IT Relation A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2023 til 31. december 2023 i relation til IT Relations hosting-ydelser

Januar 2024

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt IT Relation A/S' hosting-ydelser, 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 ved vurdering af risicene for væsentlig fejlinformation i kundernes regnskaber.

IT Relation A/S anvender Fuzion og InterXion som serviceunderleverandører af housing-ydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Fuzion og InterXion varetager for IT Relation A/S.

IT Relation A/S anvender B4Restore og Keepit som serviceunderleverandører af backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore og Keepit varetager for IT Relation A/S.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

IT Relation A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af hosting-ydelserne, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til hosting-ydelserne var udformet og implementeret, herunder redegør for:

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

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til hosting-ydelserne foretaget i perioden fra 1. januar 2023 til 31. december 2023

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til hosting-ydelserne, 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 generelle it-kontroller i relation til hosting-ydelserne, som den enkelte kunde måtte anse vigtigt efter sine 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 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2023 til 31. december 2023.

Herning, den 31. januar 2024
IT Relation A/S

Frank Bech Jensen
Head of Compliance and Security

IT Relation A/S
Dalgas Plads 7B, 1. sal
7400 Herning

2 Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2023 til 31. december 2023 i relation til IT Relation A/S' hosting-ydelser

Til: IT Relation A/S (IT Relation), IT Relations kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om IT Relations beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til hosting-ydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2023 til 31. december 2023 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

IT Relation A/S anvender Fuzion og InterXion som serviceunderleverandører af housing-ydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Fuzion og InterXion varetager for IT Relation.

IT Relation anvender B4Restore og Keepit som serviceunderleverandører af backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore og Keepit varetager for IT Relation.

Enkelte af de kontrolmål, der er anført i IT Relations beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med IT Relations kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

IT Relations ansvar

IT Relation er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør" som er udstedt af IAASB, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sine hosting-ydelser samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, 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 opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som IT Relation har specificeret og beskrevet i ledelsens udtalelse.

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

IT Relations 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 hosting-ydelserne, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

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

a) at beskrivelsen af de generelle it-kontroller i relation til hosting-ydelserne, således som de var udformet og implementeret i hele perioden fra 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2023 til 31. december 2023, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2023 til 31. december 2023.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt IT Relations hosting-ydelse, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 31. januar 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

3 IT Relations beskrivelse af generelle it-kontroller hos IT Relation A/S vedrørende regnskabsaflæggelsen for virksomhedens hostingydelser

Fra 1. januar 2023 til 31. december 2023 har virksomheden leveret serviceydelser i overensstemmelse med de systemer til styring af informationssikkerheden, der er dokumenteret i systembeskrivelsen i ISAE 3402-erklæringen for 2023, og i overensstemmelse med ISO 27001:2022.

Organisationsændringer hos IT Relation, Me'ning & itm8

Den 15. november 2023 meddeler itm8, at virksomheden igangsætter en omfattende virksomhedsfusion, der involverer alle deres selskaber. Dette indebærer konkret, at itm8 fra denne dato begynder processen med at fusionere deres 13 selskaber til en samlet enhed under navnet itm8.

Fusionsprocessen vil blive gennemført i løbet af 2024. På trods af at denne meddelelse er udsendt den 15. november 2023, forventes det ikke at påvirke leverancer, der er blevet revideret i perioden fra 1. januar 2023 til og med 31. december 2023, som er omfattet af denne revisionserklæring.

Den konsoliderede itm8-virksomhed vil på sigt levere alle sine ydelser gennem fire centrale serviceområder:

- Cloud & Infrastructure
- IT Security
- Digital Transformation
- Application Services.

Ved at samle alle aktiviteter under ét fælles itm8 har vi ambitionen om at skabe en ekstraordinær og attraktiv arbejdsplads for de mest kompetente it-specialister. Dette initiativ sigter mod at styrke vores leverancer og service, hvilket vores kunder vil opleve positivt.

Eftersom den reviderede leverance ikke ændres inden for revisionsperioden, vil virksomhederne IT Relation A/S, Me'ning og itm8 fortsat være benævnt i erklæringen, som de plejer.

Yderligere information om itm8's virksomhedsfusion kan findes ved at følge dette link: itm8 unites 13 companies in a major merger

3.1 Introduktion til IT Relation A/S

IT Relation A/S er en førende it-virksomhed med dedikation til at optimere kunders forretning ved hjælp af it-løsninger. Vores ekspertise omfatter it-strategi, hosting, servicedesk, support og hardware. Med en medarbejderstab på 700 personer – spredt over hele Danmark med kontorer i Herning, Aarhus, København, Kolding og Aalborg samt international tilstedeværelse i Tjekkiet og Filippinerne – arbejder vi målrettet for at imødekomme vores kunders behov.

IT Relation A/S opererer inden for fire nøgleforretningsområder:

- Managed Services (it-outsourcing og hosting)
- Servicedesk

- It-sikkerhed
- Hardware.

Vores mål er at fungere som en fuldkommen end-to-end-leverandør af it-løsninger ved at implementere en 360-graders tilgang. Vores kompetente og smilende it-problemknusere er tilgængelige døgnet rundt 365 dage om året i vores servicedesk.

Vi stræber efter at levere optimale it-løsninger og uovertruffen kundeservice hver eneste dag.

3.2 Introduktion til itm8

IT Relation A/S er en integreret del af itm8, en betydelig it-koncern, der består af 12 selskaber og over 1700 medarbejdere. Itm8's kerneopgave er at konsolidere ekspertise inden for it under én paraply, hvilket muliggør levering af komplette end-to-end-løsninger til vores kunder. Inden for denne struktur bidrager IT Relation A/S som et væsentligt led i koncernens samlede portefølje.

Itm8-koncernen med over 100 dedikererede medarbejdere er fokuseret på at fremme operationel effektivitet og skabe synergier blandt sine datterselskaber. Dette opnås gennem en række interne servicefunktioner, herunder:

- Datacenter
- Intern udvikling
- Intern IT
- Human Resource
- Marketing
- Finance
- Legal
- Compliance & Security.

I forbindelse med ISAE 3402-regnskabsaflæggelsen inkluderes itm8's koncernfunktioner, idet IT Relation A/S udnytter disse interne services i fuldt omfang, og idet itm8's servicefunktioner ligeledes er omfattet af IT Relations informationssikkerhedsledelsessystem. Denne integrerede tilgang sikrer en sammenhængende og effektivt supportstruktur, der er afgørende for IT Relation A/S' ydelser og succes.

3.3 Introduktion til Me'ning

IT Relation A/S er moderselskab for Me'ning, en dynamisk virksomhed specialiseret i udviklingen af Microsoft-baserede og skræddersyede løsninger. Me'ning engagerer sig i hele spektret af it-udviklingsprocessen, lige fra initial behovsafklaring til detaljeret opfølgning, og sikrer dermed levering af løsninger, der både er af høj kvalitet og præcist tilpasset kundens unikke krav.

Me'nings ekspertise strækker sig over både digital transformation og specialiseret udvikling, hvilket gør dem i stand til at skabe effektive og brugerspecifikke systemer. Deres udvalg af Microsoft-løsninger inkluderer, men er ikke begrænset til:

- Modern Workplace
- CRM-løsninger
- Data og analyse
- Baseline-værktøjer (herunder reporting, GDPR, Workplace, Whistleblower)
- SharePoint-udvikling
- Specialudvikling.

Ud over disse udvikler og vedligeholder Me'ning også en række egenudviklede systemer såsom Sikker Mail, patientjournalløsninger, OnlineLegat og VirkCollect.

Med en talentfuld stab på 70 medarbejdere fordelt på over 3 kontorer i København, Aarhus og Herning står Me'ning stærkt i markedet. I forbindelse med ISAE 3402-regnskabsaflæggelsen omfattes Me'ning også, da

det som datterselskab til IT Relation A/S fuldt ud anvender det samme ledelsessystem som både itm8-koncernfunktionen og IT Relation A/S. Dette sikrer konsistent og høj standard i alle operationelle og forvaltningsmæssige aspekter.

3.4 Introduktion til beskrivelse af serviceydelser

Dette dokument er udarbejdet med det formål at levere nødvendige oplysninger til IT Relations kunder og deres revisorer i overensstemmelse med kravene i revisionsstandarden for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402. Beskrivelsen omfatter detaljer vedrørende det etablerede system- og kontrol miljø for IT Relations drifts- og hosting-ydelser, som leveres til kunderne.

Dokumentet indeholder omfattende beskrivelser af de processer og procedurer, der implementeres for at sikre en tilfredsstillende drift af systemerne. Formålet med denne beskrivelse er at give tilstrækkelige oplysninger, så revisorer for hosting-kunder selvstændigt kan vurdere dækningen af risici for svagheder i kontrolmiljøet. Dette er særligt relevant, såfremt sådanne svagheder kunne udgøre en risiko for væsentlig fejlinformation i hosting-kundernes it-drift i perioden fra 1. januar 2023 til 31. december 2023.

3.5 Beskrivelse af IT Relations serviceydelser

Siden etableringen i 2003 har IT Relation været en fremtrædende aktør i hosting-industrien, hvor vi har leveret avancerede it-løsninger til en bred vifte af brancher. Vores ekspertise strækker sig langt ud over hosting, da vi tilbyder et diversificeret spektrum af it-relaterede tjenester.

Vores serviceydelser til hosting-markedet omfatter:

- Hosting og housing
- Fjernbackup
- Drift og driftsadministration
- Cloud-baserede løsninger
- Servicedesk.

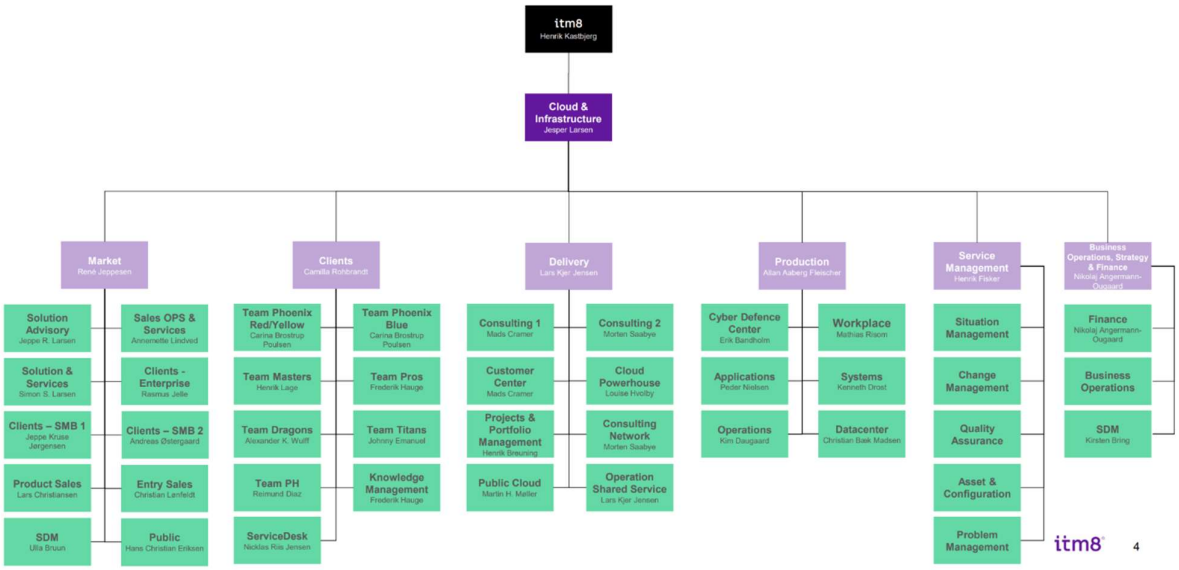
Vores systembeskrivelse giver en detaljeret oversigt over anvendte arbejdsprocesser og de gennemførte kontroller i forbindelse med disse tjenester.

Ud over de nævnte tjenester tilbyder IT Relation også assistance inden for følgende områder:

- Udvikling af it-løsninger
- Rådgivning og serviceydelser inden for it-sikkerhed på både ledelses- og teknisk niveau.
- Strategisk rådgivning på CIO-niveau
- Teknisk projektledelse
- Teknisk support og service on-site.

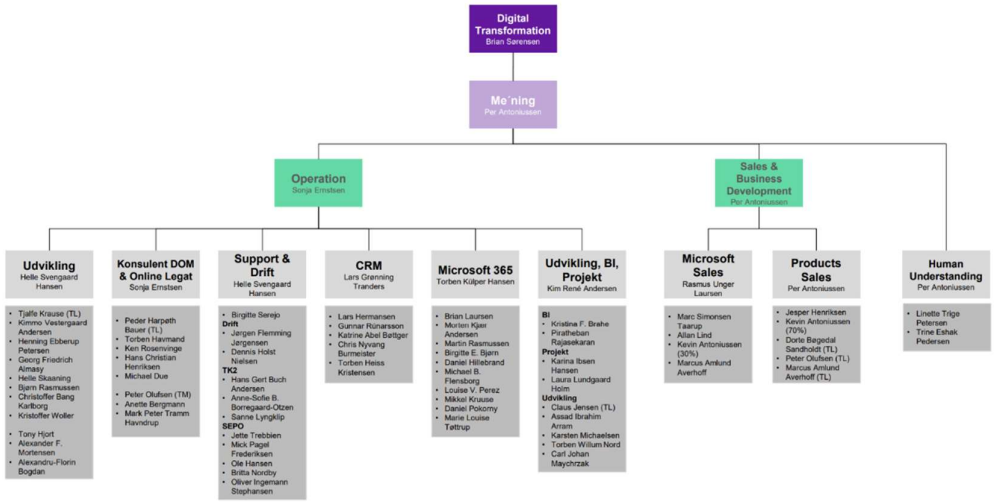
Vores mål er at levere omfattende og kvalitetsorienterede it-løsninger, der møder vores kunders unikke behov og understøtter deres forretning effektivt.

3.6 IT Relations organisation



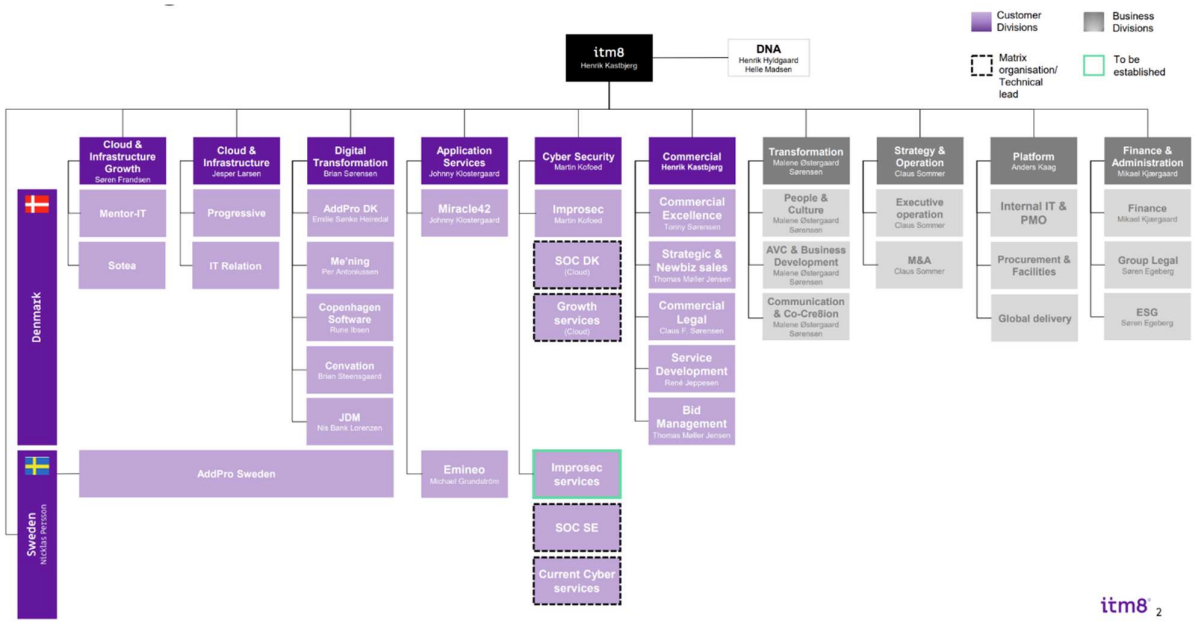
Organisationsdiagram – IT Relation A/S

3.7 Me'nings organisation



Organisationsdiagram – Me'ning

3.8 Itm8's organisation



Organisationsdiagram – itm8

3.9 Risikostyring i IT Relation

Risikostyring hos IT Relation er en flerdimensionel og systematisk proces, der foregår på tværs af forskellige områder og niveauer i organisationen. Årligt foretages der en grundig risiko- og trusselsvurdering af virksomhedens interne systemer. Denne vurdering er en samlet indsats, hvor input indsamles fra hele virksomheden. Sikkerhedsafdelingen faciliterer denne proces og udarbejder et første udkast, der præsenteres for IT Relations ledelse. Efter en intern gennemgang og diskussion, bliver denne vurdering officielt godkendt af ledelsen.

I forbindelse med projekter gennemføres der, baseret på projektets karakter, detaljerede sikkerhedsvurderinger samt en analyse af eventuelle særlige risici og usikkerheder. Disse vurderinger udføres efter en etableret og struktureret procedure.

På det operationelle niveau af projektstyring er der implementeret en kontinuerlig risikostyring. Denne styring følger en defineret projektstyringsmodel, hvor hovedansvaret for projektrelateret risikostyring er placeret hos projektlederen. I denne proces er det almindeligt, at projektlederen involverer projektdeltagere, eksterne samarbejdspartnere og eventuelt en styregruppe for at sikre en helhedsorienteret og effektiv risikohåndtering.

3.10 Kontrolramme, kontrolstruktur og kriterier for implementering af kontroller

IT Relation har etableret en informationssikkerhedspolitik og omfattende kontrolprocesser, der dækker alle systemer og tjenester leveret til kunder. Disse sikkerhedsforanstaltninger er under konstant forbedring og tilpasning, hvilket håndteres i samarbejde med højt kvalificerede specialister.

Som en ISO/IEC 27001:2022-certificeret virksomhed implementerer og overholder IT Relation standardens krav. Dette inkluderer etableringen af et informationssikkerhedsstyringssystem (ISMS), der muliggør:

- Overvågning og vurdering af informationssikkerhedsstatus
- Gennemførelse af interne audits
- Gennemførelse af interne revisioner for at evaluere sikkerhedstiltag og effektivitet
- Gennemførelse af ledelsesgennemgange med den øverste ledelse.

Formålet med ISMS er at garantere vedvarende overvågning og justering af informationssikkerhedsniveauet i forhold til det generelle trusselsbillede. Systemet er fundamentet for en kontinuerlig forbedringsproces, som sikrer effektiv håndtering af hændelser og en løbende forøgelse af informationssikkerhedsniveauet.

Årligt gennemgår IT Relation en it-revision, der resulterer i en revisionsrapport i henhold til ISAE 3402-standarden. De implementerede og reviderede kontrolforanstaltninger stemmer overens med bilag A i ISO/IEC 27001:2022-standarden.

Kontrolområderne og aktiviteterne fra denne kontrolramme er implementeret i overensstemmelse med bedste praksis for at minimere risici forbundet med IT Relations serviceydelser. De følgende kontrolområder fra den valgte model er integreret i det overordnede kontrolmiljø:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Personalesikkerhed
- Adgangsstyring
- Fysisk adgangskontrol og sikkerhed
- Sikring mod miljømæssige hændelser
- Driftssikkerhed
- Drift og overvågning
- Administration af programrettelser
- Strategi for ændringsstyring
- Netværk og kommunikationssoftware
- Systemsoftware
- Servicedesk og kundesupport
- Hændelseshåndtering
- Informationssikkerhedsaspekter ved beredskabsstyring.

Detaljerede beskrivelser af hvert af disse 15 områder findes herunder.

Informationssikkerhedspolitikker	
Formål	Der er på baggrund af en it-risikoanalyse udarbejdet en ledelsesgodkendt informationssikkerhedspolitik samt understøttende emnespecifikke politikker, som er kommunikeret til relevante medarbejdere i virksomheden.
Procedurer og kontroller	IT Relation identificerer relevante it-risici, som de fastlagte serviceydelser er udsat for. Dette håndteres via en aktuel trussels- og risikovurdering i IT Relation, dels i forbindelse med alle udviklingsprojekter og ændringer i systemmiljøer, dels ved en årlig genvurdering af risikoanalysen. Resultatet af den årlige gennemgang fremlægges for ledelsen. IT Relation giver også hosting-kundernes revisorer oplysninger til brug for deres vurdering af IT Relation som serviceleverandør. Ud over forhold vedrørende driften kan IT Relation også informere om sikkerhedsforhold, hvis det kræves af kunderne.
Tidspunkt for udførelse af kontrollen	Informationssikkerhedspolitikken samt emnespecifikke politikker genvurderes mindst en gang om året, inden der udføres it-revision og afgives erklæring.
Hvem udfører kontrollen?	Den årlige gennemgang udføres af Compliance & Security.

Kontroldokumentation	Informationssikkerhedspolitikken samt emnespecifikke politikker er underlagt dokumentkontrol.

Organisering af informationssikkerhed

Formål	At styre informationssikkerhed i virksomheden.
Procedurer og kontroller	Det primære ansvar for informationssikkerhed ligger hos direktionen i IT Relation. Dette sikrer, at procedurer og systemer altid understøtter overholdelse af den gældende it-sikkerhedspolitik. Compliance & Security beskriver de overordnede mål, og den driftsansvarlige er ansvarlig for udarbejdelse og implementering af relevante kontroller til overholdelse af informationssikkerhedspolitikken samt emnespecifikke politikker. Sikkerhedsniveauet skal være målbart og kontrollerbart, hvor dette er muligt, og det skal afspejle bedste praksis inden for de enkelte kontrolaktiviteter på de områder, hvor der tilbydes serviceydelser til kunderne. Informationssikkerhedsinitiativer drøftes løbende på Continuous Improvement-møder som afholdes i Compliance & Security, hvorefter nye og forbedrende initiativer kommunikeres ud og afstemmes med den driftsansvarlige samt ledelsen. Følgende medarbejdere er ansvarlige for forankringen af resultatet af Continuous Improvement-møder: • CTO: Anders Kaag • Head of Compliance & Security: Frank Bech Jensen • Information Security Manager: Nils Lau Frederiksen • Information Security Officer: Jeppe Gottlieb • Compliance Manager: Bo Duholm Hansen • Security Director: Johnni Meldgård Rude • Head of Cyber Defense Center: Erik M. L. Bandholm • Director of Internal IT: Thomas Møller • Technical Cloud Architect: Flemming Laursen • Cloud Citrix Specialist: Jakob Thalund Jensen • Datacenter Network Team Manager: Dan Sørup Olesen • Datacenter Specialist: Jakob Andersen.
Tidspunkt for udførelse af kontrollen	Continuous Improvement-møder afholdes hver anden måned.
Hvem udfører kontrollen?	Continuous Improvement-møder udføres af Compliance & Security, som kommunikerer til resten af de ansvarlige for informationssikkerhed.
Kontroldokumentation	Continous Improvement-møder dokumenteres i mødereferater, og udledte initiativer dokumenteres yderligere i aktivitetslogge.

Personalesikkerhed

Formål	At sikre, at medarbejdere og konsulenter forstår deres ansvarsområder og er egnede til de roller, de er tildelt. At sikre, at medarbejdere og konsulenter kender og lever op til deres ansvar i forhold til informationssikkerhed. At beskytte virksomhedens interesser i forbindelse med ansættelsesforholdets ændring eller ophør.

Procedurer og kontroller	En del af aftalen med både fastansatte og midlertidigt ansatte medarbejdere er at underskrive en ansættelseskontrakt og tilhørende ansættelsesvilkår. Ansvar og forpligtelser vedrørende it-sikkerhed er beskrevet i en erklæring, og ud over at beskrive tavsheds- og fortrolighedserklæringen omfatter vilkårene den gældende it-sikkerhedspolitik og retningslinjer. Straffeattester indhentes ved ansættelse samt kontrolleres hvert tredje år. Ledelsen skal sikre, at alle medarbejdere implementerer og opretholder informationssikkerhed i overensstemmelse med IT Relations informationssikkerhedspolitik. Ledelsesansvaret omfatter følgende for alle medarbejdere: • At de informeres tilstrækkeligt om deres roller og ansvar med hensyn til sikkerhed, inden de får adgang til virksomhedens systemer og data. • At de er blevet gjort bekendt med de nødvendige retningslinjer, så de kan leve op til IT Relations informationssikkerhedspolitik. • At de motiveres til at leve op til IT Relations informationssikkerhedspolitik og opnå et opmærksomhedsniveau i spørgsmål om it-sikkerhed, der er i overensstemmelse med deres rolle og ansvar i IT Relation. • At de overholder retningslinjerne og reglerne for rekrutteringen, herunder IT Relations informationssikkerhedspolitik. • Alle virksomhedens medarbejdere og eventuelt konsulenter bevidstgøres gennem passende træning og jævnlige opdateringer om de politikker og procedurer, der er relevante for deres jobfunktion. Medarbejderne kender og uddannes løbende i IT Relations informationssikkerhedspolitik.
Tidspunkt for udførelse af kontrollen	Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejderen eller konsulenten – og håndhæves. Når en medarbejder fratræder hos IT Relation, er medarbejderens direkte leder ansvarlig for, at alt udstyr returneres, og at de tilbagekaldte adgangsrettigheder til informationssystemer ophører. Opgaver og ansvar i forbindelse med ansættelsesforholdets ophør er beskrevet i fratrædelsespolitikken. Formålet er at sikre, at den fratrådte medarbejder kender og forstår sit ansvar efter sin fratrædelse fra IT Relation. Ved ansættelsens ophør skal det sikres, at den fratrådte medarbejder er informeret om gældende it-sikkerhedskrav og retsregler. Tavshedserklæringen gælder fortsat efter fratrædelsen, og den fratrådte medarbejder er udtrykkeligt informeret herom forinden.
Hvem udfører kontrollen?	På ansættelsestidspunktet og under vores interne træning. På fratrædelsestidspunktet.
Kontroldokumentation	HR-afdelingen kontrollerer og arkiverer kontrakter og tjeklister. Ved ansættelsens ophør kontrollerer og arkiverer HR-afdelingen tjeklisterne. Dagsordener fra infomøder om bevidsthed. Certificeringer for konkrete tekniske kompetencer.

Adgangsstyring

Formål	Adgang til systemer, data og andre it-ressourcer styres, vedligeholdes og overvåges konsekvent i overensstemmelse med kundernes krav. Adgangen er opdelt i tre områder: • Kundens medarbejdere • Medarbejdere hos IT Relation • Tredjepartskonsulenter.

Procedurer og kontroller	De konti, som IT Relation bruger på kundesystemer, er ofte konti med udvidede rettigheder. Som standard tildeles den adgang, som IT Relations medarbejdere får til kundens system, ud fra medarbejderens rolle. Det betyder, at der tildeles adgang til medarbejdere med en jobfunktion, der har et arbejdsbetinget behov for adgang til kundesystemerne. IT Relations adgang til kundesystemerne logges. Som en øget beskyttelse af IT Relations adgang til kundesystemerne tilbyder IT Relation en Just-in-Time-løsning. Just-in-Time er et system til beskyttelse af IT Relations administratorkonti. Det sikrer, at brugen af adgang logges og kan spores, at der bruges stærke adgangskoder, og at adgangskoder automatisk ændres, hver gang kontoen bruges. Med Just-in-Time er der ingen, der kender adgangskoden, når IT Relation ikke er logget ind. Dette begrænser muligheden for, at en IT Relation-konto kan bruges af en hacker til lateral bevægelse. Tredjepartskonsulenter, der skal have adgang til kundens platform, er oprettet som lokale administratorer af de konkrete systemer, som de har brug for adgang til. Tredjepartskonsulenter tildeles først adgang og rettigheder til kundesystemer efter en formel godkendelse fra kunden. Generelt oprettes tredjepartsbrugere efter en skriftlig henvendelse til driftsafdelingen i IT Relation. IT Relation afgør, hvilke af de foruddefinerede roller brugerne skal tildeles, på baggrund af kundens godkendelse.
Tidspunkt for udførelse af kontrollen	Kunder: Kontrollen udføres, når kunden anmoder om det, og når en tredjepart får adgang til kundens system. Medarbejdere hos IT Relation: Kontrollen udføres i forbindelse med ændringer i personalet.
Hvem udfører kontrollen?	Kunder: User Management Driftsafdelingen i IT Relation er ansvarlig for at sikre, at proceduren for tredjepartsadgang til kundens miljø overholdes som aftalt med kunden. Medarbejdere hos IT Relation: Konsulenten og den driftsansvarlige har ansvaret for, hvem der har adgang til hvad (kundemiljø – interne systemer).
Kontroldokumentation	Når tredjepart har brug for adgang til kundens it-miljø, opretter kundens it-chef en serviceanmodning, der beskriver omfanget af tredjepartsadgangen, i systemet til håndtering af serviceanmodninger.

Fysisk adgangskontrol og sikkerhed

Formål	Den fysiske adgang til systemer, data og andre it-ressourcer er begrænset til og planlægges med datacenterchefen.
Procedurer og kontroller	Adgangen til bygningen sker med nøgler eller elektroniske låseanordninger, som er udleveret til IT Relation. Kun personer, der har brug for adgang til serverrummet i housing-centeret, har adgang til disse nøgler. Endelig kræves der en nøgle for at få adgang til de rackskabe, som IT Relation anvender på eksterne lokationer. Listen over udleverede nøgler opbevares og holdes opdateret af housing-leverandøren.
Tidspunkt for udførelse af kontrollen	Listen valideres en gang om året.
Hvem udfører kontrollen?	Driftsafdelingen og housing-leverandøren udfører kontrollerne. Kontrol af udlevering af nøgler til datacenteret generelt er ikke en del af denne erklæring.
Kontroldokumentation	Den enkelte bruger af nøglen fra IT Relation skriver sig op i housing-centerets protokol, når nøglen hentes og afleveres.

Sikring mod miljømæssige hændelser	
Formål	It-udstyr er beskyttet mod miljøhændelser som strømsvigt, vand og brand.
Procedurer og kontroller	Serverrummet i datacenteret er beskyttet mod følgende miljømæssige hændelser: • Strømsvigt • Brand • Ekstreme klimaforhold. På alt kritisk it-udstyr er stabil strøm sikret med et UPS-anlæg, der leverer elektricitet til systemerne, indtil generatoren automatisk er startet. Teknikrummet og serverrummet er udstyret med røg- og temperatursensorer, som er koblet til det centrale brandovervågningssystem. Serverrummet er også udstyret med automatisk brandbekæmpelsesudstyr (Inergen – som aktiveres ved for høje værdier af enten røg eller varme). Brandsikringsudstyret alarmerer automatisk brandvæsenet. Varmeudviklingen i serverrummet styres gennem det fuldautomatiske kølesystem, der sørger for den korrekte temperatur til stabil drift og lang holdbarhed af it-udstyret. Der udføres løbende vedligeholdelse af disse anlæg.
Tidspunkt for udførelse af kontrollen	Der udføres kontinuerligt serviceeftersyn ud fra leverandørens specifikationer.
Hvem udfører kontrollen?	Kontrollen udføres af serviceleverandørerne.
Kontroldokumentation	Alle kontrolskemaer befinder sig hos housing-leverandørerne.

Driftssikkerhed

Backup	
Formål	Data sikkerhedskopieres og opbevares, så de kan gendannes, hvis de går tabt. IT Relation vurderer og følger op på eventuelle fejl i backuppen.
Procedurer og kontroller	Der er udarbejdet en detaljeret beskrivelse af backupproceduren. Backupproceduren er en del af den daglige drift og er derfor automatiseret i systemet. Manuelle backupprocedurer er beskrevet i driftsprocedurerne. Backupsystemet er fysisk placeret i to forskellige datacentre. Backupdata replikeres hver dag fra den primære til den sekundære lokation for at sikre, at der findes en offlinekopi i tilfælde af en katastrofe.
Tidspunkt for udførelse af kontrollen	Backuploggene kontrolleres inden for normal arbejdstid.
Hvem udfører kontrollen?	Driftsafdelingen udfører den daglige kontrol af backuploggene.
Kontroldokumentation	Skema til daglig driftskontrol samt skema til årlig kontrol.

Drift og overvågning	
Formål	Der sker proaktiv overvågning af aftalte serviceydelser for at sikre: • generel tilgængelighed • at de tilgængelige ressourcer svarer til de aftalte standarder og tærskelværdier • at de nødvendige job og batchkørsler udføres korrekt og rettidigt. IT Relation sikrer, at ovenstående serviceydelser følger de aftalte standarder, og at overvågningen sker med det forventede resultat.
Procedurer og kontroller	IT Relation har etableret en række skriftlige procedurer for alle væsentlige driftsaktiviteter, der understøtter de generelle forventninger til en tilfredsstillende drift som anført i IT Relations it- og informationssikkerhedspolitik. Driftsprocedurerne udarbejdes af driftsafdelingen i tæt samarbejde med kunden og tredjepartsleverandører. Driften håndteres via platformsværktøjer på Citrix-serverne. Diverse jobbeskrivelser for driftsafdelingen definerer, hvilken overvågning og hvilke kontroller der skal udføres hver dag, hver uge og hvert år. Fejl fundet i de udførte kontroller samt fejl fra de systematiske overvågningssystemer rettes så hurtigt som muligt i henhold til procedurer eller bedste praksis. Kunden informeres straks om omfanget og konsekvenserne af de konstaterede fejl. Følgende har adgang til kundernes it-systemer: • Medarbejdere i servicedesk • Medarbejdere i driftsafdelingen • Konsulenter.
Tidspunkt for udførelse af kontrollen	Kontrollen udføres 24/7 eller i den primære driftstid i henhold til SLA-aftalen med den enkelte kunde.
Hvem udfører kontrollen?	Kontrollerne udføres af driftsafdelingen i IT Relation. Driftscenteret overvåges 24/7 på en eller flere af vores lokationer i Herning og Viby, og, hvis kunderne har accepteret det, på IT Relations lokation i Filippinerne.
Kontroldokumentation	Alle hændelser logges i overvågningssystemet. Visse overvågningshændelser overføres endvidere til it-service management-systemet (ITSM).

Administration af programrettelser	
Formål	Administration af programrettelser sker i henhold til kundens aftale med IT Relation. Formålet er at sikre, at systemerne løbende opdateres med sikkerhedsrettelser for at opretholde et højt sikkerhedsniveau.
Procedurer og kontroller	Når en kontrakt indeholder administration af programrettelser, udfører IT Relation som standard programrettelser med Microsoft-opdateringer en gang om måneden. Programrettelserne udføres ved hjælp af et system til administration af programrettelser. IT Relation godkender programrettelserne til udsendelse hver måned umiddelbart efter Patch Tuesday. Som standard godkendes alle opdateringer, og kun hvis en programrettelse indeholder et problem, medtages den ikke. Kundeservere opdateres som: • Automatisk programrettelse. Serverne konfigureres i de fastsatte servicevinduer. Når serveren har sit servicevindue, søger klienten efter godkendte opdateringer og installerer de manglende opdateringer. Hvis opdateringerne ikke kan installeres i servicevinduet, afventer de og installeres i det næste. • Manuel programrettelse. Servicevinduet konfigureres på et bestemt tidspunkt, og programrettelsen overvåges. Endvidere foretages der kontroller efter programrettelsen.

Tidspunkt for udførelse af kontrollen	Kontrollerne udføres løbende via systemerne til administration af programrettelser.
Hvem udfører kontrollen?	Kontrollerne udføres af driftsafdelingen.
Kontroldokumentation	Alle SCCM-programrettelser logges automatisk i separate logfiler på den enkelte server og webstedsserver. De manuelle kontroller dokumenteres i it-servicestyringssystemet.

Strategi for ændringsstyring	
Formål	Ændringsstyring udføres på fælles infrastruktur og kundernes systemer, når kunden har en aftale, der indeholder ændringsstyring.
Procedurer og kontroller	IT Relation har en proces for ændringsstyring, som anvendes, når: • der foretages ændringer i IT Relations egen interne infrastruktur. • der foretages ændringer i systemer med fælles infrastruktur. • der foretages ændringer i kundesystemer for kunder, der har ændringsstyring inkluderet i deres kontrakt. Processen omfatter: • Ændringsanmodning (RFC) fra kunden eller fra IT Relation • Afdækning af vilkår og betingelser • Beskrivelse af ændringsanmodningens performance, test, fallback og risiko • Godkendelsesproces • Udførelse, test og fallback, hvis det er påkrævet • Dokumentation og lukning af ændringsanmodningen. For kunder uden ændringsstyring foretages ændringer på baggrund af en serviceanmodning i IT Relations ITSM-system.
Tidspunkt for udførelse af kontrollen	Kontrollerne udføres under rapportering til kunder.
Hvem udfører kontrollen?	Kontrollerne udføres af driftsafdelingen i IT Relation. Uden for normal arbejdstid udføres kontrollerne af en konsulent (backoffice).
Kontroldokumentation	Kontrollerne dokumenteres i it-servicestyringssystemet.

3.11 Logisk adgangskontrol – uddybning

3.11.1 Registrering af brugere

Alle brugere er registreret i et af de AD'er, som er en del af IT Relations hosting-miljø. Medarbejdere, der er ansat i IT Relations driftsafdeling, er tildelt administrative rettigheder. Derudover kan de ansvarlige for tredjepartsapplikationer have udvidede rettigheder på en konkret server. I disse tilfælde er der indgået en tredjepartsaftale mellem IT Relation, kunden og leverandøren af applikationen.

Adgangskoder

Brugeradgangskoden skal være kompleks, men samtidig mulig at huske for brugerne. Adgangskodepolitikken er fastsat i it-sikkerhedspolitikken for medarbejdere.

Normale bruger-AD-adgangskoder skal være komplekse og bestå af mindst 15 tegn.

Administrative bruger adgangskoder skal være komplekse og bestå af mindst 20 tegn.

Opbevaring af adgangskoder til de interne systemer hos IT Relation, herunder adgangskoder, der giver fuld adgang til de enkelte kundehostede servere, sker i et lukket og krypteret system til styring af aktiver. Dette kan kun tilgås med et personligt login. Adgang til adgangskoder og kopiering af adgangskoder i systemet til styring af aktiver bliver logget.

3.12 Periodisk gennemgang af brugeradgangsrettigheder

Brugere med administrative rettigheder gennemgås ved ændringer i personalet. Hvert halve år er der også en manuel gennemgang af de administrative brugere. Denne gennemgang implementeres af kvalitetschefen.

3.13 Adgang til kundesystemer

Kundesystemer tilgås via særligt privilegerede jumphosts for at forhindre adgang fra andre netværk inden for eller uden for IT Relation.

3.14 Anskaffelse, udvikling og vedligeholdelse af systemer

Netværk og kommunikationssoftware	
Formål	Netværks- og kommunikationssoftware vedligeholdes og understøttes. Ledelsen sikrer, at ændringer eller nyanskaffelser foretages efter behov, og at ændringer testes og dokumenteres tilfredsstillende.
Procedurer og kontroller	IT Relation har fuld dokumentation for netværks- og kommunikationslinjer til de tilsluttede kunder, der er indgået aftale med om drift af kundens netværksudstyr. IT Relation vurderer p.t. behovet for at opgradere firmware på netværks- og kommunikationssoftwaren. For at sikre stabil drift vil opgraderinger kun blive foretaget, hvis de er nødvendige for at sikre kommunikationen. Før en ændringer foretages, tages der en sikkerhedskopi af konfigurationsfilerne til netværkskomponenter, og efterfølgende opbevares udskiftet udstyr i en periode, i tilfælde af at det nye udstyr ikke fungerer korrekt eller optimalt. Væsentlige ændringer til netværkskonfigurationerne foretages i de servicevinduer, der er aftalt med kunderne.
Tidspunkt for udførelse af kontrollen	Kontrollen udføres i forbindelse med opgraderinger og ændringer.
Hvem udfører kontrollen?	Netværksafdelingen er ansvarlig for at forberede opgraderinger og kontrol af funktionalitet.
Kontroldokumentation	Dokumentation af opgaver udført i kundens system håndteres i it-servicestyringssystemet.

Systemsoftware	
Formål	Systemsoftware vedligeholdes og understøttes. Ledelsen sikrer, at ændringer eller nyanskaffelser foretages i overensstemmelse med virksomhedens behov, og at ændringer testes og dokumenteres tilfredsstillende.

Procedurer og kontroller	For Windows-servere indhentes tilstrækkelig systemdokumentation efter behov. IT Relation har fastlagt procedurer for anskaffelse og opdatering af systemsoftwaren på Windows-platformene. På Windows-platformen leveres opgraderingerne af Microsoft, og de rulles automatisk ud på serverne via systemet til administration af programrettelser. Der foretages altså ingen manuel vurdering af disse opgraderinger, da udbyderen har testet og vurderet de enkelte opgraderinger.
Tidspunkt for udførelse af kontrollen	Kontrollen af opgraderingerne udføres via systemet til administration af programrettelser, som indeholder logge over opgraderingerne.
Hvem udfører kontrollen?	Driftsafdelingen er ansvarlig for at forberede opgraderinger og for kontrollen heraf.
Kontroldokumentation	Bortset fra dokumentationen i systemet til administration af programrettelser genereres der ikke logge.

Styring af informationssikkerhedshændelser

Servicedesk og kundesupport	
Formål	Sikre, at der ydes tilstrækkelig support til brugere, der kontakter servicedesk, og at den aftalte support ydes inden for den aftalte tidsfrist.
Procedurer og kontroller	IT Relation har fastlagt en række skriftlige servicedesk-procedurer på de områder, der er aftalt med kunden. Servicedesk-procedurerne udarbejdes af servicedesk i tæt samarbejde med kunden og tredjepartsleverandører. Der ydes support til brugerne via TeamViewer-softwaren til fjernadgang og via platformsværktøjerne på terminalserveren. Svartiden er aftalt i kundens SLA, og prioritering sker i it-servicestyringssystemet.
Tidspunkt for udførelse af kontrollen	Servicedesk undersøger hver dag hændelser, der venter på at blive løst.
Hvem udfører kontrollen?	Kontrollerne udføres af servicedesk 24/7 på hovedkontoret i Herning.
Kontroldokumentation	Alle hændelser logges i it-servicestyringssystemet.

Hændelseshåndtering	
Formål	Hændelseshåndteringen udføres tilfredsstillende på grundlag af de aftaler, der er indgået med kunderne, og IT Relation kontrollerer, at dette sker i fuld overensstemmelse med aftalen og med det forventede resultat.
Procedurer og kontroller	IT Relation bruger et it-servicestyringssystem til at registrere og håndtere hændelser. Følgende registreres: • Fejl (fra e-mail eller manuelt oprettede sager) • Hvad der er gjort for at afhjælpe fejlene • Hvem der har udført opgaven • Tidspunktet for registrering af hændelsen • Tid brugt på hændelserne (indeholdt i driftsaftalen eller faktureres). Driftsafdelingens ledelse har ansvaret for at overvåge, at henvendelser rettet til servicedesk prioriteres, og at der afsættes ressourcer. Endvidere har den ansvaret for, at hændelseshåndteringen sker i overensstemmelse med kundeaftalerne.

Tidspunkt for udførelse af kontrollen	Hændelseshåndteringen udføres løbende hele dagen.
Hvem udfører kontrollen?	Hændelserne håndteres af servicedesk eller driftsafdelingen. Uden for normal arbejdstid håndteres hændelserne af servicedesk og de konsulenter, der har tilkaldevagt.
Kontroldokumentation	Alle hændelser logges i it-servicestyringssystemet. Der er ingen automatisk eskalering mv. i it-servicestyringssystemet, i forhold til om SLA-aftalerne overholdes. Kunderne har adgang til at følge sagerne i "selvbetjeningsportalen".

Informationssikkerhedsaspekter ved beredskabsstyring	
Formål	At sikre virksomhedens aktiviteter og beskytte kritiske forretningsprocesser mod virkningerne af større fejl eller katastrofer.
Procedurer og kontroller	IT Relation har fastlagt en beredskabsplan for driften for at sikre, at virksomhedens interne it-applikationer kan fortsætte i tilfælde af en nødsituation. Desuden er der fastlagt en beredskabsplan for cyberangreb for at sikre, at angreb håndteres effektivt. Planerne gennemgås regelmæssigt.
Tidspunkt for udførelse af kontrollen	Kontrol af opdateringer og test af beredskabsplaner udføres en gang om året.
Hvem udfører kontrollen?	Driftsafdelingen er ansvarlig for at forberede opdateringer og for kontrollen heraf.
Kontroldokumentation	Gennemgangen af beredskabsplanerne og testen af procedurerne dokumenteres, når de er foretaget.

3.15 Beredskabsplaner

IT Relation er meget afhængig af velfungerende interne it-systemer. Vi er derfor parate til at sikre hurtig genetablering af kritiske systemer i tilfælde af et alvorligt nedbrud.

Vitale systemer, der genstartes inden for 24 timer, omfatter:

- HyperV-miljø
- VMware-miljø
- Internetudbyderlinjer
- Firewall
- Intern infrastruktur
- Servere hos IT Relation A/S (DC – SQL – systemet til styring af aktiver – Citrix)
- Backupsystemer hos IT Relation A/S
- Telefoni
- Kunder af IT-Relation A/S' drift.

It-beredskabsplanen udarbejdes og vedligeholdes på baggrund af en løbende risikoanalyse af virksomhedens it-miljø.

Risikoanalyserne afdækker de enkelte enheders afhængighed af de forskellige it-systemer og services, så ledelsens krav til tilgængelighed i størst muligt omfang opfyldes og afspejles i beredskabsplanlægningen.

3.16 Problemstyring

En tekniker hos IT Relation bliver opmærksom på en alvorlig driftshændelse. Problemets omfang kortlægges, og hvis hændelsen kategoriseres som prioritet 1, igangsættes problemstyringen med det samme.

Fejlen eskaleres personligt eller telefonisk til den tilgængelige problemansvarlige.

Problemstyringen forløber derefter i henhold til de fastsatte procedurer; problemets omfang fastlægges, tilstrækkelig bemanding sikres, planlægning foretages, eksternt personale involveres, problemet løses, der gøres regelmæssigt status, information til kunder sikres mv.

Efter at problemet er løst, og de relevante og angivne kontroller er udført, lukkes problemstyringen. Inden for kort tid analyseres og evalueres hændelsen for at fastslå, om der er behov for yderligere handling.

3.17 Nøddrift

Nøddrift af servere defineres som prioriteringen af applikationer og services, der har høj prioritet, ved brug af systemer med begrænset kapacitet (serverdrift) i tilfælde af en ulykkes- eller katastrofesituation. Nøddrift kan etableres fra enten primære eller sekundære lokationer. Nøddrift af servicedesk defineres som prioriteringen af opgaver, der har høj prioritet og udføres af medarbejdere hos IT Relation, ved brug af systemer med begrænset kapacitet i tilfælde af en ulykkes- eller katastrofesituation. Nøddrift kan etableres fra enten primære eller sekundære lokationer og fra servicedesks hjemmearbejdspladser, indtil lokaler kan lejes, og eksterne linjer kan etableres.

3.18 Komplementære kontroller hos kunder

Forhold, der skal overvejes af kundernes revisorer

Leverede serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på IT Relations standardvilkår. Kundernes afvigelser fra IT Relations standardvilkår er derfor ikke omfattet af denne erklæring.

Kundernes egne revisorer bør derfor vurdere, om denne erklæring kan udvides til at omfatte den specifikke kunde, og afdække eventuelle andre risici, som er relevante for aflæggelsen af kundernes regnskaber. Hvad angår ændringsstyring, er det kun kerneinfrastrukturen, der er omfattet af standardkontrakterne, og eventuel ændringsstyring på kundeløsningerne skal dækkes af en særskilt aftale med IT Relation.

Brugeradministration

IT Relation tildeler adgang og rettigheder i overensstemmelse med kundens anvisninger, når disse er meldt ind til servicedesk. IT Relation er ikke ansvarlig for, at disse oplysninger er korrekte, og det er således kundernes ansvar at sikre, at adgangen og rettighederne til systemer og applikationer tildeles hensigtsmæssigt og i overensstemmelse med bedste praksis for funktionsadskillelse.

IT Relation tildeler også adgang til tredjepartskonsulenter – primært udviklere, der skal vedligeholde applikationer, der indgår i hosting-aftalen. Dette sker i henhold til instrukser fra IT Relations kunder.

Kundernes egne revisorer bør derfor uafhængigt vurdere, om de adgange og rettigheder til applikationer, servere og databaser, der tildeles til kundens egne medarbejdere og til tredjepartskonsulenter, er hensigtsmæssige på baggrund af en vurdering af risikoen for fejlinformationer i regnskabsaflæggelsen.

Som standard anvender IT Relation og kundens interne it-medarbejdere en fælles systemadgang (fælles administratoradgangskode). De konti, der benyttes af IT Relation, er ofte konti med udvidede rettigheder. Som en øget beskyttelse af disse konti tilbyder IT Relation en Just-in-Time-løsning. Dette er ikke en del af standardkontrakten med IT Relation. Just-in-Time er et system til beskyttelse af IT Relations administratorkonti. Det sikrer, at brugen af adgang logges og kan spores, at der bruges stærke adgangskoder, og at adgangskoder ændres, hver gang kontoen er blevet brugt. Med Just-in-Time er der ingen, der kender adgangskoden, når IT Relation ikke er logget ind. Dette begrænser muligheden for, at en IT Relation-konto

kan bruges af en hacker til lateral bevægelse, og at en medarbejder kan huske en adgangskode, når han ikke længere er ansat i IT Relation.

Beredskabsplanlægning

De generelle betingelser for hosting hos IT Relation fastlægger ikke krav til beredskabsplanlægning og gendannelse af kundernes systemmiljø i tilfælde af en nødsituation.

IT Relation sikrer generel backup af kundemiljøerne, men hosting-aftalerne omfatter ikke en garanti for fuld gendannelse af kundernes systemmiljø efter en nødsituation. Kundernes egne revisorer bør derfor uafhængigt vurdere risikoen for manglende beredskabsplanlægning og regelmæssig test heraf i forhold til en risiko for fejlinformation i regnskabsaflæggelsen.

Overholdelse af relevant lovgivning

IT Relation har planlagt procedurer og kontroller, så lovgivningen på de områder, som IT Relation er ansvarlig for, overholdes i tilstrækkelig grad. IT Relation er ikke ansvarlig for de applikationer, der kører på det hostede udstyr. Derfor omfatter denne erklæring ikke sikring af, at der er etableret tilstrækkelige kontroller i brugerapplikationerne, og at applikationerne overholder bogføringsloven, persondataloven og anden relevant lovgivning.

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

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

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

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

4.2 Testhandlinger

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

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontrollerne er implementeret og har fungeret i perioden fra 1. januar 2023 til 31. december 2023. Dette omfatter bl.a. vurdering af patching-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål 5:
Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.1	**Politikker for informationssikkerhed** *Informationssikkerhedspolitik og emnespecifikke politikker skal defineres, godkendes af ledelsen, offentliggøres, kommunikeres til og anerkendes af relevante medarbejdere og relevante interessenter og vurderes med planlagte mellemrum, samt hvis der sker væsentlige ændringer.* IT Relation har defineret og dokumenteret en informationssikkerhedspolitik, som godkendes af topledelsen og distribueres til alle medarbejdere. IT Relation har defineret og dokumenteret flere emnespecifikke politikker, som understøtter informationssikkerhedspolitikken og distribueres til alle relevante medarbejdere. Informationssikkerhedspolitikken og emnespecifikke politikker revideres mindst årligt, eller hvis der sker væsentlige ændringer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en ledelsesgodkendt og ajourført sikkerhedspolitik. Vi har inspiceret, at informationssikkerhedspolitikkerne kommunikeres til medarbejderne og relevante parter og er revideret årligt.	Ingen afvigelser noteret.
5.2	**Roller og ansvar for informationssikkerhed** *Roller og ansvar for informationssikkerhed skal defineres og allokeres i overensstemmelse med organisationens behov.* IT Relation har etableret og defineret roller og ansvar i overensstemmelse med Information Security Management System.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.3	**Adskillelse af opgaver** *Modstridende pligter og modstridende ansvarsområder skal adskilles.* IT Relation har defineret politikker for adskillelse af opgaver, som revideres mindst årligt, eller hvis der sker væsentlige ændringer for at sikre, at niveauet af adskillelse afspejler informationssikkerhedspolitikken og det nødvendige niveau af adskillelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos IT Relation, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.	Ingen afvigelser noteret.
5.4	**Ledelsens ansvar** *Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.* IT Relation kræver, at ledelsen sætter sig ind i og støtter gældende informationssikkerhedsinitiativer og uddanner sine medarbejdere i disse tiltag.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion påset, at ledelsen er bekendt med informationssikkerhedsinitiativer.	Ingen afvigelser noteret.
5.5	**Kontakt til myndigheder** *Organisationen skal etablere og vedligeholde kontakt med relevante myndigheder.* IT Relation har etableret og implementeret kommunikationsprocedurer for, hvordan man kommunikerer med relevante myndigheder i tilfælde af en sikkerhedshændelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har en kommunikationsprocedure for, hvordan der kommunikeres med relevante myndigheder i tilfælde af sikkerhedsbrud.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.7	**Underretning om trusler** *Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretninger om trusler.* IT Relation producerer trusselsefterretninger fra forskellige kilder, herunder sårbarhedsrapporter, udvalgte nyhedskilder, leverandører, myndigheder og særlige interessegrupper til brug for risikobaseret beslutningstagning.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at IT Relation indhenter og analyserer information til brug for risikobaseret beslutningstagning.	Ingen afvigelser noteret.
5.9	**Fortegnelse over information og understøttende aktiver** *Der skal udarbejdes og vedligeholdes en fortegnelse over information og understøttende aktiver, herunder ejere.* IT Relation har implementeret og vedligeholder forskellige CMDB'er afhængigt af arten af aktiverne i omfang. Dette omfatter databaser på endepunkter, servere, netværksudstyr, databaser osv., som alle har ejere og anden relevant information tildelt.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret tilstrækkelige kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver.	Ingen afvigelser noteret.
5.10	**Acceptabel brug af information og understøttende aktiver** *Regler for acceptabel brug og procedurer til håndtering af information og understøttende aktiver bør identificeres, dokumenteres og implementeres.* IT Relation har etableret og implementeret regler om acceptabel brug af IT Relationens aktiver dokumenteret i vores Politik for acceptabel brug.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at passende kontroller er på plads for at sikre dokumentation og vedligeholdelse af beholdningen af aktiver, herunder acceptabel brug af aktiver.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.12	**Klassifikation af oplysninger** *Information skal klassificeres i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.* IT Relation har etableret en dataklassificeringsordning, der omhandler, hvordan forskellige typer data skal klassificeres og håndteres i henhold til deres klassificering.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at IT Relation har etableret en dataklassificeringsordning til klassifikation af information.	Ingen afvigelser noteret.
5.14	**Overførsel af information** *Der skal være etableret regler eller procedurer for eller aftaler om overførsel af information for alle former for overførselsfaciliteter i organisationen og mellem organisationen og andre parter.* IT Relation har etableret politikker og procedurer for informationsoverførsel for at sikre, at information rejser gennem sikre og pålidelige kommunikationskanaler.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at en passende teknisk sikkerhedsarkitektur er blevet etableret i netværket, samt at der er etableret regler for informationsoverførsel.	Ingen afvigelser noteret.
5.15	**Administration af adgang** *Der skal fastlægges og implementeres regler for styring af fysisk og logisk adgang til information og understøttende aktiver på grundlag af forretnings- og informationssikkerhedskrav.* IT Relation har implementeret generelle retningslinjer for adgang til egne og kundesystemer baseret på forretnings- og informationssikkerhedskrav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har kontrolleret, at retningslinjer for adgangskontrol er implementeret, gennemgået og godkendt.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.18	**Adgangsrettigheder** *Adgangsrettigheder til information og understøttende aktiver bør tilvejebringes, vurderes, ændres og fjernes i overensstemmelse med organisationens emnespecifikke politik og regler for administration af adgang.* IT Relation gennemgår løbende medarbejderens privilegerede tekniske rettigheder i både interne og kundevendte systemer for at sikre, at rettigheden er passende og i overensstemmelse med medarbejderens arbejdsrelaterede behov. Medarbejdere, som ikke har brug for teknisk-privilegeret adgang, tildeles de nødvendige rettigheder til at bruge interne systemer. Disse standardrettigheder tilføjes og fjernes i forbindelse med ansættelse, overdragelse og opsigelse hos IT Relation. Når en medarbejder forlader IT Relation, tilbagekaldes alle adgange. Hvis en medarbejder skifter jobfunktion, tilpasses adgangen, så den afspejler den nye opgave.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, at fratrådte brugere fjernes rettidigt i driftsmiljøet efter fratrædelsen. Vi har inspiceret, at brugeradgange revurderes én gang hvert halve år.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.19	**Informationssikkerhed i leverandørforhold** *Processer og procedurer skal defineres og implementeres for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.* IT Relation har etableret procedurer for styring af sikkerhedsrisici forbundet med brugen af en leverandørs produkter og tjenester, som omfatter en årlig risikovurdering og revision af leverandører for at sikre, at leverandøren fortsat lever op til de sikkerhedskrav, IT Relation forventer.	Vi har inspiceret, at der findes en formel og dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved stikprøvevis inspektion påset, at der udarbejdes risikovurderinger med passende mellemrum på kritiske leverandører. Vi har ved inspektion påset, at IT Relation jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav.	Ingen afvigelser noteret.
5.20	**Håndtering af informationssikkerhed i leverandøraftaler** *Relevante informationssikkerhedskrav skal fastlægges og aftales med hver enkelt leverandør på grundlag af typen af leveranceforhold.* IT Relation har fastlagt sikkerhedskrav til leverandører, som behandles som en del af den kontraktlige aftale med leverandørerne og de almindelige forretningsbetingelser for leverandører, der samarbejder med IT Relation.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at en formel og dokumenteret procedure er på plads for at sikre, at nye eller genforhandlede applikations- eller serviceleverandørkontrakter valideres i forhold til en liste over definerede informationssikkerhedskrav.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.22	**Overvågning, vurdering og ændringsstyring af leverandørydelser** *Organisationen skal regelmæssigt overvåge, vurdere, evaluere og styre ændringer i leverandørens informationssikkerhedspraksis og levering af ydelser.* IT Relation har etableret procedurer for styring af sikkerhedsrisici forbundet med brugen af en leverandørs produkter og tjenester, som omfatter en årlig risikovurdering og revision af leverandører for at sikre, at leverandøren fortsat lever op til de sikkerhedskrav, IT Relation forventer. Hvis ændringer af leverandørservices påvirker kundemiljøer, services eller infrastruktur, skal disse ændringer også administreres i IT Relations change management-proces.	Vi har inspiceret, at der findes en formel, dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved inspektion af en stikprøve på underskrevne kontrakter påset, at informationssikkerhedskravene er kontraktligt aftalt. Vi har ved inspektion af stikprøver påset, at IT Relation jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav. Vi har inspiceret, at tredjepartserklæringer for hovedleverandører er modtaget og behandlet af IT Relation.	Ingen afvigelser noteret.
5.23	**Informationssikkerhed ved brug af cloud-tjenester** *Der skal fastlægges processer for anskaffelse, brug, styring og afslutning af brugen af cloud-tjenester i overensstemmelse med organisationens informationssikkerhedskrav.* IT Relation har fastlagt en strategi for brugen af cloud-tjenester i overensstemmelse med IT Relations krav til informationssikkerhed, herunder brug, styring og udtræden af cloud-tjenester.	Vi har ved inspektion påset, at der er etableret en strategi for brugen af cloud-tjenester.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.24	**Planlægning og forberedelse af incident-håndtering ved sikkerheds-incidents** *Organisationen skal planlægge og forberede sig på at håndtere informationssikkerheds-incidents ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerheds-incidents.* IT Relation har defineret, etableret og implementeret en plan for håndtering af informationssikkerhedshændelser, som omfatter en proces for hændelseshåndtering samt roller og ansvar relateret til hændelsesrespons.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at den formelle og dokumenterede proces for hændelsesstyring er blevet gennemgået og godkendt. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.
5.26	**Håndtering af informationssikkerheds-incidents** *Informationssikkerheds-incidents skal håndteres i overensstemmelse med de dokumenterede procedurer.* IT Relation har etableret procedurer for at reagere på informationssikkerhedshændelser.	Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at løsningerne er dokumenteret i et system til hændelsesstyring.	Ingen afvigelser noteret.
5.27	**Læring af informationssikkerheds-incidents** *Den viden, der opnås i forbindelse med informationssikkerheds-incidents, bør anvendes til at styrke og forbedre informationssikkerhedsforanstaltninger.* IT Relation har etableret procedurer for at lære af informationssikkerhedshændelser, hvor sikkerhedshændelser løbende gennemgås for læringsmuligheder og forbedring af IT Relations sikkerhedsposition.	Vi har kontrolleret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at alle hændelser er blevet registreret, at de nødvendige handlinger er udført, og at sikkerhedshændelser er gennemgået.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.29	**Informationssikkerhed under driftsforstyrrelse** *Organisationen skal planlægge, hvordan informationssikkerheden opretholdes på et passende niveau under driftsforstyrrelser.* IT Relation har etableret forretningskontinuitetsplaner for at sikre, at IT Relationen kan opretholde informationssikkerhed og drift på et passende niveau under driftsforstyrrelse.	Vi har inspiceret, at en formel og dokumenteret beredskabsplan vedligeholdes, gennemgås og godkendes en gang om året. Vi har inspiceret, at de bagvedliggende procedurer for beredskabsplanen er blevet gennemgået og godkendt af relevant personale.	Ingen afvigelser noteret.
5.30	**IKT-parathed til understøttelse af business continuity** *IKT-beredskab bør planlægges, implementeres, vedligeholdelse og testes på grundlag af mål for business continuity og IKT-kontinuitetskrav.* IT Relation udfører årligt IKT-beredskabstest for at sikre, at forretningskontinuitetsplaner kan understøtte det tilsigtede og passende resultat, og at organisationen handler i henhold til forretningskontinuitetsplaner.	Vi har kontrolleret, at en formel og dokumenteret forretningskontinuitetsplan vedligeholdes, revideres og godkendes årligt. Vi har inspiceret, at IKT-beredskabstest er blevet gennemgået årligt og godkendt af passende personale.	Ingen afvigelser noteret.
5.34	**Privatlivsbeskyttelse og beskyttelse af personoplysninger** *Organisationen skal identificere og opfylde kravene vedrørende privatlivsbeskyttelse og beskyttelse af personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav.* IT Relation har identificeret gældende krav vedrørende bevarelse af privatlivets fred og beskyttelse af PII og etableret passende kontroller og foranstaltninger til at opfylde disse krav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at tilstrækkelige kontroller er på plads for at sikre dokumentation og vedligeholdelse af PII.	Ingen afvigelser noteret.

Kontrolmål 5:

Organisatoriske kontroller

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
5.37	**Dokumenterede driftsprocedurer** *Driftsprocedurer for informationsbehandlingsfaciliteter bør dokumenteres og gøres tilgængelige for medarbejdere, der har brug for dem.* IT Relation har etableret tilstrækkelige og dokumenterede driftsprocedurer til at understøtte og styre driften af løsninger og services leveret af IT Relation. Dette omfatter etablering af en platform for kommunikation og tilgængelighed af disse driftsprocedurer til medarbejdere med et arbejdsrelateret behov for dem.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har kontrolleret, at der er etableret driftsprocedurer, og at disse skal opdateres mindst én gang årligt. Vi har kontrolleret, at driftsprocedurerne er tilgængelige for alle relevante medarbejdere.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.1	**Screening** *Der skal udføres verifikation af alle jobansøgeres baggrund. Verifikationen bør foretages, inden de tiltræder i organisationen og løbende, under hensyntagen til love, forskrifter og etiske regler og bør vurderes i forhold til organisationens krav, klassifikationen af den information, der skal gives adgang til, og de relevante risici.* IT Relation udfører screening af sine potentielle kandidater, hvilket omfatter indhentning af rene straffeattester på alle medarbejdere ansat i IT Relation. Alle medarbejdere er forpligtet til løbende at levere en ren straffeattest under deres ansættelse, og en sådan straffeattest indhentes af IT Relation hvert tredje ansættelsesår.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der fremlægges straffeattester, inden ansættelsen starter for både medarbejdere og eksterne konsulenter samt hvert tredje ansættelsesår. Vi har ved stikprøvevis inspektion påset, at der er erhvervet straffeattester inden ansættelsesstart for nyansatte.	Ingen afvigelser noteret.
6.2	**Ansættelsesvilkår – og betingelser** *Ansættelseskontrakterne skal beskrive medarbejdernes og organisationens ansvar for informationssikkerhed.* IT Relation har fastsat ansættelsesvilkår som en del af ansættelsesaftalen mellem en medarbejder og IT Relation. Disse omfatter forventninger om overholdelse af gældende informationssikkerhedsinitiativer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.3	**Awareness, uddannelse og træning vedrørende informationssikkerhed** *Organisationens medarbejdere og relevante interessenter skal modtage passende awareness, uddannelse og træning vedrørende informationssikkerhed samt regelmæssige opdateringer om organisationens informationssikkerhedspolitik, emnespecifikke politikker og procedurer, hvor det er relevant for deres jobfunktion.* IT Relation udfører løbende forskellige initiativer inden for sikkerhedsbevidsthed baseret på et årshjul og ad-hoc-trendende sikkerhedstrusler i verden. IT Relation udfører simuleringer af phishing-forsøg og andre forsøg på sikkerhedsbrud for at øge medarbejdernes praktiske erfaring med faktiske forsøg på sikkerhedsbrud. Endvidere er alle medarbejdere forpligtet til at sætte sig ind i gældende informationssikkerhedskrav og informationssikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation afholder introduktionskurser for nye medarbejdere, hvor kravene til informationssikkerhed gennemgås, samt at medarbejderne jævnligt skal gennemføre obligatoriske undervisningsforløb for at sikre, at virksomhedens sikkerhedskrav overholdes. Vi har inspiceret, at medarbejdere er introduceret til informationssikkerhedspolitikken.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.5	**Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold** *Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres, håndhæves og kommunikeres til relevante medarbejdere og andre interessenter.* IT Relation kommunikerer informationssikkerhedsansvar, som forbliver gyldige efter opsigelse eller ændring af ansættelsesforhold. Dette omfatter indhentning af skriftlig bekræftelse på, at den opsagte medarbejder forstår sin fortsatte forpligtelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der indhentes en skriftlig bekræftelse på, at opsagte medarbejdere forstår deres forsatte forpligtelse i forbindelse med fratrædelse.	Ingen afvigelser noteret.
6.6	**Hemmeligholdelse- og fortrolighedsaftaler** *Hemmeligholdelses- og fortrolighedsaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, dokumenteres, vurderes regelmæssigt og underskrives af medarbejdere og andre interessenter.* IT Relation etablerer fortrolighedsaftaler med sine medarbejdere som en del af de indledende, kontraktlige ansættelsesaftaler. Desuden kan nogle medarbejdere under deres ansættelse være underlagt yderligere fortrolighed eller tavshedspligt, hvis kunderne kræver det.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der indhentes fortrolighedsaftaler i forbindelse med nyansættelser.	Ingen afvigelser noteret.

Kontrolmål 6:

Personalerelaterede foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
6.7	**Distancearbejde** *Der skal være implementerede sikkerhedstiltag, når medarbejdere arbejder på afstand, for at beskytte information, der er adgang til, og som behandles eller lagres uden for organisationens lokaliteter.* IT Relation har etableret og implementeret sikkerhedsforanstaltninger for personale, der arbejder eksternt, for at sikre, at informationssikkerhedsniveauet svarer til, når medarbejderne arbejder fra kontorerne. Dette inkluderer blandt andet etablering af VPN-forbindelser og sikring af, at alt følsomt arbejde udføres på virtuelle skriveborde.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er implementeret passende sikkerhedsforanstaltninger for personale, der arbejder eksternt.	Ingen afvigelser noteret.
6.8	**Indrapportering af informationssikkerhedshændelser** *Organisationen skal sørge for, at medarbejdere kan indrapportere observerede eller formodede informationssikkerhedshændelser rettidigt via passende kanaler.* IT Relation har etableret og tilvejebringer en mekanisme, så personale kan rapportere observerede eller formodede informationssikkerhedshændelser. Proceduren for at bruge mekanismen kommunikeres til og gøres tilgængelig for alle medarbejdere.	Vi har inspiceret, at der er fastsat en formel og dokumenteret proces for hændelsesstyring. Vi har inspiceret, at processen for hændelsesstyring er blevet kommunikeret til medarbejderne.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.2	**Fysisk adgangskontrol** *Sikrede områder bør beskyttes ved hjælp af passende adgangsforanstaltninger og adgangspunkter.* IT Relation har etableret fysiske adgangskontroller til sikring af områder. Disse kontroller omfatter identifikationskort, registrering af besøg og konstant tilsyn med godkendte og ryddede medarbejdere.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at IT Relation har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
7.3	**Sikring af kontorer, lokaler og faciliteter** *Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og implementeres.* IT Relation har implementeret fysisk sikkerhed på vores kontorer, som omfatter fysiske adgangsveje, der er tilgængelige via personlige ID-kort og personlige PIN-koder, adskilte sikkerhedszoner og CCTV.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at IT Relation har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Ingen afvigelser noteret.
7.4	**Fysisk sikkerhedsovervågning** *Lokaliteter skal overvåges løbende for uautoriseret fysisk adgang.* IT Relation har etableret CCTV ved indgange til både kontorer, datacentre og andre faciliteter, der behandler følsomme oplysninger.	Vi har inspiceret, at CCTV er etableret ved alle indgange til både kontorer, datacentre og andre faciliteter, der behandler følsomme oplysninger.	Ingen afvigelser noteret.
7.6	**Arbejde i sikrede områder** *Sikkerhedsforhold for arbejde i sikrede områder skal tilrettelægges og implementeres.* IT Relation har etableret procedurer og retningslinjer for arbejde i sikre områder for at sikre, at udførelse af arbejde ikke bringer medarbejdere og informationsaktiver i fare.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at relevante sikkerhedsforhold er etableret for at sikre medarbejdere samt informationsaktiver.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.7	**Ryddeligt skrivebord og låst skærm** *Regler om at holde skriveborde ryddet for papir og bærbare lagringsmedier og om at holde skærme låst på informationsbehandlingsfaciliteter skal defineres og håndhæves på behørig vis.* IT Relation har etableret en politik om ryddet skrivebord og låst skærm, der sikrer, at følsomme oplysninger ikke efterlades uden opsyn på kontoret, og at skærme og slutpunkter låses, når de efterlades uden opsyn.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har implementeret en politik om ryddet skrivebord og låst skærm.	Ingen afvigelser noteret.
7.8	**Placering og beskyttelse af udstyr** *Udstyr skal placeres på et sikkert og beskyttet sted.* IT Relation har en politik for at sikre beskyttelse af kritisk udstyr.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har fastlagt retningslinjer for sikring mod brand, vand og varme. Vi har desuden ved inspektion påset, at IT Relation har indhentet revisionserklæring fra en underleverandør for at sikre, at tilsvarende krav overholdes, på områder hvor der er sket outsourcing.	Ingen afvigelser noteret.
7.9	**Sikring af aktiver uden for organisationens områder** *Aktiver uden for organisationens lokationer skal beskyttes.* IT Relation har etableret og kommunikeret regler for, hvordan aktiver skal beskyttes og håndteres, når de fjernes fra området.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret regler, der sikrer, at aktiver er beskyttet og håndteres korrekt, når de fjernes fra organisationens områder, samt at dette er godkendt.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.10	**Lagringsmedier** *Lagringsmedier skal styres i hele deres livscyklus i forbindelse med anskaffelse, brug, transport og bortskaffelse i overensstemmelse med organisationens klassifikationssystem og krav til håndtering.* IT Relation har etableret og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret og implementeret politikker og procedurer for håndtering af lagermedier gennem hele deres livscyklus.	Ingen afvigelser noteret.
7.11	**Forsyningssikkerhed** *Informationsbehandlingsfaciliteter skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.* IT Relation sikrer, at alt udstyr, der ejes af IT Relation, vedligeholdes efter producentens specifikation. Ydermere sikrer IT Relation, at dets partnere gør det samme.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret en fuldt redundant infrastruktur med særskilt backup.	Ingen afvigelser noteret.
7.13	**Vedligeholdelse af udstyr** *Udstyr skal vedligeholdes korrekt for at sikre tilgængelighed, integritet og fortrolighed af information.* IT Relation sørger for at vedligeholde udstyr som specificeret af producenten.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret retningslinjer for, hvordan udstyr vedligeholdes korrekt.	Ingen afvigelser noteret.

Kontrolmål 7:

Fysiske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
7.14	**Sikker bortskaffelse eller genbrug af udstyr** *Udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software slettes eller overskrives på forsvarlig vis inden bortskaffelse eller genbrug.* IT Relation har implementeret retningslinjer for bortskaffelse eller genbrug af udstyr, der sikrer, at hvis lagringsmedier bortskaffes, sker det gennem en certificeret leverandør for at sikre dets ødelæggelse.	Vi har inspiceret, at IT Relation har implementeret procedurer for sikker bortskaffelse eller genbrug af udstyr. Vi har inspiceret at bortskaffelse eller genbrug af udstyr sker igennem en certificeret leverandør.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.1	**Brugerenheder** *Information, der lagres på, behandles af eller er tilgængelig via brugerenheder, bør beskyttes.* IT Relation har implementeret forskellige sikkerhedspolitikker for enheder, der anvendes af brugerne, for at sikre, at de er tilstrækkeligt beskyttet. Dette inkluderer blandt andet fjernsletning af harddiske, malwarebeskyttelse osv.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har implementeret en politik for brugerenheder.	Ingen afvigelser noteret.
8.2	**Privilegerede adgangsrettigheder** *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* IT Relation har en politik for tildeling og begrænsning af brugere med privilegeret adgang. Alle brugere med privilegeret adgang har en dedikeret bruger til den privilegerede adgang. Listen over privilegerede brugere revideres på kvartalsbasis.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har tilrettelagt formaliserede procedurer for brugeradministration og rettighedsstyring, og at disse også gælder for brugere med privilegerede rettigheder. Vi har inspiceret, at der for autorisationer, der tildeles medarbejdere, foreligger en begrundelse for det ønskede adgangsniveau og en godkendelse fra nærmeste chef. Vi har inspiceret, at privilegerede adgangsrettigheder er revideret på kvartalsbasis.	Ingen afvigelser noteret.
8.3	**Begrænset adgang til information** *Adgang til information og understøttende aktiver skal begrænses i overensstemmelse med den fastlagte emnespecifikke politik for administration af adgang.* IT Relation har en politik om at begrænse adgangen til systemer og applikationer til medarbejdere, der har et arbejdsrelateret behov.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er implementeret en politik for begrænsning af adgange til systemer og applikationer til medarbejdere, der har et arbejdsbetinget behov.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.5	**Sikker autentifikation** *Der skal implementeres sikre autentifikationsteknologier og -procedurer på baggrund af begrænsninger i informationsadgangen og den emnespecifikke politik for administration af adgang.* IT Relation har etableret sikre autentifikationsteknologier til følsom information, som blandt andet inkluderer multifaktorautentifikation.	Vi har inspiceret, at der er implementeret en formel politik for adgangsstyring, der fastlægger tilladte tekniske autentifikationsløsninger. Vi har inspiceret, at politikken for adgangsstyring er blevet gennemgået og godkendt. Vi har inspiceret, at de omfattede applikationer og systemer håndhæver sikre logonprocedurer.	Ingen afvigelser noteret.
8.6	**Kapacitetsstyring** *Anvendelsen af ressourcer skal overvåges og tilpasses i overensstemmelse med de nuværende og forventede kapacitetskrav.* IT Relation har procedurer for månedlig rapportering om driften. Disse rapporter indeholder oplysninger om drift af produktionsmiljøet, herunder oplysninger om kapacitet. Der er etableret automatisk overvågning af driftsmiljøet og relevante systemparametre, herunder kapacitet, for at sikre, at fremtidige kapacitetskrav opfyldes.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der hver måned sendes rapporter til kunden vedrørende driften i produktionsmiljøerne hos IT Relation. Vi har ligeledes påset, at kapaciteten overvåges på produktionssystemerne hos IT Relation, så fremtidige krav til kapaciteten overholdes.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.7	**Beskyttelse mod malware** *Beskyttelse mod malware skal implementeres og understøttes af passende awareness hos brugeren.* IT Relation har implementeret procedurer for at sikre, at antivirussoftware fungerer på alle gældende systemer. Antivirussoftwaren overvåges. Beskyttelse mod malware understøttes af brugerbevidsthed gennem IT Relations platform til sikkerhedsbevidsthed, der giver viden om malwareforsvar til medarbejderne.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at medarbejdernes pc'er hos IT Relation er beskyttet med antivirussoftware – og at denne er opdateret. Vi har inspiceret, at IT Relation har etableret initiativer til brugerbevidsthed om beskyttelse mod malware til medarbejdere.	Ingen afvigelser noteret.
8.8	**Håndtering af tekniske sårbarheder** *Der skal indhentes oplysninger om tekniske sårbarheder ved brug af informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og passende foranstaltninger skal træffes.* IT Relation har en procedure til løbende at vurdere sårbarheder, der indberettes, og til at vurdere deres kritikalitet mod flere kilder i forbindelse med de tjenester, som IT Relation leverer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der løbende indhentes informationer om tekniske sårbarheder, samt at foretages passende foranstaltninger til at håndtere eventuelle risici. Vi har ligeledes ved inspektion påset, at kritiske sårbarheder kommunikeres til samtlige relevante interessenter.	Ingen afvigelser noteret.
8.9	**Konfigurationsstyring** *Konfigurationer, herunder sikkerhedskonfigurationer, af hardware, software, tjenester og netværk bør etableres, dokumenteres, implementeres, overvåges og vurderes.* IT Relation har etableret processer og procedurer for konfigurationsstyring for at sikre, at ændringer af konfigurationer håndteres og dokumenteres korrekt.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret procedurer for konfigurationsstyring, samt at konfigurationer håndteres i overensstemmelse med gældende procedurer.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.10	**Sletning af information** *Information lagret i informationssystemer, enheder eller i andre lagringsmedier skal slettes, når der ikke længere er brug for den.* IT Relation har etableret procedurer for sletning af oplysninger for at sikre, at ingen data opbevares længere end krævet af lovmæssige eller forretningsmæssige krav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at sletning af oplysninger sker i overensstemmelse med IT Relations procedurer herfor.	Ingen afvigelser noteret.
8.13	**Backup af information** *Backup af information, software og systemer skal vedligeholdes og testes regelmæssigt i overensstemmelse med den aftalte emnespecifikke politik for backup.* IT Relation udfører backup i overensstemmelse med IT Relations bedste praksis eller kundernes forretningskrav. Backupjobbene overvåges for at sikre deres kontinuerlige drift. Hvert år igangsættes en recovery-test af IT Relation.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er fastsat krav til backup i kontrakten med underleverandører, der leverer serviceydelser, hvor backup er relevant. Vi har inspiceret, at der er foretaget en fuld gendannelsestest af it-miljøerne.	Ingen afvigelser noteret.
8.14	**Redundans i faciliteter til informationsbehandling** *Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.* IT Relation har redundans i egne informationsbehandlingsfaciliteter og har mulighed for at levere redundans, hvis kunden har disse krav.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der etableret redundans på IT Relations informationsbehandlingsfaciliteter samt på kundemiljøer i overensstemmelse med gældende kundekontrakter.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.15	**Logning** *Logge, der optegner aktiviteter, undtagelser, fejl og andre relevante hændelser, skal udarbejdes, opbevares, beskyttes og analyseres.* IT Relation udfører Security Information and Event Management (SIEM) på sine egne systemer, og hvis kunden har disse krav. IT Relation registrerer logfiler for forskellige systemer på forskellige sikkerhedsniveauer. For SIEM-systemet er der fuld funktionsadskillelse. Medarbejdere, der har adgang til at slette logdata, har ingen adgang til kundesystemer og IT Relations systemer. Al adgang til kundesystemer logges i assets management-systemet. Adgangsloggen opbevares sikkert, og systemet er sat op til at kontrollere, hvem der eventuelt forsøger at ændre de lagrede oplysninger.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at hændelseslogning af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser er konfigureret. Vi har inspiceret, at adgang til kundedata bliver logget og opbevares sikkert. Vi har inspiceret, at IT Relation har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov, og at der er implementeret tilstrækkelig funktionsadskillelse i adgange til logdata.	Ingen afvigelser noteret.
8.16	**Overvågning af aktiviteter** *Netværk, systemer og applikationer skal overvåges for unormal adfærd, og der skal iværksættes passende handlinger for at evaluere potentielle informationssikkerheds-incidents.* IT Relation har implementeret et overvågningssystem, der sikrer, at kundernes systemer kører, og at der advares om eventuel unormal adfærd gennem overvågningssystemet. Systemet overvåges 24/7.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at et overvågningssystem er implementeret, samt at dette er overvåget 24/7.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.17	**Synkronisering af ure** *Urene i systemer til informationsbehandling, som organisationen anvender, skal synkroniseres med godkendte tidskilder.* IT Relation har synkroniseret alle relevante informationsbehandlingssystemer til en enkelt referencetidskilde.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret en referencetidskilde for tidssynkronisering af alle relevante informationsbehandlingssystemer.	Ingen afvigelser noteret.
8.19	**Softwareinstallation i test- og produktionssystemer** *Der skal implementeres procedurer og tiltag til sikker styring af softwareinstallationer i test- og produktionssystemer.* IT Relation har defineret et sæt standardimplementeringsbeskrivelser. Disse systemer er tilladt på kundesystemer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at softwareinstallationer håndteres hensigtsmæssigt og i overensstemmelse med gældende procedurer.	Ingen afvigelser noteret.
8.20	**Netværkssikkerhed** *Netværk og netværksenheder skal sikres, styres og kontrolleres for at beskytte information i systemer og applikationer.* IT Relation har implementeret flere politikker for at sikre en sikker kommunikation, og at manipulation af data minimeres. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsrelateret behov. Kommunikation mellem IT Relation og kundesteder udføres af valide og gennemprøvede, sikre teknologier.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, om der jf. retningslinjerne er etableret en passende sikkerhedsarkitektur på netværket, herunder: • om netværket er opdelt i sikre zoner, og om kundemiljøerne er adskilt fra IT Relations eget miljø • om fjernadgang er tildelt ved brug af tofaktorgodkendelse • om ændringer i netværksmiljøet i vores stikprøve er sket på kontrolleret vis i overensstemmelse med reglerne for ændringsstyring.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.22	**Segmentering af netværk** *Grupper af informationstjenester, brugere og informationssystemer skal adskilles i organisationens netværk.* IT Relation adskiller kundenetværk i et eller flere netværk afhængigt af behovet for adskillelse. Kunderne har ikke adgang til andre kundenetværk.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået den tekniske sikkerhedsarkitektur og ved stikprøvevis inspektion undersøgt, om der jf. retningslinjerne er etableret et passende sikkerhedsniveau, herunder: • om sikre zoner og kundemiljøer er adskilt fra IT Relations eget miljø • om adgang til netværket er opdelt i relevante brugergrupper baseret på et arbejdsbetinget behov.	Ingen afvigelser noteret.
8.23	**Webfiltrering** *Adgang til eksterne websteder skal styres for at reducere eksponeringen for skadeligt indhold.* IT Relation har implementeret webfiltreringsforanstaltninger, som omfatter beskyttelse mod og reduktion af eksponering for skadeligt indhold.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er implementeret webfiltreringsforanstaltninger.	Ingen afvigelser noteret.
8.24	**Brug af kryptografi** *Regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler, skal defineres og implementeres.* IT Relation har etableret politikker for brug af kryptografi, som omfatter regler for brug, valg af kryptografisk teknik, implementering, vedligeholdelse og bortskaffelse.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at der er etableret en passende brug af sikker kryptografi og nøglehåndtering.	Ingen afvigelser noteret.

Kontrolmål 8:

Tekniske foranstaltninger

Nr.	Serviceorganisationens kontrolaktivitet	Test udført af PwC	Resultat af PwC's test
8.32	**Ændringsstyring** *Ændringer af informationsbehandlingsfaciliteter og informationssystemer skal være underlagt procedurer for ændringsstyring.* IT Relation har etableret og implementeret en change management-proces, der sikrer, at alle ændringer af informationssystemer i produktionsmiljøer er underlagt change management, som sikrer, at ændringer ikke unødigt påvirker hinanden, og at fall-back-planer er på plads.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har udarbejdet procedurer for årlig gennemgang og opdatering af: • Hændelsesstyring • Problemstyring • Ændringsstyring • Styring af versioner og programrettelser • Brugeradministration.	Ingen afvigelser noteret.

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

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

Frank Bech Jensen
Kunde
Serienummer: 4ecdf2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c
IP: 185.203.xxx.xxx
2024-01-31 12:56:07 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 83.136.xxx.xxx
2024-01-31 13:17:18 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 208.127.xxx.xxx
2024-01-31 13:28:07 UTC