REVISIONSHUSET TAL & TANKER

NHC A/S

Kejlstrupvej 85, 8600 Silkeborg
CVR: 30534352

ISAE 3402 erklæring om generelle IT-kontroller med relevans for regnskabsaflæggelsen for Hosting ydelser hos NHC

1. januar - 31. december 2022

Indholdsfortegnelse

Udtalelse fra ledelsen hos serviceleverandøren, vedrørende generelle IT-kontroller for Hosting ydelser hos NHC	1 - 2
Beskrivelse af generelle IT-kontroller med relevans for regnskabsaflæggelse i tilknytning til drift, overvågning, vedligeholdelse, support m.v. af Hosting ydelser hos NHC	3-10
Uafhængig revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet	11-13
Revisors beskrivelse af test af kontroller	14-25

Serviceleverandørens ledelses udtalelse, vedrørende generelle IT-kontroller for Hosting ydelser hos NHC

Beskrivelsen på side 3-11 er udarbejdet til brug for NHC's kunder og disses revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller som kunderne selv har anvendt, ved vurdering af risiciene.

NHC bekræfter, at:

a) Den medfølgende beskrivelse, side 3-11 giver en retvisende beskrivelse af de generelle IT-kontroller med relevans for de generelle IT-kontroller for Hosting ydelser, der anvendes af NHC's kunder i hele perioden fra 1. januar - 31. december 2022.

b) Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

i. redegør for, hvordan kontrollerne 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 styring af de generelle IT-kontroller
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementeret hos kunderne, 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 de generelle IT-kontroller

ii. indeholder relevante oplysninger om ændringer i de generelle IT-kontroller foretaget i perioden fra 1. januar - 31. december 2022

iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold

iv. medtager kontrolmål og tilknyttede kontroller hos vores underleverandører og vores kontrolaktiviteter med disse underleverandører

c) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var

hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar - 31. december 2022.

d) Kriterierne for denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

ii. de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke 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 beføjelse i hele perioden fra 1. januar til 31. december 2022.

Med baggrund i ovenstående vurderer NHC, at vi i alle væsentlige forhold i overensstemmelse med forretningsvilkår for hosting-ydelser, generelle salgsbetingelser samt serviceaftale (SLA) og IT Sikkerhedspolitikken med tilhørende informations- sikkerhedshåndbog, har etableret effektive kontroller for Hosting ydelser placeret hos DLX.

Silkeborg, den 30. Januar 2023.

NHC A/S

Casper Søltoft
Administrerende Direktør
NHC A/S

Ole Rebbe
Teknisk Direktør
NHC A/S

Beskrivelse af generelle IT-kontroller med relevans for regnskabsaflæggelsen i tilknytning til drift, overvågning, vedligeholdelse, support m.v. af Hosting ydelser hos NHC

NHC A/S (herefter NHC) stiller gennem drift, overvågning, support og vedligeholdelse Hosting ydelser til rådighed for NHC's kunder. Denne beskrivelse med tilhørende erklæring vedrører de generelle IT-kontroller med relevans for regnskabsaflæggelsen i tilknytning til drift, overvågning, vedligeholdelse, support m.v. af Hosting ydelser.

Denne beskrivelse er udarbejdet med henblik på at levere information til brug for NHC's kunder og disses revisorer og for at opfylde kravene i "International Standard on Assurance Engagements 3402", "Erklæringer med sikkerhed om kontroller hos en serviceleverandør".

NHC tilbyder sine kunder følgende Hosting ydelse:

- Serverdrift
- Overvågning
- Sikkerhedskopiering
- Netværk
- Support
- Sikkerhed & Kommunikation

NHC's arbejde i relation til de generelle IT-kontroller, er tilrettelagt med udgangspunkt i risikovurdering og informationssikkerhedspolitik med tilhørende IT sikkerhedshåndbog samt aftale mellem NHC og den enkelte kunde, som beskrevet i forretningsvilkår for hosting-ydelser, generelle salgsbetingelser samt serviceaftale (SLA).

Beskrivelsen og erklæringen dækker perioden 1. januar - 31. december 2022.

NHC er ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med det sigte at overholde de i serviceaftalen stillede krav.

Denne erklæring er udarbejdet efter helhedsmetoden og omfatter således både kontrolmål og tilknyttede kontroller hos NHC og hos vores underleverandører. NHC har regelmæssige møder med centrale underleverandører og indhenter en årlig revisionserklæring om udvalgte kontroller.

Risikostyring

NHC arbejder proaktivt og løser langt hellere udfordringerne før de bliver til problemer. Derfor gennemføres skemalagte analyser af risikobilledet for it-systemer og hosting-ydelser. Dette sikrer, at der kan igangsætte procedurer og tiltag for at minimere risikoen for fejl.

Risikostyringen omfatter følgende:

- Identifikation af potentielle risici, der kan få indflydelse på IT-miljøerne både ud fra en

teknisk og forretningsmæssig synsvinkel.

- Vurdering af de identificerede potentielle risici, væsentlighed, sandsynlighed og konsekvenser på IT-miljøerne.
- At tiltag til reduktion af sandsynligheden for, at risici indtræder, implementeres på en kost-effektiv måde.

Risikovurderingen foretages en gang om året, samt ved større organisatoriske og/eller tekniske ændringer. Dette skal være med til at sikre, at NHC lever op til høj standard, risikovurdering af samarbejdspartnere og review af SLA, med særlig fokus på at sikre, at IT-miljøerne understøtter en høj tilgængelighed, fortrolighed og integritet af Hosting ydelser.

Baseret på risikovurderingen har NHC udarbejdet og implementeret en IT- sikkerhedspolitik med tilhørende IT sikkerhedshåndbog, som løbende vedligeholdes og revurderes. Risikovurderingen og IT-sikkerhedspolitikken er godkendt af NHC's bestyrelse.

IT sikkerhedsarbejdet

NHC har etableret en IT-sikkerhedspolitik for:

- At tilbyde et stabilt og sikkert driftsmiljø med høj tilgængelighed
- At tilbyde et højt serviceniveau
- At sikre, at medarbejdere kun har adgang til at tilgå, ændre og anvende systemer, data eller infrastruktur der relaterer sig til personens arbejdsområde, og som er godkendt af respektive ledelse.
- At uvedkommende personer ikke kan få adgang til enheder (Mobil, pc, iPad, etc.), hvor der er adgang til følsomt data.
- At IT-platformen og data i tilfælde af brand, strømsvigt og andre force majeure- lignende tilstande kan gendannes hurtigst muligt og i størst muligt omfang.
- At sikre driftsmiljøet imod tekniske og menneskeskabte trusler. Alle personer (interne så vel som eksterne) betragtes af NHC som en mulig trussel imod sikkerheden.

NHC har valgt at organisere IT-sikkerheden efter DS/ISO/IEC 27002:2015 (herefter ISO27002) og med udgangspunkt i denne standard valgt at implementere relevante kontroller indenfor følgende områder:

5. Informationssikkerhedspolitik
6. Organisering af informationssikkerhed
7. Medarbejdersikkerhed
9. Adgangsstyring
11. Fysisk sikring og miljøsikring
12. Driftssikkerhed
15. Leverandørforhold
16. Styring af Informationssikkerhedsbrudhændelser
17 Informationssikkerhedsaspekter ved nødberedskabs- og reetableringsstyring

Områderne er udvalgt med udgangspunkt i de opgaver, NHC har ansvaret for og varetager på vegne af NHC's kunder, og som er beskrevet i serviceaftalen med tilhørende bilag, samt i IT-sikkerhedspolitikken.

De implementerede kontroller hos NHC fremgår af afsnittet "Kontrolmål og implementerede kontroller fra ISO27002" på side 9-11 til denne beskrivelse.

Baseret på risikovurderingen har NHC taget stilling til:

- Kontrolformål, der er relevante for styring af sikkerheden
- Risici, der truer opnåelse af kontrolformål
- Kontroller, der imødegår risiciene.

Kontrolformål og kontroller, der imødegår risiciene, er udvalgt fra ISO 27002 og tilpasset i fornødent omfang. Tilpasningen har primært været en præcisering af kontrollerne, der i standarden præsenteres som retningslinjer og ikke egentlige kontroller, hvor effektiviteten kan vurderes. Beskrivelse af de for denne erklæring relevante kontrolformål og en mere detaljeret beskrivelse af vores implementerede kontroller til at understøtte kontrolformål fremgår af afsnittet revisors beskrivelse af test af kontroller på side 15-32. Der anvendes samme nummerering som i ISO 27002 for de enkelte kontroller.

Afsnittet "Revisors beskrivelse af test af kontroller" på side 15-32 er udarbejdet til brug for NHC's kunder og disses revisorer, som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som NHC's kunder selv har anvendt ved vurdering af risiciene ved hosting-løsningen.

Organisering af informationssikkerhed

Bestyrelsen har det overordnede ansvar for IT-sikkerhed. Den administrerende direktør er ansvarlig for at sikre, at bestyrelsens godkendte sikkerhedspolitik bliver implementeret, samt løbende holder bestyrelsen orienteret om IT sikkerheden.

Den tekniske direktør er NHC's IT-sikkerhedsleder og har det daglige ansvar for IT-sikkerhed. Han holder løbende den administrerende direktør orienteret om IT sikkerhedsniveauet. Endvidere er han ansvarlig for udarbejdelse af IT sikkerhedshåndbog, samt uddannelse af og awareness for medarbejderne.

Alle kundeforhold indrammes, medmindre andet er skriftligt aftalt, af den gældende Service Level Agreement (SLA) mellem kunden og NHC.

Medarbejdersikkerhed

NHC har udarbejdet en personalehåndbog, der omtaler forskellige forhold for medarbejderne.

Fysisk og miljømæssig sikkerhed

NHC har etableret sine hosting-ydelser på 2 forskellige fysiske lokationer. Den ene lokalitet fungerer som NHC's primære driftscenter, mens den anden fungerer som backup lokation.
Det primære datacenter efterlever følgende forhold:

- Redundant overvågning og regulering af klima
- Redundant UPS og dieselgenerator
- Redundant fibertilførsel
- Gigabit-forbindelse mellem alle fysiske rackskabe
- Patruljerende hundevagt
- Adgangssikring
- Kun adgang for godkendt, udvalgt personale

Styring af kommunikation og drift

NHC har egen dedikeret forbindelser mellem det primære datacenter og backup-lokationen. Det sikrer uhindret backup og evt. systemmigrering mellem lokationerne.

NHC's hosting-platform bygger på servere fra HP og Storage fra Hitachi. Platformen er installeret med virtualiseringssoftware som styringsværktøj til de virtuelle servere.

NHC anvender et system til håndtering af hosting-centers drift, kundehåndtering og dokumentation

NHC har vejledninger til opsætning og afvikling af faste rutiner i driften af hosting- ydelser. Denne dokumentation sikrer, at relevante medarbejdere er i stand til at reetablere driften i tilfælde af fejl eller systemnedbrud.

Den daglige drift bliver overvåget og fulgt op på log, fejlmeddelelser og alarmer. NHC skelner i forbindelse med backup mellem databærende og ikke databærende servere:

- Databærende servere ændrer sig løbende, når brugere indtaster og ændrer data.
- Ikke databærende servere ændrer sig kun, når en konsulent aktivt ændrer system-opsætninger eller installerer/fjerner programmer på serveren.

Der tages backup af alle databærende servere hver nat og backup af øvrige servere én gang om ugen. Sikkerhedskopier er placeret i et andet fysisk serverrum end driftsserverne. Der foretages en ekstra sikkerhedskopi "SAN Snapshot" hver nat til separat backup server uden for domænet.

NHC kontrollerer backup på filniveau, serverniveau og komplet kunde-setup på periodisk basis. Ligeledes kontrolleres hver uge, at alle servere er inkluderet i backup.

Alle NHCs systemer er beskyttet med antivirus-løsning, som løbende opdateres og overvåges.

Adgangsstyring

NHC sikrer korrekt beskyttelse af data på baggrund af en formel, nedskrevet procedure. Brugere oprettes, ændres eller slettes kun med skriftlig godkendelse fra kundens kontaktperson. Efter godkendelse af brugeroprettelsen er der nu implementeret en automatisk bruger oprettelse- &

sletningsprocedure. Dog er der fortsat manuel administration i forhold til fratrådte Office365 brugers postkasser.

NHC gennemfører løbende gennemgang og revurdering af interne brugere. NHC stiller krav til anvendelsen af password.
Alle bruger oprettes med egen brugerprofil, der sikrer sporbarhed på systemerne i forbindelse med anvendelse.

Change Management

NHC indgår aftale med den enkelte kunde, hvis de skal have administrative rettigheder til deres dedikerede løsning.

NHC har oprettet særskilt testmiljø til test i forbindelse med større ændringer i forhold til software, netværk, hardware og delte servere.

Testmiljøet er enten fysisk eller virtuelt afhængig af ændringernes størrelse og karakter. Før ændringer igangsættes skal de vurderes og godkendes af 2 personer

NHC laver Changes på kunders servere ved hjælp af 2 metoder.
1. Installation på en testserver, lade kunder teste, derefter installation på driftsservere.
2. Installation direkte på driftsservere.

Følgende er indeholdt i den grundlæggende patch af bagvedliggende servere:
- VM Ware ESX kritiske updates
- Switches kritiske updates
- SAN kritiske updates
- Operativsystem kritiske updates

NHC laver patches af ikke kritiske updates såfremt de vurderes som nødvendige. Typiske tages de med i de kvartalsvise servicevinduer.

Styring af informationssikkerhedshændelser

NHC har en change-log over alle hændelser, der kan på virke system, drift og/eller datasikkerheden. Denne log anvendes til at sikre en passende afhjælpning, herunder at implementere nødvendige kontroller.
Direktionen modtager en årlig rapport over sikkerhedshændelser, der har været i årets løb, som gennemgås i forbindelse med det årlige bestyrelsesmøde vedrørende årsplanen.

Beredskabsstyring

NHC har en beredskabsplan og -procedurer med tilhørende aftaler, som aktiveres hvis en nød- og eller krisesituation skulle opstå.
Beredskabsplanen er forankret i IT-risikoanalysen og vedligeholdes årligt eller ved større systemmæssige eller organisatoriske ændringer. Beredskabsplanen testes løbende som led i at kunne sikre en så sikker og stabil løsning som muligt selv i forbindelse med en nødsituation. En gang om året udføres, der en større test af IT-beredskabsplan med en eller flere realistiske testscenarier.

Overensstemmelse

NHC får udført IT revision af hostede ydelser, herunder processer og beredskab. Denne IT-

revision munder ud i afgivelse en erklæring fra uafhængige, statsautoriserede revisorer baseret på ISAE 3402.

Væsentlige ændringer i IT-miljøerne

Der har ikke i perioden været væsentlige ændringer i IT-miljøerne ud over indkøb af ekstra serverhardware i forbindelse med stigende kundetilgang. Der er foretaget almindelig vedligeholdelse og opdateringer af hardware og software til hostingmiljøet.

Komplementerende kontroller hos NHC's kunder

De enkelte kunder er ansvarlige for datatransmission mellem NHC og NHC's kunder. Det er således NHC's kunders ansvar at sikre kontrollerne i forbindelse hermed.

De enkelte kunder er selv ansvarlige for at styre adgangsrettigheder til deres brugersystemer og virtuelle netværk, herunder godkendelse af og gennemgang af rettigheder. Kunderne skal således kontrollere alt omkring brugeradministrationen.

Der er ingen krav om regelmæssig tvunget skift af NHC kunders brugerprofilers kodeord eller kvaliteten af disse. Det er således kunders ansvar selv at fastsætte krav for interval for udskiftning af kodeord.

De enkelte kunder er selv ansvarlige for at sikre, at data er korrekte. De enkelte kunder skal således selv kontrollere datas kvalitet og integritet samt fortrolighed. NHCs Generelle salgs- og leveringsbetingelser indeholder databehandleraftalen.

Kontroller omkring nødplaner og beredskabsplaner er NHC's kunders ansvar.

Har kunden fået opsat backup af lokale enheder (såkaldt Remote backup) er kunden selv ansvarlig for at sikre, at backup-jobs udføres korrekt, samt foretage regelmæssige tests heraf.

Kontrolmål og implementerede kontroller fra ISO27002

5 Informationssikkerhedspolitikker

5.1 Retningslinjer for styring af informationssikkerhed
5.1.1 Formulering af en informationssikkerhedspolitik
5.1.2 Løbende vedligeholdelse

6 Organisering af informationssikkerhed

6.1 Interne organisatoriske forhold
6.1.1 Roller og ansvar for informationssikkerhed
6.1.2 Funktionsadskillelse

7 Medarbejdersikkerhed

7.1 Før ansættelse
7.1.1 Screening
7.1.2 Ansættelsesvilkår og -betingelser
7.2 Under ansættelsen
7.2.1. Ledelsesansvar
7.2.2. Bevidsthed om uddannelse og træning i informationssikkerhed

9 Adgangsstyring

9.1 Forretningsmæssige krav til adgangsstyring
9.1.1 Politik for adgangsstyring
9.2 Administration af brugeradgang
9.2.1 Brugerregistrering og -afmelding
9.2.3 Styring af privilegerede adgangsrettigheder
9.2.4 Styring af hemmelig autentifikationsinformation om brugere
9.2.5 Gennemgang af brugernes adgangsrettigheder
9.2.6 Inddragelse eller justering af adgangsrettigheder
9.4 Styring af system- og applikationsadgang
9.4.3 System for administration af adgangskoder

11 Fysisk Sikring og miljøsikring

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder
12.1.1 Dokumenterede driftsprocedurer
12.1.2 Ændringsstyring
12.1.3 Kapacitetsstyring
12.2 Malwarebeskyttelse
12.2.1 Kontroller mod malware
12.3 Backup
12.3.1 Backup af information
12.4 Logning og overvågning
12.4.1 Hændelseslogning
12.4.3 Administrator- og operatørlogge
12.6 Sårbarhedsstyring
12.6.1 Styring af tekniske sårbarheder

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold
15.1.1 Informationssikkerhedspolitik for leverandørforhold
15.1.2 Håndtering af sikkerhed i leverandøraftaler
15.2 Styring af leverandørydelser
15.2.2 Styring af ændringer af leverandørydelser

16 Styring af Informationssikkerhedsbrudhændelser

16.1 Styring af informations sikkerhedsbrudhændelser og forbedringer
16.1.2 Rapportering af informationssikkerhedsbegivenheder
16.1.3 Rapportering af informationssikkerhedssvagheder

17 Beredskabsstyring

17.1 Informationssikkerhedsaspekter ved beredskabsstyring
17.1.1 Planlægning af informationssikkerhed beredskab
17.1.2 Implementering af beredskab for informationssikkerhed
17.1.3 Verificering, gennemgang og evaluering af informationssikkerhedskontinuitet

UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED PR. 31. DECEMBER 2022 OM BESKRIVELSEN AF HOSTINGPLATFORMEN OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING

Til ledelsen hos NHC A/S,
NHC's kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om NHC' beskrivelse på side 3-10 af generelle IT-kontroller for Hosting ydelser i hele perioden fra 1. januar til 31. december 2022 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

NHC's ansvar

NHC er ansvarlig for udarbejdelsen af beskrivelsen på side 3-10 og tilhørende udtalelse på side 1-2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om NHC's beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med "ISAE 3402 Erklæringer med sikkerhed om kontroller hos en serviceleverandør". 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, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet på side 3-10.

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

Begrænsninger i kontroller hos en serviceleverandør

NHC's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved hostingplatformen, som hver enkelt kunde måtte anse for vigtigt 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 på side 1-2. Det er vores opfattelse,

a) at beskrivelsen af de generelle IT-kontroller med relevans for NHC's kunder, således som det var udformet og implementeret i hele perioden fra 1. januar til 31. december 2022, i alle væsentlige henseender er retvisende, og

b) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar til 31. december 2022.

c) At de testede kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar til 31. december 2022

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår på side 15-25.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 14-25 er udelukkende tiltænkt NHC's 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 deres regnskaber.

Silkeborg, den 30. januar 2023

Revisionshuset Tal & Tanker
Statusautoriseret revisionspartnerselskab
Cvr-nr. 37 31 56 64

Per Jensen
Statsautoriseret revisor
Mne34087

Tests af kontroller udført af den uafhængige revisor

Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med International Auditing and Assurance Standards Board's International Standard on Assurance Engagements (ISAE) 3402, Erklæring med sikkerhed om kontroller hos en serviceleverandør.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen og som fremgår af efterfølgende sider.

Evt. andre kontrolmål, tilknyttede kontroller og kontroller hos NHC's kunder er ikke omfattet af vores gennemgang / revision. Herunder de på side 8 komplementerende kontroller.

Vores test af funktionaliteten har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden fra 1. januar – 31. december 2022.

Udførte test

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

Test metode	Hvordan udføres testen
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen.
Forespørgsler	Forespørgsel af passende personale hos NHC. Forespørgsler har omfattet hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentag den relevante kontrol. Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
1. Risikostyring (ISO27005) - Kontroller 2022			**Test af kontroller**	
Risikostyring (ISO27005)	**N/A**	NHC's risikostyring omfatter følgende: · Identifikation af potentielle risici · Vurdering af de identificerede potentielle risici, herunder deres væsentlighed, sandsynlighed og konsekvenser på Hosting- miljøerne · Implementering af tiltag for at reducere sandsynligheden for, at risici indtræder, efter en omkostningseffektiv måde.	Vi har inspiceret, at der er udarbejdet en ajourført og ledelsesgodkendt risikovurdering.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at potentielle risici er identificeret og at de kategoriseret efter sandsynlighed og konsekvens.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der for væsentlige risici er beskrevet en handlingsplan for disse.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at bestyrelsen har godkendt risikovurderingen.	Ingen væsentlige bemærkninger
Risikostyring (ISO27005)	**N/A**	Der foretages en gang årligt eller ved større organisatoriske og/eller tekniske ændringer en overordnet risikovurdering.	Vi har inspiceret, at risiko- vurderingen opdateres en gang om året og ved væsentlige ændringer.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at bestyrelsen en gang om året vurderer og godkender risikoprofilen.	Ingen væsentlige bemærkninger
Risikostyring (ISO27005)	**N/A**	NHC håndterer risici med udgangspunkt i det øjeblikkelige trusselsbillede med opgørelse af konsekvens og sandsynlighed for at hændelser indtræffer.	Vi har forespurgt den tekniske direktør hvorledes risikohåndteringen udføres.	Ingen væsentlige bemærkninger
Risikostyring (ISO27005)	**N/A**	Risikohåndteringen implementeres i forretningsgange og processer i, for at sikre hændelser behandles på rette sted og tid af rette vedkommende.	Vi har inspiceret, at elementer fra risiko-vurderingen er indarbejdet i IT sikkerheds-håndbogen.	Ingen væsentlige bemærkninger
Risikostyring (ISO27005)	**N/A**	NHC har tegnet har en erhvervs- og produktansvarsforsikring med en dækningssum på 10 mio kr. samt professionel ansvarsforsikring med en dækningssum på 1 mio. d.kr.	Vi har inspiceret, at præmie for de to forsikringer er tegnet og betalt for året 2022.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
2. Sikkerhedspolitik (ISO27002 Afsnit 5)			**Test af kontroller**	
	5.1	**< Retningslinjer for styring af informationssikkerhed >**		
Sikkerhedspolitik	**5.1.1**	Ledelsen godkender en skriftlig informationssikkerhedspolitik, som offentliggøres og kommunikeres til virksomhedens medarbejdere og relevante eksterne parter.	Vi har inspiceret, at der foreligger en opdateret og ledelsesgodkendt IT sikkerhedspolitik, der er tilgængelig for NHC's medarbejdere.	Ingen væsentlige bemærkninger
			Vi har forespurgt om udvalgte medarbejdere er bekendt med IT-sikkerhedspolitikken.	Ingen væsentlige bemærkninger
Sikkerhedspolitik	**5.1.1**	IT-sikkerhedspolitikken fastlægger det overordnede sikkerhedsniveau og de nødvendige organisatoriske rammer samt de overordnede retningslinjer for udformning af kontroller, procedurer og sikringsforanstaltninger	Vi har inspiceret IT sikkerhedspolitikken og påset, at sikkerhedsniveauet fastlægges	Ingen væsentlige bemærkninger
Sikkerhedspolitik	**5.1.1**	På baggrund af den af ledelsen godkendte IT sikkerhedspolitik udarbejdes en IT-sikkerhedshåndbog, der indeholder procedurer og retningslinjer for IT-sikkerheden.	Vi har inspiceret, at der foreligger en opdateret og ledelsesgodkendt IT sikkerheds- håndbog udarbejdet med udgangspunkt I IT-sikkerhedspolitikken, samt at den er tilgængelig for NHC's medarbejdere.	Ingen væsentlige bemærkninger
			Vi har forespurgt om udvalgte medarbejdere er bekendt med IT-sikkerhedshåndbogen.	Ingen væsentlige bemærkninger
Sikkerhedspolitik	**5.1.2**	Informationssikkerhedspolitikken revurderes en gang om året samt ved væsentlige tekniske eller organisatoriske ændringer.	Vi har forespurgt den tekniske direktør om IT-sikkerhedspolitikken opdateres regelmæssigt og ved væsentlige ændringer.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at bestyrelsen en gang om året tager informationsstrategien og – politikken til efterretning.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
3. Organisering af informationssikkerhed (ISO27002 Afsnit 6)			**Test af kontroller**	
	6.1	**< Interne organisatoriske forhold >**		
Organisering af informationssikkerhed	**6.1.1**	Sikkerhedsopgaver og -ansvar er fastlagt i overensstemmelse med NHC's retningslinjer og IT- sikkerhedspolitik.	Vi har for udvalgte medarbejdere hos NHC forespurgt om deres opgaver og ansvar vedrørende IT-sikkerhed.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at forhold om medarbejdernes ansvar og forpligtelser vedrørende IT-sikkerhed er omtalt i IT sikkerhedspolitikken og i personalehåndbogen.	Ingen væsentlige bemærkninger
			Vi har forespurgt om, der er udpeget en IT sikkerhedsleder.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der er udarbejdet en job- og ansvarsbeskrivelse for IT sikkerhedslederen.	Ingen væsentlige bemærkninger
Organisering af informationssikkerhed	**6.1.1**	Ledelsen understøtter aktivt i NHC's IT-sikkerheden ved at udlægge klare retningslinjer, udvise synligt engagement samt sikre en præcis placering af ansvar for IT-sikkerhed.	Vi har forespurgt ledelsen, hvordan de aktivt understøtter sikkerheden, herunder ved at vise retning, engagement, fordele opgaver og tage ansvar for informationssikkerhed.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at direktionens ansvar for informationssikkerhed er beskrevet i tillæg til direktørkontrakten.	Ingen væsentlige bemærkninger
Organisering af informationssikkerhed	**6.1.1**	Direktionen har ansvaret for at sikre, at strategien for informationssikkerhed er synlig, koordineret og i overensstemmelse med NHC's mål.	Vi har forespurgt udvalgte medarbejdere om, hvordan ansvaret for IT-sikkerhed defineres og placeres.	Ingen væsentlige bemærkninger
Organisering af informationssikkerhed	**6.1.2**	Der er etableret funktions- adskillelse for at minimere risikoen for uautoriserede eller utilsigtede ændringer eller misbrug af NHC's informationsaktiver.	Vi har inspiceret organisationsdiagram.	Ingen væsentlige bemærkninger
			Vi har forespurgt udvalgte medarbejdere om deres arbejdsopgaver i relation til NHC's Hosting ydelser	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
4. Medarbejdersikkerhed (ISO27002 Afsnit 7)			**Test af kontroller**	
	7.1	**< Før ansættelse >**		
Medarbejdersikkerhed < Før ansættelse >	**7.1.1**	Det er den ansættelses- ansvarlige NHC-medarbejders ansvar at foretage forsvarligt baggrundstjek af kandidaten, hvis dette er relevant for stillingen.	Vi har forespurgt den tekniske direktør, om der har været nyansættelser i perioden 1. januar – 31. december 2022.	Ingen væsentlige bemærkninger
			Vi har forespurgt den tekniske direktør, hvordan NHC sikrer rette kompetencer for kandidaten.	Ingen væsentlige bemærkninger
Medarbejdersikkerhed < Før ansættelse >	**7.1.2**	Medarbejderen skal underskrive en aftale om ansættelse, som beskriver medarbejderens og NHC's ansvar og forpligtelser vedrørende informationssikkerhed.	Vi har forespurgt, om forretningsgangen for afgivelse af tavsheds-klausuler med den HR-ansvarlige.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der i medarbejdernes ansættelses- aftaler fremgår, at medarbejdere har tavshedspligt.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at forhold om medarbejdernes ansvar og forpligtelser vedrørende informationssikkerhed er omtalt i IT sikkerhedspolitikken og i personalehåndbogen.	Ingen væsentlige bemærkninger
	7.2	**< Under ansættelsen >**		
Medarbejdersikkerhed < Under ansættelsen >	**7.2.1**	Ledelsen skal sikre sig, at alle medarbejdere implementerer og fastholder informationssikkerhed i overensstemmelse med NHC's sikkerhedspolitik, retningslinjer og procedurer.	Vi har forespurgt hvorledes Direktionen og den sikkerheds-ansvarlige sikrer sig at medarbejderne overholder sikkerhedspolitikken.	Ingen væsentlige bemærkninger
Medarbejdersikkerhed < Under ansættelsen >	**7.2.2**	NHC er ansvarlig for at introducere den nye medarbejder til gældende sikkerhedspolitik – senest på 1. arbejdsdag. Medarbejderen skal kvittere for at have læst og forstået Sikkerhedspolitikken.	Vi har for udvalgte medarbejdere hos NHC forespurgt om deres opmærksomhed og uddannelse om IT-sikkerhedspolitik.	Ingen væsentlige bemærkninger
Medarbejdersikkerhed < Under ansættelsen >	**7.2.2**	Alle NHC's medarbejdere skal løbende informeres om og uddannes i NHC's sikkerhedspolitik og -procedurer.	Vi har for udvalgte medarbejdere hos NHC forespurgt om deres opmærksomhed og uddannelse om IT-sikkerhedspolitik.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
5. Adgangsstyring (ISO27002 Afsnit 9)			**Test af kontroller**	
	9.1	**< Forretningsmæssige krav til adgangsstyring >**		
Adgangsstyring	**9.1.1**	Der foreligger dokumenterede og ajourførte retningslinjer for adgangsstyring til alle væsentlige IT-aktiver. Den Tekniske Direktør giver medarbejder de nødvendige rettigheder for at kunne udføre deres opgaver.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af adgangsrettigheder sker.	Ingen væsentlige bemærkninger
	9.2	**< Administration af brugeradgang >**		
Adgangsstyring	**9.2.1**	Brugere modtager en skriftlig bekræftelse af de tildelte rettigheder. NHC vedlige- holder fortegnelser over, hvordan bruger-ID eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.	Vi har forespurgt udvalgte medarbejdere, hvordan bekræftelse af tildeling af adgangsrettigheder sker.	Ingen væsentlige bemærkninger
Adgangsstyring < Styring af privilegerede adgangsrettigheder >	**9.2.3**	Udvidede adgangsrettigheder tildeles i begrænset omfang og kun hvis den ansatte har behov for dette til at udføre sit arbejde. Udvidede rettigheder knyttes til særlige brugeridentiteter der entydigt identificerer brugeren.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af udvidede adgangsrettigheder sker.	Ingen væsentlige bemærkninger
Adgangsstyring	**9.2.4**	Tildeling af adgangskoder styres ved en formaliseret proces.	Vi har inspiceret, hvorledes adgangskoder tildeles.	Ingen væsentlige bemærkninger
Adgangsstyring	**9.2.5**	Brugernes adgangsrettigheder gennemgås regelmæssigt.	Vi har inspiceret proceduren for gennemgang af adgangsrettigheder.	Ingen væsentlige bemærkninger
Adgangsstyring	**9.2.6**	Medarbejderen er forpligtet til at overdrage alt materiale og alle rettigheder ved fratrædelsen eller afskedigelsen.	Vi har fået en oversigt over fratrådte medarbejdere i 2022. Ifølge det oplyste er adgangsrettigheder for fratrådte medarbejdere i 2022 inddraget.	Ingen væsentlige bemærkninger
Adgangsstyring	**9.2.6**	Det vurderes individuelt, om rettighederne skal slettes eller blot spærres. Ved ophør af ansættelse lukkes adgang pr. sidste arbejdsdag.	Vi har fået en oversigt over fratrådte medarbejdere i 2022. Ifølge det oplyste er adgangsrettigheder for fratrådte medarbejdere i 2022 inddraget.	Ingen væsentlige bemærkninger
	9.4	**< Styring af system- og applikationsadgang >**		
Adgangsstyring	**9.4.3**	Systemer til styring af adgangskoder er interaktive og sikrer, at der kun benyttes adgangskoder med den fastlagte kvalitet.	Vi har forespurgt, hvordan regler er for administration af adgangskoder.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
6. Fysisk og miljømæssig sikkerhed DLX (ISO27002 Afsnit 11)			**Test af kontroller**	
Fysisk og miljømæssig sikkerhed DLX	**11.1-11.2.9**	Fysisk og miljømæssig sikkerhed hos DLX hosting (datacenter) for NHC fra 1. Jan - 31. december 2022.	Vi har inspiceret ISAE3402 erklæring fra DLX dateret 3. januar 2023.	

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
8. Driftssikkerhed (ISO27002 Afsnit 12)			**Test af kontroller**	
	12.1	**< Driftsprocedurer og ansvarsområder >**		
Driftssikkerhed	**12.1.1**	Driftsafviklingsprocedurer for forretningskritiske systemer skal dokumenteres, føres ajour og være tilgængelige for server/drift og andre med arbejdsrelateret behov.	Vi har observeret NHC's driftsprocedurer, herunder NHC's Knowledgebase.	Ingen væsentlige bemærkninger
			Vi har observeret en stikprøve af driftsprocedurer i NHC's Knowledgebase.	Ingen væsentlige bemærkninger
Driftssikkerhed	**12.1.1**	Driften i NHC's datacenter dokumenteres efter gældende interne standarder. Relevante NHC-medarbejdere har adgang til teknisk dokumentation på alle kritiske driftssystemer, som er samlet på NHC's intranet. Viden akkumuleret i det daglige arbejde dokumenteres også i en fælles Knowledge- database til brug i effektivisering/løsning af lignende problemer i fremtiden.	Vi har observeret NHC's driftsprocedurer, herunder NHC's Knowledgebase.	Ingen væsentlige bemærkninger
			Vi har observeret en stikprøve af driftsprocedurer i NHC's Knowledgebase.	Ingen væsentlige bemærkninger
Driftssikkerhed < Ændringssstyring >	**12.1.2**	Ændringer til forretningskritisk informations-behandlingsudstyr, -systemer og -procedurer styres gennem en formaliseret procedure.	Vi har observeret change management procedurer.	Ingen væsentlige bemærkninger
			Vi har forespurgt udvalgte medarbejdere om hvordan ændringshåndtering udføres.	Ingen væsentlige bemærkninger
Driftssikkerhed < Kapacitetsstyring >	**12.1.3**	Ressourceforbruget overvåges og tilpasses	Vi har observeret driftsprocesser for verificering af passende ressourcekapacitet mod anvendt ressourceforbrug.	Ingen væsentlige bemærkninger
			Vi har forespurgt udvalgte medarbejdere, hvad de gør når der stor belastning på systemkraft, diske eller tapes.	Ingen væsentlige bemærkninger
	12.2	**< Malwarebeskyttelse >**		
Driftssikkerhed < Malwarebeskyttelse >	**12.2.1**	NHC scanner alt netværkstrafik for virus via såkaldt parameter-scanning. I visse tilfælde scannes servere direkte. Såfremt data er virusbehæftet, opretholder NHC sig retten til at forsøge rensning af disse data. Såfremt dette ikke er tilstrækkeligt, forholder NHC sig retten til at slette de inficerede data.	Vi har observeret, at der er installeret opdateret antivirus software på et udvalg af servere	Ingen væsentlige bemærkninger
	12.3	**< Backup >**		
Driftssikkerhed < Backup >	**12.3.1**	Der tages sikkerhedskopier af NHC's væsentlige informationsaktiver, herunder parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har observeret processen for sikkerhedskopiering af nye versioner/releases af NHC's Hosting ydelser.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
	12.4	**< Logning og overvågning >**		
Driftssikkerhed < Logning og overvågning >	**12.4.1**	Brugen af virksomhedens informationsbehandlingssystemer overvåges og følges op løbende.	Vi har observeret, hvorledes der foretages overvågning af sikkerhedskopiering.	Ingen væsentlige bemærkninger
Driftssikkerhed < Logning og overvågning >	**12.4.1**	Fejl logges og analyseres, og nødvendige udbedringer og modforholdsregler gennemføres.	Vi har observeret, hvorledes fejl eller manglende back up jobs bliver fulgt op på. Herunder hvorledes evt. fejl bliver registreret i NHC's incident system TopDesk	Ingen væsentlige bemærkninger
Driftssikkerhed < Logning og overvågning >	**12.4.3**	Der er, så vidt der er muligt, etableret logning af alle aktiviteter, der kræver systemadministrator rettigheder, eller andre særlige rettigheder. Hvor det ikke er muligt at etablere denne logning, er der etableret kompenserende forebyggende manuelle procedurer og registreringer, så revisionssporet til stadighed er intakt.	Vi har observeret om administratorer og operatører aktiviteter logges.	Ingen væsentlige bemærkninger
	12.6	**< Sårbarhedsstyring >**		
Driftssikkerhed < Sårbarhedsstyring >	**12.6.1**	NHC indhenter løbende informationer om eventuelle sårbarheder i de anvendte systemer. Sårbarhederne evalueres, og passende foranstaltninger skal implementeres for at modvirke de nye risici.	Vi har forespurgt udvalgte medarbejdere om, hvordan sårbarheder for Hosting-miljøet indsamles, evalueres og tilhørende foranstaltninger implementeres. Evt. ifm Sikkerheds- hændelser.	Ingen væsentlige bemærkninger
Driftssikkerhed < Sårbarhedsstyring >	**12.6.1**	Windows opdateringer udføres via Microsofts værktøj WSUS (Windows Server Updates Services). Windows opdateringer implementeres ugentligt efter beskreven procedure	Vi har observeret procedurer for opdateringer.	Ingen væsentlige bemærkninger
			Vi har observeret, at der sker automatisk opdatering for kritiske og sikkerhedsmæssige opdateringer for Windows servere.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
11. Leverandørforhold (ISO27002 Afsnit 15)			**Test af kontroller**	
	15.1	**< Informationssikkerhed i leverandørforhold >**		
Leverandørforhold < Informationssikkerhed i leverandørforhold >	**15.1.1**	Ved samarbejde med andre parter, der har adgang til virksomhedens informations- aktiver gennemføres en risiko- vurdering, og relevante kontroller identificeres og implementeres.	Vi har forespurgt, hvorledes eksterne parter får adgang til it-miljøer hos NHC.	Ingen væsentlige bemærkninger
Leverandørforhold < Informationssikkerhed i leverandørforhold >	**15.1.2**	Ved serviceleverance, bliver der udarbejdet en gensidig aftale omkring det ønskede serviceniveau, eksempelvis gennem formelle SLA (Service Level Agreements) som en del af den indgåede driftsaftale. NHC sikrer sig, at aftalte sikrings- og kontrolforanstaltninger, serviceydelser og servicemål bliver etableret, leveret og opretholdt.	Vi har inspiceret, at der er indgået housing aftale.	Ingen væsentlige bemærkninger
			Vi har inspiceret ISAE3402 erklæring dateret 3. Januar 2023 for DLX og inspiceret relevante kontroller i erklæringen, som DLX udfører på vegne af NHC.	
	15.2	**< Styring af leverandørydelser >**		
Leverandørforhold < Styring af leverandørydelser >	**15.2.2**	NHC overvåger regelmæssigt serviceleverandøren. Dette sker ved gennemgang af aftalte rapporter og logninger samt udføre egentlige revisioner, for at sikre at aftalen overholdes, og at sikkerhedshændelser og - problemer håndteres betryggende.	Vi har inspiceret, at der er indgået housing aftale med DLX.	Ingen væsentlige bemærkninger
			Vi har inspiceret ISAE3402 erklæring dateret 3. januar 2023 for DLX med henblik på at indhente tilstrækkelig information og bevis om implementering og funktionalitet om kontroller hos DLX.	
			Vi har forespurgt om NHC er i dialog med DLX om IT-sikkerhed.	Ingen væsentlige bemærkninger
Leverandørforhold < Styring af leverandørydelser >	**15.2.2**	Ethvert væsentligt eksternt samarbejde er baseret på en samarbejdsaftale, som sikrer, at NHC's sikkerhedsmålsætning ikke kompromitteres.	Vi har inspiceret udvalgte samarbejdsaftaler med eksterne parter.	Ingen væsentlige bemærkninger
			Vi har forespurgt, hvordan NHC sikrer sig, at DLX efterlever NHC's sikkerhedspolitik og indgåede aftaler	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
12. Styring af informationssikkerhedsbrud (ISO27002 Afsnit 16)			**Test af kontroller**	
	16.1	**< Styring af informations sikkerhedshændelser og forbedringer >**		
Styring af informationssikkerhedsbrud < Styring af informations sikkerhedshændelser og forbedringer >	**16.1.2**	Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt.	Vi har forespurgt udvalgte medarbejdere om, hvordan de rapporterer sikkerhedshændelser.	Ingen væsentlige bemærkninger
			Vi har forespurgt ledelsen, hvordan de indsamler information om sikkerhedshændelser.	Ingen væsentlige bemærkninger
			Vi har inspiceret log over sikkerhedshændelser, der har været i perioden.	Ingen væsentlige bemærkninger
Styring af informationssikkerhedsbrud < Styring af informations sikkerhedshændelser og forbedringer >	**16.1.2**	En detaljeret beskrivelse af hændelsen skal sendes til NHC's IT-sikkerhedskonsulent.	Vi har inspiceret log over sikkerhedshændelser, der har været i perioden.	Ingen væsentlige bemærkninger
Styring af informationssikkerhedsbrud < Styring af informations sikkerhedshændelser og forbedringer >	**16.1.3**	Alle medarbejdere, samarbejdspartnere og andre brugere af systemer og tjenester har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i systemer og tjenester.	Vi har forespurgt udvalgte medarbejdere om, hvordan de rapporterer sikkerhedssvagheder.	Ingen væsentlige bemærkninger
			Vi har forespurgt ledelsen, hvordan de indsamler information om sikkerhedssvagheder.	Ingen væsentlige bemærkninger

	Ref.	ISO27002 Kontrol	Test af kontrol	Bemærkning
13. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring (ISO27002 Afsnit 17)			**Test af kontroller**	
	17.1	**< Informationssikkerhedsaspekter ved beredskabsstyring >**		
Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring	**17.1.1**	Der udarbejdes og vedligeholdes en beredskabsstyringsproces, som behandler de krav til informationssikkerhed, der er nødvendige for NHC's fortsatte drift.	Vi har forespurgt udvalgte medarbejdere om beredskabsstyring.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der er en vagtplan.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der er udarbejdet en beredskabsplan.	Ingen væsentlige bemærkninger
Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring	**17.1.2**	Der udarbejdes planer for vedligeholdelse og retablering af virksomhedens forretnings- aktiviteter inden for den fastsatte tidsramme efter en afbrydelse af eller fejl i virksomhedens kritiske forretningsprocesser.	Vi har forespurgt udvalgte medarbejdere, hvad de gør i tilfælde af en afbrydelse eller en fejl for at retablere driften.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der foreligger en opdateret katastrofe- og beredskabsplan.	Ingen væsentlige bemærkninger
Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring	**17.1.3**	NHC udfører en gang årligt verificering af beredskabsplanen for at sikre reetablering kan ske inden for 3 dage.	Vi har forespurgt den tekniske direktør, hvordan test af beredskabsplan udføres.	Ingen væsentlige bemærkninger

Dette dokument er underskrevet af nedenstående parter, der med deres underskrift har bekræftet dokumentets indhold samt alle datoer i dokumentet.

This document is signed by the following parties with their signatures confirming the documents content and all dates in the document.

Casper Søltoft

Navnet returneret af dansk MitID var:
Casper Bjørn Korup Søltoft
Direktør
ID: 507dc71f-9b72-46d6-a28c-60671052d0b5
Tidspunkt for underskrift: 03-02-2023 kl.: 13:02:17
Underskrevet med MitID

Ole Rebbe

Navnet returneret af dansk MitID var:
Ole Rebbe
ID: 45ed3f85-593d-4ea7-a45d-c2f755bd6533
Tidspunkt for underskrift: 03-02-2023 kl.: 12:04:33
Underskrevet med MitID

Per Jensen

Navnet returneret af dansk NemID var:
Per Jensen
Statsautoriseret revisor
ID: 84233143
Tidspunkt for underskrift: 03-02-2023 kl.: 14:12:45
Underskrevet med NemID