Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk

Netcompany A/S

Uafhængig revisors ISAE 3402 type 2-erklæring om generelle it-kontroller relateret til Netcompanys ydelser på Næste Generations Digital Post leveret til Digitaliseringsstyrelsen for perioden 1. januar 2022 til 31. december 2022

netcompany

Indholdsfortegnelse

Deloitte.

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3402 type 2-erklæring om generelle it-kontroller relateret til Netcompanys ydelser på Næste Generations Digital Post leveret til Digitaliseringsstyrelsen for perioden fra 1. januar 2022 til 31. december 2022.

Til ledelsen hos Netcompany A/S, Digitaliseringsstyrelsen og deres revisorer

1.1. Omfang

Vi har fået til opgave at afgive erklæring om Netcompany A/S' (Netcompany) beskrivelse i afsnit 3 af udvalgte generelle it-kontroller i forbindelse med ydelser på Næste Generations Digital Post (Løsningen) for perioden fra 1. januar 2022 til 31. december 2022 og om udformningen og funktionaliteten af de udvalgte kontroller, der knytter sig til de udvalgte kontrolmål, som er anført i beskrivelsen. De omfattede kontroller er udvalgt af Netcompany efter aftale med Digitaliseringsstyrelsen, og denne erklæring skal ses i sammenhæng med ISAE 3402-erklæring om generelle it-kontroller relateret til drifts- og hostingydelser for perioden fra 1. januar 2022 til 31. december 2022, dateret den 11. januar 2023.

Netcompany anvender serviceunderleverandørerne GlobalConnect og InterXion som housing-centre. Netcompanys systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandører.

Enkelte af de kontrolmål, der er anført i Netcompanys beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Netcompany. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

1.2. Netcompanys ansvar

Netcompany er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene og for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

1.3. Revisors 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.

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

1.4. Revisors ansvar

Vores ansvar er på grundlag af vores revisionshandlinger at udtrykke en konklusion om Netcompanys beskrivelse samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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 revisionshandlinger for at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør, omfatter udførelse af revisionshandlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af dens 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 desuden vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som Netcompany har specificeret og beskrevet i afsnit 2, "Ledelsens udtalelse".

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

1.5. Begrænsninger i kontroller hos en serviceleverandør

Netcompanys beskrivelse er udarbejdet for at opfylde de almindelige behov hos Netcompanys kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved generelle it-kontroller i forbindelse med ydelser på Næste Generations Digital Post, som hver enkelt kunde måtte anse for vigtige efter dennes særlige forhold. Desuden vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen.

1.6. Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse i afsnit 2. Det er vores opfattelse

a) at beskrivelsen af udvalgte generelle it-kontroller i forbindelse med ydelser på Næste Generations Digital Post, således som de var udformet og implementeret for perioden fra 1. januar 2022 til 31. december 2022, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de udvalgte kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet for perioden fra 1. januar 2022 til 31. december 2022

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

1.7. Beskrivelse af test af kontroller

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

1.8. Tiltænkte brugere og formål med erklæringen

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt Digitaliseringsstyrelsen samt deres revisorer, som har en tilstrækkelig forståelse til at overveje disse sammen med anden information, herunder information om egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer.

København, den 23. marts 2023

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

Dan Leitner
partner

2. Ledelsens udtalelse

Medfølgende beskrivelse i relation til Netcompanys ydelser på Næste Generations Digital Post er udarbejdet til brug for Digitaliseringsstyrelsen og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, når de opnår en forståelse af kundernes informationssystemer, som er relevante. Beskrivelsen i afsnit 3 og de tilhørende kontroller i afsnit 4 omfatter, efter aftale mellem Netcompany og Digitaliseringsstyrelsen, kun en delmængde af de kontroller, der er relevante i forhold til Netcompanys leverancer vedrørende Digital Post til Digitaliseringsstyrelsen. Beskrivelsen og kontrollerne skal således ses i sammenhæng med ISAE 3402-erklæring fra Netcompany om generelle it-kontroller relateret til drifts- og hostingydelser for perioden fra 1. januar 2022 til 31. december 2022 (efterfølgende "den generelle erklæring"), dateret den 11. januar 2023

Netcompany bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af generelle it-kontroller i forbindelse med ydelser på Næste Generations Digital Post for perioden fra 1. januar 2022 til 31. december 2022. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   i. redegør for, hvordan systemet var udformet og implementeret, , i det omfang dette afviger fra den generelle erklæring, herunder redegør for:

      - de typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant
      - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til Digitaliseringsstyrelsen
      - de tilhørende regnskabsregistreringer, underliggende information og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan information blev overført til de rapporter, der er udarbejdet til Digitaliseringsstyrelsen
      - hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
      - den proces, der blev anvendt til at udarbejde rapporter til Digitaliseringsstyrelsen
      - relevante kontrolmål og kontroller udformet til at nå disse mål. Opnåelsen af kontrolmålene er, udover kontroller i denne erklæring, også afhængig af de kontroller, der er omfattet af den generelle erklæring.
      - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, 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 (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af Digitaliseringsstyrelsens transaktioner.

   ii. ikke udelader eller forvansker information, der er relevant 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 systemet, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2022 til 31. december 2022.

Kriterierne for denne udtalelse var, at:

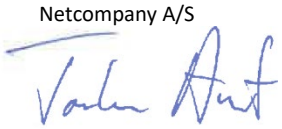
i. de risici, som truede opnåelsen af de udvalgte kontrolmål, der er anført i beskrivelsen, var identificeret.

ii. de identificerede udvalgte kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål.

iii. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse for 1. januar 2022 til 31. december 2022.

København, den 23. marts 2023

Netcompany A/S



Torben Arent
partner

3. Systembeskrivelse

3.1. Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Digitaliseringsstyrelsen og disses revisorer om de generelle it-kontroller i forbindelse med Netcompanys ydelser på Næste Generations Digital Post. Erklæringen omfatter således ikke applikationskontroller relateret til systemet. Beskrivelsen er organiseret i overensstemmelse med ISO/IEC27001-rammeværket, der ligeledes er brugt som styringsværk i forbindelse med Netcompanys interne kontroller.

Nærværende beskrivelse indeholder beskrivelser af de anvendte procedurer til sikring af en betryggende afvikling af Digital Post, herunder foranstaltninger til sikring af betryggende system-, data- og driftssikkerhed dækket af erklæringen. Formålet er at give tilstrækkelige informationer til, at Digitaliseringsstyrelsens revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet, i det omfang det kan medføre en risiko for væsentlige fejl hos Digitaliseringsstyrelsen.

3.2. Beskrivelse af Netcompany A/S' ydelser

Netcompany beskæftiger 5.000 ansatte på kontorer i Danmark, Norge, England, Polen, Holland og Vietnam. Vores primære ydelse er at levere udvikling, drift og vedligehold af forretningskritiske it-løsninger.

Netcompanys kunder er store og mellemstore virksomheder og organisationer i den private og offentlige sektor.

Denne erklæring omhandler udvalgte generelle it-kontroller på ydelser som håndtering og drift af infrastrukturydelser som storage, backup og netværk samt forsvarlig forvaltning og drift af serverinstanser tilpasset Digitaliseringsstyrelsens behov. Kontrolforanstaltningerne og sikkerhedsarbejdet er struktureret efter ISO/IEC27001-rammeværket.

3.3. Ansvar og organisering hos Netcompany A/S

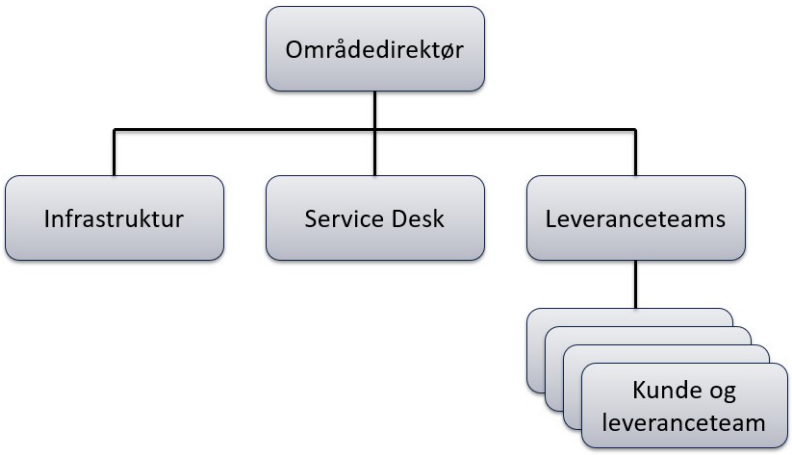
Hver systemforvaltningskunde hos Netcompany bliver tilknyttet et team af medarbejdere, der arbejder med kundens løsning. Dette sikrer, at kunden har adgang til dedikerede, kompetente og dygtige medarbejdere med dyb viden om den konkrete løsning – både forretningsmæssigt og teknisk. Teamet kan derved let indgå i en dialog med kunden på kundens præmisser. Da forvaltningen både omfatter drift og applikationsvedligehold, er der tilknyttet både et team i Operations og et dedikeret team til vedligeholdelse.

Ved fastsættelse af Netcompanys teams på kundernes løsninger tages der højde for den anvendte teknologi, så kundesystemer varetages af et team med indgående kendskab til den teknologiske platform.

Hvert team består typisk af op til 20 medarbejdere med spidskompetencer inden for en primær teknologi eller kunderelation. Der vil altid være minimum 2 personer tilknyttet den enkelte kundes løsning, således at vi kan servicere kunden under ferie og andet fravær.

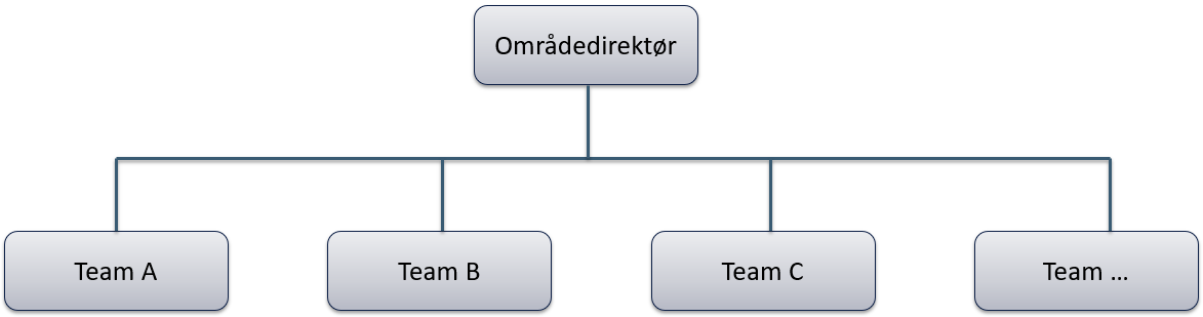
3.3.1. Organisering – Operations

Operations har en række specialiserede teams, der understøtter og leverer ydelser til de kundehenvendte leveranceteams.



Figur 1: Diagram over organisering i Netcompany Operations

3.3.2. Organisering – Applikationsvedligehold



Figur 2: Organisationen i Application Services

De enkelte teams har et begrænset antal teknologier, de er specialiseret i og yder applikationssupport og vedligehold af.

3.4. Driftsfaciliteter

Netcompany udvikler og driver løsninger, hvor applikationer, infrastruktur og driftsprocesser tilpasses og justeres forretningens eller applikationens specifikke krav. Netcompany råder gennem samarbejde med underleverandøren InterXion over to ANSI/TIA-942 Tier 3-datacentre, der befinder sig med 5 kilometers afstand fra hinanden. Digital Post driftes i begge datacentre.

3.5. Netcompanys ITSM

Netcompany anvender et egenudviklet ITSM-værktøj kaldet Toolkit.

Hver kunde får deres egen Toolkit-instans. Instansen er kun tilgængelig for kundens medarbejdere og for de Netcompany-medarbejdere, der er tilknyttet løsningen.

Toolkit-instansen leveres som standard:

- IT Service Management-værktøj (Incident & Change management)
- Configuration Management (oversigt over og opsætning af Configuration Items)
- Backupstyring
- Systemdokumentation
- Projektstyringsværktøj
- Såvel certifikat som licensstyringsværktøj
- Kontaktpersoner – oversigter over, hvem der indgår i løsningen og hvordan.

Toolkit kan efter behov udvides med yderligere funktionsmoduler såsom et patch management-værktøj til at styre patch-strategier. Da Toolkit er baseret på SharePoint og Netcompanys egenudviklede ESDH-system GetOrganized, kan det enkelte Toolkit tilpasses det behov, et projekt, en kunde eller en leverance har. Dette anvendes konkret i løsningerne over for Digitaliseringsstyrelsen, hvor koordination og fejlretning mv. dokumenteres centralt, så adgang kan gives til relevante eksterne og interne interessenter.

Toolkit anvendes til at styre og kommunikere ud fra. Alarmer, changes og incidents er tilgængelige for alle brugere på løsningen, således at Netcompany opererer transparent over for den aktuelle kunde. Løsningen har en standard for, hvordan en leverance dokumenteres, således at såvel kunde som relevante medarbejdere fra Netcompany har hurtig adgang til procedure, Configuration Items eller kontaktlister.

Der er separat rettighedsstyring, så løsningen kan indeholde følsom information, hvor der gives specifikke adgange til lister eller dokumentbiblioteker. Således kan såvel referater fra styregrupper som kommercielle aftaler forvaltes gennem løsningen.

3.6. Risikostyring

Netcompany har etableret et informationssikkerhedssystem i overensstemmelse med ISO/IEC27001-rammeværket, som løbende vedligeholdes af Netcompanys Chief Information Security Officer (CISO) og de lokale sikkerhedsansvarlige, således at driftsprocedurer lever op til krav i Netcompanys sikkerhedspolitik, lovgivning og indgåede kontrakter.

Netcompany har etableret en sikkerhedsstyringsmodel, som omfatter, at Netcompanys ledelse gennem godkendelse af sikkerhedspolitikken sikrer, at Netcompanys risikoniveau er forankret i og accepteret af ledelsen. Sikkerhedspolitikken opdateres og godkendes som minimum årligt og kommunikeres til alle medarbejdere.

Netcompany har ligeledes udarbejdet en sikkerhedshåndbog, som fastsætter kontrolkrav i forhold til sikkerhedspolitikken, og som dermed udmønter specifikke kontrolkrav, som fremgår af ISO/IEC27002 i konkret kontekst i forhold til Netcompanys løsninger.

3.7. Personalesikkerhed

Netcompany har implementeret procedurer, som sikrer, at alle medarbejdere gennemgår efterprøvning af deres baggrund og indhenter de nødvendige beviser for deres uddannelse mv. i forbindelse med deres ansættelse. Alle medarbejdere får udleveret Netcompanys sikkerhedspolitik og skal læse denne samt verificere at have læst den inden 3 dage efter start hos Netcompany. Sikkerhedspolitikken indeholder bl.a. information om, hvorledes man skal forholde sig til sikkerhedsbrud, og hvorledes sikkerhedsbrud skal rapporteres.

For adgang til krypteringsnøgler i Digital Posts produktionsmiljø kræves der af Digitaliseringsstyrelsen endvidere en PET-sikkerhedsgodkendelse.

Netcompany har udviklet uddannelseskonceptet "Netcompany Academy", som løbende sikrer, at medarbejdere uddannes, opkvalificeres og modtager information om bl.a. informationssikkerhed.

I forbindelse med opsigelse og fratrædelse gælder de sikkerhedsmæssige krav fortsat, og der påhviler bl.a. tavshedspligt efter fratrædelse.

3.8. Styring af aktiver

Som beskrevet har Netcompany et ITSM-system, som bl.a. indeholder en fortegnelse over aktiver, ansvar for aktiver og klassificering af aktiver, jf. sikkerhedspolitikkens krav. Gennem ITSM-systemet sikres det ligeledes, at alle aktiver hos medarbejdere tilbageleveres til Netcompany efter endt brug. Sikkerhedshåndbogen beskriver krav til håndtering af aktiver, herunder hvorledes det sikres, at informationer slettes fra aktiver efter endt brug, således at informationer til enhver tid er beskyttet eller slettet. ITSM-systemet indeholder for de enkelte løsninger, herunder Digital Post leveret til Digitaliseringsstyrelsen, en fuld fortegnelse over de aktiver, der indgår i driften af løsningen.

3.9. Adgangsstyring

Netcompany arbejder aktivt med at sikre passende brugerstyring og adgangskontrol. Dette sker i de enkelte kundeforhold gennem anvendelse af Toolkit og i driftsmæssig sammenhæng på de underliggende tekniske platforme. Logisk kræves en personlig bruger for at kunne tilgå Netcompanys interne systemer. Personlige brugere er reguleret med en centralt styret passwordpolitik, og adgang begrænses til, hvad der er nødvendigt for den enkeltes funktion. Netcompany har etableret procedurer, som sikrer, at kontrollerne for adgangsstyring er etableret.

Brugere, der som følge af deres jobfunktion har behov for at kunne tilgå hostede kunders løsninger, får tildelt en personlig bruger mere. Denne bruger anvendes til at tilgå en jumphost, som står i et trafikensrettet netværk, der kun kan tilgås fra Netcompanys interne netværk. Løsningen benyttes til at tilgå specifikke kunders domæner.

I forbindelse med fratrædelse fjernes relevante adgange fra den pågældende medarbejder.

Der er på centrale systemer etableret logning af sikkerhedsmæssige hændelser efter best practice.

Privilegerede adgange styres gennem Netcompanys PAM-løsning, som sikrer centraliseret styring, flerfaktorautentifikation og audit af anvendte brugeradgange. De privilegerede adgange gennemgås jævnligt.

Hemmelig autentifikationsinformation om brugere distribueres over sikre og krypterede kanaler og opbevares i sikrede vaults og keystores.

Netcompany har datacenterfaciliteter hos professionelle co-location-udbydere. Løsningerne er placeret under omfattende fysisk sikring, således at det ikke er muligt at tilgå de fysiske systemer uden forudgående godkendelse. Antallet af de medarbejdere, der har adgang til faciliteterne, er stærkt begrænset. Løsningen til Digitaliseringsstyrelsen på Digital Post-området afvikles på udstyr, der fysisk er placeret hos InterXion og GlobalConnect.

3.10. Kryptografi

Netcompanys sikkerhedsprocedurer indeholder krav om kryptering af informationer. Administration af krypteringsnøgler foretages af de enkelte kundeteams og af Netcompany Operations på de fælles systemer. Dette sikrer, at den kryptering, som anvendes, er effektiv og efterlever krav til robust sikkerhed.

3.11. Fysisk sikring og miljøsikring

Der er ikke placeret kritisk teknisk infrastruktur på Netcompanys kontorlokationer. Netcompany har på alle kontorer en perimetersikring, som omfatter adgangskontroller og alarminstallationer. Netcompanys medarbejdere arbejder med fortrolige informationer, og derfor foreligger der et krav om, at fortrolige og følsomme informationer ikke må forefindes frit liggende uden opsyn. Der er ligeledes implementeret en teknisk politik, som sikrer, at eksempelvis computerskærme låser efter en kort periode med inaktivitet.

Netcompany benytter ekstern housing til behandlingsaktiver, og Netcompany kontrollerer, at den fysiske sikring og miljøsikring er tilstrækkelig og fungerende ved årligt at få eksterne revisionserklæringer fra de pågældende co-location-udbydere. Digital Post-løsningen til Digitaliseringsstyrelsen afvikles hos InterXion og GlobalConnect.

3.12. Driftssikkerhed

Netcompany har stort fokus på driftssikkerhed, og driftsprocedurer er dokumenteret i Netcompanys ITSM-system, hvor alle relevante personer har adgang. I Netcompanys ITSM styres og kontrolleres den overordnede driftssikkerhed, og ITSM benyttes til styring af incidents samt løbende dokumentation af driften gennem driftshåndbøger, der dækker de enkelte løsninger.

Netcompany styrer gennem ITSM-systemet de forskellige driftsmiljøer, som eksisterer i forbindelse med udvikling og drift. Derfor har Netcompany oprettet deciderede miljøer til udvikling, test, præproduktion og produktion. Rettigheder er ligeledes styret gennem de forskellige miljøer for at beskytte mod uautoriseret adgang.

Alle de systemer, som anvendes af Netcompany, er beskyttet mod malware, og der følges løbende op på, at beskyttelsen er tilstrækkelig i forhold til det aktuelle trusselsbillede. Som led i beskyttelsen informeres medarbejdere løbende om, hvorledes de skal opdage og agere i forhold til malware.

Backup af systemer, der hostes i et af Netcompanys to datacentre hos GlobalConnect og InterXion, udføres og håndteres af Netcompany.

For hver kundeløsning aftales backupstrategier. Disse defineres i Toolkit pr. server og implementeres i henhold til aftalen med kunden. Alle ændringer til strategien eksekveres gennem change-processen.

Service Desk foretager en daglig kontrol af fejlede backups. Der anvendes automatisk genererede sager til opgavestyring. Fejlede backups oprettes som incidents og håndteres af backupansvarlige teknikere.

Der foretages periodevis restore-test af komplette systemkomponenter. Til formålet inddrages teknikere, der kender løsningen, og backupteknikere fra infrastrukturafdelingen. Formålet med restore-øvelsen er at sikre, at den etablerede backup kan anvendes som forventet, men også at træne teknikerne til eventuelle restore-scenarier i beredskabssituationer.

Netcompany overvåger alle kundesystemer, infrastruktur og services. Overvågning af en løsning sættes initialt op baseret på en fast skabelon, der angiver væsentlige målepunkter, som Netcompany Operations har vurderet som tilstrækkelige til at vurdere, om en løsning er sikret. Den enkelte leveranceansvarlige kan fravige målepunkter, hvis det vurderes sikkert. Når et givent målepunkt overskrides, genereres en alarm, som automatisk lægger en sag til Service Desk. Hvis alarmen er kritisk, eskalerer Service Desk sagen til den ansvarlige for løsningen.

For de enkelte delløsninger kan der udarbejdes applikationsspecifik overvågning. Punkterne er enten af teknisk eller forretningsmæssig karakter. Applikationsspecifik overvågning er ikke omfattet af nærværende erklæring.

Der er ligeledes opsat logovervågning, og der rejses alarmer, hvis bestemte logmønstre opstår i overvågede logge. Denne type overvågning anvendes ofte i transaktions- eller batchbaseret overvågning.

Overvågning anvendes både i forbindelse med fejl og udfald på systemer, men også for at danne et uvildigt datagrundlag for de aftalte tekniske SLA-mål og rapporteringen herom.

Netcompany vurderer løbende tilgængelige sikkerhedsrettelser til anvendte operativsystemer og software for at sikre passende styring af tekniske sårbarheder. I tillæg anvendes løbende sårbarhedsscanninger af operativsystemer og software i serverinfrastrukturen. Patchning sker løbende efter en patch management-plan, der er tilpasset løsningen – og opgradering sker som en integrerende del af release management-processen.

Softwareinstallationer begrænses via central registrering af software i Netcompanys CMDB og via anvendelse af politikker til afvikling af software i serverinfrastrukturen.

Alle servere synkroniseres tidsmæssigt via centrale NTP-servere, hvilket sikrer konsistente tidsstempler på tværs af serverinfrastrukturen.

3.13. Change management

Ændringer til driftsmiljøet foretages gennem en styret change management-proces. Digitaliseringsstyrelsen opretter en ændringsanmodning, der går gennem den aftalte change management-proces. Netcompany kan også oprette changes, i tilfælde af at:

- Der er behov for en change for at løse en (eller flere) serviceydelser.
- Der identificeres behov for en change ift. proaktivt at undgå incidents/problemer eller forbedre den nuværende funktionalitet i Digital Post.
- Der er behov for at gennemføre en decideret change for at løse et incident eller problem.
- Der gives en anbefaling til Digitaliseringsstyrelsen om en ændring til Digital Post.

3.14. Leverandørforhold

Netcompany anvender udelukkende leverandører, som kan efterleve Netcompanys sikkerhedspolitik, herunder vedrørende fortrolighed. De anvendte leverandøraftaler gennemgås regelmæssigt, således at det sikres, at de er relevante, og at de sikkerhedsmæssige krav fortsat er de gældende. Visse leverandører skal levere en uafhængig revisionserklæring årligt.

I forbindelse med Digital Post leveret til Digitaliseringsstyrelsen modtages og gennemgås relevant erklæring fra hhv. InterXion og GlobalConnect på årlig basis. Desuden sikrer Netcompany løbende, at vores co-location-udbydere leverer den lovede perimetersikkerhed. Ydermere udføres der selvkontrol, når Netcompany er til stede hos en af vores co-location-udbydere.

3.15. Styring af informationssikkerhedsbrud

Ledelsen har gennem godkendelse af sikkerhedspolitikken ligeledes godkendt proceduren for styring af informationssikkerhedsbrud. I Netcompany anvendes ITSM-systemet Toolkit til indrapportering og styring af sikkerhedshændelser, både i de enkelte kundeforhold og på det driftsmæssige område, som er relevant på tværs af kunder. Det er Netcompanys CISO, som har ansvaret for at vurdere sikkerhedsbrud og for den videre håndtering af de enkelte hændelser.

Netcompanys CISO anvender bl.a. sikkerhedsbrud til løbende at vurdere trusselsbilledet og sikre, at risici håndteres.

3.16. Informationssikkerhedsaspekter ved nødberedskab og reetableringsstyring

Netcompany har udarbejdet katastrofeberedskabsplaner til videreførelse af drift og fortsat leverance af service til kunder i en katastrofesituation. Katastrofeberedskabsplaner sikrer også, at sikkerhedsniveauet opretholdes i forbindelse med en katastrofe, og Netcompanys CISO indgår som ledelsesperson i planerne. Planerne sikrer nødvendig redundans, hvilket bl.a. sikres gennem årlige tests af planerne. Der er udarbejdet en specifik beredskabsplan for Digital Post

3.17. Gennemgang af informationssikkerhed

Netcompanys CISO har ansvaret for løbende at sikre, at virksomhedens kontroller, politikker, processer og procedurer er i overensstemmelse med forretningens krav. Dette inkluderer krav om at sikre, at de implementerede procedurer og processer er effektive i forhold til informationssikkerhedspolitikken og andre tilsvarende politikker.

Der foretages som minimum en årlig gennemgang af relevante dokumenter, som endvidere forelægges for ledelsen til formel godkendelse.

3.18. Komplementerende kontroller hos Digitaliseringsstyrelsen

Netcompanys kontroller er designede under forudsætning af, at der visse interne kontroller, der er implementeret hos kunderne, i dette tilfælde hos Digitaliseringsstyrelsen. Implementeringen af kontrollerne er i nogle tilfælde nødvendig for at kunne opnå kontrolmålene i afsnit 4, da kunden har et medansvar for kontrollerne i henhold til kontrakten.

Det kan nævnes, at der også i forbindelse med de forretningsmæssige processer og applikationskontroller i løsningen findes forhold, som Digitaliseringsstyrelsen skal varetage. Idet nærværende erklæring alene omhandler de generelle it-kontroller, er sådanne kontroller ikke medtaget hér.

Der kan være yderligere kontrolmål og relaterede kontroller hos Digitaliseringsstyrelsen, som kan være hensigtsmæssige for transaktioner, og som ikke er angivet i denne beskrivelse. Det er op til Digitaliseringsstyrelsen og/eller dennes revisor at vurdere det konkrete kontraktgrundlag samt behovet for lokalt implementerede kontroller i forbindelse med Digital Post.

Dette afsnit beskriver således forslag til visse kontroller, som Digitaliseringsstyrelsen kan have implementeret for at opnå de kontrolmål, som er angivet i beskrivelsen. Kontrolovervejelser, som er anført nedenfor, skal således ikke ses som en fyldestgørende liste over kontroller, der skal være implementeret hos Digitaliseringsstyrelsen:

- Brugeradministration af egne brugere. Brugeradministration ift. redaktører af Digital Post udføres af Digitaliseringsstyrelsen. Digitaliseringsstyrelsen skal have etableret processer og kontroller der sikrer oprettelse og nedlæggelse af brugere finder sted på passende tidspunkter, samt at brugeradgange gennemgås på periodisk basis
- Overvågning af lovgivning og krav ifm. ny funktionalitet. Det er Digitaliseringsstyrelsens ansvar at identificere behov for ny udvikling på baggrund af lovgivningsændringer eller på baggrund af nye krav
- Incidenthåndtering: I forbindelse med håndtering af incidents, er det Digitaliseringsstyrelsens ansvar at oprette incidents som Digitaliseringsstyrelsen opdager i rette tid i Service Desk-løsningen, således at Netcompany kan påbegynde undersøgelser og udbedring. Endvidere er det Digitaliseringsstyrelsens ansvar at reagere på Netcompanys henvendelser i forbindelse med fejlsøgning med videre for at sikre effektiv løsning af incidents.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Introduktion

Denne erklæring er udformet med henblik på at informere Digitaliseringsstyrelsen om Netcompanys udvalgte kontroller, som kan påvirke behandlingen af data, og samtidig informere om udvalgte kontroller, vi har efterprøvet, og resultatet af vores handlinger. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i kundernes forretningsprocesser, har til hensigt at hjælpe kundernes revisor med at vurdere risici for fejl, som muligvis påvirkes af kontroller hos Netcompany.

Vores test af Netcompanys kontroller er begrænset til de kontrolmål og tilknyttede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller til de generelle it-kontroller, som skal være implementeret i brugerorganisationerne for at opfylde kontrolmålene. Det er hver brugerorganisations revisors ansvar at evaluere denne information i forhold til de kontroller, som eksisterer i hver brugerorganisation. Hvis bestemte supplerende kontroller ikke er til stede i brugerorganisationerne, kan Netcompanys kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De test, der udføres i forbindelse med fastlæggelsen af kontrollers funktionalitet, består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos Netcompany
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3 Test af udformning og implementering

Vores test af de udvalgte kontrollers udformning og implementering inkluderer de test, som vi betragter som nødvendige for at vurdere, om de udførte kontroller og overholdelsen heraf er tilstrækkelige til at give høj, men ikke absolut sikkerhed for, at de specificerede kontrolmål blev opnået for perioden fra 1. januar 2022 til 31. december 2022 set i sammenhæng med de forhold, der er omfattet af den generelle erklæring fra Netcompany vedrørende generelle it-kontroller relateret til hosting og drift for 2022.

4.4 Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
5.1 Retningslinjer for styring af informationssikkerhed Formål: At give retningslinjer for at understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.				
5.1.1	Politikker for informationssikkerhed	Netcompany fastlægger en sikkerhedspolitik for informationssikkerhed, som er godkendt af Digitaliseringsstyrelsen og understøtter den gældende risikovurdering.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret dokumentation for, at Netcompany har udarbejdet en politik for informationssikkerhed, og at politikken understøtter risikovurderingen. Vi har inspiceret, at politikken er godkendt af Digitaliseringsstyrelsen.	Ingen afvigelser konstateret.
5.1.2	Gennemgang af politikker for informationssikkerhed	Netcompanys sikkerhedspolitik for Løsningen skal gennemgås med planlagte mellemrum og minimum én (1) gang årligt samt i tilfælde af væsentlige ændringer, for at sikre politikkernes fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret seneste ajourførte it-sikkerhedspolitik, som er godkendt i 2022. Vi har inspiceret, at it-sikkerhedspolitikken løbende bliver gennemgået på security committee meetings. Vi har vurderet, om it-sikkerhedspolitikken er betryggende i relation til Netcompanys forretning og valgte kontrol-framework.	Ingen afvigelser konstateret.
7.1 – Før ansættelsen Formål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, der er i betragtning til.				
7.1.1	Baggrundstjek og sikkerhedstjek af Leverandørens medarbejdere (Screening)	For medarbejdere der skal have adgang til løsningen, skal der udføres et identitetsbaseret tjek, tjek af uddannelse og tjek af strafferegistre. For medarbejdere der administrerer krypteringsnøgler i løsningen, skal der i tillæg indhentes sikkerhedsgodkendelse på niveau 3 (HEM). Det skal kontrolleres, at ledere og medarbejdere, der udfører betroede opgaver, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv, samt at	Vi har forespurgt ansvarlige Netcompany medarbejdere om kontrollen. Vi har inspiceret it-sikkerhedspolitik og observeret, at der er beskrevet krav om screening af medarbejdere. Vi har stikprøvevist inspiceret dokumentation for, at der er udført screening af kompetencer samt uddannelse for medarbejdere, der er tiltrådt i erklæringsperioden. Vi har stikprøvevis inspiceret månedlige driftsrapporter til Digitaliseringsstyrelsen og observeret, at rapporterne omfatter en liste over medarbejdere med angivelse af, at disse er sikkerhedsgodkendt. Vi har stikprøvevis inspiceret en liste over medarbejdere, der har adgang til løsningen. Vi har stikprøvevis inspiceret relevant dokumentation og observeret, at medarbejdere er sikkerhedsgodkendte, herunder er godkendt til sikkerhedsniveauet 3 "Secret/Hemmelig".	Ingen afvigelser konstateret.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
		medarbejdere og ledere har tilstrækkelig uddannelse og erfaring.		
8.3 - Mediehåndtering Formål: At forhindre autoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.				
8.3.2	Bortskaffelse af medier	Medier skal bortskaffes på ansvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer. Alle medier, som indeholder personlige, kryptografiske eller andre fortrolige eller følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde (hvis medier er bortskaffet).	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret dokumentation for, at der er etableret procedure for destruktion af data på servere og udstyr og har noteret os, at der anvendes en ekstern part til destruktion af medier, som kan indeholde forretningsdata. Vi har fået oplyst, at der ikke har været foretaget transport eller destruktion af medier i 2022.	Ingen afvigelser konstateret.
9.2 Administration af brugeradgang Formål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.				
9.2.1	Brugerregistrering og -afmelding	Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har på forespørgsel fået oplyst, at Netcompany har en overordnet politik for adgangsstyring, som er gældende på tværs af alle kundeløsninger, herunder for Digital Post. Vi har inspiceret sikkerhedspolitikken og observeret, at der er beskrevet procedure for brugeradministration, herunder registrering og afmelding af brugere.	Ingen afvigelser konstateret.
9.2.2	Tildeling af brugeradgang	Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester i relation til Løsningen.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har på forespørgsel fået oplyst, at Netcompany har en overordnet politik for adgangsstyring, som er gældende på tværs af alle kundeløsninger, herunder for Digital Post. Vi har inspiceret sikkerhedspolitikken og observeret, at der er beskrevet procedure for brugeradministration, herunder tildeling eller tilbagekaldelse af adgangsrettigheder. Vi har stikprøvevist inspiceret, at brugeradgange og rettigheder er blevet ledergodkendt inden tildeling.	Ingen afvigelser konstateret.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
9.2.3	Styring af privilegerede adgangsrettigheder	Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har på forespørgsel fået oplyst, at Netcompany har en overordnet politik for adgangsstyring, som er gældende på tværs af alle kundeløsninger, herunder for Digital Post. Vi har stikprøvevis inspiceret relevant dokumentation og observeret, at brugeradgange og rettigheder er blevet godkendt inden tildeling. Vi har stikprøvevist inspiceret, at privilegerede brugeres aktivitet overvåges.	Ingen afvigelser konstateret.
9.2.4	Styring af hemmelig autentifikationsinformation om brugere	Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret procedure for tildeling af hemmelig autentifikationsinformation. Vi har observeret, at tildeling af adgangskoder sker via AD-portalen.	Ingen afvigelser konstateret.
9.2.5	Gennemgang af brugerrettigheder	Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplan, herunder proceduren for løbende gennemgang af brugeradgange og rettigheder. Vi har stikprøvevist inspiceret dokumentation for periodiske gennemgang af brugeradgange og rettigheder.	Ingen afvigelser konstateret.
9.2.6	Inddragelse eller justering 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.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret datasikkerhedsplan og Netcompanys sikkerhedsprocedure, herunder proceduren for brugeradministration til løsningen. Vi har stikprøvevist inspiceret relevant dokumentation og observeret, at nedlæggelse af brugeradgange og rettigheder er sket uden unødigt ophold.	Ingen afvigelser konstateret.
10.1 Kryptografi Formål: At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.				
10.1.1	Politik for håndtering af livscyklus for krypteringsnøgler	Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og observeret, at der er defineret en politik for anvendelse af kryptografi til beskyttelse af informationer. For test af implementering af anvendelse af kryptografi henvises til kontrol 10.1.2.	Ingen afvigelser konstateret.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
10.1.2	Politik for håndtering af livscyklus for krypteringsnøgler	Der er udarbejdet og implementeret en politik for anvendelse, beskyttelse og levetid for krypteringsnøgler, der anvendes til Løsningen. Politikken omfatter hele livscyklussen for en krypteringsnøgle og efterleves i hele dennes livscyklus.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og observeret, at der er defineret en politik for anvendelse af kryptografi til beskyttelse af informationer. Vi har stikprøvevis inspiceret dokumentation for anvendelse af kryptering af informationer, herunder certifikaters gyldighed og anvendte krypteringsalgoritmer. Vi har endvidere observeret, at der alene anvendes anerkendte krypteringsalgoritmer til kryptering af information.	Ingen afvigelser konstateret.
12.2 Malwarebeskyttelse Formål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.				
12.2.1	Kontroller mod malware	Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og politik for informationssikkerhed og observeret, at der er beskrevet en procedure for beskyttelse mod malware. Vi har inspiceret relevant dokumentation og observeret, at der er implementeret anti-malwaresoftware på servere/databaser for udvalgte stikprøver.	Ingen afvigelser konstateret.
12.3 Backup Formål: At beskytte mod tab af data.				
12.3.1	Backup af information	Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret proceduren for backupstrategien i løsningen. Vi har stikprøvevist inspiceret relevant dokumentation og observeret, om backup for servere/databaser er opsat i henhold til backupstrategien. Vi har inspiceret den årlige restore-testrapport og observeret, at restore-testen er blevet udført i august 2022 på udvalgte servere. Det er yderligere observeret, at alle servere blev restoret uden problemer.	Ingen afvigelser konstateret.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
12.4 Logning og overvågning Formål: At registrere hændelser og tilvejebringe bevis.				
12.4.1	Hændelseslogning	Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret datasikkerhedsplanen og politik for informationssikkerhed og observeret, at der er beskrevet en procedure for logning. Vi har stikprøvevist inspiceret, at der er etableret hændelseslogning for servere og databaser. Vi har observeret, at der er implementeret SIEM-løsning, som sikrer, at der sker alarmering ved bestemte typer hændelser.	Ingen afvigelser konstateret.
12.4.2	Beskyttelse af logoplysninger	Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang. Informationer (herunder logs) skal opbevares og beskyttes, så længe de er nødvendige af hensyn til revision eller efterforskning af sikkerhedshændelser, under hensyntagen til lovgivningens begrænsninger, hvorefter de skal slettes sikkert.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret procedure for logning og observeret, at der er beskrevet sikkerhedsforanstaltninger og anvendelse af SIEM-værktøjet, som er rettet mod beskyttelse mod manipulation og uautoriseret adgang til logge. Vi har stikprøvevist inspiceret lister over medarbejdere med adgang til logge og har på baggrund af forespørgsler fået oplyst, at disse medarbejdere har arbejdsbetingede behov for adgangen. Vi har observeret, at der er implementeret SIEM-løsning, som sikrer, at der sker alarmering ved bestemte typer hændelser. Vi har inspiceret relevant dokumentation og observeret, at logs slettes efter 6 måneder.	Ingen afvigelser konstateret.
12.4.3	Administrator- og operatørlog	Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås Regelmæssigt.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret datasikkerhedsplanen og politik for informationssikkerhed og observeret, at der er beskrevet en procedure for logning. Vi har observeret, at der er implementeret SIEM-løsning (Splunk), som sikrer, at der sker alarmering ved bestemte typer hændelser. Vi har stikprøvevis inspiceret relevant dokumentation og observeret, at der i toolkit bliver generet en PAM rapport med oversigt over brugen af 'emergency accounts' og at denne bliver gennemgået og godkendt af en ansvarlig operations medarbejder, hvorefter sagen lukkes.	Ingen afvigelser konstateret.
12.4.4	Tidssynkronisering	Urene i alle relevante informationsbehandlingssystemer i relation til Løsningen eller et sikkerhedsdomæne er synkroniseret til en enkelt referencetidskilde.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret procedurerne vedrørende tidssynkronisering i løsningerne.	Ingen afvigelser konstateret.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
			Vi har stikprøvevist inspiceret dokumentation for, at der er i forbindelse med løsningen er etableret tids-synkronisering.	
12.6 Sårbarhedsstyring Formål: At forhindre, at tekniske sårbarheder udnyttes.				
12.6.1	Styring af tekniske sårbarheder	Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer. Netcompanys eksponering for sådanne sårbarheder evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Vi har forespurgt ansvarlige Netcompany-medarbejdere til kontrollen. Vi har inspiceret politik for informationssikkerhed og observeret, at der er beskrevet en procedure for styring af tekniske sårbarheder. Vi har stikprøvevis inspiceret relevant dokumentation og observeret, at identificerede sårbarheder bliver adresseret og kommunikeret.	Ingen afvigelser konstateret.
12.6.2	Begrænsninger på softwareinstallation	Der er fastlagt og implementeret regler om softwareinstallation, som foretages i driftsmiljøerne.	Vi har forespurgt ansvarlige Netcompany-medarbejdere til kontrollen. Vi har inspiceret sikkerhedspolitikken og observeret, at der er beskrevet en procedure for softwareinstallationer. Vi har inspiceret dokumentation for, at der i Netcompanys sikkerhedspolitik er taget stilling til softwareinstallation foretaget af medarbejdere. Herudover har vi inspiceret dokumentation for, at der findes central registrering af software, som må installeres.	Ingen afvigelser konstateret.
14.2 Sikkerhed i udviklings- og hjælpeprocesser Formål: At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.				
14.2.1	Sikker udviklingspolitik	Der er fastlagt og anvendt regler for udvikling af software og systemer.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og sikkerhedspolitikken og observeret, at der er beskrevet en procedure for udvikling. Vi har inspiceret dokumentation, hvoraf det fremgår, at relevante medarbejdere hos Netcompany løbende modtager uddannelse med fokus på sikker udvikling.	Ingen afvigelser konstateret.
14.2.2	Procedure for styring af systemændringer	Ændringer af systemer inden for udviklingslivscyklussen styres ved hjælp at formelle procedurer for ændringsstyring.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har for udvalgte stikprøver inspiceret relevant dokumentation og observeret, at ændringer udvikles, testes og godkendes i overensstemmelse med proceduren for udvikling.	Ingen afvigelser konstateret.

ID	Kontrolaktivitet	Etableret kontrol hos Netcompany	Udført test	Resultat af test
17.1 - Informationssikkerhedskontinuitet Formål: Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring				
17.1.3	Verificer, gennemgå og evaluer	Organisationen skal verificere de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer. Der skal foreligge en beredskabsplan, som dækker alle væsentlige områder.	Vi har forespurgt ansvarlige Netcompany-medarbejdere om kontrollen. Vi har inspiceret den løsningsspecifikke beredskabsplan for Digital Post og observeret, at planen er godkendt og opdateret i 2022. Vi har yderligere observeret, at beredskabsplanen omfatter de mest gængse katastrofescenarier, hvor handlingsplanerne fokuserer på den tekniske reetablering af tilgængelighed, fortrolighed og integritet. Vi har inspiceret testrapporten for den udførte it-beredskabstest og observeret, at testen er blevet udført i april 2022 på baggrund af udvalgte scenarier fra Digitaliseringsstyrelsen. Vi har yderligere inspiceret toolkit-sagen for it-beredskabstesten og observeret, at rapporten er blevet delt med Digitaliseringsstyrelsen, som har godkendt denne.	Ingen afvigelser konstateret.