www.pwc.dk

IT Relation A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2022 til 31. december 2022 i relation til IT Relations hosting-ydelser

Januar 2023

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

IT Relation A/S anvender B4Restore, Keepit og Front-Safe som serviceunderleverandører af backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore, Keepit og Front-Safe 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 2022 til 31. december 2022. 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 2022 til 31. december 2022

   (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 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at:

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

(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 2022 til 31. december 2022.

Herning, den 18. januar 2023
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 2022 til 31. december 2022 i relation til IT Relation A/S' hosting-ydelser

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

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 2022 til 31. december 2022 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

IT Relation anvender B4Restore, Keepit og Front-Safe som serviceunderleverandører af backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore, Keepit og Front-Safe 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.

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om 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 2022 til 31. december 2022, 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 2022 til 31. december 2022, 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 2022 til 31. december 2022.

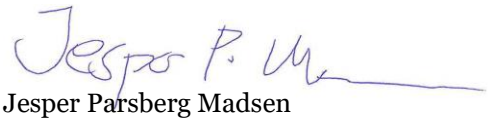
Beskrivelse af test af kontroller

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 18. januar 2023
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 2022 til 31. december 2022 har virksomheder leveret serviceydelser i overensstemmelse med de systemer til styring af informationssikkerheden, der er dokumenteret i systembeskrivelsen i ISAE 3402-erklæringen for 2022, og i overensstemmelse med ISO 27001:2013.

Én virksomhed – transitionsgruppen

I sommeren 2021 blev en transitionsgruppe bestående af medarbejdere fra både Itadel og IT Relation dannet med det formål at skabe én virksomhed. Transitionsgruppens mål er at samarbejde om fusionen og etableringen af fælles processer. Vi vil være sikre på, at vores processer skaber det rette fundament og understøtter vores behov.

Introduktion til IT Relation A/S

IT Relation A/S er en it-virksomhed, der har fokus på at optimere sine kunders forretning gennem it-løsninger. Vi er specialister i it-strategi, hosting, servicedesk, sikkerhed, support og hardware. Vores 690 medarbejdere er fordelt på lokationer i hele Danmark, og vi har kontorer i Herning, Aarhus, København, Kolding og Aalborg. Ud over de danske lokationer har vi en lokation i Tjekkiet og Filippinerne, hvor vi løser opgaver for de kunder, der har godkendt det.

IT Relation beskæftiger sig med følgende fire forretningsområder:

1. Managed services (it-outsourcing og hosting)

2. Servicedesk

3. It-sikkerhed

4. Hardware.

Vi stræber efter at være en komplet end-to-end-leverandør af it-løsninger via en 360-graders tilgang. Vores servicedesk er bemandet med kompetente, fleksible og smilende it-problemknusere 24/7, 365 dage om året. Vores ambition er at levere optimale it-løsninger og maksimal kundeservice hver eneste dag.

Introduktion til itm8

IT Relation A/S er en del af en større IT-koncern kaldet itm8.

Itm8 er en IT-koncern bestående af 12 virksomheder og 1700+ medarbejdere. Koncernens hovedfokus er at samle IT-specialister under et fælles tag for at sikre kunderne mulighed for end-to-end løsninger. Herunder indgår IT Relation A/S som én af de 12 virksomheder der er en del af itm8 koncernen.

Koncernfunktionen, itm8, skriver i dag godt 100 medarbejdere som i den operationelle dagligdag er sat i verden for at understøtte og skabe synergier i itm8's datterselskaber med nedenstående interne services:

- Datacenter
- Intern Udvikling
- Internt IT
- Human Resources
- Marketing
- Finance
- Legal & Compliance
- Compliance & Security

Denne ISAE 3402 regnskabsaflæggelse indbefatter ligeledes også itm8's koncernfunktion ved de ovennævnte afdelinger, da IT Relation benytter sig i fuldt omfang af koncernfunktionens understøttelse i form af de interne services koncernfunktionen tilbyder.

Introduktion til Me'ning

IT Relation A/S har et datterselskab kaldet Me'ning.

Me'ning er en virksomhed som specialiserer sig indenfor udvikling af Microsoft- og speciallavede løsninger. De har stor fokus på hele processen omkring udvikling af IT-løsninger, lige fra behovsafklaring til opfølgning. De besidder både kompetencer indenfor digital transformation og udvikling så de kan sikre sig at lave et system af høj kvalitet, som også opfylder kundens specifikt afdækkede behov. Deres Microsoft løsninger består bl.a af:

- Modern Workplace
- CRM-løsninger
- Data og Analyse
- Baseline værktøjer (Reporting, GDRP, Workplace, Whistleblower)
- Sharepoint udvikling
- Specialudvikling

Derudover har de også egenudviklede systemer:

- Sikker Mail
- Patientjournal-løsninger
- OnlineLegat
- VirkCollect

Me'ning har i dag 70 medarbejdere fordelt på 3 kontorer i København, Aarhus og Herning.

Denne ISAE 3402 regnskabsaflæggelse indbefatter ligeledes også Me'ning, da Me'ning er et datterselskab af IT Relation A/S og i fuldt omfang anvender samme ledelsessytem som både itm8's koncernfunktion og IT Relation A/S.

Introduktion til beskrivelse af serviceydelser

Denne beskrivelse er udarbejdet for at give oplysninger til brug for IT Relations kunder og disses revisorer i overensstemmelse med kravene i den danske revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402. Beskrivelsen indeholder oplysninger om det system- og kontrolmiljø, der er etableret for IT Relations drifts- og hosting-ydelser, som leveres til kunderne.

Dokumentet indeholder beskrivelser af de procedurer, der anvendes til at sikre en tilfredsstillende drift af systemerne. Formålet er at give tilstrækkelige oplysninger, så hosting-kundernes revisorer uafhængigt kan vurdere afdækningen af risici for svagheder i kontrolmiljøet, for så vidt disse kan indebære en risiko for væsentlig fejlinformation i hosting-kundernes it-drift for perioden fra 1. januar 2022 til 31. december 2022.

Beskrivelse af IT Relations serviceydelser

Siden grundlæggelsen i 2003 har IT Relation været en del af hosting-industrien og har leveret generationer af it-løsninger til mange forskellige brancher på markedet. Ud over hosting leverer IT Relation også en lang række andre it-relaterede ydelser.

IT Relation tilbyder følgende serviceydelser til hosting-markedet:

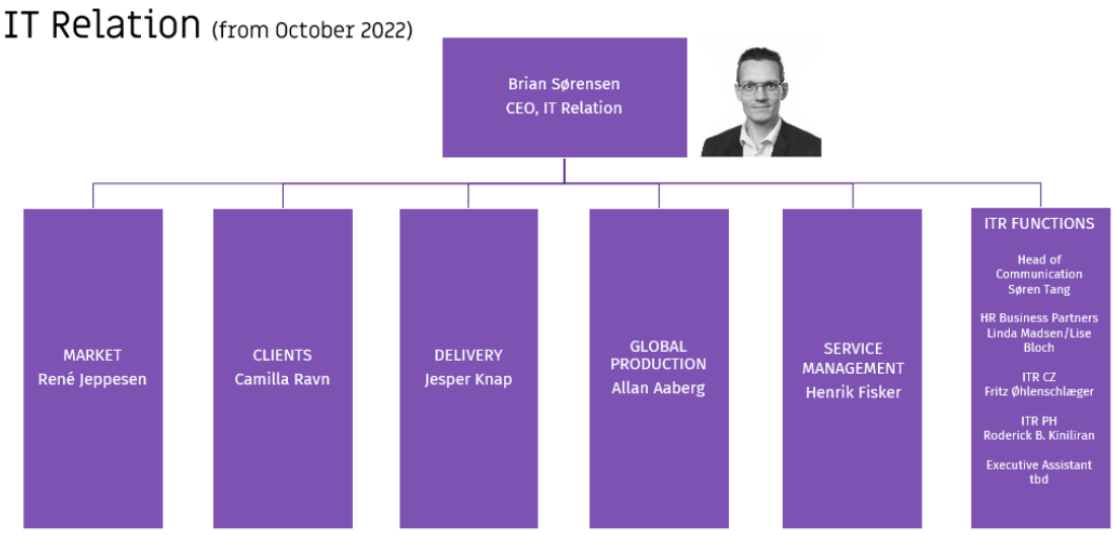
- Hosting og housing
- Fjernbackup
- Drift
- Cloud-løsninger
- Servicedesk.

Systembeskrivelsen indeholder en angivelse af de arbejdsprocesser, der er anvendt, og de kontroller, der er udført, i relation til ovennævnte serviceydelser.

Herudover tilbyder IT Relation også assistance på følgende områder:

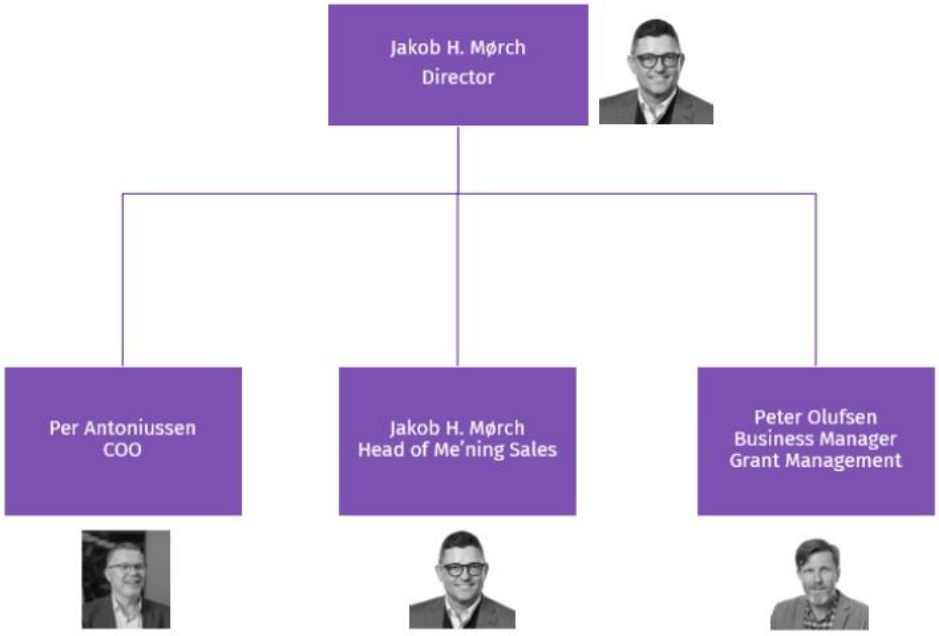
- Udvikling af it-løsninger
- Rådgivning og serviceydelser inden for it-sikkerhed på både ledelsesmæssigt og teknisk niveau
- Rådgivning på CIO-niveau
- Teknisk projektledelse
- Teknisk service onsite.

IT Relations organisation



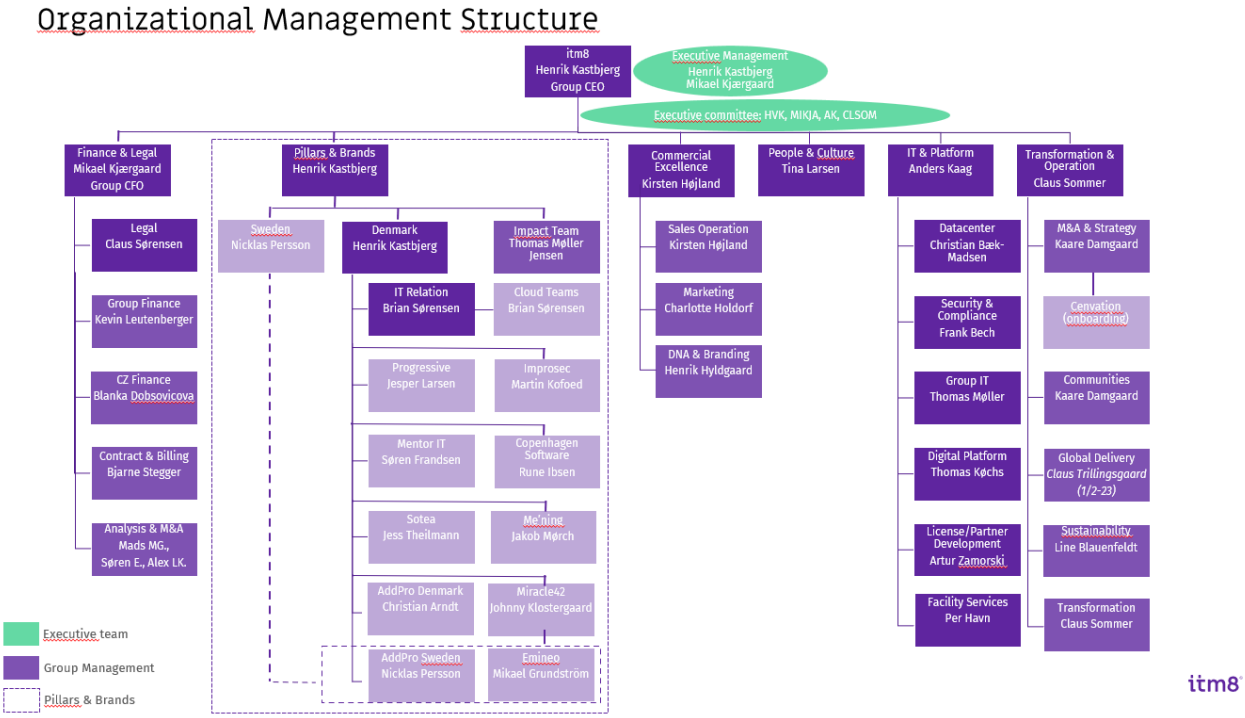
itm8

Me'nings organisation



itm8

Itm8's organisation



itm8

Risikostyring i IT Relation

Risikostyring i IT Relation udføres på flere områder og niveauer. En gang om året udføres risiko- og trusselsvurderinger af de interne systemer generelt. Der indsamles input til disse vurderinger fra hele virksomheden. Processen faciliteres af sikkerhedsafdelingen, som også udarbejder udkast til IT Relations ledelse. Efter den interne behandling godkendes vurderingerne af ledelsen. I projektanbefalingsfasen udarbejdes der afhængigt af projektets art en sikkerhedsvurdering og en vurdering af særlige risici og usikkerheder. Dette gøres i henhold til en fastsat proces.

På det operationelle projektniveau er der løbende risikostyring. Risikostyringen sker efter en fastlagt projektstyringsmodel, hvor ansvaret for den projektrelaterede risikostyring ligger hos projektlederen. Projektlederen vil ofte vælge at inddrage projektdeltagere, eksterne samarbejdspartnere og eventuelt en styregruppe i processen.

Kontrolramme, kontrolstruktur og kriterier for implementering af kontroller

It-sikkerhedspolitikkens fastlagte processer og kontrollerne i IT Relation omfatter alle de systemer og serviceydelser, der leveres til kunderne. Det fortsatte arbejde med at tilpasse og forbedre sikkerhedsforanstaltningerne varetages p.t. i samarbejde med højt kvalificerede specialister.

IT Relation er certificeret efter ISO 27001:2013-standarden. Det betyder, at kontroller fra standarden er implementeret og overholdes. Som en del af ISO 27001-standarden er der også etableret et system til styring af informationssikkerheden (ISMS).

Med dette system kan vi:

- overvåge og måle status for informationssikkerhed
- udføre interne revisioner
- evaluere informationssikkerhed og foranstaltninger
- foretage ledelsesgennemgang med den øverste ledelse.

Formålet med ISMS-systemet er at sikre løbende kontrol med informationssikkerhedsniveauet i forhold til trusselsniveauet generelt. Systemet er grundlaget for at opretholde en kontinuerlig forbedringsproces, der sikrer, at hændelser behandles, og at informationssikkerhedsniveauet løbende øges.

IT Relation er også underlagt årlig it-revision, som resulterer i en årlig revisionserklæring udarbejdet i overensstemmelse med ISAE 3402-standarden. De kontroller, der er blevet implementeret og gennemgået, er kontroller fra bilag A i ISO 27001:2013-standarden.

Kontrolområder og -aktiviteter fra denne kontrolramme er blevet implementeret i overensstemmelse med bedste praksis for at mindske den risiko, der er forbundet med serviceydelser leveret af IT Relation. Følgende kontrolområder fra den valgte kontrolmodel indgår i det overordnede kontrolmiljø:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Personalesikkerhed
- Adgangsstyring
- Fysisk sikring og miljøsikring
- 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

Hvert af de 15 områder er nærmere beskrevet i afsnittene nedenfor.

Informationssikkerhedspolitikker

Formål	Der er på baggrund af en it-risikoanalyse udarbejdet en ledelsesgodkendt it-sikkerhedspolitik, 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	It-sikkerhedspolitikken 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	It-sikkerhedspolitikken er underlagt dokumentkontrol.

Organisering af informationssikkerhed

Formål	At styre informationssikkerhed i virksomheden.
Procedurer og kontroller	Det primære ansvar for it-sikkerhed 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 it-sikkerhedspolitikken. 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. It-sikkerhedsudvalget består på nuværende tidspunkt af følgende medlemmer: • Chief Technology Officer, Anders Kaag • Head of Compliance and Security, Frank Bech Jensen • Security Director, Johnni Meldgård Rude • Technical Advisor, Flemming Laursen • Cloud Citrix Specialist, Jakob Thalund Jensen • Team Manager, Dan Sørup Olesen • Data Centre Specialist, Jakob Andersen • Compliance Manager, Bo Duholm Hansen.
Tidspunkt for udførelse af kontrollen	Udvalget mødes en gang om året for at fastlægge og følge op på målsætninger i relation til it-sikkerhed.

Hvem udfører kontrollen?	Den årlige gennemgang udføres af sikkerhedsudvalget.
Kontroldokumentation	Udvalget dokumenterer sine beslutninger i en aktivitetsliste.

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 kontrolleres hvert år. Ledelsen skal sikre, at alle medarbejdere implementerer og opretholder it-sikkerheden i overensstemmelse med IT Relations it- og 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 it- og informationssikkerhedspolitik. • At de motiveres til at leve op til IT Relations it- og 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 it- og 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 it- og 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 sikring og miljøsikring

IT Relation har primære og sekundære datacentre, hvor it-udstyr er placeret. Hvert datacenter har en datacenterchef.

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 serviceleverandører.
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-servicestyringssystemet (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 procedure for ændringsstyring, som anvendes, når: • Der foretages ændringer i systemer med fælles infrastruktur • Der foretages ændringer i kundesystemer for kunder, der har ændringsstyring inkluderet i deres kontrakt. Proceduren 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.

Logisk adgangskontrol – uddybning

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 femten tegn.

Administrative bruger adgangskoder skal være komplekse og besta af mindst tyve 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.

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.

Adgang til kundesystemer

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

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	At 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.

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.

Problemstyring

Hvis en tekniker hos IT Relation bliver opmærksom på en alvorlig driftshændelse, kortlægges problemets omfang, 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.

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.

Kundernes ansvar

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.

Kunderne 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.

Kunderne bør derfor 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. Kunderne bør derfor 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 2022 til 31. december 2022. 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

A.5 Kontrolmål: Informationssikkerhedspolitikker

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
5.1.1 Politikker for informationssikkerhed *Ledelsen skal fastlægge og godkende en række politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.* IT Relation har en sikkerhedspolitik, der er godkendt af ledelsen. Den er tilgængelig på intranettet og udleveres til alle nye medarbejdere. Sikkerhedspolitikken vedligeholdes af Compliance and Security-afdelingen, som rapporterer direkte til den øverste ledelse.	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.	Området er revideret uden bemærkninger.
5.1.2 Gennemgang af politikker for informationssikkerhed *Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og funktionalitet.* Sikkerhedspolitikkerne gennemgås en gang om året, eller når nye politikker implementeres eller opdateres.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i forbindelse med væsentlige ændringer. Vi har inspiceret, at sikkerhedspolitikken gennemgås mindst én gang årligt.	Området er revideret uden bemærkninger.

A.6 Kontrolmål: Organisering af informationssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
6.1.1 Roller og ansvarsområder for informationssikkerhed *Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.* Ansvaret for informationssikkerheden ligger hos den øverste ledelse. Den daglige udførelse foregår i en tredeling mellem Compliance and Security-afdelingen, Group IT og Cyber Security-afdelingen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at de organisatoriske ansvarsområder er defineret og fordelt til relevante personer.	Området er revideret uden bemærkninger.
6.1.2 Funktionsadskillelse *Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af virksomhedens aktiver.* IT Relation har fastsat en politik for funktionsadskillelse. Politikken gennemgås en gang om året for at sikre, at det nuværende niveau af adskillelse stadig afspejler informationssikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der er etableret passende adskillelse mellem kritiske driftsfunktioner hos IT Relation, samt at der er etableret adskillelse mellem primære og sekundære driftsdata.	Området er revideret uden bemærkninger.
6.1.3 Kontakt til myndigheder *Der bør opretholdes passende kontakt med relevante myndigheder.* IT Relation har opsat en kommunikationsprocedure for, hvordan der kommunikeres med relevante myndigheder i tilfælde af sikkerhedsbrud.	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.	Området er revideret uden bemærkninger.

A.7 Kontrolmål: Personalesikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
7.1.1 Screening *Efterprøvning af alle jobkandidaters baggrund skal udføres i overensstemmelse med relevante love, forskrifter og etiske regler og skal stå i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.* Forud for ansættelsen bekræfter IT Relation kandidatens identitet for at sikre, at personen ikke er en svindler, og kandidatens referencer kontrolleres, hvis det er relevant. Straffeattesten undersøges forud for ansættelsen og herefter hvert tredje år for at sikre, at den fortsat er ren.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der forefindes en HR-proces, der sikrer, at der fremlægges straffeattester, inden ansættelsen starter for både medarbejdere og eksterne konsulenter. Vi har ved inspektion af en stikprøve på nyansættelser påset, at der er indhentet straffeattester inden ansættelsesstart.	Området er revideret uden bemærkninger.
7.2.1 Ledelsesansvar *Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med virksomhedens fastlagte politikker og procedurer.* IT Relation har en politik for uddannelse af medarbejderne i informationssikkerhed. Alle nye medarbejdere gennemgår et onlinekursus, der uddanner dem i informationssikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion påset, at der forefindes underskrevne kontrakter for både medarbejdere og leverandører, så virksomhedens krav til informationssikkerhed opretholdes.	Området er revideret uden bemærkninger.
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed *Alle virksomhedens medarbejdere og, hvor det er relevant, kontrahenter skal ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med virksomhedens politikker og procedurer, i det omfang det er relevant for deres jobfunktion.* Alle nye medarbejdere hos IT Relation modtager en velkomstmail, der blandt andet indeholder sikkerhedspolitikken samt en medarbejdersikkerhedshåndbog.	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. Vi har inspiceret, at medarbejderne jævnligt skal gennemføre obligatoriske undervisningsforløb for at sikre, at virksomhedens sikkerhedskrav overholdes.	Området er revideret uden bemærkninger.

A.7 Kontrolmål: Personalesikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
7.2.3 Sanktioner *Der skal være etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.* IT Relation har en kommunikeret sanktionsprocedure over for medarbejdere, der overtræder sikkerhedspolitikken.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der foreligger en sanktionsproces, som er blevet kommunikeret til medarbejderne for at sikre, at alle medarbejdere kender konsekvenserne af at overtræde sikkerhedspolitikken.	Området er revideret uden bemærkninger.
7.3.1 Ansættelsesforholdets ophør eller ændring *Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.* Når en medarbejder stopper hos IT Relation, bekræftes opsigelsen af nærmeste leder med en henvendelse til, at medarbejderen fortsat er bundet af tavshedspligt samt henvisning til fortsat gældende lov om forretningshemmeligheder efter medarbejderens fratrædelse.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at medarbejdernes adgangsrettigheder til driftssystemer, netværk, databaser, mv. inddrages i forbindelse med fratrædelse.	Området er revideret uden bemærkninger.

A.8 Kontrolmål: Styring af aktiver

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
8.1.1 Fortegnelse over aktiver *Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.* IT Relation vedligeholder en CMDB-database med alle aktiver, og databasen indeholder aktivernes livscyklus. IT Relation vedligeholder desuden en liste over alle systemer, hvoraf det fremgår, hvem der er ejer af systemet, og hvem der er ansvarlig for tekniske forhold.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er etableret tilstrækkelige kontroller i relation til dokumentation og vedligeholdelse af listen over aktiver.	Området er revideret uden bemærkninger.
8.3.2 Bortskaffelse af medier *Medier skal bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.* IT Relation har fastsat retningslinjer for bortskaffelse af medier. IT Relation anvender certificerede leverandører til bortskaffelse af medier for at sikre, at medierne destrueres.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at IT Relation har fastsat formaliserede processer for behandling og destruktion af ind- og uddatamateriale.	Området er revideret uden bemærkninger.

A.9 Kontrolmål: Adgangsstyring

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

A.9 Kontrolmål: Adgangsstyring

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
9.2.3 Styring af privilegerede adgangsrettigheder *Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.* IT Relation har en politik for tildeling og begrænsning af brugere med privilegeret adgang. Alle brugere med privilegeret adgang har en dedikeret bruger med den privilegerede adgang. Listen over privilegerede brugeres adgang revideres en gang i kvartalet.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at 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.	Området er revideret uden bemærkninger.
9.2.5 Gennemgang af brugeradgangsrettigheder *Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.* IT Relation gennemgår regelmæssigt medarbejdernes privilegerede tekniske rettigheder i både interne og kundevendte systemer. Dermed sikres overensstemmelse med medarbejderens arbejdsbetingede behov. Ikke-teknisk privilegerede medarbejdere tildeles de nødvendige rettigheder til at bruge de interne systemer. Disse standardrettigheder tilføjes og fjernes i forbindelse med ansættelse, overflytning eller fratrædelse hos IT Relation.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at brugeradgange revurderes én gang hvert halve år.	Området er revideret uden bemærkninger.
9.2.6 Inddragelse eller tilpasning af adgangsrettigheder *Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller skal tilpasses efter en ændring.* Når en medarbejder forlader virksomheden, inddrages alle adgange. Hvis medarbejderen skifter jobfunktion, ændres adgangen, så den afspejler den nye funktion. Begge ændringer iværksættes af HR-afdelingen.	Vi har ved inspektion undersøgt, at der foretages regelmæssig opfølgning på brugernes rettigheder i driftsmiljøerne, og at disse rettigheder er tildelt ud fra et arbejdsbetinget behov. Vi har ved inspektion undersøgt, at fratrådte brugere fjernes rettidigt i driftsmiljøet efter fratrædelsen.	Området er revideret uden bemærkninger.

A.9 Kontrolmål: Adgangsstyring

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
9.4.1 Begrænset adgang til informationer *Adgang til information samt funktioner i applikationssystemer skal begrænses i overensstemmelse med politikken for adgangsstyring.* IT Relation har en politik om at begrænse adgangen til systemer og applikationer, til medarbejdere der har et arbejdsbetinget behov.	Vi har inspiceret, at der vedligeholdes en formel politik for adgangsstyring, der fastlægger tilladte tekniske autentifikationsløsninger. Vi har ved stikprøvevis inspektion af anmodninger om tildeling af adgang påset, at proceduren for registrering og afmelding af brugere er blevet implementeret.	Området er revideret uden bemærkninger.
9.4.2 Procedurer for sikker logon *Hvis det kræves i henhold til politikken for adgangsstyring, skal adgang til systemer og applikationer styres af en procedure for sikker logon.* IT Relation har en sikker logonprocedure for adgang til kundedata og -systemer. Ingen kan få adgang til kundedata eller -systemer uden brug af tofaktorgodkendelse.	Vi har inspiceret, at der vedligeholdes en formel politik for adgangsstyring, der fastlægger tilladte tekniske autentifikationsløsninger. Vi har inspiceret, at politikken for adgangsstyring er blevet gennemgået og godkendt. Vi har inspiceret, at de omfattede applikationer og systemer håndhæver sikre logonprocedurer.	Området er revideret uden bemærkninger.
9.4.3 System til administration af adgangskoder *Systemer til administration af adgangskoder skal være interaktive og sikre adgangskoder af høj kvalitet.* IT Relation har et system til administration af adgangskoder, der sikrer, at adgangskoder genereres tilfældigt og overholder virksomhedens politik for kompleksitet og længde.	Vi har inspiceret, at politikkerne er blevet gennemgået og godkendt. Vi har inspiceret, at politikkerne omfatter: • Applikationskrav om brug af adgangskoder • Kvalitetskrav til adgangskoder • Krav til lockoutpolitik • Log over og opfølgning på afviste adgangsforsøg • Kontrol af afviste adgangsforsøg • Krav til brug af multifaktorgodkendelse.	Området er revideret uden bemærkninger.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
11.1.1 Fysisk perimetersikring *Der skal defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.* IT Relation har klassificeret sine informationsbehandlingsfaciliteter, og adgangen til disse sker på baggrund af denne klassifikation. Faciliteterne er opdelt i tre grupper: Lukket, begrænset og åben. Gæster er kun tilladt i åbne eller begrænsede områder, hvis de ledsages af en medarbejder hos IT Relation. Adgang til lukkede områder er tilladt for gæster, hvis de har et arbejdsbetinget behov.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes.	Området er revideret uden bemærkninger.
11.1.2 Fysisk adgangskontrol *Sikre områder skal være beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.* IT Relation har sikret, at adgangen til virksomhedens lukkede områder er sikret, at adgangen til disse områder er begrænset til personer med et arbejdsbetinget behov, og at denne adgang hyppigt revideres.	Vi har ved inspektion påset, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at IT Relation har fastlagt passende adgangskontrol for at beskytte de fysiske faciliteter.	Området er revideret uden bemærkninger.
11.1.3 Sikring af kontorer, lokaler og faciliteter *Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og etableres.* IT Relation har fastlagt begrænset adgang til kontorer. Alle døre er låst og skal åbnes af en medarbejder hos IT Relation. Alle medarbejdere skal bære et synligt ID-kort med navn og billede. Alle gæster i vores kundecentre skal bære et ID-kort, der identificerer dem som gæster. Besøgscentrene har skilte, der viser gæsterne, hvor de kan færdes frit, hvor de har adgang sammen med en medarbejder hos IT Relation, eller hvor de slet ikke har adgang.	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.	Området er revideret uden bemærkninger.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
11.1.5 Arbejde i sikre områder *Procedurer for arbejde i sikre områder skal tilrettelægges og etableres.* IT Relation har en politik, der kræver, at alle medarbejdere gennemgår it-sikkerhedsmanualen en gang om året. Desuden får medarbejdere med adgang til datacentre, datacenterinfrastruktur og datacenternetværk yderligere instruktioner, inden der gives adgang.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at alle gæster med ærinde hos IT Relation tildeles et gæstekort og under hele besøget bliver fulgt rundt af en medarbejder hos IT Relation.	Området er revideret uden bemærkninger.
11.2.1 Placering og beskyttelse af udstyr *Udstyr skal placeres og beskyttes, således at risikoen for miljøtrusler og farer samt muligheden for uautoriseret adgang minimeres.* IT Relation har en politik, der skal 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.	Området er revideret uden bemærkninger.
11.2.2 Understøttende forsyninger (forsyningssikkerhed) *Udstyr skal vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet.* IT Relation sikrer, at alt udstyr, der ejes af IT Relation, vedligeholdes i henhold til producentens anvisning. Desuden sikrer IT Relation, at virksomhedens samarbejdspartnere 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.	Området er revideret uden bemærkninger.
11.2.5 Fjernelse af aktiver *Udstyr, informationer og software må ikke fjernes fra virksomheden uden forudgående tilladelse.* IT Relation har en politik, der sikrer, at ingen medarbejdere kan fjerne udstyr, informationer eller software uden tilladelse fra nærmeste leder eller systemejeren.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har fastlagt retningslinjer, som sikrer, at udstyr, informationer og software ikke fjernes fra virksomheden uden forudgående tilladelse.	Området er revideret uden bemærkninger.

A.11 Kontrolmål: Fysisk sikring og miljøsikring

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
11.2.7 Sikker bortskaffelse eller genbrug af udstyr *Alt udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.* IT Relation sikrer, at alle lagringsmedier bortskaffes på en verificeret og sikker måde for at sikre, at data ikke kan læses efter fjernelse.	Vi har inspiceret, at IT Relation har fastsat procedurer for sikker bortskaffelse eller genbrug af udstyr. Vi har inspiceret, at IT Relation har implementeret relevante kontroller i relation til håndtering af driften af driftsmiljøet.	Området er revideret uden bemærkninger.

A.12 Kontrolmål: Driftssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
12.1.1 Dokumenterede driftsprocedurer *Driftsprocedurer skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem.* IT Relation har driftsprocedurer, der er gjort tilgængelig på intranettet.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er fastlagt driftsprocedurer, som opdateres mindst én gang om året. Vi har desuden påset, at driftsprocedurerne er tilgængelige for alle relevante medarbejdere.	Området er revideret uden bemærkninger.
12.1.2 Ændringsstyring *Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres.* IT Relation har implementeret ændringsstyring på hele produktionsmiljøet.	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.	Området er revideret uden bemærkninger.
12.1.3 Kapacitetsstyring *Anvendelsen af ressourcer skal overvåges og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som* kræ-vet. IT Relation har udarbejdet procedurer for driftsrapportering på månedsbasis. Disse driftsrapporter indeholder oplysninger om driften på produktionsmiljøerne, herunder også oplysninger om kapacitet. Der er etableret automatisk overvågning af driftsmiljøet og relevante systemparametre, herunder kapaciteten, som sikrer, at fremtidige kapacitetskrav kan overholdes.	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.	Området er revideret uden bemærkninger.

A.12 Kontrolmål: Driftssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
12.2.1 Kontroller mod malware *Der skal implementeres kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.* IT Relation har fastlagt en procedure, der skal sikre, at antivirussoftware fungerer på alle relevante systemer. Antivirussoftwaren overvåges.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at medarbejdernes pc'er hos IT Relation er beskyttet med antivirussoftware – og at denne er opdateret.	Området er revideret uden bemærkninger.
12.3.1 Backup af information *Der skal tages backupkopier af information, software og systembilleder, og disse skal testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.* IT Relation foretager backup i overensstemmelse med IT Relations bedste praksis eller kundernes forretningskrav. Backupjobbene overvåges for at sikre kontinuerlig drift. Der udføres hvert år en gendannelsestest, der igangsættes 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.	Området er revideret uden bemærkninger.
12.4.1 Hændelseslogning *Hændelseslogning til registrering af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser skal udføres, opbevares og gennemgås regelmæssigt.* IT Relation har implementeret et overvågningssystem, der sikrer, at kundernes systemer er oppe at køre. Systemet overvåges 24/7 af driftsafdelingen.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at hændelseslogning af brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser er konfigureret. Vi har inspiceret, at en oversigt over logdokumentation angiver, hvornår loggene skal gennemgås.	Området er revideret uden bemærkninger.
12.4.2 Beskyttelse af logoplysninger *Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang.* IT Relation genererer logge for forskellige systemer på forskellige sikkerhedsniveauer. For almindelige performance- og oppetidsdata er der ingen funktionsadskillelse. For SIEM-systemet er der fuld funktionsadskillelse. Medarbejdere, der har adgang til at slette logdata, har ikke adgang til kunde- og IT Relation-systemer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret logningsfaciliteter, som kun er tilgængelige for medarbejdere med et arbejdsbetinget behov. Vi har inspiceret, at logoplysningerne ikke kan redigeres eller slettes. Desuden tager IT Relation backup af logoplysningerne flere gange dagligt, og adgangen er begrænset til få personer.	Området er revideret uden bemærkninger.

A.12 Kontrolmål: Driftssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
12.4.3 Administrator- og operatørlog *Aktiviteter udført af systemadministrator og systemoperatør skal logges, og loggen skal beskyttes og gennemgås regelmæssigt.* Al adgang til kundesystemer logges i systemet til styring af aktiver. Adgangsloggen gemmes sikkert, og systemet er sat op til at overvåge, hvem der eventuelt forsøger at ændre de gemte oplysninger. Compliance and Security-afdelingen bliver underrettet, hvis nogen ændrer dataene.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Desuden har vi påset, at logningsparametrene er konfigureret til at sikre, at handlinger udført af brugere med udvidede adgangsrettigheder logges. Vi har endvidere ved stikprøvevis inspektion påset, at der foretages tilstrækkelig opfølgning på logge fra kritiske systemer.	Området er revideret uden bemærkninger.
12.4.4 Tidssynkronisering *Urene i alle relevante informationsbehandlingssystemer i en virksomhed eller et sikkerhedsdomæne skal være synkroniseret til en enkelt referencetidskilde.* IT Relation har synkroniseret alle relevante informationsbehandlingssystemer ud fra en enkel 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.	Området er revideret uden bemærkninger.

A.12 Kontrolmål: Driftssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
12.5.1 Softwareinstallation på driftssystemer *Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.* IT Relation har fastsat en række beskrivelser af standardimplementeringer. Disse systemer er tilladt på kundesystemer.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion af de systemer, der anvendes til at dokumentere ændringer, undersøgt, om ændringer i driftsmiljøet sker via en kontrolleret proces jf. retningslinjerne, herunder: • at der udføres en godkendt test af ændringerne inden idriftsættelse • at test og godkendelse af nødændringer til driftsmiljøet dokumenteres umiddelbart efter idriftsættelsen.	PwC har konstateret at en ud af seks interne IT Relation Domain Controllere ikke var patchet med nyeste sikkerhedsopdateringer. PwC har konstateret at seneste patch var fra marts 2022. PwC har efterfølgende konstateret, at IT Relation har identificeret årsagen, som skyldes en fejl i serverens rapportering til patch overvågningssystemet. PwC har konstateret at IT Relation har udbedret manglende patch på Domain Controlleren samt at der er opsat foranstaltninger for at lignende fejl ikke kan opstå igen. Området er revideret uden yderligere bemærkninger.
12.6.1 Styring af tekniske sårbarheder *Der skal løbende indhentes informationer om tekniske sårbarheder, som skal evalueres og iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.* IT Relation har en procedure for kontinuerligt at vurdere alle sårbarheder der reporteres og vurdere deres kritikalitet op imod flere kilder i forbindelse med de services IT Relation leverer. Hvis der findes kritiske sårbarheder, vil IT Relation's Trusted Advisor informere samtlige interessenter, som benytter denne service.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion påset, at der løbende indhentes informationer omkring tekniske sårbarheder samt at foretages passende foranstaltninger, til at håndtere eventuelle risici. Vi har ligeledes ved inspektion påset, at kritiske sårbarheder kommunikeres til samtlige interessenter.	Området er revideret uden bemærkninger.

A.12 Kontrolmål: Driftssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
12.7.1 Kontroller i forbindelse med revision af informationssystemer *Revisionskrav og -aktiviteter, der omfatter verificering af driftssystemer, skal planlægges og aftales omhyggeligt for at minimere afbrydelser af forretningsprocesserne.* IT Relation anvender bedste praksis til at sikre, at der overvåges nok variabler, uden at overvågningen påvirker systemets ydeevne negativt. Dette gøres i vid udstrækning ved hjælp af tredjepartssystemer udviklet til opgaven.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Desuden har vi påset, at logningsparametrene er konfigureret til at sikre, at handlinger udført af brugere med udvidede adgangsrettigheder logges. Vi har endvidere ved stikprøvevis inspektion påset, at der foretages tilstrækkelig opfølgning på logge fra kritiske systemer.	Området er revideret uden bemærkninger.

A.13 Kontrolmål: Kommunikationssikkerhed

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
13.1.1 Styring af netværkssikkerhed *Netværk skal styres og kontrolleres for at beskytte informationer i systemer og applikationer.* IT Relation har implementeret flere politikker for at sikre, at kommunikationen er sikker, og at manipulation af data minimeres. Adgang til netværksenheder er begrænset til medarbejdere med et arbejdsbetinget behov. Kommunikationen mellem IT Relation og kundesites foregår ved hjælp af anerkendte og gennemprøvede sikre teknologier.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion undersøgt, om der jf. retningslinjerne er etableret en passende sikkerhedsarkitektur på netværket, herunder: • om netværket er opdelt i sikre zoner, og om kundemiljøerne er adskilt fra 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.	Området er revideret uden bemærkninger.
13.1.3 Opdeling af netværk *Grupper af informationstjenester, brugere og informationssystemer skal opdeles i netværk.* IT Relation opdeler kundenetværk i et eller flere netværk afhængigt af behovet for opdeling. Kunder kan ikke få 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.	Området er revideret uden bemærkninger.
13.2.1 Politikker og procedurer for informationsoverførsel *Der skal foreligge formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.* IT Relation har en netværkspolitik, der beskriver, hvem der er ansvarlig for at sikre, at kommunikationskanalerne er sikre og pålidelige.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion undersøgt, om der er implementeret en tilstrækkelig netværkspolitik til at sikre, at netværkskommunikationen er sikker.	Området er revideret uden bemærkninger.

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

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
14.1.1 Analyse og specifikation af informationssikkerhedskrav *Kravene vedrørende informationssikkerhed skal være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.* IT Relation foretager en risikovurdering af alle nye kritiske systemer, der anskaffes. Dette sker for at sikre, at systemet lever op til IT Relations politikker vedrørende informationssikkerhed.	Vi har forespurgt om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at IT Relation har etableret en sikkerhedsorganisation, der sikrer et passende og tilstrækkeligt informationssikkerhedsniveau i systemerne.	Området er revideret uden bemærkninger.

A.15 Kontrolmål: Leverandørforhold

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
15.1.1 Informationssikkerhedspolitik for leverandørforhold *Informationssikkerhedskravene til at minimere risici forbundet med leverandørers adgang til virksomhedens aktiver skal aftales med leverandøren og skal dokumenteres.* IT Relation foretager en årlig risikovurdering af sine leverandører. Det sker for at sikre, at de fortsat lever op til de sikkerhedskrav, som 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 inspektion af en stikprøve på underskrevne kontrakter påset, at informationssikkerhedskravene er kontraktligt aftalt. Vi har ved inspektion af en stikprøve på måneder 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.	Området er revideret uden bemærkninger.
15.2.1 Overvågning og gennemgang af leverandørydelser *Virksomheder skal regelmæssigt overvåge, gennemgå og revidere leverandørydelser.* IT Relation foretager en årlig risikovurdering af alle leverandører. Derudover foretages en mere omfattende risikovurdering af de mest kritiske leverandører som hardware-, datacenter- og softwareleverandører til datacenteret.	Vi har inspiceret, at der findes en formel, dokumenteret procedure, der sikrer, at nye eller genforhandlede applikations- eller leverandørkontrakter valideres i forhold til en liste over fastsatte informationssikkerhedskrav. Vi har ved inspektion af en stikprøve på underskrevne kontrakter påset, at informationssikkerhedskravene er kontraktligt aftalt. Vi har ved inspektion af en stikprøve på måneder påset, at IT Relation jævnligt reviderer hovedleverandører på baggrund af aftalte informationssikkerhedskrav. Vi har inspiceret, at tredjepartserklæringer for hovedleverandører er modtaget og behandlet af IT Relation.	Området er revideret uden bemærkninger.

A.16 Kontrolmål: Styring af informationssikkerhedshændelser

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

A.17 Kontrolmål: Informationssikkerhedsaspekter ved beredskabsstyring

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
17.1.1 Planlægning af informationssikkerheds-kontinuitet *Virksomheden skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.* IT Relation har en beredskabsplan for, hvordan virksomheden kan komme tilbage i drift hurtigst muligt i tilfælde af en katastrofe. Beredskabsplanen testes en gang om året.	Vi har inspiceret, at en formel og dokumenteret beredskabsplan vedligeholdes, gennemgås og godkendes en gang om året. Vi har inspiceret, at der er udarbejdet en beredskabsplan for hvordan, virksomheden kan komme tilbage i drift i tilfælde af en katastrofe. Vi har inspiceret, at de bagvedliggende procedurer for beredskabsplanen er blevet gennemgået og godkendt af relevant personale.	Området er revideret uden bemærkninger.
17.1.2 Implementering af informationssikkerhedskontinuitet *Virksomheden skal fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.* IT Relation har implementeret en beredskabsplan for hvert af sine kritiske systemer, så kunderne oplever så få gener som muligt i tilfælde af nedbrud af et kritisk system.	Vi har inspiceret, at en formel og dokumenteret beredskabsplan vedligeholdes, gennemgås og godkendes en gang om året. Vi har inspiceret, at der er udarbejdet en beredskabsplan for kritiske systemer.	Området er revideret uden bemærkninger.
17.1.3 Verificering, gennemgang og evaluering af informationssikkerhedskontinuiteten *Virksomheden skal med jævne mellemrum verificere de fastlagte og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.* Virksomheden verificerer med jævne mellemrum de fastlagte og implementerede kontroller vedrørende informationssikkerhedskontinuiteten for at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har inspiceret, at de bagvedliggende procedurer for forretningskontinuiteten gennemgås og opdateres. Vi har inspiceret, at de bagvedliggende procedurer er blevet testet for at sikre, at de er tidssvarende og effektive i kritiske situationer.	Området er revideret uden bemærkninger.

A.18 Kontrolmål: Overensstemmelse

IT Relations kontrolaktivitet	PwC's udførte test	Resultater af tests
18.1.1 Afdækning af gældende lovgivning og kontraktkrav *Alle relevante lov- og kontraktkrav samt virksomhedens metode til overholdelse af disse krav skal være klart identificeret, dokumenteret og opdateret for hvert informationssystem.* IT Relation anvender standardkontrakter. Hvis en kunde ikke kan leve op til forretningskravet i standardkontrakten, kan en tilpasset kontrakt aftales. I en sådan situation er kontrakten ejet af en service delivery manager, der er ansvarlig for at implementere de bestemmelser, der ikke er en del af en standardkontakt.	Vi har inspiceret, at en formel politik for overholdelse af relevant lovgivning vedligeholdes, gennemgås og godkendes.	Området er revideret uden bemærkninger.