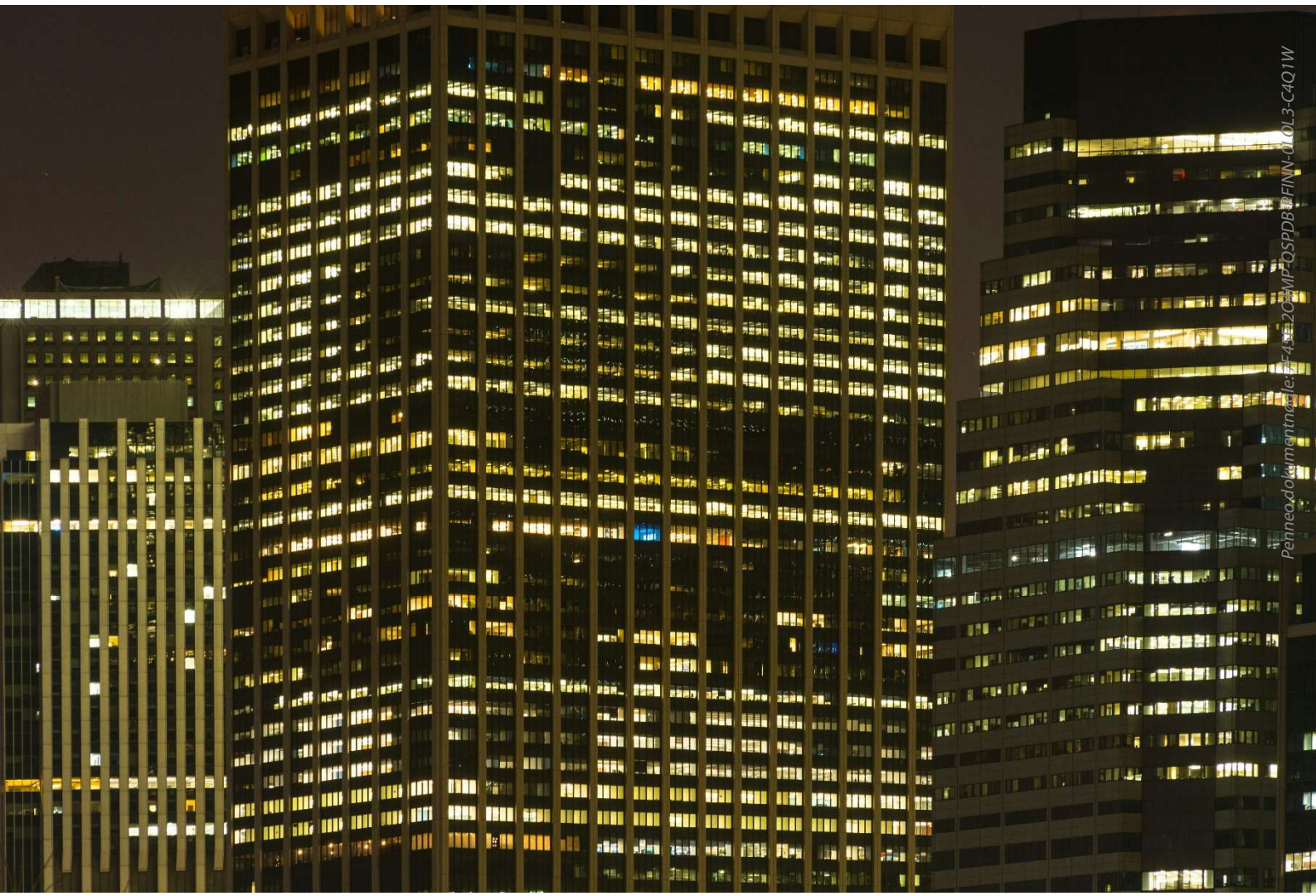
itm8 | Progressive A/S

Lyskær 3 B
2730 Herlev
CVR.nr. 25 22 33 30

ISAE 3402

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller relateret til regnskabsaflæggelsen i forbindelse med generelle driftsydelser i perioden 1. januar 2023 – 31. december 2023



Indhold

S.nr. 346315

JR/SO

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt itm8 | Progressive A/S' generelle driftsydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunder selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i den enkelte kundes regnskab.

itm8 | Progressive A/S bekræfter, at:

a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af de generelle kontroller i tilknytning til itm8 | Progressive A/S' generelle driftsydelser, der er anvendt af kunder i perioden 1. januar 2023 – 31. december 2023. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   (i) redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
   - De typer af ydelser, der er leveret, når det er relevant
   - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
   - relevante kontrolmål og kontroller, udformet til at nå disse mål
   - kontroller, som vi med henvisning til systemets 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 sammen med de specifikke kontrolmål, som vi ikke selv kan nå
   - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

   (ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system, foretaget i perioden fra 1. januar 2023 til 31. december 2023

   (iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som kunder måtte anse for at være vigtigt efter dennes 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 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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

Herlev, den 5. februar 2024
itm8 | Progressive A/S

Torben Friedrichsen
Chief Technology Officer

2. ITM8 | Progressive A/S' beskrivelse af generelle IT-kontroller for levering af generelle driftsydelser til kunder

Dette afsnit beskriver virksomheden Progressive A/S og den logiske afdeling "Progressive Datacenter".

Kort om Progressive A/S

Progressive IT blev stiftet i 1999 og har siden 2003 drevet hosting virksomhed. Selskabet har siden maj 2021 indgået i ITM8 gruppen.

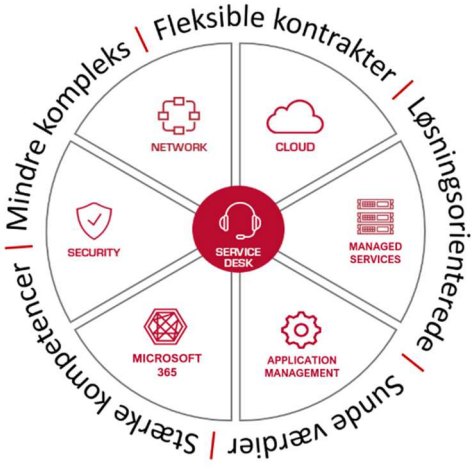
Progressive A/S har kontorer i Herlev og Aarhus, der servicerer virksomheder over hele landet med fokus på langvarige kunderelationer og sikre løsninger, der forbedrer Progressives kunders konkurrenceevne.

Progressives principper for kundeengagementer er:

- Fleksible kontrakter
- Løsningsorienterede
- Sunde værdier
- Stærke kompetencer
- Mindre kompleks

Erklæringens omfang

Progressive A/S rådgiver, designer, implementerer, servicerer og drifter IT løsninger både i egne datacentre, i public cloud og på vores kunders lokationer. Nedenstående diagram illustrerer Progressives serviceydelser:



Centrum for ydelserne er Progressives døgnbemandede Servicedesk, der udelukkende er bemandet med fastansat dansktalende personale placeret på kontorerne i Herlev og Aarhus. Servicedesk og bagvagter håndterer årligt 75.000 sager.

Progressives kunder kan afvikle deres løsninger på:

- eget udstyr på egne lokationer ('on premise')
- eget udstyr i Progressives datacentre ('housing')
- dedikeret udstyr lejet i Progressives datacentre ('hosting)'
- virtualiseringsplatform i udlandet ('public cloud')
- virtualiseringsplatform i Progressives datacentre ('private cloud')

Progressive driver egne datacentre til 'housing', 'hosting' og 'private cloud' tjenesterne.

De primære datacentre er placeret i København. Det ene på et fiberknudepunkt hvilket bevirker, at flere fiberleverandører lejer sig ind i datacenteret. Datacentrene i København er placeret ca. 10 km fra hinanden. Det tredje datacenter er et backup-datacenter.

Nærværende erklæring omfatter drift og overvågning samt datacentre.

Erklæringen omfatter ikke public cloud (såsom Microsoft Azure eller AWS) infrastruktur, konsulentydelser, udviklingsydelser eller leverancer af hard- eller software.

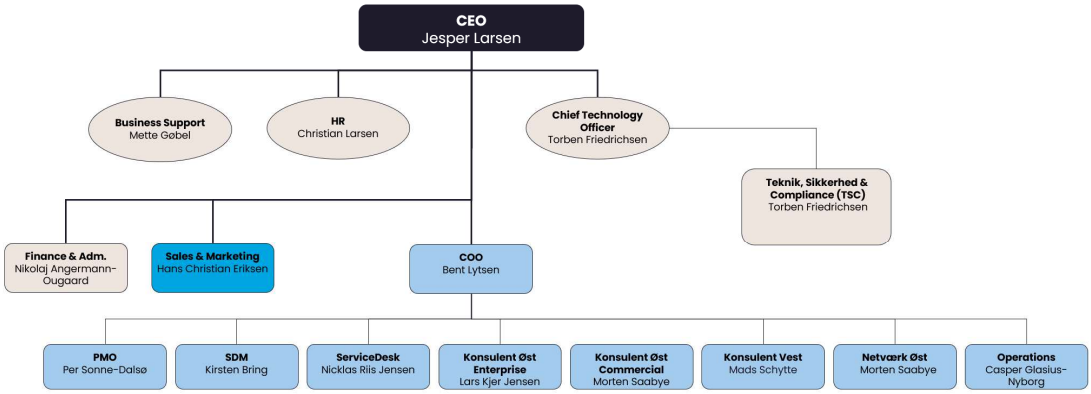
Erklæringen, inklusive beskrivelse, må kun anvendes af de virksomheder, der benytter Progressives driftsydelser samt disse virksomheders revisorer, og må ikke bruges til andre formål.

Organisation

Overordnet opbygning

Progressives overordnede organisation, hvor ledelsen har det øverste ansvar for informationssikkerheden.

Progressive organisation



progressive

Progressive er organiseret på den måde, at kerne infrastrukturen til 'private cloud' ligger i Operations, og det er 'Konsulent Øst & Konsulent Vest' konsulentorganisationen, der står for de kundespecifikke løsninger.

Konsulent Øst/Vest

Konsulent Øst/Vest rådgiver kunderne og etablerer løsninger i forhold til den enkelte kundes specifikke behov, så kundernes løsninger afvikles på den mest hensigtsmæssige platform og måde i forhold til økonomi, ydeevne, funktionelle krav og kundens egen organisation.

Herudover udføres projektarbejde indenfor Progressives ekspertiseområder i henhold til kundernes behov og ønsker. Større projekter udføres under styring af Project Management Office (PMO)

Kundernes egen driftsorganisation eller Progressives konsulentafdeling kan helt eller delvis varetage de løbende drifts-opgaver på en løsning i henhold til specifikke aftaler.

Servicedesk

Servicedesk har den primære daglige kontakt med kunderne. Servicedesk håndterer langt de fleste henvendelser, der enten løses med det samme eller videregives til andre i organisationen, konsulenter, operationsfolk og bagvagter i Progressive.

SDM

Service Delivery Managers (SDM) håndterer den daglige kontakt med kunderne og evt. intern opfølgning. SDM sikrer desuden den interne koordinering og planlægning af ressourcer.

Operations og Netværk

Operations og Netværk etablerer, driver og udbygger datacenter-, servervirtualiserings-, storage-, overvågnings- og backupinfrastrukturen og løser herudover kundespecifikke netværksopgaver. Derudover håndterer Operations og Netværk planlagte servicevinduer i datacentrene.

Risikostyring

Progressives ledelse har det overordnede ansvar for risikovurderingen og informationssikkerheden i virksomheden. Derfor gennemgår og godkender CEO og ledelse risikovurderingen én gang årligt, og Udvalget for Informationssikkerhed behandler løbende risiciene og eskalerer revurderede og nytilkomne risici til ledelsen.

Risikostyringen er i overensstemmelse med ISO 27001 og ISO 27005 defineret "Risk Assesment and Treatment Process" (ISMS06002), der er detaljeret beskrevet i Progressives ISMS (Information Security Management System).

Risici vurderes ud fra konsekvens ("impact") og sandsynlighed ("likelihood") inden for områderne kundedrift, lov- og standardoverholdelse, sikkerhed, knock-out konsekvens, sundhed, økonomi og omdømme.

Både konsekvens og sandsynlighed bliver vurderet inden for fem veldefinerede niveauer, hvor fem er højeste niveau, og det risikoniveau for de enkelte risici er produktet af konsekvens og sandsynlighed, og vil altså være et tal mellem 1 og 25.

Risikoniveauet bruges til at klassificere de enkelte risici inden for 3 kategorier og sætter rammen for initiativer til risikoreduktion prioriteres i forhold til niveauerne HØJ (12-25), MIDDEL (5-10) og LAV (1-4).

Der arbejdes med forebyggende og udbedrende tiltag indenfor procedurer, teknisk udstyr og de fysiske rammer:

	Forebyggende Tiltag	**Udbedrende Tiltag**
Procedure Tiltag	Bagvagter Change Management med CAB Compliance Audit Daglige driftskoordineringsmøder Døgnbemandet Servicedesk DPO - Data Protection Officer Enterprise Architecture Informationssikkerhedsudvalg ISMS (ISO 27001 struktur) Passwordpolitik Service aftaler med leverandører Straffeattest ved ansættelse Uddannelse	Beredskabsplan Disaster Recovery Procedure Logging Major Incident Procedure Security Breach Review

	Forebyggende Tiltag	Udbedrende Tiltag
Tekniske Tiltag	Antivirus/EDR Firewalls Monitorering Patch Management Redundans Staging miljøer (test, QA, demo)	Backup/Restore Backup lokation Intrusion detection Server Snapshots
Fysiske Tiltag	Adgangskontrol Alarmsystem Generatortest Strømfilter Videoovervågning	Alarmcentral Dieselgeneratorer Inergen brandslukning UPS (A+B strøm)

Kontrolmiljø

Progressive tager udgangspunkt i ISO 27000 serien, der benyttes som rammeværk til etablering af kontrolmiljøet.

Hovedområderne i ISO 27001 er:

- Kap 4. Organisationens kontekst
- Kap 5. Lederskab
- Kap 6. Planlægning
- Kap 7. Support
- Kap 8. Drift
- Kap 9. Evaluering
- Kap 10. Forbedring

Indenfor hovedområderne defineres:

- Politikker: Hensigter og udviklingsretninger, der er udtrykt af topledelsen
- Retningslinjer: Rammer der afspejler hvilke valgte ÍSO 27001 elementer der skal efterleves
- Processer: Beskrivelser af specifikke aktiviteter (hvem gør hvad?)
- Instrukser: Konkrete arbejdsbeskrivelser (hvordan gøres det?)

Derudover er der en række kontroller inden for nedenstående områder:

- A.5 Informationssikkerhedspolitikken
- A.6 Organisering af informationssikkerhed
- A.7 Personalesikkerhed
- A.8 Styring af aktiver
- A.9 Adgangsstyring
- A.10 Kryptografi
- A.11 Fysisk sikring og miljøsikring
- A.12 Driftssikkerhed
- A.13 Kommunikationssikkerhed
- A.14 Anskaffelse, udvikling og vedligeholdelse af systemer
- A.15 Leverandørforhold
- A.16 Styring af informationssikkerhedsbrud
- A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetablering
- A.18 Overensstemmelse

IT-kontrollerne udføres med ISO 27002 som referenceramme.

A.6 Organisering af Informationssikkerhed

Progressive har et udvalg for Informationssikkerhed, der mødes månedligt for at behandle sikkerheden og eventuelle sikkerhedshændelser. Udvalget vurderer også, om der er ændringer i ydre eller indre omstændigheder, der bør afstedkomme en revurdering af den forebyggende eller kontrollerende indsats.

I udvalget er CEO, COO, CTO, DPO, Security & Compliance Manager samt Data Protection Advisor.

Ledelsen har ansvaret for udarbejdelsen, vedligeholdelsen og formidlingen af sikkerhedspolitik, risikovurdering, beredskabsplaner, driftsrutiner og dokumentation af forretningsgange.

Operations har ansvaret for den tekniske sikkerhed, og varetager implementering og ajourføring af sikkerheds- og kvalitetsprocedurer.

Security & Compliance Manager forestår den primære kontakt til revisorer og auditorer, driver udførelsen af egenkontroller, samt udarbejder og ajourfører beredskabsplanen i samarbejde med Operations.

Der er etableret et ISMS (Information Security Management System) til at understøtte arbejdet, der er organiseret i henhold til ISO 27001, og hvor al information er versioneret på sådan en måde, at en hvilken som helst version kan sammenlignes med en anden, så ledes at der er fuldt revisionsspor i de enkelte politikker og retningslinjer, processer og instrukser samt beviserne for de gennemførte kontroller.

Progressives Informationssikkerhedspolitik er forankret i virksomhedens personalehåndbog, som alle nye medarbejdere modtager ved ansættelsen, og hvor den seneste version til enhver tid er tilgængelig på intranettet.

Progressive laver årligt en overordnet kompetencekortlægning og uddannelsesplan på baggrund af strategi, vedligeholdelse af certificeringer og oplæg fra de enkelte personaleledere. Medarbejdere er berettiget og forpligtet til relevant videreuddannelse, der aftales med nærmeste overordnede, og hvor alle omkostninger afholdes af Progressive. Derudover påhviler det den enkelte medarbejder selv at følge den faglige udvikling inden for sit område. Uddannelsesaftaler og opfølgning dokumenteres på de regelmæssige dialogmøder mellem medarbejder og leder.

Der er driftskontrakter med de aftalte ydelser for alle kunder enten i form af standardkontrakter eller i form af kundespecifikke aftaler.

A.7 Medarbejdersikkerhed

Progressives ledelse har ansvaret for, at alle medarbejdere er kvalificerede og egnede til opgaven, og at de er bekendt med deres roller og ansvar i organisationen.

Der foreligger en fast procedure for ansættelse og ophør af medarbejdere. Ved ansættelse gennemføres blandt andet en psykologisk test på kandidater og nye medarbejdere skal indlevere en straffeattest før arbejdet påbegyndes.

Fortrolighed om Progressives og kunders forhold under og efter ansættelsen er en del af de generelle vilkår, der er beskrevet i enhver medarbejders ansættelseskontrakt.

A.8 Styring af Aktiver

Politiken for Styring af Aktiver er understøttet af procedurer og politiker såsom

- Håndtering af flytbare medier
- Klassifikation af information
- Backup politik
- Fjernarbejde politik

A.9 Adgangsstyring

Der skal være et funktionsbestemt behov for at få adgang til IT-systemer, hvad enten det er interne systemer eller kundesystemer, og al adgang styres via AD (Active Directory) opsætning.

AD bliver løbende gennemgået med henblik på at afgøre, om der er nogle personer, der har en adgang, som de ikke bør have.

Alle medarbejdere er underlagt en IT bruger politik (A.5), der omfatter brug af stærke kodeord og f.eks. pauseskærms-politik.

Til opbevaring af kundespecifikke kodeord bruges der et Password Management System. Det sikrer kodeord og fuld sporbarhed.

Der bruges to-faktor godkendelse for alle Progressives medarbejdere på kontoret, ved fjernarbejde og alle public cloud services, samt yderligere to-faktor godkendelse til adgang til produktionssystemer.

A.10 Kryptografi

Der forefindes en politik for brug af kryptografi, og valg af kryptografisk metode foretages ud fra en risikovurdering og bran-chepraksis.

A.11 Fysisk Sikkerhed

Adgangskontrol til kontor

Alle medarbejdere forsynes med adgangskort og kode, der skal bruges for at komme ind på kontoret og bevæge sig rundt mellem zonerne.

Besøgende skal skrive sig ind i receptionens logbog, hvorefter de afhentes af deres vært, der har ansvaret for dem under besøget, og som skal sikre, at de besøgende eskorteres tilbage til udgangen og skriver sig ud i logbogen.

Adgangskontrol til datacentre

Det er kun medarbejdere, der har et arbejdsbetinget behov for datacenteradgang, som får adgangskort med mulighed for at komme ind i datacentrene.

Alle datacentre er ud over alarm og video forsynet med et elektrisk metalgitter, der er lukket, når der ikke er medarbejdere til stede.

A.12 Driftssikkerhed

Datacentre

Alle datacentre er forsynet med flere fiberforbindelser for at nedbringe risikoen for nedetid pga. mulige fejl hos netværksle-verandører. Hoveddatacenteret er fiberknudepunkt for flere leverandører.

Den overordnede arkitektur er, at datacentrene i København er de primære, og datacenteret i Herlev er backup center. Det vil sige, at al backup af datacentrene i København er placeret i Herlev. Kortidsbackup ligger på disk og langtidsarkivering ligger på bånd.

Der er to dieselgeneratorer og to nødstrømsanlæg i de primære datacentre, der også kan tåle, at et køletårn falder ud af drift. I backup-datacenteret er der køle og nødstrømsanlæg.

Change Management

Progressive arbejder konsekvent efter en Change Management politik for kerneinfrastrukturen, ligesom der for en række kunder er aftalt en specifik Change Management procedure i samarbejdshåndbogen

Den overordnede procedure er

1. En RFC (Request For Change) udarbejdes med beskrivelse af ændringsanmodningen
2. Ændringsanmodningen behandles af CAB (Change Advisory Board) især med fokus på
    a. Risiko- og konsekvensvurdering - også i forhold til kapacitets planlægning
    b. Vurdering af en eventuelt test rapport
    c. Detaljeret køreplan – ned til minutniveau – for indgrebet
    d. Fall-back kriterier og planer
    e. Hypercare planer
    f. 'Operational Readiness' og dokumentation
3. Logning af hvordan indgrebet og selve ændringen er forløbet
    a. Retrospektiv gennemgang af forløbet, hvis der er problemer

Der er en række definerede ændringer af sådan en karakter, at de ikke kræver et møde i CAB, men alle ændringer vil uden undtagelse blive registreret i Operations Change Calendar.

Backup og Disaster Recovery

Progressive benytter to førende backupteknologier, nemlig IBM Spectrum Protect (tidligere kendt som TSM - Tivoli Storage Manager) til almindelig backup og Veeam til såkaldt image backup.

For begge teknologiers vedkommende bliver backup foretaget fra datacentrene i København til datacenteret i Herlev.

Backup er underlagt overvågning og hver dag gennemgås backup-alarmerne. Backups der ikke har kørt automatisk i løbet af natten køres manuelt.

Data Backup

Data backup foretages mindst en gang i døgnet.

Disaster Recovery

Disaster Recovery Backup benyttes til at hurtig genetablering af virtuelle servere ved brug af Veeam.

Logning og overvågning

Logning

Alle adgange i interne systemer og produktionssystemer logges. Logningen sker til et lukket logningssystem, som kun godkendt personale har adgang til. Logdata opbevares i 6 måneder.

Der opsamles blandt andet information vedr.:

- Dato og tid på log on/log off
- Succes og afviste adgangsforsøg
- Ændringer i systemparametre og konfigurationer
- Brug af applikationer

Overvågning

Proaktiv gennemgang af audit logs foretages på basis af IT-kontroller, der er oprettet som gentagelsesopgaver i ITSM-systemet eller i forlængelse af fornyede risikovurderinger. Gennemgangen prioriteres iht. nedenstående kriterier:

- Forretningskritiske applikationer

- Adgange hvor klassifikation af data er involveret
- Systemer der er eksponeret mod eksterne netværk

Patch Management

Kerneinfrastrukturen patches automatisk (f.eks. Microsofts "patch Tuesday") og varetages af Operations, hvorimod kundernes systemer opdateres efter de specifikke aftaler, og det varetages af konsulentafdelingen for at sikre, at en opdatering ikke forstyrrer driften af kundernes forretningskritiske systemer.

A.13 Kommunikationssikkerhed

Der bruges altid sikker kommunikation. Al infrastruktur bruger certifikater og der bruges en høj grad af segmentering i forhold til funktion.

E-mail afsendes altid med højeste niveau af kryptering og der bruges altid krypteret linjer både internt og eksternt ved adgang til forretningssystemer.

A.14 & 15 Anskaffelse, Udvikling og Vedligeholdelse af Informationsbehandlingssystemer

Nyanskaffelser af servere, storage, netværk, software og services bliver håndteret på struktureret vis, hvor de relevante interessenter bliver hørt før anskaffelsen, og hvor sikkerhedsaspekterne (inkl. leverandør-vurdering) medtages som såkaldt NFR (non-functional requirement).

A.16 Styring af Sikkerhedshændelser

Medarbejderne har ansvaret for omgående at rapportere sikkerhedsbrister eller mistanke herom til ledelsen, og det er ledelsens ansvar at overvåge sikkerhedsbrister og følge op på dem.

Sikkerhedsbrister vil blive håndteret som Major Incidents med den forskel, at de også vil blive logget i en journal over sikkerhedsbrister, og få en særskilt mærkat i driftskalenderen.

Derudover vil en sikkerhedsbrist blive behandlet på førstkommende møde i Udvalget for Informationssikkerhed, hvor der især vil være fokus på, om de gældende procedurer er tilstrækkelige, eller om der skal tages yderligere forebyggende tiltag for fremover at undgå en lignende hændelse.

A.17 Beredskabsstyring

Identifikation af Kritiske Processer

Selskabet har via forretningsnødplaner ("business continuity plan") fokus på at sikre den fortsatte drift af såvel kunders som egne IT-miljøer og systemer.

Information og Kommunikation

Det centrale i enhver beredskabssituation er at sikre relevant og rettidig kommunikation til alle relevante interessenter, som både kan være de interessenter, der skal få systemet tilbage i fuld drift, som dem der skal begrænse eventuelle følgeskader eller overveje alternative løsninger.

Progressive har med udgangspunkt i ITIL defineret en Major Incident procedure, hvor en Incident Manager er ansvarlig for opsamling og kommunikation.

Kontrolaktiviteter

Katastrofeplanen forefindes i både i ISMS og som udskrift, som Operations medarbejdere er i besiddelse af, og der er beskrevne kontrolmål og kontrolaktiviteter.

A.18 Overensstemmelse & Kravoverholdelse

Lovbestemte Krav

Progressive har tilknyttet en IT Advokat med henblik på sikring af, at ledelse og Udvalget for Informationssikkerhed løbende bliver gjort bekendt med domme og kommende lovkrav, der er relevante for informationssikkerheden.

Standarder

Progressive ønsker i videst muligt omfang at tage udgangspunkt i internationale standarder uanset om det er formelle standarder som ISO (f.eks. ISO 27001) eller 'de facto' standarder. Fordelene er, at det er mere transparent for kunderne, og at medarbejderne i tidligere virke har været vant til at arbejde efter dem.

Kontraktkrav

Progressive bliver årligt revideret af en ekstern revisor, der skal afgive ISAE 3402 Type 2 erklæring med ISO 27002 som referenceramme for vores IT-kontroller.

Industrikrav

Progressive deltager i relevante industrifora og -foreninger i det omfang vi mener, at det er en fordel for kunderne. Progressive er medlem af Danish Cloud Community (tidl. BFIH - Brancheforeningen for IT Hosting).

3. Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning

Til ledelsen hos itm8 | Progressive A/S, kunder og disses revisorer

Omfang
Vi har fået som opgave at afgive erklæring om itm8 | Progressive A/S's beskrivelse i afsnit 2 af it-kontroller for perioden 1. januar 2023 til 31. december 2023 og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende beskrivelse omfatter ikke kundespecifikke forhold.

itm8 | Progressive A/S' ansvar
itm8 | Progressive A/S 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 at udforme, implementere og effektivt udføre 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, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

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

Revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om itm8 | Progressive A/S's beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, *Erklæringer med sikkerhed om kontroller hos en serviceleverandør*, som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet 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 sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet.

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

Begrænsninger i kontroller hos en dataansvarlig
itm8 | Progressive A/S's beskrivelse er udarbejdet for at opfylde de almindelige behov hos kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som kunder måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelig 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 i afsnit 1. Det er vores opfattelse,

(a) at beskrivelsen af itm8 | Progressive A/S' generelle driftsydelser, således som de var udformet og implementeret i perioden 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er retvisende, og
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2023 til 31. december 2023, og
(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i perioden 1. januar 2023 til 31. december 2023.

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

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder og disses revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i kunders regnskab.

Søborg, 5. februar 2024

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
statsautoriseret revisor

Simon Okkels
IT revisor, CISA

4. Kontrolmål, kontroller, test og resultat heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som itm8 | Progressive A/S har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 1. januar 2023 til 31. december 2023.

Vi har således ikke nødvendigvis testet alle de kontroller, som itm8 | Progressive A/S har nævnt i beskrivelsen i afsnit 2.

Kontroller udført hos itm8 | Progressive A/S' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Test af kontrollernes design, implementering og operationelle effektivitet er foretaget via følgende metoder:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel til passende personale hos itm8 | Progressive A/S er udført for alle væsentlige kontrolaktiviteter. Forespørgsler er udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres. Endvidere for at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation, som indeholder information om udførelse af kontrollen. Det omfatter gennemlæsning og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Observation	Observation af kontrollens udførelse.
Genudførelse af kontrol	Den relevante kontrol er genudført med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores test af de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

4 Risikovurdering

Kontrolmål 4.1 (Retningslinjer for risikovurderinger)

Virksomheden har en procedure for udarbejdelse af risikovurdering og der er udarbejdet en aktuel og godkendt risikoanalyse, ligesom der udarbejdes planer for håndtering af risici.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der skal udarbejdes risikovurdering. Risikovurderingen skal udarbejdes minimum årligt og godkendes af ledelsen. Risikovurderingen skal indeholde planer for håndtering af risici.	Vi har forespurgt ledelsen om en skriftlig procedure for risikovurdering. Vi har forespurgt ledelsen om den aktuelle risikoanalyse. Vi har inspiceret, at der findes en aktuel risikoanalyse, denne har været gennemgået i Informationssikkerhedsudvalget, og ledelsen har godkendt risikoanalysen. Vi har inspiceret at der foreligger planer for håndtering af risici.	Vi har ikke konstateret væsentlige afvigelser.

5 Informationssikkerhedspolitikker

Kontrolmål 5.1 (Retningslinjer for styring af informationssikkerhed)

At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
5.1	Sikkerhedspolitikker skal være dokumenteret og vedligeholdes ved gennemgang mindst en gang årligt. Sikkerhedspolitikken skal være godkendt af ledelsen. Sikkerhedspolitikken er gjort tilgængelig for medarbejdere f.eks. via intranettet. Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt ledelsen om seneste sikkerhedspolitik. Vi har inspiceret, at der forefindes en sikkerhedspolitik og ledelsen har godkendt sikkerhedspolitikken. Vi har inspiceret, at sikkerhedspolitikken er let tilgængelig for medarbejderne. Vi har inspiceret at sikkerhedspolitikken som minimum er revurderet én gang årligt.	Vi har ikke konstateret væsentlige afvigelser.

6 Organisering af informationssikkerhed

Kontrolmål 6.1 (Intern organisering)

At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
6.1	Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver. Der skal opretholdes passende kontakt med relevante myndigheder. Der skal opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer. Informationssikkerhed skal anvendes ved projektstyring.	Vi har forespurgt ledelsen om de organisatoriske roller og ansvar, der gælder i forbindelse med styring af informationssikkerheden. Vi har inspiceret, at det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret via udvalgte referater fra mødeaktiviteter. Vi har inspiceret at forhold omkring funktionsadskillelse er vurderet og tilstrækkeligt implementeret hvor muligt. Vi har inspiceret at der er uddelegeret ansvar for kontakt med relevante myndigheder. Vi har forespurgt hvordan der opretholdes kontakt med særlige interessegrupper. Vi har forespurgt ledelsen om retningslinjerne for projektledelse.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 6.2 (Mobilt udstyr og fjernarbejdspladser) At sikre fjernarbejdspladser og brugen af mobilt udstyr.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
6.2	Der er udarbejdet politikker og retningslinjer for brugen af mobile enheder. Der er udarbejdet politikker og retningslinjer for fjern- og hjemmearbejdspladser.	Vi har forespurgt ledelsen om politikker og retningslinjer for medarbejderes brug af mobile enheder. Vi har inspiceret, at der er udarbejdet politikker og retningslinjer for brugen af mobile enheder herunder medarbejders eget udstyr (BYOD). Vi har forespurgt ledelsen om politikker og retningslinjer for medarbejderes brug af hjemmearbejdspladser/fjernarbejdspladser. Vi har inspiceret, at der er udarbejdet politikker og retningslinjer for hjemmearbejde. Vi har inspiceret VPN opsætning til fjernopkobling til internt netværk.	Vi har ikke konstateret væsentlige afvigelser.

7 Personalesikkerhed

Kontrolmål 7.1 (Før ansættelsen)

At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.1	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. Der er i denne henseende indført retningslinjer om at påse straffeattest i forbindelse med rekruttering af medarbejdere, ligesom der kan være tilfælde hvor medarbejdere skal sikkerhedsgodkendes via FE og/eller PE. Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed..	Vi har forespurgt ledelsen om procedurerne for rekruttering af medarbejdere. Vi har inspiceret, at der foretages screening af nyansættelser. Vi har inspiceret, at ansættelsesvilkårene indeholder beskrivelser af ansvar i forbindelse med informationssikkerhed. Vi har inspiceret at der underskrives en fortrolighedsaftale. Vi har inspiceret at ansøgere i rekrutteringsforløbet introduceres for retningslinjerne for informationssikkerhed.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 7.2 (Under ansættelsen)

At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.2	Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer. Medarbejdere skal løbende informeres og gennemgå awarenestræning for at sikre forståelsen for deres ansvar og rolle, således, at de kan opfylde deres informationssikkerhedsansvar.	Vi har forespurgt ledelsen til beskrivelsen af kravene til ledere i forhold til opretholdelse af ansvar for informationssikkerheden. Vi har inspiceret, at ledelsesforholdene er velbeskrevne, og der forefindes let tilgængelige og opdaterede organisationsdiagrammer. Vi har inspiceret, at der har været gennemført relevant uddannelse og awarenestræning.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 7.3 (Ansættelsesforholdets ophør eller ændring) At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.3	Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med ansættelsesophør. Vi har inspiceret, at der findes en proces til sikring af tilbagelevering af væsentlige aktiver i forbindelse med fratrædelse, og suspendering af brugerrettigheder eller lign. Vi har inspiceret at brugerrettigheder vurderes i forbindelse med en væsentlig ændring i ansættelsesforholdet. Vi har foretaget stikprøvekontrol for dokumentation for udførelsen.	Vi har ikke konstateret væsentlige afvigelser.

8 Styring af aktiver

Kontrolmål 8.1 (Ansvar for aktiver)

At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
8.1	Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver. Der skal udpeges en ejer i organisationen for hvert aktiv. Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og implementeres. Alle medarbejdere og eksterne brugere skal aflevere alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med identifikation af informationsaktiver. Vi har stikprøvevis inspiceret fortegnelsen over kritiske informationsaktiver. Vi har inspiceret, at det organisatoriske ansvar for informationsaktiver er dokumenteret og implementeret, og at der er placeret ejerskab i forhold til ansvar for den tilhørende informationssikkerhed. Vi har forespurgt ledelsen om procedurerne vedr. accepteret brug af aktiver. Vi har inspiceret et udvalg af fratrædelser og påset kvitteringer for tilbagelevering af udleverede aktiver.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 8.2 (Klassifikation af information) At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
8.2	Information skal klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring. Der skal udarbejdes og implementeres et passende sæt af procedurer til mærkning af information i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget. Der skal udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, organisationen har vedtaget.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med klassifikation af informationsaktiver. Vi har forespurgt ledelsen om procedurer for mærkning af information i henhold til klassifikationssystemet. Vi har forespurgt ledelsen om procedurer for håndtering af aktiver i relation til klassifikation.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 8.3 (Mediehåndtering) At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
8.3	Der skal implementeres procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget. Medier skal bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer. Medier der indeholder information, skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med styring af bærbare medier. Vi har inspiceret, at der findes en procedure til sikker bortskaffelse af informationsbærende medier. Vi har forespurgt eksempler på udført bortskaffelse af informationsbærende medie.	Vi har ikke konstateret væsentlige afvigelser.

9 Adgangsstyring

Kontrolmål 9.1 (Forretningsmæssige krav til adgangsstyring)

At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.1	En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav. Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Vi har inspiceret politikken for adgangsstyring, herunder om denne er opdateret og godkendt. Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester. Vi har inspiceret et udvalg af brugere med henblik på at konstatere, at de kun har adgang til netværkstjenester, der er tildelt på baggrund af et arbejdsrelateret behov.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 9.2 (Administration af brugeradgange) At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.2	Alle brugere skal være registeret med et unikt bruger-id, og deres rettigheder til netværk og systemer skal være i overensstemmelse med virksomhedens politikker. Endvidere sikres det, at rettigheder begrænses mest muligt, er betinget af et arbejdsrelateret behov, er godkendt og oprettet korrekt i systemerne. Administratorkonti kontrolleres med jævne mellemrum for at sikre systemets integritet. Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp af formel administrationsproces Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder. Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller skal tilpasses efter en ændring.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med brugeradministration. Vi har stikprøvevis indhentet oversigter over brugerkonti på systemer og netværk. Vi har stikprøvevis udvalgt nye brugere og inspiceret, at anmodning om adgang fra disse var dokumenteret og godkendt i overensstemmelse med relevant sikkerhedspolitik. Vi har forespurgt ledelsen om procedurerne for hemmelig autentifikationsinformation. Vi har inspiceret et udvalg af brugerreview rapporter, herunder de konklusioner der er foretaget. Vi har stikprøvevis sammenholdt oversigten over ophørte brugere med oversigten over aktuelle brugerkonti og inspiceret, at brugerkonti var deaktiveret eller slettet.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 9.3 (Brugernes ansvar) At gøre brugere ansvarlige for at sikre deres autentifikationsinformation			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.3	Det skal være et krav, at brugerne følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation. Adgange til systemer, netværk, databaser og datafiler, er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde, kompleksitet og udløbstid ligesom passwordopsætninger medfører, at password ikke kan genbruges. Endvidere bliver brugeren deaktiveret ved gentagne fejlagtige forsøg på login.	Vi har inspiceret passwordpolitikken. Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordadministration. Vi har inspiceret password-settings i serverinfrastruktur, og databaser ved inspektion af konfigurationsudtræk. Vi har forespurgt om der udføres test af "weak password", og påset dokumentation herfor.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 9.4 (Styring af system- og applikationsadgang) At forhindre uautoriseret adgang til systemer og applikationer			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9.4	Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring. Adgang til systemer og applikationer styres af en procedure for sikker log-on. Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet. Brugen af systemer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med retningslinjerne for begrænsning af adgang til information. Vi har inspiceret at der er implementeret en procedure for sikker log-on. Vi har forespurgt ledelsen om anvendelsen af systemer til administration af adgangskoder.	Vi har ikke konstateret væsentlige afvigelser.

10 Kryptografi

Kontrolmål 10.1 (Kryptografiske kontroller)

At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
10.1	Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information. Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi. Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet.	Vi har ikke konstateret væsentlige afvigelser.

11 Fysisk sikring og miljøsikring

Kontrolmål 11.1 (Sikre områder)

At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
11.1	Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter. Adgang til sikrede lokaler er styret via adgangskontrolsystem. Kun personer med gyldigt personligt adgangskort med billede har adgang. Kode er påkrævet. Personer uden autorisation, som har behov for adgang til lokaler, vil altid have ledsaget adgang af en person med gyldig adgang. Adgang til kontorer og øvrige lokaler kræver gyldigt adgangskort. Gæster kan registrere sig til et gæstekort i receptionen, disse kort kan kun benyttes i normal kontortid. Normale adgangskort kræver brug af kode uden for normal kontortid.	Vi har stikprøvevis inspiceret, at der er implementeret perimetersikring af lokaler og bygninger i overensstemmelse med beskrivelserne. Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med fysisk adgangskontrol for lokaler og bygninger. Vi har inspiceret selskabets datacenter og observeret, at adgang til sikre områder er begrænset ved anvendelse af adgangskontrol. Vi har stikprøvevis inspiceret procedurerne for fysisk sikkerhed vedrørende sikrede områder, for at vurdere om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse. Vi har inspiceret procedurerne vedr. besøg fra gæster.	Vi har ikke konstateret væsentlige afvigelser.

11 Fysisk sikring og miljøsikring

	Der er etableret beskyttelse mod naturkatastrofer og ondsindede angreb eller ulykker. Procedurer for arbejde i sikre områder skal tilrettelægges og etableres. Adgangssteder som fx områder til af- og pålæsning og andre steder, hvor uautoriserede personer kan komme ind på området, skal kontrolleres og så vidt muligt adskilles fra informationsbehandlingsfaciliteter for at undgå uautoriseret adgang.	Vi har inspiceret datacenterlokationen, med henblik på at teste forholdene omkring beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker.	

Kontrolmål 11.2 (Udstyr) At undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
11.2	Datacenteret er beskyttet mod skader som følge af f. eks. brand, vand, varme og uautoriseret adgang. Der er reaktiv overvågning af datacenter infrastrukturen. Udstyr er beskyttet mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyning. Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, er beskyttet mod aflytning, interferens og skader. Udstyr vedligeholdes regelmæssigt via eftersyn og afprøvninger, for sikring af fortsat tilgængelighed og korrekt funktion. Der skal etableres sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationens lokaler. Alt udstyr med lagringsmedier slettes eller destrueres eller overskrives forsvarligt inden bortskaffelse og genbrug. Brugere er via retningslinjer gjort opmærksom på deres ansvar for udstyr uden opsyn, herunder er der etableret foranstaltninger som f.eks. Passwordbeskyttede pauseskærme. Der er er etableret "clean desk policy".	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres samt de sikkerhedsforanstaltninger der er etableret i forbindelse med indretningen af eget datacenter. Dokumentation for løbende vedligeholdelse og test af udstyr og alarmer er gennemgået. Vi har inspiceret tilstedeværelsen af forebyggelsessystemer i datacenter, herunder: Hævet gulv, sikret mod fugt, installeret fugtdetektorer, servere forsynes fra to forskellige faser, installeret UPS og nødstrømsgenerator, brandslukningssystem, installeret videoovervågning og redundant internetforbindelse. Vi har inspiceret at kabling er foretaget af autoriseret elektriker, hvor branchestandarder er anvendt til sikring af kabler og kabelføring. Vi har stikprøvevis inspiceret vedligeholdelsesplanerne for datacenterets grundlæggende infrastruktur. Vi har inspiceret retningslinjerne for brugernes ansvar for udstyr uden opsyn. Vi har inspiceret retningslinjerne og inspiceret via besøg på hovedkontoret at retningslinjerne følges.	Vi har ikke konstateret væsentlige afvigelser.

12 Driftssikkerhed

Kontrolmål 12.1 (Driftsprocedurer og ansvarsområder)

At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.1	Der skal være tilfredsstillende procedurer og forretningsgange for opretholdelse af driften. Herunder findes overvågning, registrering af hændelser og opfølgning på disse. Nye systemer og væsentlige opgraderinger bliver testet, herunder brugeraccepttest af kvalificerede medarbejdere og dokumenteres og godkendes før implementering i produktionsmiljøet. Der udføres endvidere efterfølgende verifikation af implementeringer. Problemer identificeret under udvikling og implementering af nye systemer og væsentlige opdateringer bliver løst tilfredsstillende. Ændringer er underlagt konfigurationsstyring. Nødændringer af systemer og netværk uden om den normale forretningsgang bliver testet og godkendt efterfølgende. Anvendelsen af ressourcer skal styres og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemerne fungerer som krævet. Der er implementeret politikker og procedurer til sikring af funktionsadskillelse i virksomheden. Disse politikker og procedurer omfatter krav til at: • Ansvar og aktiviteter for udvikling, test og produktion er adskilte • Administratorer med ansvar for produktion har ikke adgang til	Vi har forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret. I forbindelse med revisionen af de enkelte driftsområder har vi kontrolleret, at der foreligger dokumenterede procedurer, samt at der stikprøvevis er overensstemmelse mellem dokumentationen og de handlinger som faktisk udføres. Vi har stikprøvevis inspiceret ændringsønsker for følgende: • Dokumenteret test af ændringer, herunder godkendelse. • Godkendelse skal være opnået før implementering. • Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende • Dokumenteret plan for tilbagerulning, hvor relevant. Vi har inspiceret brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi har ikke konstateret væsentlige afvigelser.

12 Driftssikkerhed

	applikationer og transaktioner. • Administratorer med ansvar for produktion har ikke adgang til applikationer og transaktioner.		

Kontrolmål 12.2 (Beskyttelse mod malware)

At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.2	Der er installeret centralt overvåget antivirus på workstations og laptops. Disse funktioners databaser opdateres regelmæssigt og kan ikke modificeres af de enkelte medarbejdere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med malwarebeskyttelse. Vi har inspiceret tilstedeværelsen af antivirusprogrammer på workstations og laptops.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 12.3 (Backup)

At beskytte mod tab af data.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.3	Det sikres, at der foretages løbende backup af relevante komponenter i infrastrukturen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med backup. Vi har stikprøvevis inspiceret backupprocedurer til bekræftelse af, at de er formelt dokumenteret. Vi har stikprøvevis inspiceret backuplogs vedrørende backups til bekræftelse af, at backups er gennemført succesfuldt, alternativt, at der foretages afhjælpning i tilfælde af mislykkede backups. Vi har stikprøvevis inspiceret restorelogs.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 12.4 (Logning og overvågning) At registrere hændelser og tilvejebringe bevis.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.4	Der udføres hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser, som opbevares og gennemgås regelmæssigt. Logningsfaciliteter og log-oplysninger er beskyttet mod manipulation og uautoriseret adgang. Transaktioner eller aktiviteter samt brugere med privilegerede rettigheder (f.eks. superbrugere) bliver logget. Dette inkluderer også databaser. Afvigende forhold undersøges og løses rettidigt. Der er etableret tidssynkronisering i hele infrastrukturen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med overvågning af systemanvendelse og logning. Vi har stikprøvevis inspiceret log-settings ud fra systemudtræk af platforme og systemer. Vi har forespurgt til proces og foranstaltninger til sikring mod manipulation af logs. Vi har stikprøvevis inspiceret logs for administratorer og systemoperatører. Vi har forespurgt til konceptet for tidssynkronisering.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 12.5 (Styring af driftssoftware) At sikre integriteten af driftssystemer.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.5	Der bør implementeres procedurer til styring af softwareinstallationen i driftssystemer.	Vi har forespurgt ledelsen om procedure og kontrolaktiviteter som udføres i forbindelse med software installationer i driftssystemer.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 12.6 (Sårbarhedsstyring) At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
12.6	Der er etableret procedurer for patch management, således at kritiske netværkskomponenter, servere og andre enheder holdes opdateret på et passende niveau og overvåges for sikkerhedsmæssige kritiske rettelser. Der er fastlagt og implementeret regler for softwareinstallation, som foretages af brugerne.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med patch management. Vi har stikprøvevis inspiceret ændringer til kritiske netværkskomponenter og servere.	Vi har ikke konstateret væsentlige afvigelser.

13 Kommunikationssikkerhed

Kontrolmål 13.1 (Styring af netværkssikkerhed)

At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
13.1	Virksomheden opretter selvstændige virtuelle netværk til kunderne. Der oprettes selvstændige VLAN, virtuelle firewalls og virtuelle routingtabeller. Administration af netværksudstyr håndteres udelukkende af autoriseret personale. Der udføres sårbarheds- og penetrationstests mod netværk, hvor dette er fundet relevant eller aftalt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med netværksstyring. Vi har foretaget en inspektion af firewall-konfigurationen, samt at der gøres brug af Intrusion Detection systemer, som løbende og aktivt giver oplysninger om mulige ændringer, der kan påvirke fortroligheden, integriteten og tilgængeligheden i data. Vi har foretaget inspektion af, at netværket er opsat med selvstændige VLAN og DMZ-zoner. Vi har inspiceret, at der er foretaget periodisk sårbarheds- og penetrationstest. Vi har inspiceret, at der er taget stilling til konstaterede svagheder samt iværksat tiltag til udbedring.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 13.2 (Informationsoverførsel) At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
13.2	Der skal være tilfredsstillende procedurer og forretningsgange for datakommunikation, der på hensigtsmæssig måde sikrer mod risiko for tab af ægthed, integritet og fortrolighed. Adgang for administration af kunders systemer kan udelukkende foretages fra virksomhedens kontrollerede netværk. Dette kan enten være via kablet netværk, sikret trådløst netværk eller sikret krypteret VPN forbindelse fra eksterne lokationer. Aftaler skal omhandle sikker overførsel af forretningsinformation mellem organisationen og eksterne parter. Der er sikret tidssvarende kryptering af mailkommunikation. Der er defineret krav til fortrolighed- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information.	Vi har forespurgt ledelsen om procedurer og kontrolaktiviteter der udføres i forbindelse med sikker datakommunikation. Vi har foretaget en inspektion af, at administrationen af kunders systemer udelukkende kan foretages via kablet netværk, sikret trådløst netværk eller VPN. Vi har inspiceret konfiguration som sikrer at der anvendes tilstrækkelig kryptering af mailkommunikation. Vi har forespurgt til procedure for etablering af fortrolighedsaftaler. Vi har inspiceret et udvalg af underskrevne fortrolighedsaftaler med henblik på at konstatere, om proceduren efterleves ved ansættelse af nye medarbejdere.	Vi har ikke konstateret væsentlige afvigelser.

15 Leverandørforhold

Kontrolmål 15.1 (Informationssikkerhed i leverandørforhold)

At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
15.1	Der er etableret passende kontroller til sikring af informationssikkerheden i forbindelse med serviceydelser leveret af underleverandør, hvor underleverandøren har adgang til virksomhedens systemer. Hvis relevant for den leverede service, så kræves kontrolerklæringer fra underleverandøren, som vurderes med hensyn til mulige informationssikkerhedsmæssige svagheder i kontrollerne.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med styring af leverandører. Vi har stikprøvevist inspiceret at der er indhentet kontrolerklæringer for relevante leverandører. Vi har stikprøvevist inspiceret at der er indhentet kontrolerklæringer for relevante leverandører.	Vi har ikke konstateret væsentlige afvigelser.

16 Styring af informationssikkerhedsbrud

Kontrolmål 16.1 (Styring af informationssikkerhedsbrud og forbedringer)

At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
16.1	Der er placeret ledelsesansvar og etableret procedurer til at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud. Alle sikkerhedshændelser rapporteres til og behandles i Informationssikkerhedsudvalget, som sikrer at hændelserne gennemgås med det primære formål at sikre passende tiltag til forebyggelse af gentagelser. Medarbejdere er via retningslinjerne instrueret om at indrapportere alle informationssikkerhedssvagheder de måtte mistænke eller opdage.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med håndtering af sikkerhedshændelser. Vi har inspiceret udleveret materiale vedrørende behandling af sikkerhedshændelser i mødereferater fra Informationssikkerhedsudvalget og security incident logs. Vi har inspiceret retningslinjerne.	Vi har ikke konstateret væsentlige afvigelser.

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Kontrolmål 17.1 (Informationssikkerhedskontinuitet)

Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
17.1	Den samlede katastrofeplan er opbygget af en overordnet katastrofestyringsprocedure samt operationelle katastrofeplaner for de konkrete katastrofeområder. Den operationelle katastrofeplan indeholder beskrivelse af katastrofeorganisationen med de ledelsesmæssige funktions-beskrivelser, kontaktinformationer, varslingslister samt instrukser for de nødvendige indsatsgrupper. For de enkelte platforme er udarbejdet detaljerede indsatsgruppeinstrukser for reetablering i forhold til nøddrift. Der skal være implementeret disaster recovery planer for de kunder der har bestilt denne sikring. Liste over kunder samt procedurebeskrivelser skal være på plads. Der foretages minimum årlig test af katastrofeberedskabet i form af såvel skrivebordstest som faktiske testscenarier. Disse tests kan være i form af almindelige operationelle procedure i forbindelse med system vedligeholdelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret det udleverede materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser. Vi har inspiceret dokumentation vedrørende test af centrale områder i katastrofeberedskabet, herunder, hvordan beredskabet ved spontane strømafbrydelser i datacenteret afprøves.	Vi har ikke konstateret væsentlige afvigelser.

Kontrolmål 17.2 (Redundans) At sikre tilgængelighed af informationsbehandlingsfaciliteter.			
Nr.	itm8 | Progressive A/S kontrolaktivitet	Revisors udførte test	Resultat af revisors test
17.2	Alle datacenterets fælles infrastrukturenheder er dimensioneret med redundante enheder. Internetforbindelsen er ligeledes redundant.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret udleveret materiale vedrørende strøm (herunder UPS), køling, firewalls, servere (hosts), disksystemer og internetforbindelse.	Vi har ikke konstateret væsentlige afvigelser.

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

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

Torben Bring Friedrichsen
Chief Technology Officer
På vegne af: Progressive A/S
Serienummer: 4da3d1f0-0b95-4974-bd13-fb9568039489
IP: 77.75.xxx.xxx
2024-02-05 14:36:47 UTC

Simon Okkels
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
IT-revisor
Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a
IP: 93.165.xxx.xxx
2024-02-06 08:56:21 UTC

John Richardt Søbjærg
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Statsautoriseret revisor
Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a
IP: 93.165.xxx.xxx
2024-02-06 08:57:53 UTC