inforevision

Lector ApS

Ordrupvej 101
2920 Charlottenlund

ISAE 3402, type 1

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller relateret til regnskabsaflæggelsen i forbindelse med softwareløsninger pr. 2. september 2022

CVR.NR. 10 02 16 18

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

Indhold

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

S.nr. 326624

JR/SO

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Lector ApS' generelle IT-kontroller, 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 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 pr. 2. september 2022. 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) 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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt pr. 2. september 2022. 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 pr. 2. september 2022.

Charlottenlund, 2. september 2022
Lector ApS

Tue Villum Sørensen
Adm. direktør

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

2. Lector ApS' beskrivelse af generelle IT-kontroller for levering af drifts-ydelser til kunder

Systembeskrivelse

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 bygger på tre forretningsområder

- Sags- og Dokumenthåndtering, med produkterne TeamShare og ESS
- Toldhåndtering med produktet Logistics Trading Services , LTS
- Konsulentarbejde, hvor Lector leverer færdige software projekter eller ressourcer til kunder. Vi leverer her IT konsulenter på tekniske platforme som .NET, Java, Oracle, SQL Server og tilhørende IT-arkitektur, og organisatoriske konsulenter inden for projektledelse og Scrum/SAFe.

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.

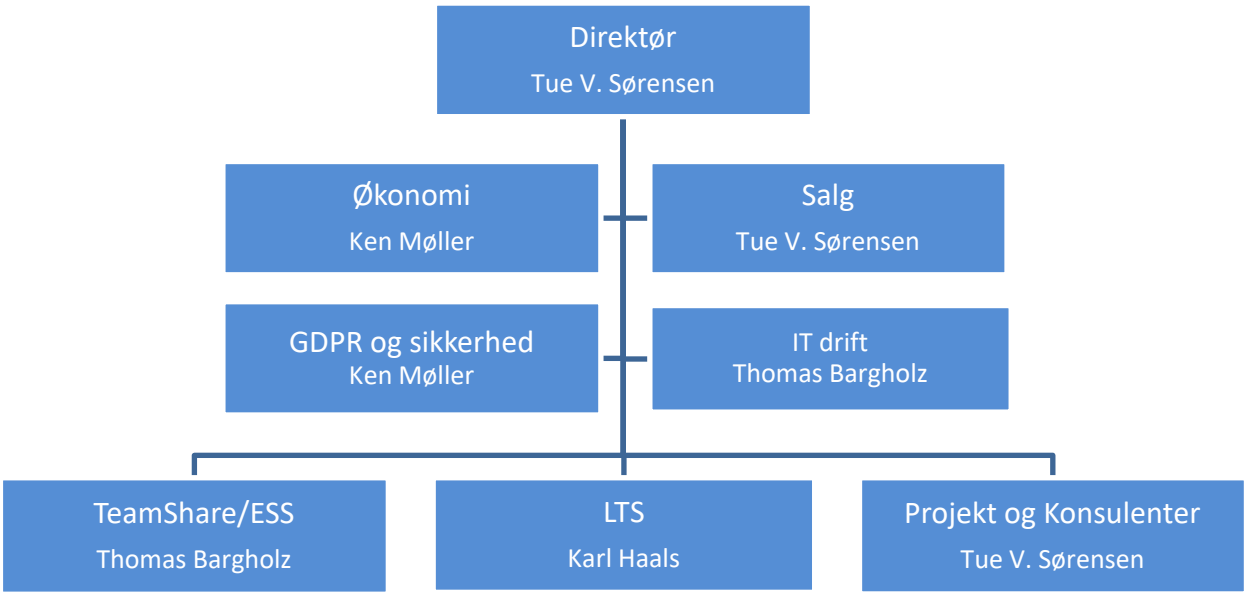
Når Lector leverer cloud SaaS udgaver af TeamShare og ESS, håndteres dette via servere og services i Microsoft Azure West-Europe, og ved at bruge kundernes egne Office 365 SharePoint Online platform, i det datacenter de har valg. Microsoft Azure leverer servere, netværk, hypervisor, storage, backup, monitorering, mv.. 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 er ansvarlig for den fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage. Kimo Consulting 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.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

Organisationsdiagram



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.

Lectors it-sikkerhedspolitik er udarbejdet med afsæt i ISO 27001-standarden, og udvalget foretager en årlig vurdering af denne it-sikkerhedspolitik samt de tilknyttede retningslinjer – herunder at disse lever op til de eksterne forpligtelser udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidig, om der er behov for fornyet risikovurdering. Sikkerhedshændelser rapporteres til medlemmer af it-sikkerhedsrådet, hvor disse behandles.

Når it-sikkerhedspolitikken, it-sikkerhedshåndbogen og beredskabsplanerne opdateres, kommunikeres dette til medarbejdere, hvorigennem medarbejderne derefter kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til it-sikkerhedskoordinatoren, der sørger for relevante rettelser.

Risikostyring

Der bliver løbende foretaget risikoanalyse med henblik på integritet, fortrolighed og tilgængelighed samt beskyttelse af alle systemer og data, både interne og kunders. Denne risikoanalyse gennemgås kvartalsvist mellem den IT-sikkerhedsansvarlige og den administrerende direktør, samt mindst en gang om året, eller ved større ændringer, af hele ledelsesgruppen.

Til at imødegå allerede identificerede risici er der etableret faste test af beredskabsplanen med dertilhørende dokumentation. Testplanen er bygget op over test vedrørende den fysiske sikkerhed samt test af kunderelaterede systemer.

I den aktuelle risikoanalyse forefindes der ikke risici kategoriseret som kritiske.

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,

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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.
Der er indarbejdet adgangsstyring for håndtering og godkendelse af brugerid'er. Der er fastlagte passwordpolitikker for autentifikation og to-faktor-autentifikation, som er udmøntet i standarder.
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.

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.

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 respek-tive leverandørers forskrifter.

Lector indhenter SOC 2 eller ISAE-erklæring fra disse leverandører.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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's beskrivelse i afsnit 2 af generelle it-kontroller pr. 2. september 2022 og om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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.

Inforevision er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Lector ApS's beskrivelse samt om udformningen 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen 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. 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. 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.

Som nævnt har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

Begrænsninger i kontroller hos en dataansvarlig
Lector ApS's 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.

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' generelle IT-kontroller, således som de var udformet og implementeret pr. 2. september 2022, 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 pr. 2. september 2022.

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, 2. september 2022

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
statsautoriseret revisor

Simon Okkels
IT revisor, CISA

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

4. Kontrolmål, kontroller, test og resultat heraf

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 pr. 2. september 2022.

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

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

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: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 væsentlige 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 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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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. Der skal opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer. 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 hvordan der opretholdes kontakt med særlige interessegrupper. Vi har forespurgt ledelsen om retningslinjerne for projektledelse.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 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 ikke konstateret væsentlige 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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

Kontrolmål 7.2 (Under ansættelsen) At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
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 awarenestræning for at sikre forståelsen for deres ansvar og rolle, således, at de kan opfylde deres informationssikkerhedsansvar.	Vi har forespurgt ledelsen til beskrivelsen af kravene til ledere i forhold til opretholdelse af ansvar for informationssikkerheden. Vi har inspiceret, at der har været gennemført relevant uddannelse og awarenestræning.	Vi har ikke konstateret væsentlige 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 har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 har ikke konstateret væsentlige afvigelser.

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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 er 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 væsentlige 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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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. 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 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.	Vi har forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 væsentlige 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 væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 forespurgt til proces og foranstaltninger til sikring mod manipulation af logs. Vi har forespurgt til konceptet for tidssynkronisering.	Vi har ikke konstateret væsentlige 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 bør implementeres 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 væsentlige afvigelser.

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.	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 ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 kvartalsvise sårbarheds- og penetrationstests mod kunders netværk, hvis dette er aftalt med kunden.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med netværksstyring. Vi har foretaget en inspektion af firewall-konfigurationen, samt at der gøres brug af Intrusion Detection systemer, som løbende og aktivt giver oplysninger om mulige ændringer, der kan påvirke fortroligheden, integriteten og tilgængeligheden i data. Vi har foretaget inspektion af, at netværket er opsat med selvstændige VLAN og DMZ-zoner. Vi har forespurgt ledelsen til procedure for periodisk sårbarheds- og penetrationstest.	Vi har ikke konstateret væsentlige afvigelser.

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. Aftaler skal omhandle sikker overførsel af forretningsinformation mellem organisationen og eksterne parter. Der er sikret muligheder for tidssvarende kryptering af mailkommunikation. Der er defineret krav til fortrolighed- og 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 forespurgt til procedure for etablering af fortrolighedsaftaler.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 bør være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer. Informationer i forbindelse med applikationstjenester over offentlige netværk bør beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring. Informationer i forbindelse med handelsapplikationer og -tjenester bør beskyttes for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse, uautoriseret kopiering eller retransmission af meddelelser.	Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med analyse og specifikation af informationssikkerhedskrav til evt. nye systemer. Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med sikring af applikationstjenester på offentlige netværk (internettet). Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med indkøb eller udvikling af handelsapplikationer og -tjenester.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 bør fastlægges og anvendes regler for udvikling af software og systemer i organisationen. Ændringer af systemer indenfor udviklingscyklussen bør styres ved hjælp af formelle procedurer for ændringsstyring. Ved ændring af driftsplatforme bør forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed. Ændringer i softwarepakker bør vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer børe styres effektivt. Principper for udvikling af sikre systemer bør fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med implementering af informationssystemer. Virksomheden har etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus.	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 ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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 bør udvælges omhyggeligt og beskyttes og kontrolleres.	Vi har inspiceret de procedurer / kontrolaktiviteter, der udføres i forbindelse med anvendelsen af test data i udviklingsopgaver.	Vi har ikke konstateret væsentlige afvigelser.

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.	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 væsentlige afvigelser.

Kontrolmål 15.2 (Styring af leverandørydelser) At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.			
Nr.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
15.2	Organisationer bør regelmæssigt overvåge, gennemgå og auditere leverandørydelser.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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.	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 security incident logs. Vi har inspiceret retningslinjerne.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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. Den operationelle katastrofeplan indeholder beskrivelse af katastrofeorganisationen med de ledelsesmæssige funktions-beskrivelser, kontaktinformationer, varslingslister samt instrukser for de nødvendige indsatsgrupper. For de enkelte platforme er udarbejdet detaljerede indsatsgruppeinstrukser for reetablering i forhold til nøddrift. Der skal være implementeret disaster recovery planer for de kunder der har bestilt denne sikring. 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 ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

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.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.	Vi har ikke konstateret væsentlige afvigelser.

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

PENNEO

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

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

Tue Villum Sørensen
Adm. direktør
Serienummer: PID:9208-2002-2-314936226653
IP: 94.18.xxx.xxx
2022-09-05 14:21:51 UTC
NEM ID

Simon Okkels
IT-revisor
Serienummer: ee2c922a-6010-4e0f-8f53-592c10ff891b
IP: 80.162.xxx.xxx
2022-09-06 07:18:03 UTC
MitID

John Richardt Søbjærg
Statsautoriseret revisor
Serienummer: CVR:19263096-RID:1265358432438
IP: 93.165.xxx.xxx
2022-09-06 08:53:55 UTC
NEM ID

Penneo dokumentnøgle: QHBUF-38ZK3-WF7DD-3H6IM-UB5TB-4AD3T

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validate**