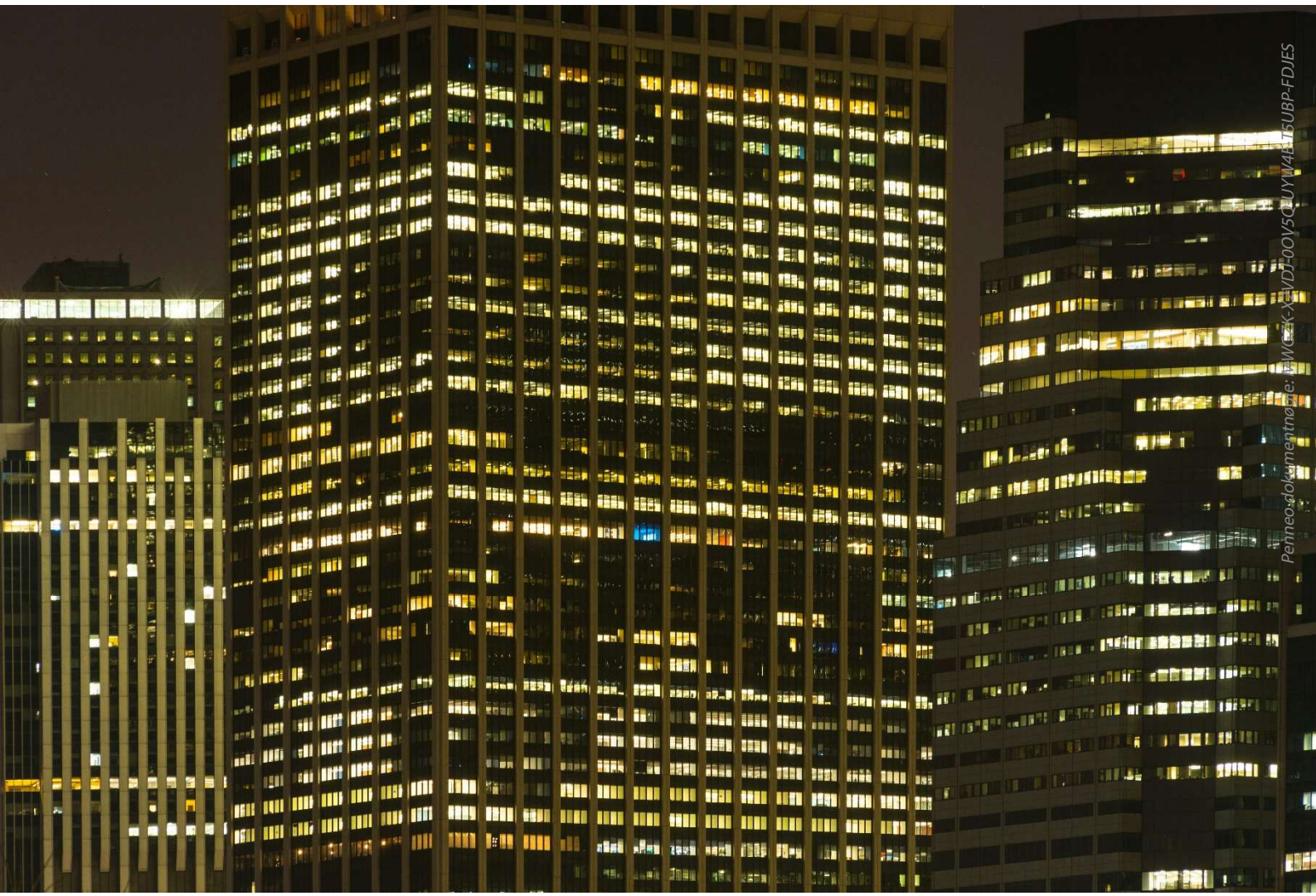
Lector ApS

Gladsaxevej 363
2860 Søborg
CVR.NR. 10 02 16 18

ISAE 3402, type 2

Uafhængig revisors ISAE 3402-erklæring vedrørende
generelle it-kontroller i forbindelse med softwareløsninger i perioden
1. juni 2025 – 31. maj 2026



Penneo dokumentnøgle: HWEZK-XVVDT-OOVSC-UYV4E-I5UBP-FDJES

Indhold

1. Ledelsens udtalelse 1
2. Beskrivelse af generelle IT-kontroller for levering af driftsydelser til kunder 3
3. Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning 8
4. Kontrolmål, kontroller, test og resultat heraf 10

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

S.nr. 326624

AOG/JR

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Lector ApS' softwareløsninger, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunder selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i den enkelte kundes regnskab.

Lector ApS anvender Microsoft Azure og Kimo Consult ApS som underdatabehandlere for anvendt hosting og web. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Microsoft Azure og Kimo Consult ApS varetager for Lector ApS.

Enkelte af de kontrolmål, der er ført i beskrivelsen i afsnit 2, kan kun nås, hvis de komplementærekontroller hos Lector ApS' kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen om- fatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Lector ApS bekræfter, at:

a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af de generelle kontroller i tilknytning til Lector ApS' softwareløsninger , der er anvendt af kunder i perioden 1. juni 2025 – 31. maj 2026. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   (i) redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
   - De typer af ydelser, der er leveret, når det er relevant
   - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
   - relevante kontrolmål og kontroller, udformet til at nå disse mål
   - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
   - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

   (ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system, foretaget i perioden fra 1. juni 2025 til 31. maj 2026

   (iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som kunder måtte anse for at være vigtigt efter dennes særlige forhold

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

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. juni 2025 til 31. maj 2026. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) kontrollerne var anvendt konsistent, som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelser i perioden fra 1. juni 2025 til 31. maj 2026.

Søborg, den 28. juli 2026
Lector ApS

Tue Villum Sørensen
Adm. direktør

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

2. Beskrivelse af generelle IT-kontroller for levering af driftsydelser til kunder

Intro om Lector

Lector er en innovativ IT-konsulent-, projekt- og produktvirksomhed, som transformerer viden om Software og domæner til kundeværdi.

Vores medarbejdere tager ansvar for kundens forretningsmæssige mål og for deres kolleger via økonomisk bæredygtige løsninger.

Vi udfordrer "status quo" ved løbende at stille spørgsmål - hos vores kunder og hos os selv.

Lector ApS har siden 2024 været ejet af den franske softwarevirksomhed Conex SAS som led i et generationsskifte i ejerkredsen. Denne nye ejerstruktur markerer en betydelig milepæl for Lector ApS og vores kunder.

Conex bringer en stor mængde ressourcer, ekspertise og innovation til Lector, hvilket vil hjælpe os med at forbedre vores produkter og tjenester i fremtiden, samt bidrage til øget internationalisering af vores ydelser.

Organisationens ser således ud:

Ledelsen har vurderet, at opkøbet ikke har påvirket indflydelsen på Lector ApS´ driftsmæssige eller sikkerhedsmæssige forhold, og der foreligger således ingen risici som følge heraf. Opkøbet medfører hverken ændringer i organisationens interne kontroller, it-miljø, forretningsgange eller i efterlevelsen af de forpligtelser, der er omfattet af nærværende erklæring. Eksisterende kundeaftaler og serviceniveauer forbliver uændrede, og Lector ApS´ ansvar i relation til erklæringen opretholdes fuldt ud.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Beskrivelse af ydelser

Lector bygger på to forretningsområder

- Sags- og Dokumenthåndtering, med produkterne TeamShare og ESS
- Toldhåndtering med produktet Logistics Trading Services, LTS

På produkterne TeamShare, ESS og LTS leverer Lector produktudvikling, support af produkterne, konsulentydelser ved implementering/til integrationer og kan levere hosting af de leverede installationer. Hvor TeamShare og ESS kan leveres som on-premise løsning eller som enten private eller public cloud SaaS løsninger, leveres LTS udelukkende som SaaS.

Når Lector leverer cloud SaaS udgaver af TeamShare og ESS, håndteres dette via servere og services i Microsoft Azure West-Europe, og ved at bruge kundernes egne Office 365 SharePoint Online platform, i det datacenter de har valg. Microsoft Azure leverer servere, netværk, hypervisor og storage. Azure revideres og leverer rapportering i form af årlig opdateret SOC II rapport.

Private cloud SaaS udgaver af produkterne TeamShare og ESS kan som option leveres fra et dansk hostingcenter, i samarbejde med vores underleverandør Kimo Consulting ApS. Kimo Consulting ApS er ansvarlig for den fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage. Kimo Consulting ApS revideres og leverer rapportering årligt ift. ISAE 3000 og ISEA 3402.

Lector varetager alt drift af vores LTS SaaS produkt for alle kunder. Dette drives på servere i Amazon AWS. AWS står her for servere, netværk, hypervisor og storage. AWS revideres og leverer rapportering i form af årlig opdateret SOC II rapport.

It-informationssikkerhedspolitikker og organisering af informationssikkerhed

For at sikre sammenhæng mellem arbejdet med it-sikkerhed og organisationen er der oprettet et it-sikkerhedsudvalg. It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, samt driftsmedarbejdere. It-sikkerhedsudvalget refererer direkte til direktionen i Lector. Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik de principper og retningslinjer, der skal sikre målopfyldelsen. Udvalget behandler alle it-sikkerhedsspørgsmål af principiel karakter.

Lector's it-sikkerhedspolitik er udarbejdet med afsæt i ISO 27001 standarden. Lector foretager løbende, minimum en gang årligt, en vurdering af denne it-sikkerhedspolitik samt de tilknyttede retningslinjer – herunder at disse lever op til de eksterne forpligtelser, udtrykt i lovgivning og kontrakter/aftaler. Procedurer dækker bl.a. sikkerhed i supporten af kunder, kontrol af underleverandører, kontrol af databehandleraftaler, håndtering af persondata anmodninger, mv. Der udføres løbende risikovurdering af alle relevante områder. Sikkerhedshændelser inkl. brud på persondatasikkerhed rapporteres til Lectors it–sikkerhedsansvarlige, som registrerer disse, og varetager videre kommunikation med evt. berørte parter. Lector har etableret procedurer for identifikation, registrering, klassifikation og håndtering af sikkerhedshændelser, herunder brud på persondatasikkerheden. Hændelser vurderes med henblik på nødvendig eskalering, kommunikation til relevante parter samt iværksættelse af korrigerende og forebyggende handlinger.

Når politikker og procedurer/SOP (standard operating procedures) opdateres, kommunikeres dette til medarbejdere. For den helt centrale IT Sikkerhedspolitik, underskriver medarbejderen at denne er læst, forstået og følges. Politikker og proceduren er tilgængelige i vores egen interne instans af vores eget TeamShare produkt, hvor medarbejderne altid kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til den it-sikkerhedsansvarlige, der sørger for relevante rettelser.

Alle medarbejdere i Lector er blevet undervist i persondatasikkerhed, og ledelsen tager løbende temaer og emner op over for medarbejderne for at styrke processer og forretningsgange og for at understøtte medarbejdernes it-awareness.

Medarbejdersikkerhed

Lector har udarbejdet procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for kompetenceudvikling og instruktion af medarbejdere, der behandler personoplysninger og IT-awareness, herunder gennemførelse af løbende oplysning til medarbejdere.

Gennem interne procedurer for ansættelse sikrer Lector sig dels en screening af medarbejdere, dels en aktiv tavshedsklausul. Desuden holdes medarbejdere ajour med de relevante sikkerhedskrav og pligter.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Styring af aktiver
Lector har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over IT-aktiver og data. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer.

Adgangsstyring
Lector har indført procedurer, der sikrer brugeroprettelser, ændringer og sletning, og at adgang til systemer og data er beskyttet af et autorisationssystem. Brugere oprettes med unik brugeridentifikation og tofaktorgodkendelse (password), og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. For at sikre, at ingen har fået uautoriseret adgang i Lector og hos Lector's kunder, foretages årligt stikprøvekontrol til gennemgang af rettighedsgrupperne. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf. Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Risikovurdering
Ledelsen i Lector er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som Lector til enhver tid står over for, så indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

- Der gennemføres kvartalsvis en risikoanalyse for at klarlægge risici.
- Alle medarbejdere i Lector er blevet undervist i persondatasikkerhed, og ledelsen tager løbende
- temaer og emner op over for medarbejderne for at styrke processer og forretningsgange og for at understøtte medarbejdernes it-awareness.
- Lector har en operationel risikostyring der sikrer, at der i det daglige arbejde både er fokus på at identificere operationelle fejl og risici, og at der reageres og sættes ind på de områder, der kan minimere risici til et acceptabelt niveau.
- Risikostyring omfatter kvartalsvise risikovurderinger, som løbende opdateres med relevante trusselsbilleder, herunder cybertrusler, ransomware, cloud-relaterede risici samt risici forbundet med leverandører og tredjepartsafhængigheder.

Der foretages således løbende vurdering af, hvilke sikkerhedsniveauer der er passende i Lector og hos kunderne. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Kryptering
Der anvendes kryptering på al ekstern kommunikation til og fra datacentreret. Der anvendes enten VPN eller SSL.

Driftssikkerhed
Tilgængeligheden af systemer og data sikres gennem en fortsat drift i tilfælde af mulige forstyrrelser. Dette sikres bl.a. gennem kontroller, der er forebyggende, detektive og korrigerende. Kontrollerne ligger inden for fysiske kontroller, procedurekontroller, tekniske kontroller og lovmæssigt styrede kontroller. Disse kontroller dækker bl.a. over følgende: autentifikation, antivirus, firewall, incident management, monitorering, backup og beredskabsplaner.

De fysiske datacentre leveret via Microsoft Azure, Amazon AWS, eller Kimo Consulting, varetager fysisk sikkerhed, i form af låse, brandslukningsudstyr, nødstrømsudstyr, mv.

Lector anvender kontroller for styring af adgang til systemer og data med henblik på at sikre, at kun autoriserede brugere får adgang. Adgang til administrative funktioner og følsomme systemer er underlagt stærk autentifikation, herunder multifaktorautentifikation (MFA), hvor dette er understøttet.

Adgangsrettigheder tildeles og administreres efter princippet om mindste privilegium, og der foretages løbende vurdering og vedligeholdelse af brugerrettigheder.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kundens data sikres, ved at struktureringen af netværket opbygges af VLANs, så de enkelte kunder kun kan tilgå deres eget netværk.

Systemer overvåges automatisk via de værktøjer som Microsoft og Amazon stiller til rådighed som en del af deres drifts-center løsninger. For systemer, der ikke kan monitoreres automatisk, er der etableret fastlagte manuelle driftsrutiner og backuprutiner. Ved fejl eskaleres disse til den ansvarlige.

Al trafik mellem internettet og netværk kontrolleres af firewall. Adgang ude fra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter.

Alle arbejdsstationer og servere er beskyttet mod virus og malware. Der sker en løbende automatisk opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau, og der er opsat en løbende overvågning af disse systemer.

Lector har procedurer, der sikrer, at systemer og data sikkerhedskopieres (backup) for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Sikkerhedskopier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde. Der tjekkes på alle hverdage rapporter for sikkerhedskopiering.

Styring af informationssikkerhedsnedbrud

Lector besidder en IT-beredskabsplan, som sikrer, at systemer internt og hos kunder genetableres hurtigst muligt i tilfælde af en hændelse, og at omfanget af skader begrænses mest muligt. Beredskabsplanen opdateres årligt. Sikkerhændelser dokumenteres. Lector har indført procedure for håndtering af hændelser og underretning om sikkerhedsbrud til kunder.

Support og Kommunikation

Der ydes support på alle produkter, der er udviklet af Lector.

I forbindelse med eventuelle sikkerhedshændelser kontaktes berørte kunder så hurtigt som muligt pr. telefon.

Når politikker og procedurer/SOP (standard operating procedures) opdateres, kommunikeres dette til medarbejdere. For den helt centrale IT Sikkerhedspolitik, underskriver medarbejderen at denne er læst, forstået og følges. Politikker og proceduren er tilgængelige i vores egen interne instans af vores eget TeamShare produkt, hvor medarbejderne altid kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til den it-sikkerheds-ansvarlige, der sørger for relevante rettelser.

Vedligehold af systemer

Lector udfører patch management på systemer i datacentrene. Formålet er at sikre, at der sker sikkerhedsopdatering af kritiske systemer. Det gælder både systemer, som benyttes internt, og systemer, som benyttes af eksterne kunder (kundesystemer)

Lector har en fast procedure for patchning af Windows og Linus servere og tilhørende standard programmel, der patches hver måned med seneste patch niveau fra Microsoft. Dette sker i et fastsat service-vindue som fremgår af den SLA der er indgået med kunden.

Opdatering og patchning af Lectors systemer, TeamShare, ESS og LTS, sker dette når der er relevante opdateringer og i aftale med kunden. Dette sker i et fastsat service-vindue som fremgår af den SLA der er indgået med kunden.

Sikkerhedshændelser

Hvis der konstateres en sikkerhedshændelse, adviseres de berørte kunder så hurtigt som muligt, og samtidigt tages der skridt til at sikre data og systemer. Efterfølgende udarbejdes en "root cause analysis"-rapport til kunden, for så vidt muligt at sikre at hændelsen ikke kan optræde igen.

Alle sikkerhedshændelser rapporteres til it-sikkerhedsudvalget og dermed til ledelsen.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Leverandørforhold

Lector har outsourcet hardwaredrift og det virtuelle applikationslag til eksterne leverandører. Hos leverandørerne er serverrummene sikret mod miljømæssige trusler som brand, vandindtrængning, fugt, overophedning, strømudfald og overspænding. Systemer til miljømæssig sikring af driftsfaciliteter er serviceret og vedligeholdt løbende efter de respektive leverandørers forskrifter.
Lector indhenter SOC 2 eller ISAE-erklæring fra disse leverandører.

Komplementerende kontroller hos de dataansvarlige

Som led i leveringen af ydelserne forudsættes det, at de dataansvarlige har implementeret og opretholder en række komplementerende kontroller. Disse kontroller er væsentlige for, at de af leverandøren udførte kontroller kan understøtte opfyldelsen af de fastsatte kontrolmål.
De komplementerende kontroller omfatter blandt andet, at den dataansvarlige:

- Sikrer, at de behandlede personoplysninger er korrekte, fuldstændige og løbende ajourførte i de relevante systemer og registre
- Etablerer og vedligeholder procedurer for løbende datakvalitetskontrol, herunder håndtering af fejl og uoverensstemmelser i data
- Sikrer, at behandlingsinstruksen til enhver tid er lovlig i forhold til gældende databeskyttelsesretlig regulering (herunder GDPR)
- Sikrer, at behandlingsinstruksen er tydelig, tilstrækkelig og operationelt anvendelig i forhold til databehandleraftalen og den konkrete ydelse
- Sikrer, at kun relevante og autoriserede brugere er oprettet, og at brugeroplysninger samt rettigheder løbende ajourføres
- Gennemfører regelmæssig gennemgang af brugeradgange, herunder rettighedsniveauer og behovsprincippet
- Sikrer, at interne processer for godkendelse, ændring og ophør af brugeradgange er dokumenterede og efterleves
- Sikrer, at ændringer i forretningsprocesser, datagrundlag eller systemanvendelse, som har betydning for databehandlingen, kommunikeres rettidigt til databehandler
- Sikrer, at hændelser, fejl eller brud på persondatasikkerheden identificeres, håndteres og hvor relevant meddeles databehandler uden unødig forsinkelse
- Sikrer, at der foreligger passende organisatoriske og tekniske foranstaltninger hos den dataansvarlige, som understøtter de aftalte sikkerhedskrav

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

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

Til ledelsen hos Lector ApS, kunder og disses revisorer

Omfang
Vi har fået som opgave at afgive erklæring om Lector ApS' beskrivelse i afsnit 2 af it-kontroller for perioden 1. juni 2025 til 31. maj 2026 og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Lector ApS anvender Microsoft Azure og Kimo Consult ApS som underdatabehandlere for anvendt hosting og web. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Microsoft Azure og Kimo Consult ApS varetager for Lector ApS.

Enkelte af de kontrolmål, der er ført i beskrivelsen i afsnit 2, kan kun nås, hvis de komplementærekontroller hos Lector ApS' kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen om- fatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Lector ApS' ansvar
Lector ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

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

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

Revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Lector ApS' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de 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 planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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

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

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Begrænsninger i kontroller hos en dataansvarlig
Lector ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som kunder måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelig eller svigte.

Konklusion
Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse i afsnit 1. Det er vores opfattelse,

(a) at beskrivelsen af Lector ApS' softwareløsninger , således som de var udformet og implementeret i perioden 1. juni 2025 til 31. maj 2026, i alle væsentlige henseender er retvisende, og
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. juni 2025 til 31. maj 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 perioden 1. juni 2025 til 31. maj 2026.

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder og disses revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i kunders regnskab.

Søborg, den 28. juli 2026

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
statsautoriseret revisor

Simon Okkels
Partner, Lead IT-auditor (CISA)

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

4. Kontrolmål, kontroller, test og resultat heraf

4.1 Formål og omfang

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Lector ApS har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 1. juni 2025 til 31. maj 2026.

Vi har således ikke nødvendigvis testet alle de kontroller, som Lector ApS har nævnt i beskrivelsen i afsnit 2.

Denne erklæring er afgivet efter den partielle metode, og omfatter ikke kontrolmål og tilknyttede kontroller hos Lector ApS' underleverandører og underdatabehandlere.

Kontroller udført hos Lector ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

4.2 Udførte testhandlinger

Test af kontrollernes design, implementering og operationelle effektivitet er foretaget via følgende metoder:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel til passende personale hos Lector ApS er udført for alle væsentlige kontrolaktiviteter. Forespørgsler er udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres. Endvidere for at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation, som indeholder information om udførelse af kontrollen. Det omfatter gennemlæsning 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.
Observation	Observation af kontrollens udførelse.
Genudførelse af kontrol	Den relevante kontrol er genudført med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores test af de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

4 Risikovurdering

Kontrolmål 4.1 (Retningslinjer for risikovurderinger)

Virksomheden har en procedure for udarbejdelse af risikovurdering og der er udarbejdet en aktuel og godkendt risikoanalyse, ligesom der udarbejdes planer for håndtering af risici.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der skal udarbejdes risikovurdering. Risikovurderingen skal udarbejdes minimum årligt og godkendes af ledelsen. Risikovurderingen skal indeholde planer for håndtering af risici.	Vi har forespurgt ledelsen om en skriftlig procedure for risikovurdering. Vi har forespurgt ledelsen om den aktuelle risikoanalyse. Vi har inspiceret, at der findes en aktuel risikoanalyse, denne har været gennemgået i Informationssikkerhedsudvalget, og ledelsen har godkendt risikoanalysen. Vi har inspiceret at der foreligger planer for håndtering af risici.	Vi har ikke konstateret afvigelser.

5 Informationssikkerhedspolitikker

Kontrolmål 5.1 (Retningslinjer for styring af informationssikkerhed)

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

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
5.1	Sikkerhedspolitikker skal være dokumenteret og vedligeholdes ved gennemgang mindst en gang årligt. Sikkerhedspolitikken skal være godkendt af ledelsen. Sikkerhedspolitikken er gjort tilgængelig for medarbejdere f.eks. via intranettet. Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt ledelsen om seneste sikkerhedspolitik. Vi har inspiceret, at der forefindes en sikkerhedspolitik og ledelsen har godkendt sikkerhedspolitikken. Vi har inspiceret, at sikkerhedspolitikken er let tilgængelig for medarbejderne. Vi har inspiceret at sikkerhedspolitikken som minimum er revurderet én gang årligt.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

6 Organisering af informationssikkerhed

Kontrolmål 6.1 (Intern organisering)

At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
6.1	Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver. Der skal opretholdes passende kontakt med relevante myndigheder. Informationssikkerhed skal anvendes ved projektstyring.	Vi har forespurgt ledelsen om de organisatoriske roller og ansvar, der gælder i forbindelse med styring af informationssikkerheden. Vi har inspiceret, at det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret via udvalgte referater fra mødeaktiviteter. Vi har inspiceret at forhold omkring funktionsadskillelse er vurderet og tilstrækkeligt implementeret hvor muligt. Vi har inspiceret at der er uddelegeret ansvar for kontakt med relevante myndigheder. Vi har forespurgt ledelsen om retningslinjerne for projektledelse.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 6.2 (Mobilt udstyr og fjernarbejdspladser) At sikre fjernarbejdspladser og brugen af mobilt udstyr.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
6.2	Der er udarbejdet politikker og retningslinjer for brugen af mobile enheder. Der er udarbejdet politikker og retningslinjer for fjern- og hjemmearbejdspladser.	Vi har forespurgt ledelsen om politikker og retningslinjer for medarbejderes brug af mobile enheder. Vi har inspiceret, at der er udarbejdet politikker og retningslinjer for brugen af mobile enheder herunder medarbejders eget udstyr (BYOD). Vi har forespurgt ledelsen om politikker og retningslinjer for medarbejderes brug af hjemmearbejdspladser/fjernarbejdspladser. Vi har inspiceret, at der er udarbejdet politikker og retningslinjer for hjemmearbejde. Vi har inspiceret VPN opsætning til fjernopkobling til internt netværk.	Vi har ikke konstateret afvigelser.

7 Personalesikkerhed

Kontrolmål 7.1 (Før ansættelsen) At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.1	Efterprøvning af alle jobkandidaters baggrund skal udføres i overensstemmelse med relevante love, forskrifter og etiske regler og skal stå i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici. Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har forespurgt ledelsen om procedurerne for rekruttering af medarbejdere. Vi har inspiceret, at der foretages screening af nyansættelser. Vi har inspiceret, at ansættelsesvilkårene indeholder beskrivelser af ansvar i forbindelse med informationssikkerhed. Vi har inspiceret at der underskrives en fortrolighedsaftale. Vi har inspiceret at ansøgere i rekrutteringsforløbet introduceres for retningslinjerne for informationssikkerhed.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 7.2 (Under ansættelsen) At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerheds-ansvar.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.2	Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer. Medarbejdere skal løbende informeres og gennemgå awarenesstræning for at sikre forståelsen for deres ansvar og rolle, således, at de kan opfylde deres informationssikkerheds-ansvar.	Vi har forespurgt ledelsen til beskrivelsen af kravene til ledere i forhold til opretholdelse af ansvar for informationssikkerheden. Vi har inspiceret, at ledelsesforholdene er velbeskrevne, og der forefindes let tilgængelige og opdaterede organisationsdiagrammer. Vi har inspiceret, at der har været gennemført relevant uddannelse og awarenesstræning.	Vi har ikke konstateret afvigelser.

Kontrolmål 7.3 (Ansættelsesforholdets ophør eller ændring) At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.3	Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med ansættelsesophør. Vi har inspiceret, at der findes en proces til sikring af tilbagelevering af væsentlige aktiver i forbindelse med fratrædelse, og suspendering af brugerrettigheder eller lign. Vi har inspiceret at brugerrettigheder vurderes i forbindelse med en væsentlig ændring i ansættelsesforholdet. Vi har foretaget stikprøvekontrol for dokumentation for udførelsen.	Vi er blevet oplyst at der ikke har været eksempler på ændringer i medarbejderes position som har krævet en revurdering af adgangsrettigheder. Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

8 Styring af aktiver

Kontrolmål 8.1 (Ansvar for aktiver)

At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
8.1	Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver. Der skal udpeges en ejer i organisationen for hvert aktiv. Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og implementeres. Alle medarbejdere og eksterne brugere skal aflevere alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med identifikation af informationsaktiver. Vi har stikprøvevis inspiceret fortegnelsen over kritiske informationsaktiver. Vi har inspiceret, at det organisatoriske ansvar for informationsaktiver er dokumenteret og implementeret, og at der er placeret ejerskab i forhold til ansvar for den tilhørende informationssikkerhed. Vi har forespurgt ledelsen om procedurerne vedr. accepteret brug af aktiver. Vi har inspiceret et udvalg af fratrædelser og påset kvitteringer for tilbagelevering af udleverede aktiver.	Vi har ikke konstateret afvigelser.

Kontrolmål 8.3 (Mediehåndtering)

At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
8.3	Der skal implementeres procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget. Medier skal bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer. Medier der indeholder information, skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med styring af bærbare medier. Vi har inspiceret, at der findes en procedure til sikker bortskaffelse af informationsbærende medier. Vi har forespurgt eksempler på udført bortskaffelse af informationsbærende medie.	Vi er blevet oplyst om, at der ikke har været eksempler på udført bortskaffelse af informationsbærende medier i perioden. Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

9 Adgangsstyring

Kontrolmål 9.1 (Forretningsmæssige krav til adgangsstyring)

At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.1	En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav. Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Vi har inspiceret politikken for adgangsstyring, herunder om denne er opdateret og godkendt. Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester. Vi har inspiceret et udvalg af brugere med henblik på at konstatere, at de kun har adgang til netværkstjenester, der er tildelt på baggrund af et arbejdsrelateret behov.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 9.2 (Administration af brugeradgange) At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.2	Alle brugere skal være registeret med et unikt bruger-id, og deres rettigheder til netværk og systemer skal være i overensstemmelse med virksomhedens politikker. Endvidere sikres det, at rettigheder begrænses mest muligt, er betinget af et arbejdsrelateret behov, er godkendt og oprettet korrekt i systemerne. Administratorkonti kontrolleres med jævne mellemrum for at sikre systemets integritet. Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp af formel administrationsproces Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder. Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller skal tilpasses efter en ændring.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med brugeradministration. Vi har stikprøvevis indhentet oversigter over brugerkonti på systemer og netværk. Vi har stikprøvevis udvalgt nye brugere og inspiceret, at anmodning om adgang fra disse var dokumenteret og godkendt i overensstemmelse med relevant sikkerhedspolitik. Vi har forespurgt ledelsen om procedurerne for hemmelig autentifikationsinformation. Vi har inspiceret et udvalg af brugerreview rapporter, herunder de konklusioner der er foretaget. Vi har stikprøvevis sammenholdt oversigten over ophørte brugere med oversigten over aktuelle brugerkonti og inspiceret, at brugerkonti var deaktiveret eller slettet.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 9.3 (Brugernes ansvar) At gøre brugere ansvarlige for at sikre deres autentifikationsinformation			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.3	Det skal være et krav, at brugerne følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation. Adgange til systemer, netværk, databaser og datafiler, er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde, kompleksitet og udløbstid ligesom passwordopsætninger medfører, at password ikke kan genbruges. Endvidere bliver brugeren deaktiveret ved gentagne fejlagtige forsøg på login.	Vi har inspiceret passwordpolitikken. Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordadministration. Vi har inspiceret password-settings i serverinfrastruktur, og databaser ved inspektion af konfigurationsudtræk.	Vi har ikke konstateret afvigelser.

Kontrolmål 9.4 (Styring af system- og applikationsadgang) At forhindre uautoriseret adgang til systemer og applikationer			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.4	Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring. Adgang til systemer og applikationer styres af en procedure for sikker log-on. Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet. Brugen af systemer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt. Adgang til kildekoder til programmer skal begrænses.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med retningslinjerne for begrænsning af adgang til information. Vi har inspiceret at der er implementeret en procedure for sikker log-on. Vi har forespurgt ledelsen om anvendelsen af systemer til administration af adgangskoder. Vi har forespurgt ledelsen om anvendelsen af privilegerede systemprogrammer. Vi har forespurgt ledelsen om retningslinjerne for adgang til kildekode.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

10 Kryptografi

Kontrolmål 10.1 (Kryptografiske kontroller)

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

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
10.1	Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information. Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi. Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet.	Vi har ikke konstateret afvigelser.

11 Fysisk sikring og miljøsikring

Kontrolmål 11.1 (Sikre områder)

At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
11.1	Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter. Personer uden autorisation, som har behov for adgang til lokaler, vil altid have ledsaget adgang af en person med gyldig adgang.	Vi har stikprøvevis inspiceret, at der er implementeret perimetersikring af lokaler og bygninger i overensstemmelse med beskrivelserne. Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med fysisk adgangskontrol for lokaler og bygninger. Vi har inspiceret procedurerne vedr. besøg fra gæster.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 11.2 (Udstyr) At undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
11.2	Udstyr, information og software fjernes ikke fra organisationen uden forudgående tilladelse. Brugere er via retningslinjer gjort opmærksom på deres ansvar for udstyr uden opsyn, herunder er der etableret foranstaltninger som f.eks. Passwordbeskyttede pauseskærme. Der er er etableret "clean desk policy".	VI har inspiceret retningslinjerne for sikker bortskaffelse af udstyr med lagringsmedier. Vi har inspiceret retningslinjerne for brugernes ansvar for udstyr uden opsyn. Vi har inspiceret retningslinjerne og inspiceret via besøg på hovedkontoret at retningslinjerne følges.	Vi har ikke konstateret afvigelser.

12 Driftssikkerhed

Kontrolmål 12.1 (Driftsprocedurer og ansvarsområder) At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.1	Der skal være tilfredsstillende procedurer og forretningsgange for opretholdelse af driften. Herunder findes overvågning, registrering af hændelser og opfølgning på disse. Nye systemer og væsentlige opgraderinger bliver testet, herunder brugeraccepttest af kvalificerede medarbejdere og dokumenteres og godkendes før implementering i produktionsmiljøet. Der udføres endvidere efterfølgende verifikation af implementeringer. Problemer identificeret under udvikling og implementering af nye systemer og væsentlige opdateringer bliver løst tilfredsstillende. Ændringer er underlagt konfigurationsstyring. Anvendelsen af ressourcer skal styres og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemerne fungerer som krævet. Der er implementeret politikker og	Vi har forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret. I forbindelse med revisionen af de enkelte driftsområder har vi kontrolleret, at der foreligger dokumenterede procedurer, samt at der stikprøvevis er overensstemmelse mellem dokumentationen og de handlinger som faktisk udføres. Vi har inspiceret brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi er blevet oplyst at der ikke har været foretaget nogen nye ændringer eller væsentligt opdateringer af driften i erklæringsperioden og kan derfor ikke teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

12 Driftssikkerhed

	procedurer til sikring af funktionsadskillelse i virksomheden. Disse politikker og procedurer omfatter krav til at: • Ansvar og aktiviteter for udvikling, test og produktion er adskilte • Administratorer med ansvar for produktion har ikke adgang til applikationer og transaktioner.		

Kontrolmål 12.2 (Beskyttelse mod malware)

At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.2	Der er installeret centralt overvåget antivirus på workstations og laptops. Disse funktioners databaser opdateres regelmæssigt og kan ikke modificeres af de enkelte medarbejdere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med malwarebeskyttelse. Vi har inspiceret tilstedeværelsen af antivirusprogrammer på workstations og laptops.	Vi har ikke konstateret afvigelser.

Kontrolmål 12.3 (Backup)

At beskytte mod tab af data.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.3	Det sikres, at der foretages løbende backup af relevante komponenter i infrastrukturen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med backup. Vi har stikprøvevis inspiceret backupprocedurer til bekræftelse af, at de er formelt dokumenteret. Vi har stikprøvevis inspiceret backuplogs vedrørende backups til bekræftelse af, at backups er gennemført succesfuldt, alternativt, at der foretages afhjælpning i tilfælde af mislykkede backups. Vi har stikprøvevis inspiceret restorelogs.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 12.4 (Logning og overvågning) At registrere hændelser og tilvejebringe bevis.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.4	Der udføres hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser, som opbevares og gennemgås regelmæssigt. Logningsfaciliteter og log-oplysninger er beskyttet mod manipulation og uautoriseret adgang. Transaktioner eller aktiviteter samt brugere med privilegerede rettigheder (f.eks. superbrugere) bliver logget. Dette inkluderer også databaser. Afvigende forhold undersøges og løses rettidigt. Der er etableret tidssynkronisering i hele infrastrukturen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med overvågning af systemanvendelse og logning. Vi har stikprøvevis inspiceret log-settings ud fra systemudtræk af platforme og systemer. Vi har forespurgt til proces og foranstaltninger til sikring mod manipulation af logs. Vi har stikprøvevis gennemgået logs for administratorer og systemoperatører. Vi har forespurgt til konceptet for tidssynkronisering.	Vi har ikke konstateret afvigelser.

Kontrolmål 12.5 (Styring af driftssoftware) At sikre integriteten af driftssystemer.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.5	Der er implementeret procedurer til styring af softwareinstallationen i driftssystemer.	Vi har forespurgt ledelsen om procedure og kontrolaktiviteter som udføres i forbindelse med software installationer i driftssystemer.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 12.6 (Sårbarhedsstyring) At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.6	Der er etableret procedurer for patch management, således at kritiske netværkskomponenter, servere og andre enheder holdes opdateret på et passende niveau og overvåges for sikkerhedsmæssige kritiske rettelser. Der er fastlagt og implementeret regler for softwareinstallation, som foretages af brugerne.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med patch management. Vi har stikprøvevis inspiceret ændringer til kritiske netværkskomponenter og servere.	Vi har i forbindelse med vores test konstateret, at 12 ud af 43 enheder fortsat kører på Windows 10, som ikke længere opdateres. Disse enheder vil derfor ikke modtage fremtidige sikkerheds- eller softwareopdateringer og kan som følge heraf være eksponeret for sårbarheder. Ingen yderligere afvigelser fundet.

13 Kommunikationssikkerhed

Kontrolmål 13.1 (Styring af netværkssikkerhed) At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
13.1	Virksomheden opretter selvstændige virtuelle netværk til kunderne. Der oprettes selvstændige VLAN, virtuelle firewalls og virtuelle routingtabeller. Administration af netværksudstyr håndteres udelukkende af autoriseret personale. Der udføres sårbarheds- og penetrationstests mod netværk, hvor dette er fundet relevant eller aftalt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med netværksstyring. Vi har foretaget inspektion af, at netværket er opsat med selvstændige VLAN og DMZ-zoner. Vi har inspiceret, at der er foretaget periodisk sårbarheds- og penetrationstest. Vi har inspiceret, at der er taget stilling til konstaterede svagheder samt iværksat tiltag til udbedring.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 13.2 (Informationsoverførsel) At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
13.2	Der skal være tilfredsstillende procedurer og forretningsgange for datakommunikation, der på hensigtsmæssig måde sikrer mod risiko for tab af ægthed, integritet og fortrolighed. Adgang for administration af kunders systemer kan udelukkende foretages fra virksomhedens kontrollerede netværk. Dette kan enten være via kablet netværk, sikret trådløst netværk eller sikret krypteret VPN forbindelse fra eksterne lokationer. Aftaler skal omhandle sikker overførsel af forretningsinformation mellem organisationen og eksterne parter. Der er sikret tidssvarende kryptering af mailkommunikation. Der er defineret krav til fortrolighedsog hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information.	Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med sikker datakommunikation. Vi har foretaget en inspektion af, at administrationen af kunders systemer udelukkende kan foretages via kablet netværk, sikret trådløst netværk eller VPN. Vi har inspiceret konfiguration som sikrer at der anvendes tilstrækkelig kryptering af mailkommunikation. Vi har forespurgt til procedure for etablering af fortrolighedsaftaler. Vi har inspiceret et udvalg af underskrevne fortrolighedsaftaler med henblik på at konstatere, om proceduren efterleves ved ansættelse af nye medarbejdere.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

14 Anskaffelse, udvikling og vedligeholdelse af systemer

Kontrolmål 14.1 (Sikkerhedskrav til informationssystemer)

At sikre at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
14.1	Informationssikkerhedsrelaterede krav er omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer. Informationer i forbindelse med applikationstjenester over offentlige netværk beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring.	Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med analyse og specifikation af informationssikkerhedskrav til evt. nye systemer implementeret i perioden. Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med sikring af applikationstjenester på offentlige netværk (internettet).	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 14.2 (Sikkerhed i udviklings- og hjælpeprocesser) At sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
14.2	Der er fastlagt og anvendes regler for udvikling af software og systemer i organisationen. Ændringer af systemer indenfor udviklingscyklussen styres ved hjælp af formelle procedurer for ændringsstyring. Ved ændring af driftsplatforme gennemgås og testes forretningskritiske applikationer for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed. Ændringer i softwarepakker vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer styres effektivt. Principper for udvikling af sikre systemer er fastlagt, dokumenteret, opretholdt og anvendt i forbindelse med implementering af informationssystemer. Organisationer bør etablere sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus. Test af sikkerhedsfunktionalitet udføres ved udvikling. Der er etableret godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.	Vi har inspiceret procedurer / kontrolaktiviteter i forbindelse med sikker udvikling. Vi har inspiceret procedurer / kontrolaktiviteter i forbindelse med teknisk ændring af driftsplatformen. Vi har forespurgt ledelsen om procedure / kontrolaktiviteter i forbindelse med rettigheder og begrænsning i implementering af ændringer. Vi har forespurgt ledelsen om procedure / kontrolaktiviteter i forbindelse med etablerede sikre udviklingsmiljøer. Vi har inspiceret procedurer / kontrolaktiviteter i forbindelse med udførelse af løbende sikkerhedstest i udviklingsprocessen.	Vi har ikke konstateret afvigelser.

Kontrolmål 14.3 (Testdata) At sikre beskyttelse af data, som anvendes til test.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
14.3	Testdata udvælges omhyggeligt, beskyttes og kontrolleres.	Vi har inspiceret de procedurer / kontrolaktiviteter, der udføres i forbindelse med anvendelsen af test data i udviklingsopgaver.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

15 Leverandørforhold

Kontrolmål 15.1 (Informationssikkerhed i leverandørforhold)

At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
15.1	Der er etableret passende kontroller til sikring af informationssikkerheden i forbindelse med serviceydelser leveret af underleverandør, hvor underleverandøren har adgang til virksomhedens systemer. Hvis relevant for den leverede service, så kræves kontrolerklæringer fra underleverandøren, som vurderes med hensyn til mulige informationssikkerhedsmæssige svagheder i kontrollerne. Alle relevante informationssikkerhedskrav er fastlagt og aftalt med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information. Aftaler med leverandører indeholder krav til håndtering af informationssikkerhedsrisici forbundet med forsyningskæden for IKT-tjenester og -produkter.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med styring af leverandører. Vi har stikprøvevist inspiceret at der er indhentet kontrolerklæringer for relevante leverandører.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

16 Styring af informationssikkerhedsbrud

Kontrolmål 16.1 (Styring af informationssikkerhedsbrud og forbedringer)

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

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
16.1	Der er placeret ledelsesansvar og etableret procedurer til at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud. Alle sikkerhedshændelser rapporteres til og behandles i Informationssikkerhedsudvalget, som sikrer at hændelserne gennemgås med det primære formål at sikre passende tiltag til forebyggelse af gentagelser. Medarbejdere er via retningslinjerne instrueret om at indrapportere alle informationssikkerhedssvagheder de måtte mistænke eller opdage. Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud. Informationssikkerhedsbrud håndteres i overensstemmelse med de dokumenterede procedurer. Viden opnået ved at analysere og løse informationssikkerhedshændelser bruges til at reducere sandsynligheden for eller virkningen af fremtidige hændelser. Organisationen har defineret og anvender procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som beviser.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med håndtering af sikkerhedshændelser. Vi har inspiceret udleveret materiale vedrørende behandling af sikkerhedshændelser i mødereferater fra Informationssikkerhedsudvalget og security incident logs. Vi har inspiceret retningslinjerne.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Kontrolmål 17.1 (Informationssikkerhedskontinuitet)

Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
17.1	Den samlede katastrofeplan er opbygget af en overordnet katastrofestyringsprocedure samt operationelle katastrofeplaner for de konkrete katastrofeområder. Liste over kunder samt procedurebeskrivelser skal være på plads. Der foretages minimum årlig test af katastrofeberedskabet i form af såvel skrivebordstest som faktiske testscenarier. Disse tests kan være i form af almindelige operationelle procedure i forbindelse med system vedligeholdelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret det udleverede materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser. Vi har inspiceret dokumentation vedrørende test af centrale områder i katastrofeberedskabet, herunder, hvordan beredskabet ved spontane strømafbrydelser i datacenteret afprøves.	Vi har konstateret, at disaster recovery planerne ikke har været opdateret i erklæringsperioden. Ingen yderligere afvigelser fundet.

Kontrolmål 17.2 (Redundans)

At sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
17.2	Alle datacenterets fælles infrastrukturenheder er dimensioneret med redundante enheder. Alle systemer har derfor en individuel backup. Internetforbindelsen er ligeledes redundant.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

18 Overensstemmelse

Kontrolmål 18.1 (Overensstemmelse med lov- og kontraktkrav)

At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav

Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
18.1	Alle relevante lov-, myndigheds- og kontraktkrav samt organisationens metode til overholdelse af disse krav er klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen. Der er implementeret passende procedurer til at sikre, at der er overensstemmelse med lov-, myndigheds- og kontraktkrav i relation til immaterielle rettigheder og anvendelse af beskyttede softwareprodukter. Registreringer er beskyttet mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds- og kontraktkrav samt forretningsmæssige krav. Privatlivets fred og personoplysninger beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter. Kryptografi anvendes i overensstemmelse med alle relevante aftaler, love og forskrifter.	Vi har forespurgt ledelsen om politikker og kontroller i forbindelse med identificering og overholdelse af relevante lov-, myndigheds- og kontraktkrav. Vi har forespurgt ledelsen om politikker og kontroller i forbindelse med overholdelse af immaterielle rettigheder og anvendelse af beskyttede softwarepakker (licenser). Vi har forespurgt ledelsen om og inspiceret informationssikkerhedspolitikkernes overordnede formål om at beskytte data mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds- og kontraktkrav samt forretningsmæssige krav. Vi har forespurgt ledelsen om politikker og kontroller i forbindelse med overholdelse af lov om beskyttelse af personoplysninger.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

Kontrolmål 18.2 (Gennemgang af informationssikkerhed) At sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.			
Nr.	Lector ApS' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
18.2	Organisationens metode til styring af informationssikkerhed og implementering heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt og separat med planlagt mellemrum eller i tilfælde af væsentlige ændringer. Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav. Informationssystemerne undersøges regelmæssigt for, om de er i overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder.	Vi har forespurgt ledelsen og inspiceret politikker og kontroller i forbindelse med styring af informationssikkerhed og implementering heraf, herunder at kontrolmål, kontroller, politikker, processer og procedurer gennemgås uafhængigt, jævnligt og i tilfælde af væsentlige ændringer. Vi har forespurgt ledelsen og inspiceret politikker og kontroller for hvordan ledere i organisationen tager ansvar for hvorvidt egne ansvarsområder/afdelinger lever op til relevante sikkerhedspolitikker, standarder m.v.	Vi har ikke konstateret afvigelser.

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

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."

Tue Villum Sørensen
Adm. direktør
Serienummer: e558b121-cb89-4e24-9c08-212e8fef3400
IP: 94.18.xxx.xxx
2026-07-28 11:16:39 UTC

Mit ID

Simon Okkels
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Partner, Lead IT-auditor (CISA)
Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a
IP: 172.225.xxx.xxx
2026-07-28 12:18:03 UTC

Mit ID

John Richardt Søbjærg
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Statsautoriseret revisor
På vegne af: inforevision a/s
Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a
IP: 87.60.xxx.xxx
2026-07-28 14:12:16 UTC

Mit ID

Penneo dokumentnøgle: MWGZK-X2VDJ-0OV5Q-UYW4E-T5UBP-FDJES

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 underskriveres digitale underskrifter er vedhæftet dokumentet.

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