KOMiT a.m.b.a.

Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende generelle it-kontroller pr. 15. marts 2025 i relation til KOMiT a.m.b.a.s udviklings-, drifts- og udviklingsydelser til andelshavere

April 2025

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

Indhold

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet af KOMiT a.m.b.a. (KOMiT) til brug for andelshavere, der har anvendt udviklings-, drifts- og udviklingsydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som andelshaverne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber.

KOMiT anvender Microsoft, NetIP A/S og Scannet A/S til hosting og backup. Erklæringen anvender partielmetoden, og beskrivelsen i afsnit 3 omfatter alene kontrolmål og tilhørende kontroller hos KOMiT og ikke kontrolmål og tilhørende kontroller hos Microsoft, NetIP A/S og Scannet A/S. Vores vurdering har ikke omfattet kontroller hos Microsoft, NetIP A/S og Scannet A/S.

Det fremgår af beskrivelsen, at visse kontrolmål anført heri kun kan nås, hvis de komplementære kontroller hos andelshaverne, der er forudsat i udformningen af vores kontroller, er hensigtsmæssigt designet og implementeret. Erklæringen omfatter ikke hensigtsmæssigheden af designet og implementeringen af sådanne komplementære kontroller hos andelshaverne.

KOMiT bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en hensigtsmæssig præsentation af udviklings-, drifts- og udviklingsydelser, der har behandlet andelshaveres transaktioner pr. 15. marts 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til udviklings-, drifts- og udviklingsydelser var designet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret
   - De processer i både it-systemer og manuelle systemer, der er anvendt til styring af generelle it-kontroller
   - Relevante kontrolmål og kontroller designet og implementeret til at nå disse mål
   - Kontroller, som vi med henvisning til udviklings-, drifts- og udviklingsydelser har forudsat ville være implementeret af andelshaverne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for generelle it-kontroller

   (ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af generelle it-kontroller i relation til udviklings-, drifts- og udviklingsydelser, der er beskrevet, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af andelshavere og deres revisorer og derfor ikke kan omfatte alle aspekter ved generelle it-kontroller i relation til udviklings-, drifts- og udviklingsydelser, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt designet og implementeret pr. 15. marts 2025. 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.

Odense, 1. april 2025
KOMiT a.m.b.a.

Anders Banke
administrerende direktør

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

2. Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres design og implementering

Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende generelle it-kontroller pr. 15. marts 2025 i relation til KOMiTs udviklings-, drifts- og udviklingsydelser til andelshavere

Til: KOMiT a.m.b.a. (KOMiT), deres andelshavere og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om KOMiTs beskrivelse i afsnit 3 af generelle it-kontroller i relation til udviklings-, drifts- og udviklingsydelser, der har behandlet andelshaveres transaktioner pr. 15. marts 2025 (beskrivelsen), og om hensigtsmæssigheden af designet og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

KOMiT anvender Microsoft, NetIP A/S og Scannet A/S til hosting og backup. Erklæringen anvender partielmetoden, og beskrivelsen i afsnit 3 omfatter alene kontrolmål og tilhørende kontroller hos KOMiT og ikke kontrolmål og tilhørende kontroller hos Microsoft, NetIP A/S og Scannet A/S. Vores gennemgang har ikke omfattet kontroller hos Microsoft, NetIP A/S og Scannet A/S.

Det fremgår af beskrivelsen, at visse kontrolmål anført heri kun kan nås, hvis de komplementære kontroller hos andelshaverne, der er forudsat i udformningen af KOMiTs kontroller, er hensigtsmæssigt designet og implementeret. Erklæringen omfatter ikke hensigtsmæssigheden af designet og implementeringen af sådanne komplementære kontroller hos andelshaverne.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

KOMiTs ansvar

KOMiT er ansvarlig for udarbejdelsen af beskrivelsen og den 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 fastlægge kontrolmålene og anføre dem i beskrivelsen; for at identificere de risici, der truer opnåelsen af kontrolmålene; for at identificere kriterierne samt for at designe og implementere 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, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer 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 hensigtsmæssigheden af præsentationen af KOMiTs beskrivelse samt om hensigtsmæssigheden af designet og implementeringen af kontroller, der knytter sig til de kontrolmål, som 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, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og implementeret.

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen af en serviceleverandørs system og om designet og implementeringen af kontroller hos en serviceleverandør, omfatter udførelse af handlinger for at opnå bevis for beskrivelsen samt for kontrollernes design og implementering. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er hensigtsmæssigt præsenteret, og at kontrollerne ikke er hensigtsmæssigt designet og implementeret. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt relevansen af de kriterier, som KOMiT har specificeret og beskrevet i afsnit 1.

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

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Iboende begrænsninger

KOMiTs beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af andelshavere og deres revisorer og omfatter derfor ikke nødvendigvis alle aspekter ved udviklings-, drifts- og udviklingsydelser, som den enkelte kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser i udviklings-, drifts- og udviklingsydelser.

Konklusion

På baggrund af kriterierne og de kontrolmål, der er beskrevet i KOMiTs udtalelse i afsnit 1, er det vores opfattelse:

a) at beskrivelsen af generelle it-kontroller i relation til udviklings-, drifts- og udviklingsydelser, som designet og implementeret pr. 15. marts 2025, i alle væsentlige henseender er hensigtsmæssigt præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet og implementeret med henblik på at opnå høj grad af sikkerhed for, at de anførte kontrolmål ville være opnået, hvis de beskrevne kontroller var operationelt effektive pr. 15. marts 2025, og hvis andelshaverne udførte de komplementære kontroller, der er omtalt i afsnit 3.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse tests fremgår af afsnit 4.

Tiltænkte brugere og formål

Vi har af KOMiT fået til opgave at afgive erklæring, og derfor er denne erklæring samt beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf tiltænkt KOMiT.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

Vi tillader kun, at KOMiT – efter eget skøn – offentliggør denne erklæring i dens fulde længde, herunder beskrivelsen i afsnit 4 af test af kontroller og resultaterne heraf. Offentliggørelse må kun ske til andelshavere, der har anvendt KOMiTs udviklings-, drifts- og udviklingsydelser pr. 15. marts 2025, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information om kontroller, som andelshaverne selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber. PwC påtager sig intet ansvar over for andelshaverne eller deres revisorer.

Vores erklæring må ikke anvendes til andre formål og må ikke udleveres til andre parter.

Aarhus, 1. april 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

3. Systembeskrivelse

KOMiT a.m.b.a. (KOMiT) er et selvstændigt andelsselskab, som blev stiftet af 60 repræsentanter fra frie skoler i 1985 med det formål at digitalisere økonomistyringen i skolerne.

Andelshaverne består i dag af højskoler, efterskoler, frifagskoler, private fri- og grundskoler samt fri- og valgmenigheder. Det er kun andelshavere, der kan gøre brug af programmer og services fra KOMiT.

De leverede programmer er udelukkende udviklet til andelshavernes brug og er derfor også målrettet denne gruppe. Programmerne, som er blevet revideret, er:

- **KOMiT**
  Komplet administrativt system

- **KOMiT Løn**
  Komplet lønsystem

- **ViGGO**
  Ledelses- og kommunikationssystem til driften af organisationen og kommunikation med elever/forældre eller andre eksterne interessenter.

Alle programmer udvikles og testes af KOMiT, inden de leveres/frigives til andelshaverne.

Revisionens omfang

Denne ISAE 3402-revision dækker følgende forhold hos KOMiT for både drift, udvikling og support:

- IT-sikkerhed
- Organisering af IT-sikkerhed
- Ansættelser/medarbejdere
- Hardware
- Adgangskontrol og brugerrettigheder
- Fysisk adgang og adgangskontrol
- Operationelle procedurer
- Sikkerhed i udvikling og supportprocesser
- Leverandørerservice og sikkerhed i leverancen
- Management af brud på IT-sikkerhed og forbedringer
- Informationssikkerhedskontinuitet (beredskaber).

Der er etableret passende kontroller for alle områder.

Alle områder er dækket af politikker eller procedurer, og disse er beskrevet nærmere i det følgende.

IT-sikkerhed

KOMiT har en IT-politik, der dækker alle processer i virksomheden, der er relateret til de leverede programmer og ydelser. Politikken indeholder henvisninger til flere områder, hvor de enkelte kontroller er nærmere beskrevet.

Den overordnede styring af kontroller sker efter et årshjul, hvor alle aspekter af driften kontrolleres for overholdelse af procedurerne med jævne mellemrum. Kontrollerne er hensigtsmæssigt placeret ift. årshjul for revision.

Organisering af IT-sikkerhed

IT-sikkerhedsarbejdet er velorganiseret i KOMiT og dækker alle medarbejdere.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

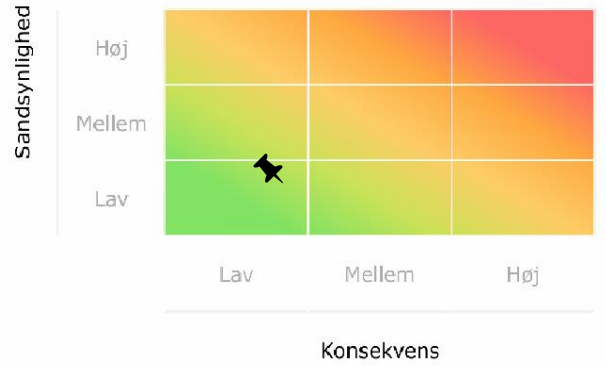
Der er klare funktioner og roller for forskellige medarbejdere i relation til IT- og informationssikkerhed og en klar funktionsadskillelse i udviklingsprocesserne.

Rollefordelingen er som følger:

Rolle	**Ansvarsområde**
Ledelsen	Sikrer overordnet ramme for denne politik og tildeler ressourcer til informationssikkerhed.
Informationssikkerhedsansvarlig	Udpeget af ledelsen som den ansvarlige for at implementere og vedligeholde informationssikkerhedspolitikken i organisationen samt løbende rapportere til ledelsen ifm. behov for vedligeholdelse af systemet.
Driftsansvarlig	Sikrer, at systemer lever op til det fastlagte sikkerhedsniveau, herunder at der udarbejdes de nødvendige retningslinjer, procedurer for brugen og kontrol af systemerne. Deltager desuden i at vedligeholde, gennemgå og udvikle politikken i samarbejde med den informationssikkerhedsansvarlige.
Driftstekniker	Har ansvaret for hardware.
Software-arkitekt	Har ansvaret for sikkerhedsarkitekturen i nyudviklede programmer.
Medarbejdere	Er ansvarlige for at følge politikken og rapportere eventuelle sikkerhedsbrud til den informationssikkerhedsansvarlige.
Eksterne parter	Er ansvarlige for at sikre, at politikken overholdes i deres service, og at de skal levere en sikkerhed for deres faciliteter, der lever op til standard certificeringerne ISAE 3000, ISAE 3402, ISO27001, ISO27002:2022. Det bemærkes, at KOMiT følger partielmetoden, og eksterne leverandører indgår derfor ikke i processer, men det valideres én gang årligt, om certificering fortsat eksisterer.

En vigtig del af IT-sikkerhedsarbejdet er risikovurdering, og KOMiT har vurderet sandsynlighed og konsekvens for en lang række mulige hændelser efter SIL-metoden:

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01



For alle potentielle hændelser er der etableret sikkerhedsforanstaltninger, som sikrer fortsat drift, hvis hændelserne skulle indtræffe.

Ansættelser/medarbejdere

KOMiT har processer, der dækker alle aspekter af en medarbejders ansættelse i virksomheden – fra ansættelsessamtaler, indhentning af børneattest og ren straffeattest til offboarding.

Et fast omdrejningspunkt er awareness-træning, som kører efter en fast kalender og adresseres i 1-til-1-samtalerne månedsvist.

KOMiT indgår fortrolighedsaftaler med alle ansatte og freelancere/konsulenter, som får adgang til fortrolige informationer eller personoplysninger.

Hardware

KOMiT har faste processer for, hvilke typer hardware der udleveres til medarbejdere/freelancere/konsulenter, og der sker en registrering både ved udlevering og aflevering.

Der er etablerede procedurer for, hvilke programmer de enkelte medarbejdere har adgang til at bruge, og det følger et princip om kun at give adgang til det nødvendige.

Driftsteknikeren er ansvarlig for at holde styr på hardware, og én gang årligt er der revision af beholdningen.

Adgangskontrol og brugerrettigheder

Adgang til netværk er begrænset af VPN og firewalls med et højt sikkerhedsniveeau.

Medarbejdernes adgange til systemer styres gennem brug af PIM-systemer, og der er faste processer for at tildele og fratage rettigheder til systemer/databaser, som følger et princip om kun at give adgang til det nødvendige. Adgange er tidsbegrænsede, og én gang årligt sker der en kontrol af aktive privilegerede brugerrettigheder.

Globale administratorroller er styret efter en fast politik, og der er etableret procedure for adgange, i fald flere globale administratorer skulle miste tilgang til systemerne.

Fysisk adgang og adgangskontrol

KOMiTs kontorer er sikret med adgangschips, og besøgende har kun adgang i følgeskab med ansatte.

Der er etableret døgnovervågning og vagtordning på kontoret, og vagten har kort responstid.

Hosting sker hos eksterne partnere, som har et højt sikkerhedsniveau og deres egne ISAE 3402/ISAE 3000/ISO 27001-revisioner/certificeringer.

KOMiTs personalehåndbog og infobog til nye ansatte beskriver i detaljer, hvordan medarbejdere skal agere ift. den fysiske sikkerhed.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

Operationelle procedurer

KOMiT har en høj grad af sikkerhed omkring systemerne generelt og klare processer for at få nye andelshavere onboardet på programmerne på en hensigtsmæssig måde ift. IT-sikkerhed og persondata. Der er også processer for offboarding af andelshavere, selvom dette er sjældent.

Udviklings- og driftsmiljøer er segmenterede, og der anvendes kun fantomdata ifm. test. Alle systemer har relevante sikkerhedscertifikater.

Det tekniske miljø har regler for passwords, som følger internationale standarder, og der er etableret beskyttelser mod virus/malware.

Data sikkerhedskopieres efter en fast procedure til backup, og systemer overvåges og sårbarhedsscannes løbende enten af KOMiT selv eller af leverandører.

Andelshavere er selv ansvarlige for drift af on-premise-databaser, hvor disse findes.

Overordnet beskrivelse af KOMiTs udviklingsproces

Vores interne udviklings- og godkendelsesprocesser sikrer, (1) at vi har en sikker proces med klare roller til alle deltagere, og (2) at alle programmer og moduler er udviklet i henhold til gældende lovgivning, herunder den europæiske persondataforordning.

KOMiT anvender ScanNet A/S/team.blue A/S, Microsoft Azure og NetIP A/S som underdatabehandler for hosting af udviklingsmiljøer samt support. Ifm. udviklingsopgaver anvender KOMiT fra tid til anden freelancere/konsulenter, som underlægges samme IT-sikkerhedsstyring som ansatte i selskabet. Alle udviklere har kun adgang til de nødvendige informationer og områder.

Alle vores medarbejdere er instrueret i overholdelse af god skik for IT-sikkerhed og relevant lovgivning, og der følges løbende op med awareness-træning på en digital platform.

Udvalgte medarbejdere har til opgave at følge lovgivningen inden for de områder, der berører et specifikt program, for ad den vej at sikre, at vores andelshavere til enhver tid anvender programmer, der er i overensstemmelse med gældende lovgivning.

Ved opstart af et projekt defineres en projektgruppe, hvor de enkelte medarbejdere får specifikke roller med klart definerede ansvarsområder. Vi har følgende roller:

- Projektleder
- Løsningstovholder
- Projekttovholder
- Udvikler
- Konsulent.

Udvikling opdeles i (1) ny udvikling og (2) driftsudvikling, som, trods forskellig karakter, håndteres efter de samme principper. I udviklingsprocessen anvendes DevOps, og ingen funktioner releases, uden at en konsulent (med ansvar for kundevinklen i udviklingen) har godkendt.

Samtidig sikres kvaliteten af udviklingsprocessen gennem pull request på alle funktioner, så der altid er en anden udvikler på godkendelsen før release. Formålet hermed er at give andelshaverne stærke programmer til deres drift.

Beskrivelse af sikring af IT-sikkerhed og persondata i udviklingsprocesserne

Udviklingsprocesserne for KOMiT-programmer er i store træk ens, uanset hvilket program der er tale om. Fælles for udviklingsprocesserne er, at (1) de alle følger et klart flow, der er en tillempet udgave af agil udvikling, og at (2) der ikke på noget tidspunkt anvendes aktive persondata i forbindelse med udvikling og test.

Udviklingen foregår efter privacy-by-default- og privacy-by-design-principperne, hvilket vil sige, at persondatasikkerhed ikke kan til- og fravælges, men er indbygget i designet, herunder også at der tages højde for de registreredes rettigheder: retten til berigtigelse, retten til begrænsning i behandling, retten til indsigt,

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

retten til at blive glemt (slettet). Her sikres det, at de IT-programmer, som KOMiT udvikler, understøtter disse krav.

Grundprincipperne for udvikling er, at privatlivsbeskyttelsen er proaktiv og er en standardindstilling, at persondatasikkerhed er indbygget i designet, at der er fuld funktionalitet, brugervenlighed og sikkerhed, at sikkerhed generelt indtænkes i hele systemets livscyklus, og at der er fuld synlighed og transparens, hvor der foregår integration eller er grænseflader mellem services. Der forefindes ikke persondata i løbet af udviklingsprocessen.

Udviklingen testes med anonymiserede data/"fiktive data". Heller ikke i testfasen af udviklingsprocessen er der persondata. På flere af programmer hjælpes kunden med opgradering til nye versioner i andelshavernes produktive miljø. Ved denne type assistance arbejdes der på andelshavernes instruks og med brugere mv. opsat og styret af andelshavere. Adgangene lukkes igen af andelshaveren, når der ikke er behov for yderligere adgang.

Beskrivelse af håndtering af IT-sikkerhed og persondata i supportprocesserne

Der ydes support på alle programmer, der er udviklet af KOMiT. Der forefindes som udgangspunkt ikke persondata i supportprocessen, og KOMiT vil i forbindelse med support kun tilgå persondata på begæring af andelshaver.

Alle henvendelser fra andelshavere registreres i vores servicedesk-system. Alle supportopgaver registreres med, om der er anvendt fjernsupport af hensyn til sporbarhed i forbindelse med support i andelshaveres data.

Alle andelshavere har adgang til vores servicedesk-system, hvor de kan oprette supportbegæringer og følge med i udviklingen af oprettede supportopgaver.

Fører en supportsag til nødvendig udvikling, følger dette de fastlagte processer for udvikling.

Henvendelser fra de dataansvarlige ift. support på datahåndtering af persondata

KOMiT har en procedure for håndtering og dokumentation af henvendelser fra dataansvarlige i relation til bistand for håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse mv.).

Dokumentation af henvendelser fra dataansvarlige vedrørende fx indsigtsret, sletning, berigtigelse mv. håndteres i vores supportsystem.

Leverandørservice og sikkerhed i leverancen

KOMiT har et godt og tillidsfuldt samarbejde med leverandører af hosting, diverse systemer, freelancere og konsulenter.

Hvor relevant adgang gives til informationer, som er dækket af IT-sikkerhed eller persondatasikkerhed, stilles krav om relevante revisioner/certificeringer, og der indgås databehandler- og fortrolighedsaftaler.

Revisioner og certifikater relateret til ISAE 3402/ISAE 3000/ISO 27001 indhentes årligt efter et årshjul, der er afstemt efter leverandørernes normale tidspunkt for revision/auditering.

Management af brud på IT-sikkerhed og forbedringer

Skulle der sker brud på IT-sikkerheden eller persondatasikkerheden, har KOMiT et beredskab klar til at skabe sikkerhed igen. Dette har højeste prioritet i alle afdelinger.

Ved brud adviseres de relevante myndigheder, personer og organisationer, og der føres log over hændelser. Hændelser vurderes i ledergruppen for læring og forbedring af processer efterfølgende.

Informationssikkerhedskontinuitet (beredskaber)

Alle kan blive ramt af et angreb, og derfor er det magtpåliggende for KOMiT at have beredskabsplaner til forskellige hændelser, som gør det muligt at reetablere driften hurtigst muligt.

Der er etableret redundant hosting/databaser på flere lokationer, og der gennemføres med jævne mellemrum restore-øvelser.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

Ift. brand eller lignende på kontoret er der også en beredskabsplan, som medarbejderne gøres opmærksom på ved tiltrædelse.

Generelt prioriteres sikkerhed højt for både programmerne, databaser og medarbejdere, da alle dele er nødvendige for fortsat drift, i det tilfælde at uheldet er ude.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolmål og kontrolaktiviteter er beskrevet.

Komplementerende kontroller hos andelshavere

Andelshaverne har følgende forpligtelser:

- At sikre sig, at nye versioner af systemerne introduceres i organisationen
- At sikre sig, at brugere med adgang til systemerne matcher kundens behov.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

4. Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1. Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", og de yderligere krav, der er gældende i Danmark.

Vores test af kontrollernes design, implementering og operationelle effektivitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos andelshavere er ikke omfattet af vores testhandlinger.

Vores test af den operationelle effektivitet har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået.

4.2. Testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumen-tation for at vurdere, om specifikke kontroller er designet, så de kan forventes at være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

4.3. Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

A.5 Kontrolmål: Informationssikkerhedspolitikker

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
5.1.1 Politikker for informationssikkerhed *Ledelsen skal fastlægge og godkende en række politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.* KOMiT har en sikkerhedspolitik, der er godkendt af bestyrelsen. Den er tilgængelig på intranettet og udleveres til alle nye medarbejdere. Sikkerhedspolitikken vedligeholdes af compliance- og sikkerhedsafdelingen, som rapporterer direkte til bestyrelsen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en ledelsesgodkendt og ajourført sikkerhedspolitik. Vi har inspiceret, at informationssikkerhedspolitikkerne kommunikeres til medarbejderne og relevante parter.	Ingen afvigelser noteret.
5.1.2 Gennemgang af politikker for informationssikkerhed *Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og funktionalitet.* Sikkerhedspolitikkerne gennemgås en gang om året, eller når nye politikker implementeres eller opdateres.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i forbindelse med væsentlige ændringer. Vi har inspiceret, at sikkerhedspolitikken gennemgås mindst én gang årligt.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.6 Kontrolmål: Organisering af informationssikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
6.1.1 Roller og ansvarsområder for informationssikkerhed *Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.* Ansvaret for informationssikkerheden ligger hos direktionen og bestyrelsen. Den daglige udførelse varetages af lederne i afdelingerne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer.	Ingen afvigelser noteret.
6.1.2 Funktionsadskillelse *Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af virksomhedens aktiver.* KOMiT har fastsat en politik for funktionsadskillelse. Politikken gennemgås en gang om året for at sikre, at det nuværende niveau af adskillelse stadig afspejler informationssikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos KOMiT, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.	Ingen afvigelser noteret.
6.1.3 Kontakt med myndigheder *Der skal opretholdes passende kontakt med relevante myndigheder.* KOMiT har etableret oversigt over relevante myndigheder og procedurer for kontakt til disse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret oversigt over relevante myndigheder og procedurer for kontakt til disse.	Ingen afvigelser noteret.
6.1.5 Informationssikkerhed ved projektstyring *Informationssikkerhed skal anvendes ved projektstyring, uanset projekttype.* KOMiT har etableret politik og procedurer for involvering af compliance og sikkerhed i større projekter.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret politik og procedurer for involvering af compliance og sikkerhed i større projekter.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.7 Kontrolmål: Personalesikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
7.1.1 Screening *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.* Forud for ansættelsen bekræfter KOMiT kandidatens identitet, og kandidatens referencer kontrolleres, hvis det er relevant. Straffeattesten undersøges forud for ansættelsen og herefter en gang årligt for at sikre, at den er ren.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der fremlægges straffeattester, inden ansættelsen starter for både medarbejdere og eksterne konsulenter. Vi har ved inspektion af en stikprøve på nyansættelser påset, at der er indhentet straffeattester inden ansættelsesstart.	Ingen afvigelser noteret.
7.1.1 Ansættelsesvilkår og-betingelser *Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed.* Ved alle ansættelser udleveres relevante politikker mv. til den nyansatte, og den ansatte skal bekræfte, at det udleverede materiale er udleveret.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der udleveres politikker mv. Vi har ved inspektion af en stikprøve på nyansættelser påset, at der er sket udlevering af politikker mv. ved ansættelsesstart.	Ingen afvigelser noteret.
7.2.1 Ledelsesansvar *Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med virksomhedens fastlagte politikker og procedurer.* KOMiT har en politik for uddannelse af medarbejderne i informationssikkerhed. Alle nye medarbejdere gennemgår træning, der uddanner dem i informationssikkerhed.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der sker træning af medarbejdere. Vi har ved inspektion af en stikprøve på nyansættelser påset, at der er gennemført træning.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.7 Kontrolmål: Personalesikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed *Alle virksomhedens medarbejdere og, hvor det er relevant, kontrahenter skal ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med virksomhedens politikker og procedurer, i det omfang det er relevant for deres jobfunktion.* Alle nye medarbejdere hos KOMiT modtager en velkomstmail, der blandt andet indeholder en introduktionsvideo om sikkerhedspolitikken. Alle medarbejdere gennemfører en række årlige undervisningsforløb i relation til informationssikkerhed.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås. Vi har inspiceret, at medarbejderne jævnligt skal gennemføre obligatoriske undervisningsforløb for at sikre, at virksomhedens sikkerhedskrav overholdes.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.8 Kontrolmål: Styring af aktiver

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
8.1.1 Fortegnelse over aktiver *Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.* KOMiT vedligeholder en fortegnelse med alle aktiver, og databasen indeholder aktivernes livscyklus. KOMiT vedligeholder desuden en liste over alle systemer, hvoraf det fremgår, hvem der er ejer af systemet, og hvem der er ansvarlig for tekniske forhold.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er etableret tilstrækkelige kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver.	Ingen afvigelser noteret.
8.1.3 Acceptabel brug af information og understøttende aktiver *Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og implementeres.* KOMiT har fastsat retningslinjer for sikker anvendelse af information og aktiver.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har implementeret retningslinjer for sikker anvendelse af information og aktiver.	Ingen afvigelser noteret.
8.2.1 Klassifikation *Information skal klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.* KOMiT har fastsat retningslinjer for klassifikation af information.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har implementeret retningslinjer for klassifikation af informationer.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.9 Kontrolmål: Adgangsstyring

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
9.1.1 Politik for adgangsstyring *En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.* KOMiT har fastsat generelle retningslinjer for adgang til andelshavernes systemer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at retningslinjer for adgangskontrol er blevet fastlagt, gennemgået og godkendt.	Ingen afvigelser noteret.
9.1.2 Adgang til netværk og netværkstjenester *Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.* Alle adgange til driftssystemer, netværk, databaser og datafiler, der stilles til rådighed for nye og eksisterende brugere, revideres for at sikre overholdelse af virksomhedens politikker. Der træffes også foranstaltninger for at sikre, at adgangstilladelser afhænger af kravene til jobfunktionen, og at de godkendes og sættes korrekt op i systemerne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at adgang til netværk- og netværkstjenester tildeles på baggrund af medarbejdernes arbejdsbetingede behov og ledergodkendelser.	Ingen afvigelser noteret.
9.2.1 Brugerregistrering og -afmelding *Der skal implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.* KOMiT har en proces for registrering af brugere. Processen sikrer, at hver bruger har de adgange, der kræves i deres jobfunktion, og ikke flere. Når en medarbejder forlader virksomheden eller skifter jobfunktion, enten inddrages eller ændres hans/hendes adgange, så de afspejler den nye funktion.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er tilrettelagt procedurer for brugeradministration. Vi har ved stikprøvevis inspektion desuden påset, at proceduren for registrering og afmelding af brugere er blevet implementeret.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.9 Kontrolmål: Adgangsstyring

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
9.2.3 Styring af privilegerede adgangsrettigheder *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* KOMiT har en politik for tildeling og begrænsning af brugere med privilegeret adgang. Alle brugere med privilegeret adgang har en dedikeret bruger med den privilegerede adgang. Listen over privilegerede brugeres adgang revideres en gang i kvartalet.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har tilrettelagt formaliserede procedurer for brugeradministration og rettighedsstyring, og at disse også gælder for brugere med privilegerede rettigheder. Vi har inspiceret, at der for autorisationer, der tildeles medarbejdere, foreligger en begrundelse for det ønskede adgangsniveau og en godkendelse fra nærmeste chef.	Ingen afvigelser noteret.
9.2.5 Gennemgang af brugeradgangsrettigheder *Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder*. KOMiT gennemgår regelmæssigt medarbejdernes privilegerede tekniske rettigheder i både interne og kundevendte systemer. Dermed sikres overensstemmelse med medarbejderens arbejdsbetingede behov.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at brugeradgange revurderes én gang hvert halve år.	Ingen afvigelser noteret.
9.2.6 Inddragelse eller tilpasning af 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.* Når en medarbejder forlader virksomheden, inddrages alle adgange. Hvis medarbejderen skifter jobfunktion, ændres adgangen, så den afspejler den nye funktion. Begge ændringer iværksættes af HR-afdelingen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, at der foretages regelmæssig opfølgning på brugernes rettigheder i driftsmiljøerne, og at disse rettigheder er tildelt ud fra et arbejdsbetinget behov. Vi har ved inspektion undersøgt, at fratrådte brugere fjernes rettidigt i driftsmiljøet efter fratrædelsen.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.9 Kontrolmål: Adgangsstyring

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
9.4.2 Procedurer for sikker logon *Hvis det kræves i henhold til politikken for adgangsstyring, skal adgang til systemer og applikationer styres af en procedure for sikker logon.* KOMiT har en sikker logonprocedure for adgang til kundedata og -systemer. Ingen kan få adgang til kundedata eller -systemer uden brug af tofaktorgodkendelse.	Vi har inspiceret, at der vedligeholdes en formel politik for adgangsstyring, der fastlægger tilladte tekniske autentifikationsløsninger. Vi har inspiceret, at politikken for adgangsstyring er blevet gennemgået og godkendt. Vi har inspiceret, at de omfattede applikationer og systemer håndhæver sikre logonprocedurer.	Ingen afvigelser noteret.
9.4.4 Brug af privilegerede systemprogrammer *Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.* KOMiT har etableret kontroller til sikring af, at anvendelsen af privilegerede systemprogrammer er begrænset til få personer.	Vi har inspiceret, at anvendelsen af privilegerede systemprogrammer er begrænset til få personer.	Ingen afvigelser noteret.
9.4.5 Styring af adgang til kildekoder til programmer *Adgang til kildekoder til programmer skal begrænses.* KOMiT har etableret procedurer og kontroller til sikring af, at adgang til kildekode kun er for personer for arbejdsbetinget behov. KOMiT har etableret systemunderstøttelse til styring af kildekode.	Vi har inspiceret, at adgang til kildekode er begrænset til personer med arbejdsbetinget behov herfor.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.11 Kontrolmål: Fysisk sikring og miljøsikring

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
11.1.1 Fysisk perimetersikring *Der skal defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.* KOMiT har klassificeret sine informationsbehandlingsfaciliteter, og adgangen til disse sker på baggrund af denne klassifikation. Gæster er kun tilladt i åbne eller begrænsede områder, hvis de ledsages af en medarbejder hos KOMiT. Adgang til lukkede områder er tilladt for gæster, hvis de har et arbejdsbetinget behov.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes.	Ingen afvigelser noteret.
11.1.2 Fysisk adgangskontrol *Sikre områder skal være beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.* KOMiT har sikret, at adgangen til virksomhedens lukkede områder er sikret, at adgangen til disse områder er begrænset til personer med et arbejdsbetinget behov, og at denne adgang hyppigt revideres.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at KOMiT har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
11.1.3 Sikring af kontorer, lokaler og faciliteter *Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og etableres.* KOMiT har fastlagt begrænset adgang til kontorer. Alle døre er låst og skal åbnes af en medarbejder hos KOMiT. Alle medarbejdere skal bære et synligt ID-kort med navn og billede. Alle gæster skal bære et ID-kort, der identificerer dem som gæster.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at KOMiT har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.11 Kontrolmål: Fysisk sikring og miljøsikring

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
11.2.9 Politik for ryddeligt skrivebord og blank skærm *Der skal udarbejdes en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.* KOMiT har som del af sikkerhedspolitikken krav til at holde skriveborde ryddet samt aktivering af blank skærm, når man er væk fra sin arbejdsstation.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er etableret en politik herfor, samt at der er aktiveret automatisk skærmlås ved inaktivitet.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.12 Kontrolmål: Driftssikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
12.1.1 Dokumenterede driftsprocedurer *Driftsprocedurer skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem.* KOMiT har etableret driftsprocedurer for de relevante områder ud fra ydelser til andelshaverne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er etableret formaliserede driftsprocedurer.	Ingen afvigelser noteret.
12.1.2 Ændringsstyring *Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres.* KOMiT har implementeret ændringsstyring på kritisk infrastruktur og for andelshavere, der har ændringsstyring som et forretningskrav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har udarbejdet procedurer for årlig gennemgang og opdatering af: • Hændelsesstyring • Problemstyring • Ændringsstyring • Styring af versioner og programrettelser • Brugeradministration.	Ingen afvigelser noteret.
12.1.4 Adskillelse af udviklings-, test- og produktionsmiljøer *Udviklings-, test- og driftsmiljøer skal adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.* KOMiT har etableret særskilte udviklings-, test- og driftsmiljøer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret særskilte udviklings-, test- og driftsmiljøer	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.12 Kontrolmål: Driftssikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
12.2.1 Kontroller mod malware *Der skal implementeres kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.* KOMiT har fastlagt en procedure, der skal sikre, at antivirussoftware fungerer på alle relevante systemer. Antivirussoftwaren overvåges.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at medarbejdernes pc'er hos KOMiT er beskyttet med antivirussoftware – og at denne er opdateret.	Ingen afvigelser noteret.
12.3.1 Backup af information *Der skal tages backupkopier af information, software og systembilleder, og disse skal testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.* KOMiT foretager backup i overensstemmelse med KOMiTs bedste praksis eller andelshavernes krav. Backupjobbene overvåges for at sikre kontinuerlig drift. Der udføres periodiske gendannelsestest, der igangsættes af KOMiT.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er fastsat krav til backup i kontrakten med underleverandører, der leverer serviceydelser, hvor backup er relevant. Vi har inspiceret, at der er foretaget en fuld gendannelsestest af it-miljøerne.	Ingen afvigelser noteret.
12.4.1 Hændelseslogning *Hændelseslogning til registrering af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser skal udføres, opbevares og gennemgås regelmæssigt.* KOMiT har implementeret et overvågningssystem, der sikrer, at andelshavernes systemer er oppe at køre. KOMiT har etableret procedurer for overvågning af driften.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at hændelseslogning af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser er konfigureret. Vi har inspiceret, at en oversigt over logdokumentation angiver, hvornår loggene skal gennemgås.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.12 Kontrolmål: Driftssikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
12.4.2 Beskyttelse af logoplysninger *Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang.* KOMiT genererer logs for forskellige systemer på forskellige sikkerhedsniveauer. KOMiT har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov. Vi har inspiceret, at logoplysningerne ikke kan redigeres eller slettes. Desuden tager KOMiT backup af logoplysningerne flere gange dagligt, og adgangen er begrænset til få personer.	Ingen afvigelser noteret.
12.6.1 Styring af tekniske sårbarheder *Der skal løbende indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.* KOMiT har etableret procedurer til løbende sårbarhedsscanning af infrastruktur og systemer. Det er etableret procedurer til opfølgning på identificerede sårbarheder.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret sårbarhedsscanninger, samt at der foretages opfølgning herpå.	Ingen afvigelser noteret.
12.6.2 Begrænsninger på softwareinstallation *Der skal fastlægges og implementeres regler om softwareinstallation, som foretages af brugerne.* KOMiT har etableret procedurer i forhold til installation af software, som brugerne selv foretager. Der er en godkendelsesproces i forhold til nyt software.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret procedurer for håndtering af installation af software hos brugerne.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.13 Kontrolmål: Kommunikationssikkerhed

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
13.1.1 Styring af netværkssikkerhed *Netværk skal styres og kontrolleres for at beskytte informationer i systemer og applikationer.* KOMiT har implementeret flere politikker for at sikre, at kommunikationen er sikker, og at manipulation af data minimeres. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsbetinget behov. Kommunikationen mellem KOMiT og kundesites foregår ved hjælp af anerkendte og gennemprøvede sikre teknologier.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, om der jf. retningslinjerne er etableret en passende sikkerhedsarkitektur på netværket, herunder: • om netværket er opdelt i sikre zoner, og om kundemiljøerne er adskilt fra KOMiTs eget miljø • om fjernadgang er tildelt ved brug af tofaktorgodkendelse • om ændringer i netværksmiljøet i vores stikprøve er sket på kontrolleret vis i overensstemmelse med reglerne for ændringsstyring.	Ingen afvigelser noteret.
13.2.4 Fortroligheds- og hemmeligholdelsesaftaler *Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, gennemgås regelmæssigt og dokumenteres.* KOMiT har etableret procedurer for indhentning af fortrolighedsaftaler mv. fra medarbejdere og samarbejdspartnere.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret procedurer for indhentning af fortrolighedsaftaler fra medarbejdere og samarbejdspartnere. Vi har ved inspektion af en stikprøve på nyansættelser påset, at der er indhentet fortrolighedsaftale.	Ingen afvigelse noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.14 Kontrolmål: Anskaffelse, udvikling og vedligeholdelse af systemer

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
14.2.1 Sikker udviklingspolitik *Der skal fastlægges og anvendes regler for udvikling af software og systemer i organisationen.* KOMiT foretager en risikovurdering af alle nye systemer, der anskaffes. Dette sker for at sikre, at systemet lever op til KOMiTs politikker vedrørende informationssikkerhed. KOMiT har etableret en politik for sikker udvikling.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret en sikkerhedsorganisation, der sikrer et passende og tilstrækkeligt informationssikkerhedsniveau i systemerne. Vi har inspiceret, at KOMiT har etableret en politik for sikker udvikling.	Ingen afvigelser noteret.
14.2.2 Procedurer for styring af systemændringer *Ændringer af systemer inden for udviklingslivscyklussen skal styres ved hjælp af formelle procedurer for ændringsstyring.* KOMiT har etableret en politik for styring af ændringer, herunder f.eks. ændringer til driftsplatformen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret en politik for styring af ændringer, herunder f.eks. ændringer til driftsplatformen.	Ingen afvigelser noteret.
14.2.3 Teknisk gennemgang af applikationer efter ændringer af driftsplatforme *Ved ændring af driftsplatforme skal forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.* KOMiT har etableret en politik for styring af ændringer, herunder f. eks. ændringer til driftsplatformen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret en politik for styring af ændringer, herunder f.eks. ændringer til driftsplatformen.	Ingen afvigelser noteret.
14.2.4 Begrænsning af ændringer af softwarepakker	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.14 Kontrolmål: Anskaffelse, udvikling og vedligeholdelse af systemer

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
Ændringer af softwarepakker skal vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer skal styres effektivt. KOMiT foretager en risikovurdering af alle nye systemer, der anskaffes. Dette sker for at sikre, at systemet lever op til KOMiTs politikker vedrørende informationssikkerhed. KOMiT har etableret en politik for sikker udvikling.	Vi har inspiceret, at KOMiT har etableret en sikkerhedsorganisation, der sikrer et passende og tilstrækkeligt informationssikkerhedsniveau i systemerne. Vi har inspiceret, at KOMiT har etableret en politik for sikker udvikling.	
14.2.5 Principper for udvikling af sikre systemer *Principper for udvikling af sikre systemer skal fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med alle implementeringer af informationssystemer.* KOMiT har etableret en politik for sikker udvikling. Politikken indeholder relevante emner i forhold til udviklingsprocessen, herunder code review.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret en sikkerhedsorganisation, der sikrer et passende og tilstrækkeligt informationssikkerhedsniveau i systemerne. Vi har inspiceret, at KOMiT har etableret en politik for sikker udvikling. Vi har ved en stikprøve inspiceret, at principperne for sikker udvikling følges.	Ingen afvigelser noteret.
14.2.6 Sikkert udviklingsmiljø *Organisationer skal etablere sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus* KOMiT har etableret særskilte udviklings-, test- og driftsmiljøer. Alle miljøerne er sat op ens sikkerhedsmæssigt.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret konfiguration af de opsatte miljøer.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.14 Kontrolmål: Anskaffelse, udvikling og vedligeholdelse af systemer

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
14.2.8 Systemgodkendelsestest *Test af sikkerhedsfunktionalitet skal udføres ved udvikling.* KOMiT har som led i sikker udvikling etableret en række godkendelser, sikkerhedstest og brugertest. Disse er alle systemunderstøttet i forskellige værktøjer. Dette omfatter hele processen fra udviklingsønske til release af nye versioner til systemerne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret kontroller i udviklingsprocessen omfattende godkendelser, sikkerhedstest og brugertest samt testet, at disse alle er systemunderstøttet. Vi har ved en stikprøve inspiceret, at kontroller er udført jf. den beskrevne proces og politikkerne på området.	Ingen afvigelser noteret.
14.2.9 Sikkerhedstest under udvikling og godkendelse *Der skal etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.* KOMiT har som led i sikker udvikling etableret en række godkendelser, sikkerhedstest og brugertest. Disse er alle systemunderstøttet i forskellige værktøjer. Dette omfatter hele processen fra udviklingsønske til release af nye versioner til systemerne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at KOMiT har etableret kontroller i udviklingsprocessen omfattende godkendelser, sikkerhedstest og brugertest, samt testet, at disse alle er systemunderstøttet. Vi har ved en stikprøve inspiceret, at kontroller er udført jf. den beskrevne proces og politikkerne på området.	Ingen afvigelser noteret.
14.3.1 Sikring af testdata *Testdata skal udvælges omhyggeligt og skal beskyttes og styres.* *O*plysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af oplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på en enkelt udviklings- og testdatabase, at oplysningerne heri er pseudonymiseret eller anonymiseret.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.15 Kontrolmål: Leverandørforhold

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
15.2.1 Overvågning og gennemgang af leverandørydelser *Virksomheder skal regelmæssigt overvåge, gennemgå og revidere leverandørydelser.* KOMiT foretager en årlig risikovurdering af alle leverandører. Derudover foretages en mere omfattende risikovurdering af de mest kritiske leverandører som hardware-, datacenter- og softwareleverandører til datacenteret.	Vi har inspiceret, at der findes en formel, dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved inspektion af en stikprøve på underskrevne kontrakter påset, at informationssikkerhedskravene er kontraktligt aftalt. Vi har ved inspektion af en stikprøve på måneder påset, at KOMiT jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav. Vi har inspiceret, at tredjepartserklæringer for hovedleverandører er modtaget og behandlet af KOMiT.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.16 Kontrolmål: Styring af informationssikkerhedshændelser

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
16.1.1 Ansvar og procedurer *Ledelsesansvar og procedurer skal fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedshændelser.* KOMiT har en procedure, der beskriver håndtering og rapportering under et brud på informationssikkerheden. Alle medarbejdere i KOMiT er blevet informeret om, hvad de skal gøre i tilfælde af en hændelse eller opdagelse af et sikkerhedsproblem for at sikre en hurtig reaktion, og at der indsamles erfaringer.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at den formelle og dokumenterede proces for hændelsesstyring er blevet gennemgået og godkendt. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring.	Ingen afvigelser noteret.
16.1.2 Rapportering og håndtering af informationssikkerhedshændelser og sikkerhedsbrud *Informationssikkerhedshændelser skal rapporteres ad passende ledelseskanaler så hurtigt som muligt.* Medarbejdere og kontrahenter, som bruger virksomhedens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester. Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring og rapporteret via informationssikkerhedsudvalget.	Ingen afvigelser noteret.
16.1.3 Rapportering af informationssikkerhedssvagheder *Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller*	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.16 Kontrolmål: Styring af informationssikkerhedshændelser

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
mistanke om svagheder i informationssystemer og -tjenester. Medarbejdere og kontrahenter, som bruger virksomhedens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester. Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring og rapporteret via informationssikkerhedsudvalget.	
16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser *Informationssikkerhedshændelser skal vurderes, og det skal besluttes, om de skal klassificeres som informationssikkerhedsbrud.* KOMiT har en procedure, der beskriver håndtering og rapportering under et brud på informationssikkerheden. Alle medarbejdere i KOMiT er blevet informeret om, hvad de skal gøre i tilfælde af en hændelse eller opdagelse af et sikkerhedsproblem for at sikre en hurtig reaktion, og at der indsamles erfaringer.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at den formelle og dokumenterede proces for hændelsesstyring er blevet gennemgået og godkendt. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

A.17 Kontrolmål: Informationssikkerhedsaspekter ved beredskabsstyring

KOMiTs kontrolaktivitet	PwC's udførte test	Resultater af tests
17.1.1 Planlægning af informationssikkerhedskontinuitet *Virksomheden skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.* KOMiT har en beredskabsplan for, hvordan virksomheden kan komme tilbage i drift hurtigst muligt i tilfælde af en katastrofe. Beredskabsplanen testes en gang om året.	Vi har inspiceret, at en formel og dokumenteret beredskabsplan vedligeholdes, gennemgås og godkendes en gang om året. Vi har inspiceret, at der er foretaget en konsekvensanalyse for at fastlægge kravene til en beredskabsplan. Vi har inspiceret, at de bagvedliggende procedurer for beredskabsplanen er blevet gennemgået og godkendt af relevant personale.	Ingen afvigelser noteret.

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

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."

Anders Jørgen Banke
Kunde
Serienummer: 3a74628c-7b2c-4fde-ad0d-41ed8ea67b7b
IP: 82.192.xxx.xxx
2025-04-01 11:50:42 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-04-01 11:52:19 UTC

Penneo dokumentnøgle: 3XQ57-RRWMS-MZU7O-9IFYM-PMJUP-MKN01

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

Dette dokument er forseglet med et kvalificeret elektronisk segl med brug af certifikat og tidsstempel fra en kvalificeret tillidstjenesteudbyder.

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