Fonden F&P Formidling

ISAE 3000-erklæring for perioden 1. januar - 31 december 2018 om generelle it-kontroller relateret til WebEDI-systemet

Building a better working world

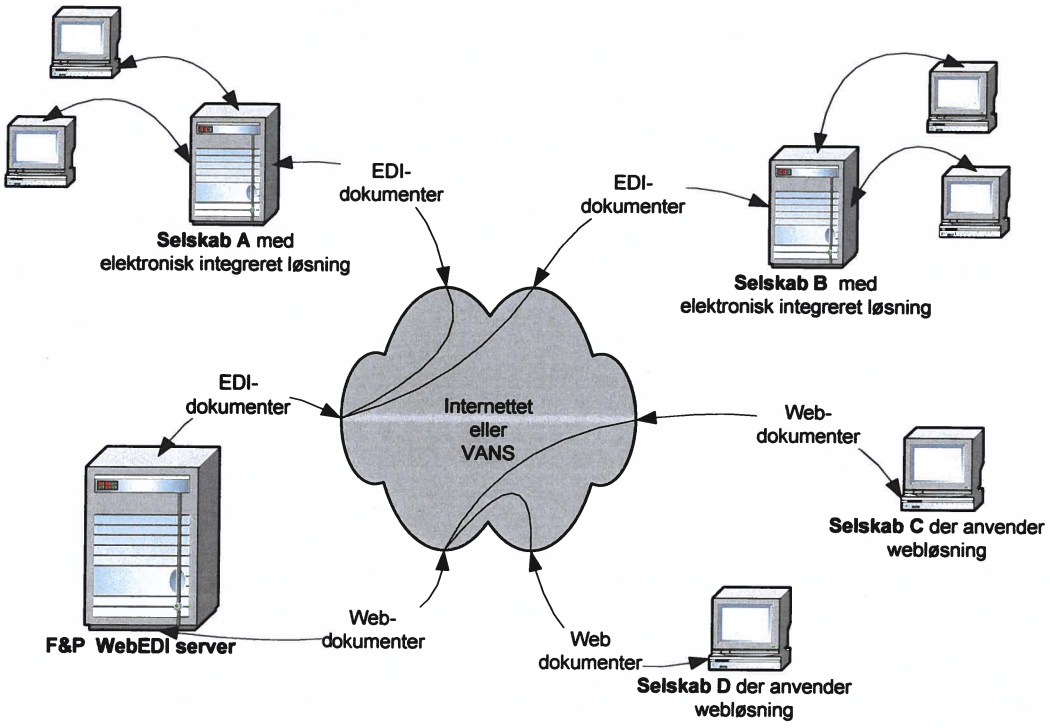
Indhold

1 Beskrivelse af F&P's WebEDI-system

Fonden F&P Formidling (herefter F&P) har udviklet en EDI-løsning, der integrerer udveksling via webblanketter, EDIFACT og XML. Systemet afvikles på en Windows-platform med underliggende SQL-databaser.

Udveksling via WebEDI-systemet er baseret på, at de deltagende parter kan udveksle dokumenter enten via en webgrænseflade eller en EDI-grænseflade eller alternativt via en kombination af web og EDI. Løsningen sikrer, at alle tilsluttede virksomheder i princippet kan udveksle data elektronisk, således at de tilsluttede virksomheder, der investerer i en elektronisk integreret løsning, ikke parallelt skal håndtere en alternativ manuel arbejdsgang.

F&P's WebEDI-servere udgør den centrale udvekslingsplatform for udveksling af dokumenter for forsikringsselskaber, pensionsselskaber samt banker og leasingselskaber, og alle oplysninger vedrørende ordningerne Opsigelser, Regres, Panthaverdeklarationer, LD-ordninger, § 41 mellem pensionsselskaber, § 41 mellem bank og pensionsselskaber, Skadehistorik og FP-attester distribueres gennem serveren. Miljøet kan skitseres således:



Miljøet hos F&P omfatter følgende væsentlige it-komponenter:

System	It-komponenter
Servere	2 produktionsservere fordelt på 2 lokationer (2-centerdrift) samt 1 testserver 2 databaseservere fordelt på 2 lokationer (2-centerdrift)
Operativsystem	Windows 2012 R2
Databasesystem	SQL Server 2012

Kommunikationsforbindelser til udveksling af elektroniske dokumenter mellem brugerne af WebEDI-systemet hos F&P sker via VANS-netværk eller internettet og varetages af brugerne selv. Brugerne er ansvarlige for sikkerheden på området, jf. aftalebetingelserne for tilslutning til og anvendelse af F&P's WebEDI-system.

F&P har ansvaret for, at der i medfør af F&P's sikkerhedspolitik er implementeret de fornødne generelle it-kontroller omkring WebEDI-systemet.

Denne erklæring omhandler de generelle it-kontroller, der understøtter WebEDI-systemet. Erklæringen er udarbejdet efter helhedsmetoden som beskrevet i ISAE 3402-standarden og omfatter således både kontrolmål og kontroller hos F&P og hos vores serviceunderleverandør Sentia A/S (tidligere Jaynet A/S).

Erklæringen omhandler ikke applikationskontroller i WebEDI-systemet.

Erklæringen dækker perioden 1. januar 2018 - 31. december 2018.

1.1 Risikostyring

F&P har foretaget en risikoanalyse for at sikre, at fornødne generelle it-kontroller til understøttelse af WebEDI-systemet er implementeret.

Risikoanalysen har været tilrettelagt med henblik på at identificere og undersøge både interne og eksterne risici.

Den samlede risikoanalyse har bestået af en indledende overordnet Business Impact-analyse og en efterfølgende detaljeret risikoanalyse.

Business Impact-analysen (BIA-analyse)

BIA-analysen har omfattet en vurdering af de forretningsmæssige konsekvenser ved:

- Brud på fortrolighed
- Brist i datas integritet, herunder fuldstændighed og nøjagtighed
- Manglende tilgængelighed af EDI-system

BIA-analysen har været baseret på Sprint-metoden fra Information Security Forum (ISF).

Risikoanalyse

Med udgangspunkt i den overordnede BIA-analyse er der gennemført en detaljeret risikoanalyse baseret på OCTAVE-metoden, som er en kvalitativ og systematisk risikovurderingsmetode udviklet ved CERT Coordination Center (CERT/CC) ved Carnegie Mellon Universitetets Software Engineering Institute (SEI) i USA.

OCTAVE-metoden er valgt, fordi metodens principper er internationalt anerkendte, og fordi den lever op til ISO 27002:2013, som F&P's informationssikkerhedspolitik er baseret på.

Risikoanalysen har omfattet en vurdering af risikoen for, at forskellige trusler/hændelser indtræffer, dvs. først vurderes sandsynligheden for, at de indtræffer, og dernæst vurderes konsekvenserne, hvis det sker. Vurderingen har været baseret på F&P's indhentede erfaringer fra den hidtidige brug af WebEDI-systemet.

1.2 Organisering af sikkerheden i it-miljøerne

Informationssikkerhedspolitik

Tilrettelæggelse og implementering af generelle it-kontroller vedrørende WebEDI-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	Medarbejdersikkerhed	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 retableringsstyring
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 følgende hovedprocesser, der er baseret på standarden ISO27001:2013 og følger den overordnede struktur. De følgende beskrivelser refererer til afsnittene i standarden:

5 Overordnede retningslinjer

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 sin 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 Driftsikkerhed

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 og 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 retableringsstyring

Omfatter F&P 's krav til beredskabsstyring, herunder beredskabsplaner, afprøvning og retablering 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 WebEDI-systemet til Sentia. Det er derfor væsentligt, at F&P's informationssikkerhedspolitik også implementeres og efterleves i forbindelse med drift af WebEDI-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

- Skadehistorik-løsningen er udvidet med private motorkøretøjer og kommunikationen mellem selskab og EDI-serveren på denne løsning er ændret fra SOAP WebServices til Rest Api. Derudover er sikkerheden på denne løsning opgraderet til OAuth2 flow.
- Der er indført automatiserede slettepolitikker i overensstemmelse med GDPR på hele EDI-løsningen.

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 WebEDI-systemet i forhold til brugeradministration, passwordpolitik, periodisk gennemgang af brugernes adgangsrettigheder og beredskab.

Brugeradministration (oprettelse, ændring, sletning)	F&P	Brugere af WebEDI-systemet
Medarbejdere hos brugere af F&P		x
Medarbejdere hos F&P	x	

Passwordpolitik	F&P	Brugere af WebEDI-systemet
Medarbejdere hos brugere af F&P		x
Medarbejdere hos F&P	x	

Regelmæssig gennemgang af adgangsrettigheder	F&P	Brugere af WebEDI-systemet
Medarbejdere hos brugere af F&P		x

Regelmæssig gennemgang af adgangsrettigheder	F&P	Brugere af WebEDI-systemet
Medarbejdere hos F&P	x[1]	

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

Beredskab	F&P	Brugere af WebEDI-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 WebEDI-systemet
Sikkerheden i management-netværk hos Sentia	x	
Sikkerheden i netværks-forbindelser mellem Sentia og brugerne		x

2 Udtalelse fra ledelsen

Medfølgende beskrivelse er udarbejdet til brug for brugerne af F&P's WebEDI-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 anvendt, når de opnår en forståelse af brugernes informationssystemer.

F&P anvender serviceunderleverandøren Sentia. Denne erklæring er udarbejdet efter helhedsmetoden, og beskrivelsen i afsnit 1 omfatter kontrolmål og tilknyttede kontroller hos Sentia.

F&P bekræfter, at:

(a) den medfølgende beskrivelse i afsnit 1 giver en retvisende beskrivelse af de generelle it-kontroller med relevans for WebEDI-systemet, der har været anvendt af brugerne i perioden fra 1. januar - 31. december 2018. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:

- de typer af ydelser, der er leveret
- de processer i både it-systemer og manuelle systemer, der er anvendt til styring af de generelle it-kontroller
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til kontrollernes udformning har forudsat, ville være implementeret af brugerne af WebEDI-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
- hvordan andre betydelige begivenheder og forhold end transaktioner behandles
- 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 de generelle it-kontroller foretaget i perioden fra 1. januar - 31. december 2018

(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 en bred kreds af brugere af WebEDI-systemet og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte bruger af WebEDI-systemet måtte anse for vigtigt efter deres særlige forhold

(iv) medtager kontrolmål og tilknyttede kontroller hos vores underleverandører og vores kontrolaktiviteter med disse underleverandører.

(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar - 31. december 2018. 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 anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar - 31. december 2018.

Hellerup, den 26. marts 2019

Thomas Brenøe
vicedirektør

Peder Herbo
it- & digitaliseringschef

3 Den uafhængige revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

Til: Forsikring & Pension

Omfang

Vi har fået som opgave at afgive erklæring om F&P's beskrivelse i afsnit 1 om generelle it-kontroller vedrørende WebEDI-systemet i perioden fra 1. januar - 31. december 2018 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

F&P anvender serviceunderleverandøren Sentia. Ledelsens beskrivelse af generelle it-kontroller omfatter kontrolmål og tilknyttede kontroller hos serviceunderleverandøren. Denne erklæring er udarbejdet efter helhedsmetoden. Vores handlinger omfatter også kontroller hos serviceunderleverandøren.

F&P's ansvar

F&P er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (etiske regler for revisorer), som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Firmaet anvender ISQC 1[1] og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om F&P'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 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. 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 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 kontrolmål samt hensigtsmæssigheden af de kriterier, som F&P har specificeret og beskrevet i afsnit 2.

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

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

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 WebEDI-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 funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

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

(a) beskrivelsen af de generelle it-kontroller med relevans for WebEDI-systemet, således som de var udformet og implementeret i perioden 1. januar - 31. december 2018, i alle væsentlige henseender er retvisende

(b) 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 - 31. december 2018

(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 fungeret effektivt i hele perioden fra 1. januar - 31. december 2018.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt brugere, der har anvendt WebEDI-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 risiciene vedrørende brug af WebEDI-systemet.

København, den 26. marts 2019
ERNST & YOUNG
Godkendt Revisionspartnerselskab
CVR nr.: 30 70 02 28

Claus Thaudahl Hansen
statsaut. revisor
mne19675

Christian H. Riis
senior manager, CISA

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 funktionalitet 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 WebEDI-systemet, der anvender løsningen beskrevet i afsnit 1, er ikke omfattet af vores test.

Test af funktionaliteten har omfattet de kontroller, som blev vurderet nødvendige for kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden fra 1. januar til 31. december 2018.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers funktionalitet 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 2018. Dette omfatter bl.a. vurdering af patchningsniveau, tilladte services, segmentering, passwordkompleksitet 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.
Genudføre kontrollen	Gentag den relevante kontrol. Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

For den del af it-miljøerne, der i perioden 1. januar - 31. december 2018 har været outsourcet til Sentia, har vi foretaget test af design, implementering og 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 WebEDI-system.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A5	**Informationssikkerhedspolitikker**		
A5.1	**Retningslinjer for styring af informationssikkerhed** Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden 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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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.
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.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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 procedure for funktionsadskillelse. Inspiceret informationssikkerhedspolitikken for funktionsadskillelse af roller og ansvarsområder. Inspiceret procedurehåndbog for proces for funktionsadskillelse i roller og ansvarsområder. **Sentia:** Inspiceret, at organisationsdiagram viser adskillelse mellem modstridende funktioner og ansvarsområder. Inspiceret, at AD-grupper for relevante systemer kun indeholder personer fra de korrekte grupperinger i organisationsdiagrammet.	Der er ikke etableret funktionsadskillelse mellem udviklings-, test- og produktionsmiljø for udviklere. F&P har besluttet, at udviklere skal have adgang til produktionsmiljøet af hensyn til muligheden for at kunne foretage hurtig afhjælpning af eventuelle driftsproblemer. Ingen andre afvigelser konstateret.
A6.1.3	**Kontakt med myndigheder** Der opretholdes passende kontakt med relevante myndigheder.	**F&P:** Forespurgt om procedure for kontakt med myndigheder.	Ingen afvigelser konstateret.
A6.1.5	**Informationssikkerhed ved projektstyring** Informationssikkerhed anvendes ved projektstyring, uanset projekttype.	**F&P:** Forespurgt om procedure for anvendelse af informationssikkerhed i projektstyring. Stikprøvevis inspiceret, at informationssikkerhed indgår i kravspecifikationen i projekter.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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 procedure for mobilt udstyr. Inspiceret informationssikkerhedspolitikken for betjening af mobile enheder. Inspiceret retningslinjer vedrørende sikker brug af mobiltelefoner.	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 tiltænkt.		
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, klassificering en af den information, der skal gives adgang til, og de relevante risici.	**F&P:** Forespurgt om proceduren for screening af jobkandidater. Inspiceret informationssikkerhedspolitikken for screeningsproces for personer, der vil få adgang til it-kritiske data. Inspiceret, at der foreligger dokumentation for, at tiltrådte har gennemgået screeningsprocessen før ansættelse.	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 procedure for udarbejdelse af kontrakter til medarbejdere og kontrahenter. Inspiceret, at en standardansættelseskontrakt indeholder pågældendes og virksomhedens ansvar for informationssikkerhed. Inspiceret, at tiltrådte har underskrevet kontrakter indeholdende pågældendes og virksomhedens ansvar for informationssikkerhed. **Sentia:** Forespurgt om procedure for udarbejdelse af kontrakter til medarbejdere og kontrahenter. Inspiceret, at en standardansættelseskontrakt indeholder pågældendes og virksomhedens ansvar for informationssikkerhed.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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.
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, 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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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 vedrørende medarbejderens ansvar for sikker brug af it. Herunder observeret, at der er etableret en proces for sanktioner i forbindelse med informationssikkerhedsbrud.	Vi er informeret om, at der i perioden ikke har været registreret informationssikkerhedsbrud, hvorfor det ikke har været muligt at teste effektiviteten. 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 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, at fratrådte medarbejdere har tilbageleveret deres aktiver. **Sentia:** Inspiceret sikkerhedshåndbogen for medarbejderforpligtelser ved fratrædelse. 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:** Forespurgt om procedure for bortskaffelse af medier. Inspiceret, at der i kontrakten mellem Sentia og F&P foreligger et afsnit omkring destruktion af medier.	Vi er informeret om, at der ikke er foretaget destruktion af medier i revisionsperioden, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen. Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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:** Forespurgt om proceduren for adgangsstyring. 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 godkendt ultimo 2017 af økonomidirektøren. 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.	**F&P:** Forespurgt om proceduren for adgang til netværk og netværkstjenester. Inspiceret procedurehåndbogen vedrørende tildeling af adgange til netværk. **Sentia:** Inspiceret proceduren for personaleadgang, herunder proceduren for adgang til netværkstjenester. Inspiceret personale-it-sikkerhedshåndbogen for procedure vedrørende tilslutning til netværk. Stikprøvevis inspiceret, at medarbejdere med adgang til netværket er autoriseret.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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, at fratrådte medarbejdere disables i systemerne, og at den beskrevne procedure følges. **Sentia:** Inspiceret procedure for personaleadgang, herunder beskrivelse af roller og ansvar i forbindelse med brugerregistrering og -afmelding. Inspiceret procedure for brugerafmelding. Stikprøvevis inspiceret, at fratrådte medarbejderes adgang afmeldes. Stikprøvevis inspiceret, at brugerregistreringer godkendes inden oprettelse.	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. **Sentia:** Inspiceret procedure for personaleadgang, herunder beskrivelse af roller og ansvar i forbindelse med brugerregistrering og -afmelding. Inspiceret procedure for brugerafmelding. Stikprøvevis inspiceret, at fratrådte medarbejderes adgang afmeldes. Stikprøvevis inspiceret, at brugerregistreringer godkendes inden oprettelse.	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 systembeskrivelsen indeholder politik for passwordopsætning. Inspiceret, at passwordopsætningen følger politikken. **Sentia:** Inspiceret, at passwordpolitikken 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 procedure 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, 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:** Inspiceret, at informationssikkerhedspolitikken indeholder procedure for administration af passwords. Inspiceret proceduren for kryptografi. Inspiceret passwordopsætningen for EDI-systemet. **Sentia:** Inspiceret, at passwordopsætningerne 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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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.
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 administration af krypteringsnøgler. Inspiceret informationssikkerhedspolitikken vedrørende procedure 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
A11	**Fysisk sikring og miljøsikring**		
A11.1	**Sikre områder** Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.		
A11.1.1	**Fysisk perimetersikring** Der er defineret og anvendt perimetersikring til beskyttelse af områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.	**Sentia:** Inspiceret Datacenterbeskrivelsen for fysisk sikkerhed. Observeret, at der skal bruges adgangsbrik til indgangen til datacentret, personligt adgangskort, irisscanner til sluse samt kort og pinkode til produktionsmiljøerne i datacentret.	Ingen afvigelser konstateret.
A11.1.2	**Fysisk adgangskontrol** Sikre områder er beskyttet med passende adgangskontroller for at sikre, at kun autoriseret personale får adgang.	**Sentia:** Inspiceret Datacenterbeskrivelsen, og at sikkerhedsregler indeholder procedure for fysisk adgangskontrol. Observeret, at der skal bruges adgangsbrik til indgangen til datacentret, personligt adgangskort, irisscanner til sluse samt kort og pinkode til produktionsmiljøerne i datacentret. Inspiceret udtræk over adgange til datacentret for Sentias medarbejdere. Inspiceret, at listen over medarbejdere med adgang til datacentret gennemgås regelmæssigt. Observeret, at tilsvarende standarder for fysisk adgangskontrol også er gældende for fysisk adgang til backup-sitet.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A11.1.3	**Sikring af kontorer, lokaler og faciliteter** Fysisk sikring af kontorer, lokaler og faciliteter er tilrettelagt og etableret.	**Sentia:** Inspiceret Datacenterbeskrivelsen, og at sikkerhedsregler indeholder procedure for sikring af kontorer, lokaler og faciliteter. Observeret, at der kræves adgangskort for at få adgang til kontorer og mødelokaler.	Ingen afvigelser konstateret.
A11.1.4	**Beskyttelse mod eksterne og miljømæssige trusler** Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret.	**Sentia:** Inspiceret Datacenterbeskrivelsen, og at sikkerhedsregler indeholder procedure for brandslukning. Observeret, at der forefindes brandslukning med serviceaftale og godkendt servicetjek. Observeret, at gulvet i datacentret er hævet.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A11.2	**Udstyr** Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.		
A11.2.1	**Placering og beskyttelse af udstyr** Udstyr er placeret og beskyttet, således at risikoen for miljøtrusler og farer samt muligheden for uautoriseret adgang er nedsat.	**Sentia:** Inspiceret, at Datacentersikkerhedsregler indeholder beskrivelse af krav for sikkerheden, herunder dataopbevaring og vareindlevering. Observeret, at vareindlevering foretages bag nøddøren, og der derved ikke opbevares udstyr i datacentret, der ikke skal være der. Observeret, at alt udstyr er placeret i datacenterrummet, således at det er beskyttet af "bygning i bygning"-princippet.	Ingen afvigelser konstateret.
A11.2.2	**Understøttende forsyninger (forsyningssikkerhed)** Udstyr er beskyttet mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.	**Sentia:** Inspiceret, at Datacenterbeskrivelsen indeholder beskrivelse af sikring af udstyr imod strømsvigt. Observeret, at der er opsat fire generatorer samt diverse UPS både inden og uden for datacentret. Stikprøvevis inspiceret, at der er udført månedlig generatortest i 2018.	Ingen afvigelser konstateret.
A11.2.3	**Sikring af kabler** Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, er beskyttet mod indgreb og skader.	**Sentia:** Forespurgt om procedure for sikring af kabler. Observeret, at der er opstillet farveskema for, hvordan kabelføringen sker i rackskabene.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A11.2.4	**Vedligeholdelse af udstyr** Udstyr vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet.	**Sentia:** Forespurgt om proceduren for vedligeholdelse af udstyr. Stikprøvevis inspiceret, at der foretages regelmæssige vedligeholdelsestjek af generel infrastruktur. Stikprøvevis inspiceret, at servere opdateres.	Ingen afvigelser konstateret.
A11.2.7	**Sikker bortskaffelse eller genbrug af udstyr** Alt udstyr med lagringsmedier verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.	**Sentia:** Forespurgt om procedure for bortskaffelse og genbrug af udstyr. Observeret, at der i datacentret står en hydraulisk presse til destruktion af diske, der er defekte.	Ingen afvigelser konstateret.
A11.2.8	**Brugerudstyr uden opsyn** Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.	**F&P:** Inspiceret informationssikkerhedspolitikken for, hvordan udstyr skal placeres, således at risici mindskes. **Sentia:** Forespurgt om procedure for sikring af udstyr uden opsyn. Observeret, at der er opsat screensaver settings, samt at det ikke er muligt for brugeren at ændre disse settings.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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 Sentias wiki site for driftsprocedure. Inspiceret, at procedure for driftsnedbrud står beskrevet på Sentias wiki site. Inspiceret, at listen over adgange til Sentias wiki 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:** Forespurgt om proceduren for ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden. Stikprøvevis inspiceret, at der foreligger dokumentation for ændringer i ticket-systemet på baggrund af en forespørgsel fra F&P.	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:** Inspiceret Sentias wiki site samt netværksdiagram for adskillelse mellem udviklings-, test- og driftsmiljøer.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.2	**Malwarebeskyttelse** 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 procedure for sikring mod malware. Inspiceret, om personalehåndbogen indeholder beskrivelse af, hvordan medarbejdere skal forholdes sig i tilfælde af malware-angreb. Observeret, at det ikke er muligt for brugeren at ændre indstillinger og derved stoppe de implementerede kontroller mod malware.	Ingen afvigelser konstateret.
A12.3	**Backup** Kontrolmål: At beskytte mod tab af data.		
A12.3.1	**Backup af informationer** Der er taget backupkopier af informationer, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	**Sentia:** Forespurgt om procedure for backup af informationer, software og systembilleder. Observeret, at der er foretaget succesfuld backup, jf. proceduren, samt at disse gemmes. Inspiceret stikprøve af driftsrapporter, hvor vi kan se, at der er foretaget restore af tilfældige filer for at sikre, at backupdata kan genskabes.	Vi har konstateret, at det ikke har været muligt at modtage dokumentation for succesfuld backup før juli 2018. Ingen andre 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	**Hændelseslogning** Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	**Sentia:** Forespurgt om procedure for hændelseslogning. Stikprøvevis inspiceret, at der er opsat hændelseslogning på servere.	Ingen afvigelser konstateret.
A12.4.2	**Beskyttelse af log-oplysninger** Logningsfaciliteter og log-oplysninger er beskyttet mod manipulation og uautoriseret adgang.	**Sentia:** Forespurgt om procedure for beskyttelse af logning.	Vi har konstateret, at der ikke er etableret særskilt beskyttelse af log-oplysninger i Windows-miljøet. Ingen andre afvigelser konstateret.
A12.4.3	**Administrator- og operatørlogge** Aktiviteter udført af systemadministrator og systemoperatør logges, og loggene beskyttes og gennemgås regelmæssigt.	**Sentia:** Forespurgt om procedure for logning af systemadministratorer m.v. Stikprøvevis inspiceret, at der er opsat logning af aktiviteter udført af systemadministratorer m.v. på servere.	Vi har konstateret, at logs ikke gennemgås regelmæssigt. Ingen andre 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 procedure 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 softwareinstallationen i driftssystemer.	**Sentia:** Forespurgt om procedure for softwareinstallation på driftssystemer. Inspiceret Sentias wiki site for procedure for patch management. Inspiceret dokumentation for gennemført patchning.	Ingen afvigelser konstateret.
A12.6	**Sårbarhedsstyring** Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.		
A12.6.1	**Styring af tekniske sårbarheder** Der indhentes løbende informationer om tekniske sårbarheder 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 driftssystemer. Inspiceret Sentias wiki site for procedure for patch management. Inspiceret dokumentation for gennemført patchning.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.6.2	**Begrænsninger på softwareinstallation** Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.	**Sentia:** Forespurgt om begrænsninger på softwareinstallation for bruger-pc'er. Inspiceret personale-it-sikkerhedshåndbogen for procedure for installation af software på pc'er. Observeret, at det ikke er muligt for brugeren at ændre indstillinger og derved stoppe de implementerede kontroller mod malware.	Vi er informeret om, at der ikke er nogen teknisk begrænsning på installation af software, som foretages af brugere. Ingen andre afvigelser konstateret.
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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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:** Forespurgt om procedure for netværksstyring. Observeret, at der anvendes MPLS og VLAN til beskyttelse af kundenetværk. Inspiceret netværkstegning for sikkerhed i netværket samt opdeling af brugere og informationssystemer.	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 beskyttelse 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 entitet.		
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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A13.2.4	**Fortroligheds- og hemmeligholdelsesaftaler** Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler virksomhedens behov for at beskytte informationer, er identificeret og evalueres regelmæssigt og dokumenteres.	**F&P:** 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.	Ingen afvigelser konstateret.
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. 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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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. Inspiceret procedure for deployment af kildekode. Stikprøvevis inspiceret, at der for ændringer foreligger fallback-procedure, samt at der er udført test, inden ændring bliver lagt i produktion.	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 informationssikkerhedspolitikken indeholder procedure for styring af systemændringer. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet. **Sentia:** Inspiceret procedure for styring og implementering af systemændringer. Stikprøvevis inspiceret, at ændringer foretages på baggrund af forespørgsel fra F&P, samt at ændringen implementeres og lukkes efter foretaget test.	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 informationssikkerhedspolitikken indeholder procedure for teknisk gennemgang af applikationer efter ændringer af driftsplatforme. Vi er informeret om, at der ikke har været foretaget ændringer til driftsplatforme i 2018.	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.	Ingen afvigelser konstateret.
A14.2.8	**Systemsikkerhedstest** Ved udvikling udføres der test af sikkerhedsfunktionaliteten.	**F&P:** Inspiceret informationssikkerhedspolitikken for procedure for test af sikkerhedsfunktionaliteten ved udvikling. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet.	Det har ikke været muligt at fremfinde dokumentation for, at der er udført test af sikkerhedsfunktionalitet ved udviklingsopgaver. Ingen andre afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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. 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.	Ingen afvigelser konstateret.
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.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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 risiciene 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. Forespurgt, om brugere fra Sentia med adgang til AD-gruppen for EDI-systemet alle har et arbejdsbetinget behov for adgangen.	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 leverandøraftalerne.		
A15.2.1	**Overvågning og gennemgang af leverandørydelser** Virksomheden overvåger, gennemgår og auditerer leverandørydelser regelmæssigt.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder beskrivelse af overvågning og gennemgang af leverandørydelser. Stikprøvevis inspiceret, at outsourcede ydelser overvåges via månedlige driftsrapporter. Observeret, at Sentia fremsender mail til F&P, hvis der opstår en alarm.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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, at informationssikkerhedspolitikken indeholder beskrivelse af ledelsesansvar og procedurer. Inspiceret, at Sentias wiki site indeholder procedure for håndtering af informationssikkerhedsbrud. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Vi er informeret om, at der i perioden ikke har været nogen registrerede informationssikkerhedshændelser, hvorfor det ikke har været muligt at teste effektivitet af kontrollen. Ingen afvigelser konstateret.
A16.1.2	**Rapportering af informationssikkerhedshændelser** Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder beskrivelse af ledelsesansvar og procedurer. Inspiceret, at intro-program til it indeholder procedure for rapportering af informationssikkerhedshændelser. **Sentia:** Inspiceret it-sikkerhedspolitikken for rapportering af sikkerhedsbrud. Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Vi er informeret om, at der i perioden ikke har været nogen registrerede informationssikkerhedshændelser, hvorfor det ikke har været muligt at teste effektivitet af kontrollen. Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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:** Inspiceret, at informationssikkerhedspolitikken indeholder beskrivelse af ledelsesansvar og procedurer. Inspiceret, at intro-program til it indeholder procedure for rapportering af informationssikkerhedssvagheder. **Sentia:** Inspiceret it-sikkerhedspolitikken for rapportering af sikkerhedsbrud. Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Vi er informeret om, at der i perioden ikke har været nogen registrerede informationssikkerhedshændelser, hvorfor det ikke har været muligt at teste effektivitet af kontrollen. Ingen afvigelser konstateret.
A16.1.4	**Vurdering af og beslutning om informationssikkerhedshændelser** Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud.	**F&P:** Inspiceret informationssikkerhedspolitikken for vurdering af og beslutning om informationssikkerhedshændelser. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Vi er informeret om, at der i perioden ikke har været nogen registrerede informationssikkerhedshændelser, hvorfor det ikke har været muligt at teste effektivitet af kontrollen. Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A16.1.5	**Håndtering af informationssikkerhedsbrud** Informationssikkerhedsbrud håndteres i overensstemmelse med de dokumenterede procedurer.	**F&P:** Forespurgt om proceduren for håndtering af informationssikkerhedsbrud. Inspiceret informationssikkerhedspolitikken for procedure for håndtering af informationssikkerhedsbrud. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Vi er informeret om, at der i perioden ikke har været nogen registrerede informationssikkerhedshændelser, hvorfor det ikke har været muligt at teste effektivitet af kontrollen. 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. **Sentia:** Inspiceret procedurer for håndtering af informationssikkerhedsbrud, herunder definition af roller og ansvar.	Vi er informeret om, at der i perioden ikke har været nogen registrerede informationssikkerhedshændelser, hvorfor det ikke har været muligt at teste effektivitet af kontrollen. Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A17	**Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring**		
A17.1	**Informationssikkerhedskontinuitet** Kontrolmål: Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og retableringsstyring.		
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 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 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 beredskabsplanen, samt at denne er tilgængelig for både F&P og Sentia. Inspiceret, at beredskabsplanen er opdateret og testet i 2018.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
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. Observeret, at der er etableret redundante servere samt et backupdatacenter til anvendelse i tilfælde af nedbrud.	Ingen afvigelser konstateret.
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.