F&P Brancheløsninger

Uafhængig revisors ISAE 3000-erklæring for perioden 1. januar – 31. december 2023 om generelle it-kontroller relateret til Autotaks-systemet

Indhold

1 Beskrivelse af Autotaks

Autotaks er bilforsikringsselskabernes fælles skadeopgørelsessystem. F&P har drevet og udviklet Autotaks siden 1990, og systemet har gennem årene udviklet sig til et stort og forretningskritisk system. Hvert år opgøres ca. 750.000 bilskader i Autotaks til mere end 10 mia. kr. i samlede erstatningsudgifter.
Systemet indeholder vejledende reparationstider og reservedelspriser for 40 forskellige bilmærker omfattende mere end 1100 bilmodeller og anvendes pt. af følgende brugergrupper:

- ca. 300 taksatorer,
- ca. 1000 sagsbehandlere og
- ca. 4800 autoværksteder.

Ansvaret for Autotakssystemet er placeret i Privatforsikringsdirektørforum. Den daglige prioritering og udvikling foregår i tæt samarbejde med Ekspertudvalget for Autotaks Udvikling, hvor Tryg, Top, GF, Gjensidige, IF, Codan og Taksatorringen er repræsenteret.

Autotaks/Forsi.dk kan primært opdeles i to hovedområder, kalkulationsdelen og "casemanager".

Kalkulationsdelen

Kalkulationsdelen består af et internationalt anerkendt autoskadeopgørelsessystem leveret af det amerikanske firma Solera. Opgørelsessystemet anvendes i dag i ca. 100 lande.

Systemet kendetegnes ved at kunne udføre en beregning af nødvendig arbejdstid, lakering og reservedelsomfang på en given forsikringsskade på henholdsvis person-/varebiler. Systemet arbejder med en homogen arbejdsproces på tværs af alle bilfabrikater og kan således håndteres af brugere uanset tilhørsforhold til specifikt bilfabrikat. Brugeren behøver således ikke at have mærkespecifik baggrund for at kunne foretage den nødvendige beregning.

Systemet beregner reparationen på baggrund af bilfabrikkernes reparationslitteratur og bilimportørens vejledende udsalgspriser på reservedele.

Systemet består af både en frontend og en backend:

- Frontenden er Javascript/HTML gui, som indeholder en detaljeret sprængskitse af alle bilens komponenter (reservedele) vist i "naturlige" sammenhænge. Det er i dette software brugeren, der angiver skadens omfang og bestemmer de nødvendige reparationsprocesser.
- Backend er en "beregningsmotor", som på basis af det ovennævnte skadesomfang kan finde den nødvendige arbejdstid og beskrivelser samt medgåede reservedele og derved udregne en arbejdstid.
- Systemet indeholder en komplet database med samtlige arbejdsbeskrivelser og reservedele samt modeloptioner for hver bilmodel indeholdt i Autotaks/Forsi.dk-sortimentet (p.t. ca. 1100 bilmodeller) og samtlige billeder, som anvendes i forbindelse med takseringen.

Casemanager

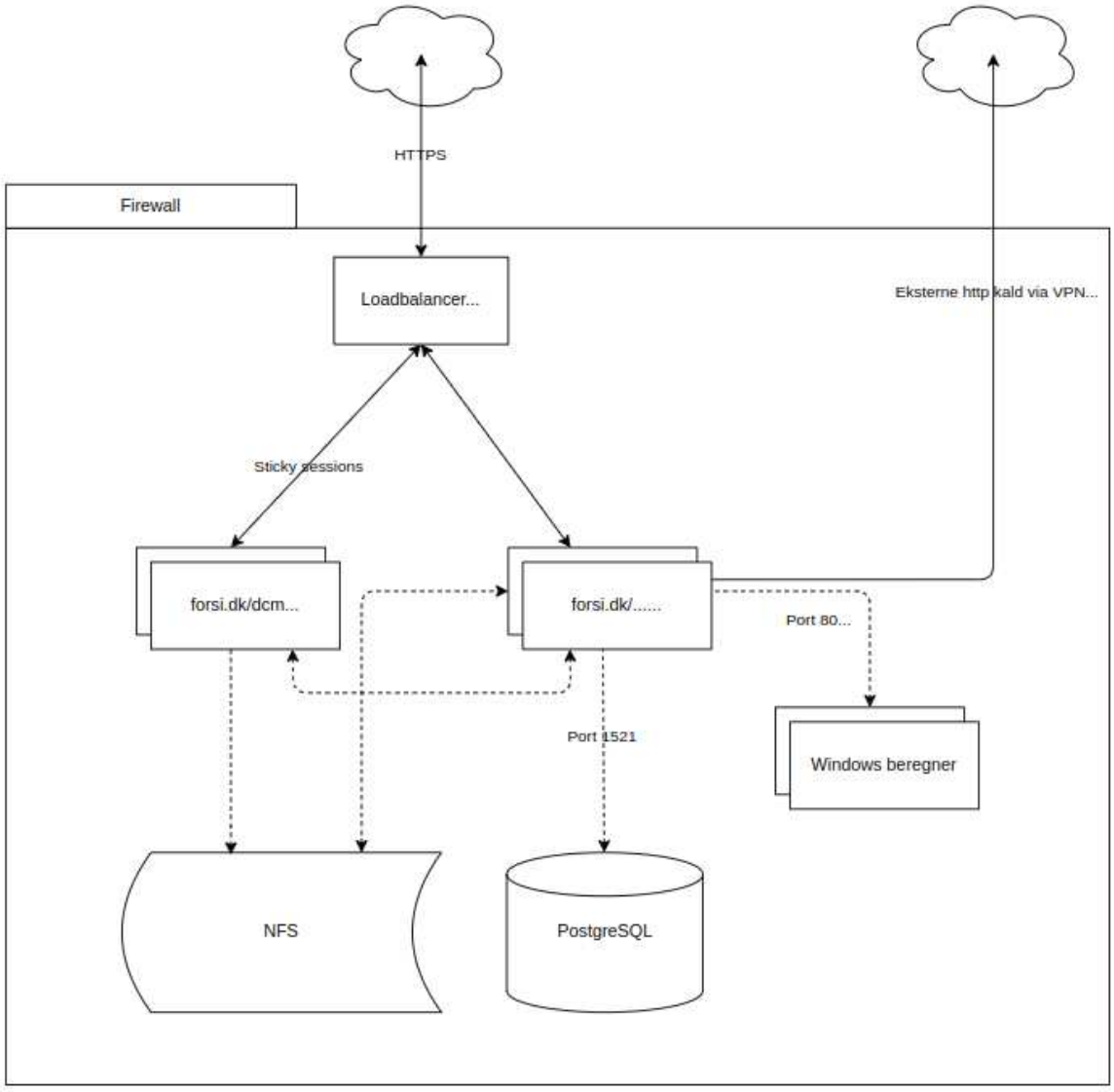
Casemanager består af en Javascript/HTML-frontend og en Java-baseret backend, som binder alle brugere i autoskadeopgørelsesprocessen sammen i en arbejdsplatform. De primære brugere er forsikringsselskabets taksatorer og Danmarks autoskadereparatører. Samarbejdsformen er, at reparatøren beregner et reparationstilbud til forsikringsselskabets autotaksator i www.Forsi.dk, og reparationstilbuddet overføres automatisk til den forudbestemte autotaksator i selskabet. Det er muligt for det enkelte forsikringsselskab at tilpasse denne relation mellem reparatør og taksator alt efter samarbejdsformen i selskabet. Nogle autotaksatorer arbejder som enkeltpersoner, og andre arbejder i teams – eller i kombination af begge former.

Når taksator har godkendt (og måske ændret) værkstedstilbuddet, bliver tilbuddet til en gældende taksatorrapport, og selskabets sagsbehandler kan behandle og udbetale erstatningsbeløbet. Taksatorrapporten bliver samtidig synlig for reparatøren og står til rådighed for yderligere processer, såsom arbejdskort, planlægning og lagerstyring.

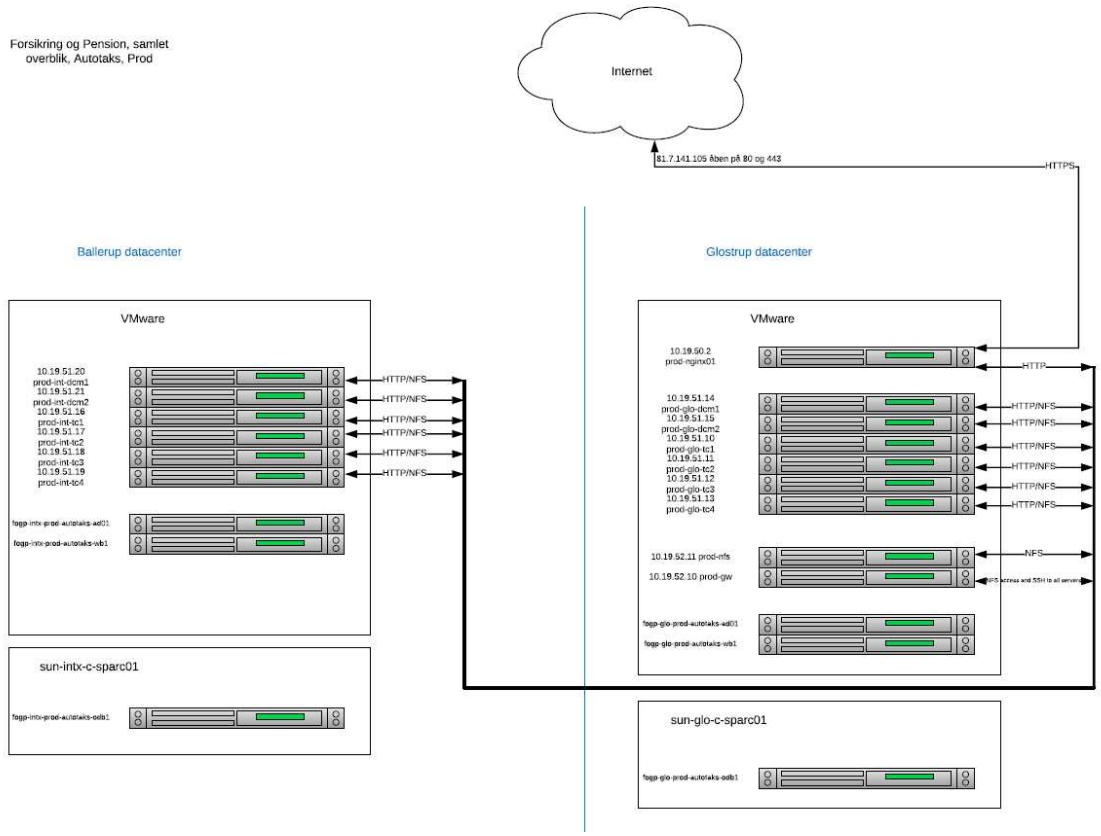
Forsi.dk er som tidligere omtalt autotaksatorernes primære værktøj og understøtter, som sådan alle de processer, forsikringsselskaberne og lovgivningen forlanger.

Af hensyn til Autotaks-systemets driftsstabilitet er drifts- og produktionsmiljøerne adskilte. Løsningen kører både i test og produktion i et dubleret setup på to forskellige geografiske lokationer. Hvis det ene datacenter lukker ned, vil det andet datacenter tage over. De to datacentre er begge aktive under normal drift, og de er begge dimensioneret, så de kan overtage den samlede belastning og stadig give gode svartider i forhold til brugerne.

Autotaks-miljøet kan skitseres således:



Følgende diagram viser antallet af de forskellige servere, samt opdelingen i de to datacentre. Dette diagram er specifikt for PROD. Der er en tilsvarende, men mindre opbygning til TEST-miljøet.



1.1 Risikostyring

F&P har i 2023 gennemført en it-risikovurdering for Autotaks.

Med risikovurderingen har vi været interesserede i at forstå og besvare følgende spørgsmål:

- Hvad er det samlede risikoniveau for Autotaks?
- Hvordan er risikoniveauet sammenholdt med risikoappetitten?
- Hvad kan vi og medlemmerne risikere at miste i forbindelse med dette system?
- Hvordan ser et typisk tab for Autotaks ud?
- Hvordan er sikkerhedsniveauet for Autotaks?
- Hvordan rangerer de forskellige typer af it-risici i forhold til hinanden?
- Hvilke risikoreducerende foranstaltninger kan vi med fordel implementere for at nedbringe risikoniveauet?

Den anvendte metode i risikovurderingen er forholdsvis ny i forhold til tidligere år. Dette skift er dels sket for at følge bedste praksis på området, og dels for at give mere kvantitative svar på direktionens og bestyrelsens spørgsmål om it-risiko. Det er et skridt i retning af at få en endnu bedre forståelse for de tab, som it-området potentielt kan give F&P og deres medlemmer. Risikovurderingen redegør for trusselsbilledet i sandsynlig frekvens sat op imod størrelsen af tab i kroner og ører. I forbindelse med risikovurderingen er risikoniveauet også sat i forhold til F&P's risikotolerance for systemet, og det ligger generelt meget tæt på eller under tolerancen for de forskellige trusselsområder.

Estimater afgivet af personale fra F&P og fra udvalgte medlemmer ligger til grund for de resultater og nøgletal som risikovurderingen præsenterer.

Fortsat opsamling af data fra hændelser, opfølgning på effekten af implementerede sikringsforanstaltninger og iagttagelse af relevant ekstern statistik i de kommende 12 måneder skal medvirke til at forbedre de estimater, der ligger til grund for næste års vurdering. Denne kontinuerlige optimering skal løbende modne F&P's it-risikostyring frem mod at blive blandt de bedste på it-risikostyringsområdet.

1.2 Organisering af sikkerheden i it-miljøerne

Informationssikkerhedspolitik

Tilrettelæggelse og implementering af generelle it-kontroller vedrørende Autotaks-systemet sker med udgangspunkt i F&P's informationssikkerhedspolitik, som er baseret på den internationale it-sikkerhedsstandard ISO27002:2013. Standarden omfatter nedenstående hovedområder.

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

F&P har med udgangspunkt i hovedområderne udvalgt kontrolmål for styringen af informationssikkerheden og relaterede kontroller, der er implementeret. Kontrolmålene og kontrollerne fremgår af oversigten i afsnit 4.3.

Organisering af it-sikkerhed i it-miljøerne sker gennem nedenstående hovedprocesser, der er baseret på standarden ISO27002:2013 og følger den overordnede struktur. De følgende beskrivelser refererer til afsnittene i standarden.

5 Informationssikkerhedspolitikker

It-sikkerhedspolitikken udarbejdes af direktionen og godkendes af bestyrelsen. It-sikkerhedspolitikken er gældende, uanset om it-anvendelsen finder sted internt i F&P, hos en samarbejdspartner eller i forbindelse med outsourcing.

6 Organisering af informationssikkerhed

Arbejdet med it-sikkerhed indgår i de daglige arbejdsrutiner, så det ønskede it-sikkerhedsniveau, opnås med færrest mulige administrative og organisatoriske ressourcer. Alle medarbejdere i F&P er fortrolige med it-sikkerhedspolitikken og forretningsgange, der er relevante for den enkeltes funktion og arbejdsopgaver.

7 Personalesikkerhed

Medarbejdersikkerhed stiller krav om tiltag for at reducere risici ved menneskelige fejl samt misbrug, bedrageri og lignende. Alle har pligt til at rapportere brud på sikkerheden til deres leder og/eller F&P's sikkerhedschef.

8 Styring af aktiver

It-sikkerhedspolitikken omfatter alle aktiver, som understøtter F&P's forretningsområder og organisation. Disse består af data, systemer, fysiske aktiver samt tekniske forsyninger, der understøtter it-anvendelsen.

9 Adgangsstyring

Adgangsstyring stiller krav til sikring af adgang til systemer og data. Systemer og data, herunder teknisk basissoftware, er sikret mod uberettiget eller utilsigtet adgang. Adgangen til anvendelse af terminaler, pc-arbejdspladser og servere er beskyttet ved logisk adgangskontrol. Tildeling af adgangsrettigheder m.v. sker ud fra et arbejdsbetinget behov og under hensyntagen til en effektiv funktionsadskillelse.

10 Kryptografi

F&P anvender forskellige krypteringsteknikker afhængig af, hvorledes systemerne risikovurderes.

11 Fysisk sikring og miljøsikring

Fysisk sikkerhed stiller krav til sikring af bygninger, forsyninger og tekniske installationer, der er relevante for F&P.

12 Driftssikkerhed

Styring af kommunikation og drift stiller krav til stabilitet, overvågning og sikkerhed i forbindelse med afvikling af den daglige produktion samt i de anvendte netværksløsninger. Der er etableret dokumentation af driftsprocesser, driftsafvikling, udstyr, systemer og datakommunikationsforbindelser i et sådant omfang, at det muliggør en effektiv vedligeholdelse samt hurtig og korrekt indgriben ved nødsituationer.

13 Kommunikationssikkerhed

Herunder stilles krav til stabilt netværk, hvor datatransmissionen mellem F&P og kunder/samarbejdspartnere er beskyttet mod uautoriseret adgang, forvanskning samt utilgængelighed.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

Anskaffelse, udvikling og vedligeholdelse af systemer stiller krav til F&P's kontroller til sikring af kvalitet, sikkerhed og dokumentation af brugersystemer og basissoftware. De godkendte udviklingsmetoder sikrer systemudvikling med standardiseret brugergrænseflade, høj kvalitet og lav fejlrate. Desuden sikrer udviklingsmodellen, at der tidligt i udviklingsforløbet tages stilling til det ønskede sikkerhedsniveau, herunder at relevante sektor- og lovkrav overholdes. Alle produktionssystemer er dokumenterede, testede og godkendte forud for idriftsættelse.

15 Leverandørforhold

Omfatter informationssikkerhedskravene til at styre risici forbundet med leverandører og outsourcingpartners adgang til F&P's aktiver. Der skal foreligge dokumenterede aftaler med de relevante leverandører.

16 Styring af informationssikkerhedsbrud

Styring af sikkerhedsbrud stiller krav til kontroller for at sikre overblik over indtrufne sikkerhedshændelser samt en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Omfatter F&P 's krav til beredskabsstyring, herunder beredskabsplaner, afprøvning og reetablering i tilfælde af større driftshændelser.

18 Overensstemmelse

Overensstemmelse med lovbestemte og kontraktlige krav stiller krav til kontroller for at forhindre brud på relevante sikkerhedskrav samt indgåede kontraktlige forpligtelser. F&P overvåger og tilpasser løbende sikkerheden til gældende sektor- og lovgivningskrav.

F&P har outsourcet it-drift vedrørende Autotaks-systemet til Sentia. Det er derfor væsentligt, at F&P's informationssikkerhedspolitik også implementeres og efterleves i forbindelse med drift af Autotaks-systemet hos Sentia. Med henblik på at sikre dette har F&P indgået en aftale med Sentia, som indeholder en række sikkerhedsmæssige krav, der skal overholdes af Sentia.

F&P følger løbende op på Sentias overholdelse af kravene ved gennemgang af driftsrapportering, deltagelse i driftsstyregruppemøder med Sentia m.v. samt ved gennemgang og vurdering af resultatet af årlig revisionsmæssig gennemgang af it-sikkerheden hos Sentia.

1.3 Væsentlige ændringer i it-miljøerne

I februar 2023 migrerede vi vores database fra Oracle til seneste stabile version af Postgresql. Den nye Postgresql server hostes samme sted som vores tidligere Oracle (Sentia).

I forbindelse med migreringen, har vi efter ca. 4 måneders drift på det ny system, fået destrueret den gamle installation af Sentia. Vedlagt (Acknowledgement letter - Sletning af data på datamedier - F&P Brancheløsninger.pdf)

1.4 Komplementerende kontroller hos brugerne

Kontroller hos F&P er udformet sådan, at nogle af kontrollerne nævnt i denne erklæring skal suppleres med kontroller hos brugerne.

Oversigten nedenfor beskriver overordnet fordelingen af kontroller mellem F&P og brugerne af Autotaks-systemet i forhold til brugeradministration, password-politik, periodisk gennemgang af brugernes adgangsrettigheder og beredskab.

Brugeradministration (oprettelse, ændring, sletning)	F&P	Brugere af Autotaks-systemet
Medarbejdere hos brugere af F&P		x
Medarbejdere hos F&P	x	
Passwordpolitik	**F&P**	**Brugere af Autotaks-systemet**
Medarbejdere hos brugere af F&P		x
Medarbejdere hos F&P	x	
Regelmæssig gennemgang af adgangsrettigheder	**F&P**	**Brugere af Autotaks-systemet**
Medarbejdere hos brugere af F&P		x
Regelmæssig gennemgang af adgangsrettigheder	**F&P**	**Brugere af Autotaks-systemet**
Medarbejdere hos F&P	x [1]	

[1] De applikationsspecifikke kontroller med adgangsrettigheder og funktionsadskillelse i Autotaks-systemet indgår ikke i denne ISAE 3000 om generelle it-kontroller.

Beredskab	F&P	Brugere af Autotaks-systemet
Iværksættelse af beredskabsplaner ved større hændelser og information om hændelsen til brugerne	x	
Iværksættelse af brugernes egne beredskabsplaner baseret på information fra F&P om hændelserne		x

Netværk	F&P	Brugere af Autotaks-systemet
Sikkerheden i management-netværk hos Sentia	x	
Sikkerheden i netværksforbindelser mellem Sentia og brugerne		x

2 Udtalelse fra ledelsen

Medfølgende beskrivelse er udarbejdet til brug for brugerne af F&P Brancheløsninger's (F&P) Autotaks-system og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som brugerne selv har udført, når de opnår en forståelse af brugernes informationssystemer.

F&P anvender Sentia til drift af Autotaks-systemet. Beskrivelsen i sektion 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia.

F&P anvender Microsoft Azure til arkivering af billeder og andre dokumenter. Beskrivelsen i sektion 1 medtager kun kontrolmål og kontrolaktiviteter hos F&P og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Microsoft Azure. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørels kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af F&Ps kontroller, er passende designet og er operationelt effektive sammen med relaterede kontroller hos F&P. Beskrivelsen omfatter ikke kontrolaktiviteter udført af kunder.

F&P bekræfter, at:

(a) den medfølgende beskrivelse i sektion 1 giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Autotaks-systemet, der har været anvendt af brugerne af F&P's Autotaks-system i perioden fra 1. januar - 31. december 2023. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) redegør for, hvordan kontrollerne var designet 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 de generelle it-kontroller
- hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
- processen, der blev anvendt til at udarbejde rapporter til kunder
- ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden
- relevante kontrolmål og kontroller designet til at nå disse mål
- kontroller, som vi med henvisning til kontrollernes design har forudsat, ville være implementeret af brugerne af Autotaks-systemet, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

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

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

(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i perioden fra 1. januar - 31. december 2023, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af F&P's kontroller i perioden fra 1. januar – 31. december 2023. Kriterierne for dette udsagn 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 udført konsistent som designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar – 31. december 2023.

Hellerup, den 23. februar 2024

Thomas Brenøe
direktør

Peder Herbo
it-direktør

3 Den uafhængige revisors erklæring om beskrivelsen af kontroller, deres design og operationel effektivitet

Til: F&P Brancheløsninger (F&P)

Omfang

Vi har fået som opgave at afgive erklæring om F&P's beskrivelse i sektion 1 om generelle it-kontroller vedrørende Autotaks-systemet i perioden fra 1. januar - 31. december 2023 (beskrivelsen) og om designet og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af F&P's kontroller, er passende designet og operationelt effektive sammen med relaterede kontroller hos F&P. Vores handlinger har ikke omfattet kontrolaktiviteter udført af kunderne, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos kunderne.

F&P anvender Sentia til drift af Autotaks-systemet. Beskrivelsen i sektion 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia. Vores handlinger har omfattet vurdering af beskrivelsen samt designet og operationel effektivitet af kontrolmål og relaterede kontroller hos Sentia.

F&P anvender Microsoft Azure til billedarkiv. Beskrivelsen i sektion 1 medtager kun kontrolmål og relaterede kontroller hos F&P og medtager således ikke kontrolmål og relaterede kontroller hos Microsoft Azure. Visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af F&P's kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos F&P. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Microsoft Azure, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

F&P's ansvar

F&P er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; identifikation af de risici, der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier, der er præsenteret i ledelsens udtalelse; samt for designet, implementeringen og operationelt effektive kontroller for at nå de anførte kontrolmål.

Vores 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.

EY Godkendt Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM1, 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.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om F&P's beskrivelse samt om design og operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger, som er udstedt af IAASB, og yderligere krav ifølge dansk revisorlovgivning med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i

alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og operationelt effektive.

En erklæringsopgave med sikkerhed om beskrivelsen, designet og operationel effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes design og operationel effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risicierne for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive.

Vores handlinger har omfattet test af den operationelle effektivitet 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 kontrolmål samt hensigtsmæssigheden af de kriterier, som F&P har specificeret og beskrevet i sektion 2.

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

F&P's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af brugere af Autotaks-systemet og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de generelle it-kontroller, som hver enkelt bruger måtte anse for vigtigt efter deres særlige forhold.

Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet 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 sektion 2. Det er vores opfattelse, at:

(a) beskrivelsen af de generelle it-kontroller med relevans for Autotaks-systemet, således som de var designet og implementeret i perioden 1. januar – 31. december 2023, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden fra 1. januar – 31. december 2023 for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis de relaterede kontroller var operationelt effektive i perioden fra 1. januar – 31. december 2023, og hvis kontroller hos underleverandører og komplementerende kontroller hos brugerne af F&P's Autotaks-system var hensigtsmæssigt designet og implementeret i perioden fra 1. januar – 31. december 2023 som forudsat i designet af F&P's kontroller, og

(c) 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 været operationelt effektive i perioden fra 1. januar – 31. december 2023, hvis kontroller hos underleverandører har været operationelt effektive og hvis de komplementerende kontroller hos brugerne af F&P's Autotaks-system, der forudsættes i designet af F&P's kontroller, har været operationelt effektive i perioden fra 1. januar – 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i sektion 0.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 0 er udelukkende tiltænkt brugere, der har anvendt Autotaks-systemet, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den

sammen med anden information, herunder information om brugernes egne kontroller, når de vurderer risici vedrørende brug af Autotaks-systemet.

København, den 23. februar 2024
EY Godkendt Revisionspartnerselskab
CVR nr. 30 70 02 28

Jesper Due Sørensen
partner

Nils B. Christiansen
statsaut. revisor
mne34106

4 Tests udført af EY

4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3000 andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af kontrollers design, implementering og operationelle effektivitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 1. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos de brugere af Autotaks-systemet, der anvender løsningen beskrevet i afsnit 1, er ikke omfattet af vores test.

Test af den operationelle effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden 1. januar - 31. december 2023.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers operationelle effektivitet er beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring 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 blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller 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 kontroller er implementeret og har fungeret i perioden 1. januar – 31. december 2023. Dette omfatter bl.a. vurdering af patchning-niveau, tilladte services, segmentering, password-kompleksitet m.v. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af passende personale. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

For den del af it-miljøerne, der i perioden 1. januar – 31. december 2023 har været outsourcet til Sentia, har vi foretaget test af design, implementering og operationel effektivitet af kontrollerne hos Sentia.

4.3 Resultater af tests

I nedenstående oversigt opsummeres tests udført af EY som grundlag for at vurdere de generelle it-kontroller med relevans for F&P's Autotaks-system.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A5	**Informationssikkerhedspolitikker**		
A5.1	**Informationssikkerhedsstrategi** Kontrolmål: At ledelsen viser retning for og understøtter informationssikkerhed i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.		
A5.1.1	**Politikker for informationssikkerhed** Et sæt politikker for informationssikkerhed er fastlagt, godkendt af ledelsen og kommunikeret til medarbejdere og relevante eksterne parter.	**F&P:** Inspiceret, at informationssikkerhedspolitikken er opdateret og godkendt. Observeret, at informationssikkerhedspolitikken er kommunikeret og tilgængelig for medarbejdere. **Sentia:** Inspiceret, at informationssikkerhedspolitikken er opdateret og godkendt. Observeret, at informationssikkerhedspolitikken er kommunikeret og tilgængelig for medarbejdere. Observeret, at det bliver registreret, hvilke medarbejdere der har læst og forstået informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
A5.1.2	**Gennemgang af politikker for informationssikkerhed** Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og effektivitet.	**F&P:** Forespurgt om proceduren for årlig gennemgang af politikker for informationssikkerhed. Inspiceret, at informationssikkerhedspolitikken er gennemgået og godkendt. **Sentia:** Forespurgt om proceduren for årlig gennemgang af politikker for informationssikkerhed samt it-sikkerhedshåndbogen. Inspiceret, at informationssikkerhedspolitikken samt sikkerhedshåndbogen er gennemgået og godkendt.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A6	**Organisering af informationssikkerhed**		
A6.1	**Intern organisering** Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.		
A6.1.1	**Roller og ansvarsområder for informationssikkerhed** Alt ansvar for informationssikkerhed er tydeligt defineret og fordelt.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder beskrivelse af fordeling af roller og ansvarsområder. Inspiceret, at procedurehåndbog for Autotaks-systemet indeholder en beskrivelse af rollerne i systemet.	Ingen afvigelser konstateret.
A6.1.2	**Funktionsadskillelse** Modstridende funktioner og ansvarsområder er adskilt for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af virksomhedens aktiver.	**F&P:** Forespurgt om proceduren for funktionsadskillelse. Inspiceret informationssikkerhedspolitikken for funktionsadskillelse af roller og ansvarsområder. Inspiceret procedurehåndbog for proces for funktionsadskillelse i roller og ansvarsområder. Stikprøvevis inspiceret, at der er funktionsadskillelse ved udviklingsopgaver. **Sentia:** Forespurgt til opdeling af ansvarsområder og modstridende funktioner. Inspiceret, at organisationsdiagram viser adskillelse mellem modstridende funktioner og ansvarsområder.	Ingen afvigelser konstateret.
A6.1.3	**Kontakt med myndigheder** Der opretholdes passende kontakt med relevante myndigheder.	**F&P:** Forespurgt om proceduren for opretholdelse af passende kontakt med relevante myndigheder. Inspiceret, at der foreligger en opdateret kontaktliste for kontakt til relevante myndigheder.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A6.1.5	**Informationssikkerhed ved projektstyring** Informationssikkerhed er anvendt ved projektstyring, uanset projekttype.	**F&P:** Forespurgt om proceduren for anvendelse af informationssikkerhed i projektstyring. Stikprøvevis inspiceret, at der er taget stilling til informationssikkerhed ifm. udviklingsopgaver.	Ingen afvigelser konstateret.
A6.2	**Mobilt udstyr og fjernarbejdspladser** Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.		
A6.2.1	**Politik for mobilt udstyr** En politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr, er implementeret.	**F&P:** Forespurgt om proceduren for mobilt udstyr. Inspiceret, om proceduren for brugen af mobilt udstyr er defineret i informationssikkerhedspolitikken. Inspiceret proceduren Retningslinjer for sikker brug af it for brugen af mobilt udstyr.	Ingen afvigelser konstateret.
A7	**Medarbejdersikkerhed**		
A7.1	**Før ansættelsen** Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.		
A7.1.1	**Screening** Efterprøvelse af jobkandidaters, kontrahenters og eksterne brugeres baggrund udføres i overensstemmelse med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassificeringen af den information, der skal gives adgang til, og de relevante risici.	**F&P:** Forespurgt om proceduren for screening af jobkandidaters baggrund. Inspiceret informationssikkerhedspolitikken for screeningsproces for personer, der vil få adgang til it-kritiske data. Stikprøvevis inspiceret, at screening er foregået i forbindelse med ansættelser.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A7.1.2	**Ansættelsesvilkår og -betingelser** Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og virksomhedens ansvar for informationssikkerhed.	**F&P:** Forespurgt om proceduren for udarbejdelse af kontrakter til medarbejdere og kontrahenter. Inspiceret, at en standardansættelseskontrakt indeholder pågældendes og virksomhedens ansvar for informationssikkerhed. **Sentia:** Forespurgt om proceduren for udarbejdelse af kontrakter til medarbejdere og kontrahenter. Inspiceret, at en standardansættelseskontrakt indeholder pågældendes og virksomhedens ansvar for informationssikkerhed.	Ingen afvigelser konstateret.
A7.2	**Under ansættelse** Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.		
A7.2.1	**Ledelsesansvar** Ledelsen kræver, at alle medarbejdere og kontrahenter fastholder informationssikkerhed i overensstemmelse med virksomhedens fastlagte politikker og procedurer.	**F&P:** Inspiceret informationssikkerhedspolitikken vedrørende medarbejderes og kontrahenters efterlevelse af informationssikkerhedspolitikken. Inspiceret retningslinjer vedrørende sikker brug af pc'er, iPhone/ iPad, passwords, data, internet, sociale medier og Outlook. Inspiceret, at der i standardansættelseskontrakten er en henvisning til informationssikkerhedspolitikken.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A7.2.2	**Bevidsthed om uddannelse og træning i informationssikkerhed** Alle virksomhedens medarbejdere, og hvor det er relevant, kontrahenter og eksterne brugere bevidstgøres om informationssikkerhed samt holdes regelmæssigt ajour med virksomhedens politikker og procedurer, i det omfang det er relevant for deres jobfunktion.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder et afsnit omkring ansvar og retningslinjer for informationssikkerhed. Inspiceret, at det fremgår af procedure for oprettelse af nye brugere, at der skal afholdes introduktion for husets it-systemer og sikkerhedspolitikker. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Inspiceret, at standardansættelseskontrakten indeholder henvisning til personalehåndbogen og retningslinjer for sikker brug af it. Inspiceret, at der i disse er defineret ansvar og retningslinjer for brugen af it.	Ingen afvigelser konstateret.
A7.2.3	**Sanktioner** Der er etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.	**F&P:** Inspiceret retningslinjer for sikker brug af it for medarbejderens ansvar for sikker brug af it, herunder proces for sanktioner i forbindelse med informationssikkerhedsbrud. Forespurgt, om der er medarbejdere der har begået informationssikkerhedsbrud.	F&P har oplyst, at der i perioden ikke har været registreret informationssikkerhedsbrud, der har medført sanktioner. Ingen afvigelser konstateret.
A7.3	**Ansættelsesforholdets ophør eller ændring** Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.		
A7.3.1	**Ansættelsesforholdets ophør eller ændring** Informationssikkerhedsansvar og –forpligtelser, som gælder efter ansættelsens ophør eller ændring, er defineret og kommunikeret til medarbejderen eller kontrahenten og håndhæves.	**F&P:** Inspiceret retningslinjer for sikker brug af it for medarbejdernes ansvar for at udvise fornuftig adfærd ved brugen af it-udstyr og systemer. Inspiceret en standardansættelseskontrakt vedrørende ansvar og forpligtelser efter ansættelsens ophør. **Sentia:** Inspiceret personale-it-sikkerhedshåndbogen for beskrivelse af tavshedspligt. Inspiceret en standardansættelseskontrakt vedrørende ansvar og forpligtelser efter ansættelsens ophør.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A8	**Styring af aktiver**		
A8.1	**Ansvar for aktiver** Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.		
A8.1.3	**Accepteret brug af aktiver** Der er identificeret, dokumenteret og implementeret regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter.	**F&P:** Inspiceret retningslinjer for sikker brug af it for, hvordan brugen af aktiver vedrørende informationsbehandlingsfaciliteter skal benyttes. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Inspiceret informationssikkerhedspolitikken for ejerskab af aktiver, accepteret brug samt tilbagelevering af aktiver.	Ingen afvigelser konstateret.
A8.1.4	**Tilbagelevering af aktiver** Alle medarbejdere og eksterne brugere afleverer alle organisationens aktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.	**F&P:** Inspiceret, at der i proceduren for tilbagelevering af aktiver er defineret en række ting, som den fratrædende har ansvaret for at tilbagelevere. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Stikprøvevis inspiceret, at fratrådte medarbejdere har tilbageleveret deres aktiver. **Sentia:** Inspiceret sikkerhedshåndbogen vedrørende medarbejderforpligtelser ved fratrædelse. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Stikprøvevis inspiceret, at fratrådte medarbejdere har tilbageleveret deres aktiver.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A8.3	**Mediehåndtering** Kontrolmål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.		
A8.3.2	**Bortskaffelse af medier** Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem i overensstemmelse med formelle procedurer.	**Sentia:** Inspiceret proceduren for bortskaffelse af medier. Inspiceret, at der i kontrakten mellem Sentia og F&P foreligger et afsnit omkring destruktion af medier. Inspiceret, at Sentia har aftale med leverandør om destruktion. Inspiceret, at Sentia har leveret destruktionsbevis til F&P.	Ingen afvigelser konstateret.
A9	**Adgangsstyring**		
A9.1	**Forretningsmæssige krav til adgangsstyring** Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.		
A9.1.1	**Politik for adgangsstyring** En politik for adgangsstyring er udarbejdet, dokumenteret og gennemgået på grundlag af forretnings- og informationssikkerhedskrav.	**F&P:** Inspiceret informationssikkerhedspolitikken vedrørende krav til adgangsstyring. Inspiceret, at informationssikkerhedspolitikken er opdateret og godkendt. Inspiceret procedurehåndbogen vedrørende brugeradministration. **Sentia:** Inspiceret proceduren for personaleadgang, hvor roller og ansvar er defineret, og at denne er ledelsesgodkendt. Observeret, at der kræves adgangskort for at få adgang til informationsbehandlingsfaciliteterne.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.1.2	**Adgang til netværk og netværkstjenester** Brugere får kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	**Sentia:** Inspiceret proceduren for personaleadgang, herunder proceduren for adgang til netværkstjenester. Inspiceret, at medarbejdere med adgang til netværket er autoriserede	Ingen afvigelser konstateret.
A9.2	**Administration af brugeradgang** Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.		
A9.2.1	**Brugerregistrering og -afmelding** Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.	**F&P:** Inspiceret informationssikkerhedspolitikken for brugerregistrerings- og afmeldingsproces. Inspiceret flowcharts for proces over oprettelse og nedlæggelse af brugere. Inspiceret liste over til- og fratrådte medarbejdere fra HR. Stikprøvevis inspiceret, at tiltrådte medarbejderes adgang oprettes, jf. proceduren. Stikprøvevis inspiceret, at fratrådte medarbejderes adgang afmeldes. **Sentia:** Inspiceret procedure for personaleadgang, herunder beskrivelse af roller og ansvar i forbindelse med brugerregistrering og -afmelding. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Stikprøvevis inspiceret, at fratrådte medarbejderes adgang afmeldes.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.2.2	**Tildeling af brugeradgang** Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	**F&P:** Inspiceret informationssikkerhedspolitikken for tildeling af brugeradgange. Inspiceret flowcharts for oprettelse af brugere. Stikprøvevis inspiceret, at tiltrådte medarbejderes adgang oprettes, jf. proceduren. **Sentia:** Inspiceret procedure for personaleadgang, herunder beskrivelse af roller og ansvar i forbindelse med brugerregistrering og -afmelding. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Stikprøvevis inspiceret, at tiltrådte medarbejderes adgang godkendes inden oprettelsen. Stikprøvevis inspiceret, at fratrådte medarbejderes adgang afmeldes.	Ingen afvigelser konstateret.
A9.2.3	**Styring af privilegerede adgangsrettigheder** Tildeling og anvendelse af privilegerede adgangsrettigheder er begrænset og styret.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder styring af privilegerede adgangsrettigheder. Inspiceret listen over brugere med privilegerede adgangsrettigheder og fået bekræftet, at disse har et arbejdsbetinget behov for adgangen. **Sentia:** Forespurgt om proceduren for styring af privilegerede adgangsrettigheder. Inspiceret listen over brugere med privilegerede adgange samt forespurgt, hvorvidt disse brugere har et arbejdsbetinget behov for adgangen.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.2.4	**Styring af hemmelig autentifikationsinformation om brugere** Tildeling af hemmelig autentifikationsinformation er styret ved hjælp af en formel administrationsproces.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder politik for passwordopsætning. Inspiceret, at passwordopsætningen følger politikken. **Sentia:** Inspiceret, at password-politikken følger leverandørens anbefalinger.	Ingen afvigelser konstateret.
A9.2.5	**Gennemgang af brugernes rettigheder** Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	**F&P og Sentia:** Forespurgt om proceduren for gennemgang af brugernes rettigheder. Stikprøvevis inspiceret, at der er afholdt statusmøder, hvor alle brugere er gennemgået.	Ingen afvigelser konstateret.
A9.2.6	**Inddragelse eller justering af adgangsrettigheder** Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører eller tilpasses efter en ændring.	**F&P:** Inspiceret informationssikkerhedspolitikken for fratrædelsespolitik. Inspiceret liste over til- og fratrådte medarbejdere fra HR med adgang til Autotaks-systemet. Inspiceret, at fratrådte medarbejderes adgange lukkes ved fratrædelse. **Sentia:** Forespurgt om proceduren for inddragelse og justering af adgangsrettigheder. Stikprøvevis inspiceret, at fratrådte medarbejderes adgange lukkes ved fratrædelse.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.4	**Styring af system- og applikationsadgang** Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.		
A9.4.3	**System for administration af adgangskoder** Systemer til administration af adgangskoder er interaktive og sikrer, at koderne er af høj kvalitet.	**F&P og Sentia:** Inspiceret, at informationssikkerhedspolitikken indeholder procedure for administration af passwords. Inspiceret password-opsætningen for Autotaks-systemet. Inspiceret, at password-opsætningerne lever op til leverandørens anbefalinger.	Ingen afvigelser konstateret.
A9.4.5	**Styring af adgang til kildekoder til programmer** Adgang til kildekoder til programmer er begrænset.	**F&P:** Forespurgt om procedure for styring af adgang til kildekoder til programmer. Inspiceret informationssikkerhedspolitikken for kontrol med adgang til kildekode. Inspiceret brugere med adgang til kildekode og forespurgt, hvorvidt disse har et arbejdsbetinget behov for adgangen.	Ingen afvigelser konstateret.
A10	**Kryptografi**		
A10.1	**Kryptografiske kontroller** Kontrolmål: At sikre korrekt og effektiv brug af kryptografi for at beskytte informationernes fortrolighed, autenticitet og/eller integritet.		
A10.1.1	**Politik for anvendelse af kryptografi** Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	**F&P:** Forespurgt om proceduren for anvendelse af kryptografi. Inspiceret proceduren for kryptografi. Inspiceret dokumentation for opsætningen af kryptografi, herunder at der foreligger et validt certifikat.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A10.1.2	**Administration af nøgler** Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	**F&P:** Forespurgt om proceduren for anvendelse af kryptografi. Inspiceret proceduren for kryptografi. Inspiceret dokumentation for opsætningen af kryptografi, herunder at der foreligger et validt certifikat.	Ingen afvigelser konstateret.
A12	**Driftssikkerhed**		
A12.1	**Driftsprocedurer og ansvarsområder** Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.		
A12.1.1	**Dokumenterede driftsprocedurer** Driftsprocedurer dokumenteres og gøres tilgængelige for alle de brugere, der har brug for dem.	**F&P:** Inspiceret driftsprocedure. Inspiceret, at procedure for driftsnedbrud står beskrevet på Sentias wiki site. Inspiceret, at listen over adgange til Sentias wiki site kun indeholder medarbejdere med et arbejdsbetinget behov for adgangen. **Sentia:** Inspiceret, at Sentias wiki site indeholder dokumentation om drift, opsætning samt diverse management-information omkring systemet. Inspiceret, at listen over adgange til Sentias wiki kun indeholder medarbejdere med et arbejdsbetinget behov for adgangen.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.1.2	**Ændringsstyring** Ændringer af virksomheden, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, er styret.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder procedure for ændringshåndtering. Inspiceret, at Sentias wiki site indeholder procedure for ændringshåndtering. Stikprøvevis inspiceret, at der afholdes periodiske driftsstatusmøder, hvor ændringer gennemgås. **Sentia:** Stikprøvevis inspiceret, at ændringer testes og godkendes, inden de bliver lagt i produktion, samt at de er afsluttet. Stikprøvevis inspiceret, at der afholdes periodiske driftsstatusmøder, hvor ændringer gennemgås. Forespurgt om proceduren for ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden.	Ingen afvigelser konstateret.
A12.1.3	**Kapacitetsstyring** Anvendelsen af ressourcer er styret og tilpasset, og der er foretaget fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemerne fungerer som påkrævet.	**F&P og Sentia:** Inspiceret Sentias wiki site for procedure vedrørende kapacitetsstyring. Stikprøvevis inspiceret, at der udarbejdes månedlige driftsrapporter, hvor overvågningen af kapaciteten fremgår.	Ingen afvigelser konstateret.
A12.1.4	**Adskillelse af udviklings-, test- og driftsmiljøer** Udviklings-, test- og driftsmiljøer er adskilt for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.	**Sentia:** Forespurgt på adskillelse mellem udviklings-, test- og driftsmiljøer. Inspiceret opsætning i det virtuelle miljø samt netværksdiagram for adskillelse mellem udviklings-, test- og driftsmiljøer.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.2	**Malware-beskyttelse** Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.		
A12.2.1	**Kontroller mod malware** Der er implementeret kontroller til detektering, forhindring og gendannelse med henblik på at beskytte mod malware, kombineret med passende brugerbevidsthed.	**Sentia:** Forespurgt om proceduren for sikring mod malware. Inspiceret, om personalehåndbogen indeholder beskrivelse af, hvordan medarbejdere skal forholde sig i tilfælde af malwareangreb. Inspiceret, at servere har opdaterede antivirus systemer.	Ingen afvigelser konstateret.
A12.3	**Backup** Kontrolmål: At beskytte mod tab af data.		
A12.3.1	**Backup af informationer** Der er taget backup af informationer, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backup-politik.	**Sentia:** Forespurgt om proceduren for backup af informationer, software og systembilleder. Stikprøvevis inspiceret, at der er foretaget succesfuld backup, jf. proceduren. Inspiceret stikprøve af driftsrapporter, hvor vi kan se, at der er foretaget restore af tilfældige filer for at sikre, at backupdata kan genskabes.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.4	**Logning og overvågning** Kontrolmål: At registrere hændelser og tilvejebringe bevis.		
A12.4.1	**Hændelses-logning** Hændelses-logning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres og opbevares.	**Sentia:** Forespurgt om proceduren for hændelses-logning. Stikprøvevis inspiceret, at der er opsat hændelses-logning på servere.	Hændelseslogning er ikke konfigureret, jf. leverandørens anbefalinger, på 2 parameter, for 2 ud af 2 Windows-servere. Ingen yderligere afvigelser konstateret.
A12.4.2	**Beskyttelse af log-oplysninger** Lognings-faciliteter og log-oplysninger er beskyttet mod manipulation og uautoriseret adgang.	**Sentia:** Forespurgt om proceduren for beskyttelse af logning. Inspiceret, at kun autoriserede personer har adgang til logs.	Ingen afvigelser konstateret.
A12.4.3	**Administrator- og operatør-logs** Aktiviteter udført af systemadministrator og systemoperatør logges, og loggene beskyttes.	**Sentia:** Forespurgt om proceduren for logning af systemadministratorer m.v. Stikprøvevis inspiceret, at der er opsat logning af aktiviteter udført af systemadministratorer m.v. på servere.	Hændelseslogning er ikke konfigureret, jf. leverandørens anbefalinger, på 2 parameter, for 2 ud af 2 Windows-servere. Ingen yderligere afvigelser konstateret.
A12.4.4	**Tidssynkronisering** Urene i alle relevante informationsbehandlingssystemer i virksomheden eller et sikkerhedsdomæne er synkroniseret til en enkelt referencetidsangivelseskilde.	**Sentia:** Forespurgt om proceduren for tidssynkronisering for de relevante informationssystemer. Inspiceret, at der er opsat aktiv tidssynkronisering på produktionsmiljøet.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.5	**Styring af driftssoftware** Kontrolmål: At sikre integriteten af driftssystemer.		
A12.5.1	**Softwareinstallation i driftssystemer** Der er implementeret procedurer til styring af software-installationen i driftssystemer.	**Sentia:** Forespurgt om proceduren for software-installation på drifts-systemer. Inspiceret Sentias wiki site for procedure for patch manage-ment. Inspiceret dokumentation for gennemført patchning. Inspiceret, at der er tilkøbt forlænget support til Oracle-plat-formen.	Ingen afvigelser konstateret.
A12.6	**Sårbarhedsstyring** Kontrolmål: At forhindre, at tekniske sårbarheder udnyt-tes.		
A12.6.1	**Styring af tekniske sårbarheder** Der indhentes løbende informationer om tekniske sårbar-heder i anvendte informationssystemer, virksomhedens eksponering for sådanne sårbarheder evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	**Sentia:** Forespurgt om procedure for softwareinstallation på driftssy-stemer. Inspiceret procedure for patch management. Inspiceret dokumentation for gennemført patchning. Inspiceret dokumentation for at sårbarheder evalueres, og for-anstaltninger iværksættes.	Ingen afvigelser konstateret.
A12.6.2	**Begrænsninger på softwareinstallation** Der er fastlagt og implementeret regler om software-in-stallation, som foretages af brugerne.	**Sentia:** Forespurgt om begrænsninger på software-installation for bruger-pc'er. Inspiceret personale-it-sikkerhedshåndbogen for procedure for installation af software på pc'er.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A13	**Kommunikationssikkerhed**		
A13.1	**Styring af netværkssikkerhed** Kontrolmål: At sikre beskyttelse af informationer i netværk og beskyttelse af understøttende informationsbehandlingsfaciliteter.		
A13.1.1	**Netværksstyring** Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	**Sentia:** Forespurgt om procedure for netværksstyring. Observeret, at der anvendes MPLS og VLAN til beskyttelse af kundenetværk. Inspiceret netværksdiagram samt opdeling af brugere og informationssystemer.	Ingen afvigelser konstateret.
A13.1.2	**Sikring af netværkstjenester** Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i en aftale om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.	**Sentia:** Inspiceret, at sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester indgår i kontrakten.	Ingen afvigelser konstateret.
A13.1.3	**Opdeling i netværk** Grupper af informationstjenester, brugere og informationssystemer er opdelt i netværk.	**Sentia:** Forespurgt om procedure for netværksstyring. Inspiceret, at der anvendes MPLS og VLAN til opdeling af kundenetværk. Inspiceret netværkstegning for sikkerhed i netværket samt opdeling af brugere og informationssystemer.	Ingen afvigelser konstateret.
A13.2	**Informationsoverførsel** Kontrolmål: At opretholde informationssikkerhed ved overførsel internt i organisationen og til en ekstern part..		
A13.2.2	**Aftaler om informationsoverførsel** Aftaler omhandler sikker overførsel af forretningsinformation mellem virksomheden og eksterne parter.	**F&P:** Inspiceret informationssikkerhedspolitikken for procedure for informationsoverførsel. Inspiceret aftalen mellem F&P og Sentia for aftale om informationsoverførsel.	Ingen afvigelser konstateret.
A13.2.4	**Fortroligheds- og hemmeligholdelsesaftaler**	**F&P:**	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
	Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler virksomhedens behov for at beskytte informationer, er identificeret og evalueres regelmæssigt og dokumenteres.	Inspiceret informationssikkerhedspolitikken for krav til fortroligheds- og hemmeligholdelsesaftaler, samt at denne er opdateret og godkendt. Inspiceret, at standardansættelseskontrakten indeholder et afsnit omkring krav til fortroligheds- og hemmeligholdelsesaftaler. Stikprøvevis inspiceret, at nyansatte medarbejdere har en underskrevet ansættelseskontrakt. **Sentia:** Inspiceret, at 'Code of Practice' indeholder beskrivelse om opbevaring og sletning af personhenførbare data i overensstemmelse med GDPR.	

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A14	**Anskaffelse, udvikling og vedligeholdelse af systemer**		
A14.1	**Sikkerhedskrav til informationssystemer** Kontrolmål: At sikre, at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.		
A14.1.1	**Analyse og specifikation af informationssikkerhedskrav** Informationssikkerhedsrelaterede krav er omfattet af kravene til nye informationssystemer eller forbedringer til eksisterende informationssystemer.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder krav til informationssikkerheden i forbindelse med nye systemer. Inspiceret, at Autotaks' procedurehåndbog indeholder procedure for strukturering af informationssikkerhedskrav ved hver iteration af forbedring til eksisterende informationssystemer. Stikprøvevis inspiceret, at informationssikkerhed er en del af kravene til udviklingsopgaver/projekter, samt at der foretages test af ændringer, inden de bliver lagt i produktion.	Ingen afvigelser konstateret.
A14.2	**Sikkerhed i udviklings- og hjælpeprocesser** Kontrolmål: At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.		
A14.2.1	**Sikker udviklingspolitik** Der er fastlagt og anvendes regler for udvikling af software og systemer i virksomheden.	**F&P:** Inspiceret procedurehåndbogen for procedure for ændringshåndtering.	Ingen afvigelser konstateret.
A14.2.2	**Procedurer for styring af systemændringer** Ændringer af systemer inden for udviklingscyklussen er styret ved hjælp af formelle procedurer for ændringsstyring.	**F&P:** Inspiceret, at procedurehåndbogen indeholder procedure for styring af systemændringer. Inspiceret, at udvikling følger en fast proces i udviklingsstyringsværktøjet. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A14.2.3	**Teknisk gennemgang af applikationer efter ændringer af driftsplatforme** Ved ændring af driftsplatforme er forretningskritiske applikationer gennemgået og testet for at sikre, at ændringen ikke indvirker negativt på virksomhedens drift eller sikkerhed.	**F&P:** Inspiceret, at procedurehåndbogen indeholder procedure for teknisk gennemgang af applikationer efter ændringer af driftsplatforme. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet. Observeret, at der anvendes en testserver adskilt fra produktions- og udviklingsmiljøet.	Ingen afvigelser konstateret.
A14.2.5	**Principper for udvikling af sikre systemer** Principper for udvikling af sikre systemer er fastlagt, dokumenteret, opretholdt og anvendt i forbindelse med implementering af informationssystemer.	**F&P:** Inspiceret procedurehåndbogen for udvikling af sikre systemer.	Ingen afvigelser konstateret.
A14.2.6	**Sikkert udviklingsmiljø** Virksomheden har etableret sikre udviklingsmiljøer for systemudvikling og –integration, som dækker hele systemudviklingens livscyklus.	**F&P:** Inspiceret procedurehåndbogen for sikring af udviklingsmiljø. Inspiceret informationssikkerhedspolitikken for sikker udviklingspolitik. Forespurgt, om brugere med adgang til kildekoden har et arbejdsbetinget behov herfor. Observeret, at der foreligger et virtuelt testmiljø, der er logisk adskilt fra produktionsmiljøet. Inspiceret, at adgangen til udviklingsmiljøet styres og er begrænset til udviklere.	Ingen afvigelser konstateret.
A14.2.8	**Systemsikkerhedstest** Ved udvikling udføres der test af sikkerhedsfunktionaliteten.	**F&P:** Inspiceret, at procedurehåndbogen for udvikling foreskriver procedure gældende for informationssikkerhedsfunktionalitet ved udvikling. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet.	Ingen afvigelser konstateret.
A14.2.9	**Systemgodkendelsestest** Der er etableret godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.	**F&P:** Inspiceret informationssikkerhedspolitikken for procedure for test af sikkerhedsfunktionaliteten ved udvikling.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet. Stikprøvevis inspiceret, at der afholdes månedlige driftsstatusmøder med Sentia.	
A14.3	**Testdata** Kontrolmål: At sikre beskyttelse af data, som anvendes til test.		
A14.3.1	**Sikring af testdata** Testdata er udvalgt omhyggeligt og beskyttes og kontrolleres.	**F&P:** Forespurgt om proceduren for sikring af testdata. Inspiceret informationssikkerhedspolitikken for sikring af testdata. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet.	Ingen afvigelser konstateret.
A15	**Leverandørforhold**		
A15.1	**Informationssikkerhed i leverandørforhold** Kontrolmål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.		
A15.1.1	**Informationssikkerhedspolitik for leverandørforhold** Informationssikkerhedskrav til at minimere risici forbundet med leverandørs adgang til virksomhedens aktiver er aftalt med leverandøren og dokumenteret.	**F&P:** Inspiceret informationssikkerhedspolitikken for retningslinjer om leverandørforhold. Stikprøvevis inspiceret, at brugeres adgange gennemgås periodisk på driftsstatusmøderne. Inspiceret Active Directory-gruppen for Sentia-brugere. Forespurgt, om brugere i Sentia AD-gruppen for Autotaks-systemet alle har et arbejdsbetinget behov for den tildelte adgang.	Ingen afvigelser konstateret.
A15.1.2	**Håndtering af sikkerhed i leverandøraftaler** Alle relevante informationssikkerhedskrav er fastlagt og aftalt med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere it-infrastrukturkomponenter til virksomhedens information.	**F&P:** Inspiceret informationssikkerhedspolitikken for håndtering af sikkerhed i leverandøraftaler. Inspiceret, at leverandøraftalen mellem Sentia og F&P indeholder krav til informationssikkerhed.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A15.2	**Styring af leverandørydelser** Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandør-aftalerne.		
A15.2.1	**Overvågning og gennemgang af leverandørydelser** Virksomheden overvåger, gennemgår og auditerer leverandørydelser regelmæssigt.	**F&P:** Inspiceret, om informationssikkerhedspolitikken indeholder beskrivelse af overvågning og gennemgang af leverandørydelser. Stikprøvevis inspiceret, at outsourcede ydelser overvåges via månedlige driftsrapporter. **Sentia:** Inspiceret, at Sentia løbende laver opfølgning af serviceleverandører.	Ingen afvigelser konstateret.
A16	**Styring af informationssikkerhedsbrud**		
A16.1	**Styring af informationssikkerhedsbrud og forbedringer** Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og –svagheder.		
A16.1.1	**Ansvar og procedurer** Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	**F&P:** Inspiceret, om informationssikkerhedspolitikken indeholder beskrivelse af ledelsesansvar og procedurer. Inspiceret, at der foreligger procedurer for håndtering af sikkerhedshændelser og databrud. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A16.1.2	**Rapportering af informationssikkerhedshændelser** Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	**F&P:** Forespurgt, om der er sket Informationssikkerhedshændelser. Inspiceret, at informationssikkerhedspolitikken indeholder beskrivelse af ledelsesansvar og procedurer. Inspiceret, at intro-program til it indeholder procedure for rapportering af informationssikkerhedshændelser. Observeret liste af hændelser og databrud for hele F&P. **Sentia:** Inspiceret it-sikkerhedspolitikken for rapportering af sikkerhedsbrud. Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar. Inspiceret liste af incidents relateret til F&P.	Ingen afvigelser konstateret.
A16.1.3	**Rapportering af informationssikkerhedssvagheder** Medarbejdere og kontrahenter, som bruger virksomhedens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i informationssystemer og -tjenester.	**F&P:** Forespurgt, om der er sket Informationssikkerhedshændelser. Inspiceret, at informationssikkerhedspolitikken indeholder beskrivelse af ledelsesansvar og procedurer. Inspiceret, at intro-program til it indeholder procedure for rapportering af informationssikkerhedssvagheder. Observeret liste af hændelser og databrud for hele F&P. **Sentia:** Inspiceret it-sikkerhedspolitikken for rapportering af sikkerhedsbrud. Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A16.1.4	**Vurdering af og beslutning om informationssikkerhedshændelser** Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	**F&P:** Forespurgt, om der er sket Informationssikkerhedshændelser. Inspiceret informationssikkerhedspolitikken for vurdering af og beslutning om informationssikkerhedshændelser. Observeret liste af hændelser og databrud for hele F&P. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Ingen afvigelser konstateret.
A16.1.5	**Håndtering af informationssikkerhedsbrud** Informationssikkerhedsbrud håndteres i overensstemmelse med de dokumenterede procedurer.	**F&P:** Forespurgt om proceduren for håndtering af informationssikkerhedsbrud. Forespurgt, om der er sket Informationssikkerhedshændelser. Inspiceret informationssikkerhedspolitikken for procedure for håndtering af informationssikkerhedsbrud. Observeret liste af hændelser og databrud for hele F&P. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Ingen afvigelser konstateret.
A16.1.6	**Erfaring fra informationssikkerhedsbrud** Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.	**F&P:** Inspiceret informationssikkerhedspolitikken for procedure for brug af erfaring fra informationssikkerhedsbrud. Observeret liste af hændelser og databrud for hele F&P. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Ingen afvigelser konstateret.
A17	**Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring**		
A17.1	**Informationssikkerhedskontinuitet** Kontrolmål: Informationssikkerhedskontinuiteten er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.		

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A17.1.1	**Planlægning af informationssikkerhedskontinuitet** Virksomheden har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.	**F&P og Sentia:** Inspiceret informationssikkerhedspolitikken for håndtering af beredskabsplan. Inspiceret, at proceduren for driftsnedbrud er tilgængelig for både F&P og Sentia. Inspiceret beredskabsplanen, samt at denne er tilgængelig for både F&P og Sentia.	Ingen afvigelser konstateret.
A17.1.2	**Implementering af informationssikkerhedskontinuitet** Virksomheden har fastlagt, dokumenteret, implementeret og vedligeholdt processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.	**F&P og Sentia:** Inspiceret informationssikkerhedspolitikken for håndtering af beredskabsplan. Inspiceret, at proceduren for driftsnedbrud er tilgængelig for både F&P og Sentia. Inspiceret beredskabsplanen, samt at denne er tilgængelig for både F&P og Sentia.	Ingen afvigelser konstateret.
A17.1.3	**Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten** Virksomheden verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	**F&P og Sentia:** Inspiceret informationssikkerhedspolitikken for håndtering af beredskabsplan. Inspiceret, at proceduren for driftsnedbrud er tilgængelig for både F&P og Sentia. Inspiceret, at beredskabsplanen er opdateret og testet i 2023.	Ingen afvigelser konstateret.
A17.2	**Redundans** Kontrolmål: At sikre tilgængelighed af information om behandlingsfaciliteter.		
A17.2.1	**Tilgængelighed af informationsbehandlingsfaciliteter** Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	**F&P og Sentia:** Inspiceret informationssikkerhedspolitikken for tilgængelighed af datacenterløsningen. Inspiceret, at der er etableret redundante servere samt et backupdatacenter til anvendelse i tilfælde af nedbrud.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A18.2	**Gennemgang af informationssikkerhed** Kontrolmål: At sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.		
A18.2.1	**Uafhængig gennemgang af informationssikkerhed** Virksomhedens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt og separat med planlagte mellemrum eller i tilfælde af væsentlige ændringer.	**F&P:** Inspiceret, at der findes krav om uafhængig revisionsgennemgang af informationssikkerheden. Inspiceret, at der er gennemført revision af udvalgte væsentlige områder.	Ingen afvigelser konstateret.
A18.2.3	**Undersøgelse af teknisk overensstemmelse** Informationssystemer kontrolleres regelmæssigt for overensstemmelse med virksomhedens informationssikkerhedspolitikker og -standarder.	**Sentia:** Forespurgt om kontrol af informationssystemer og deres overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder.	Ingen afvigelser konstateret.

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."

Peder Herbo
F&P Brancheløsninger P/S CVR: 42855588
It-direktør
På vegne af: F&P Brancheløsninger
Serienummer: a7ebdab7-0425-4b51-92da-a0f81b43d65c
IP: 188.244.xxx.xxx
2024-02-23 11:39:53 UTC

Thomas Brenøe
Direktion
På vegne af: F&P Brancheløsninger
Serienummer: d811ad1d-89fe-4adb-805c-98b50180b8ba
IP: 188.244.xxx.xxx
2024-02-23 11:43:37 UTC

Nils Bonde Christiansen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1
IP: 165.225.xxx.xxx
2024-02-23 11:53:50 UTC

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 80.208.xxx.xxx
2024-02-23 12:52:04 UTC