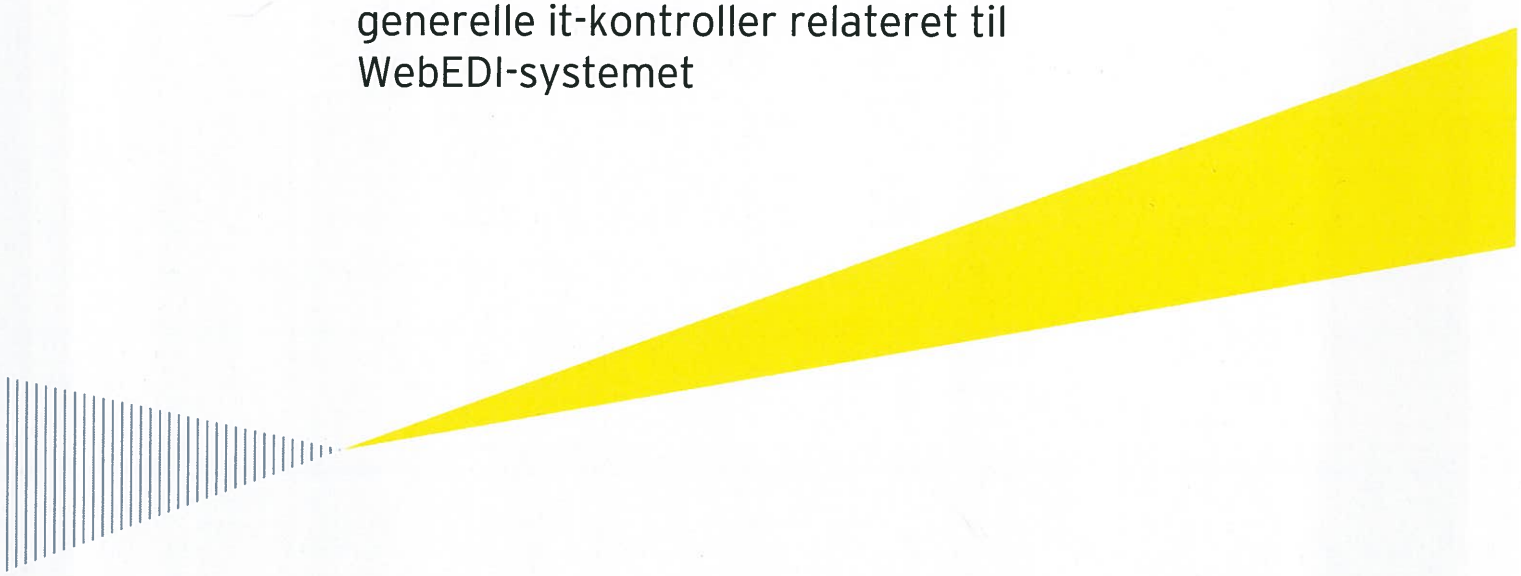
Fonden F&P formidling

ISAE 3000-erklæring for perioden 1. januar - 31. december 2016 om generelle it-kontroller relateret til WebEDI-systemet



Building a better working world

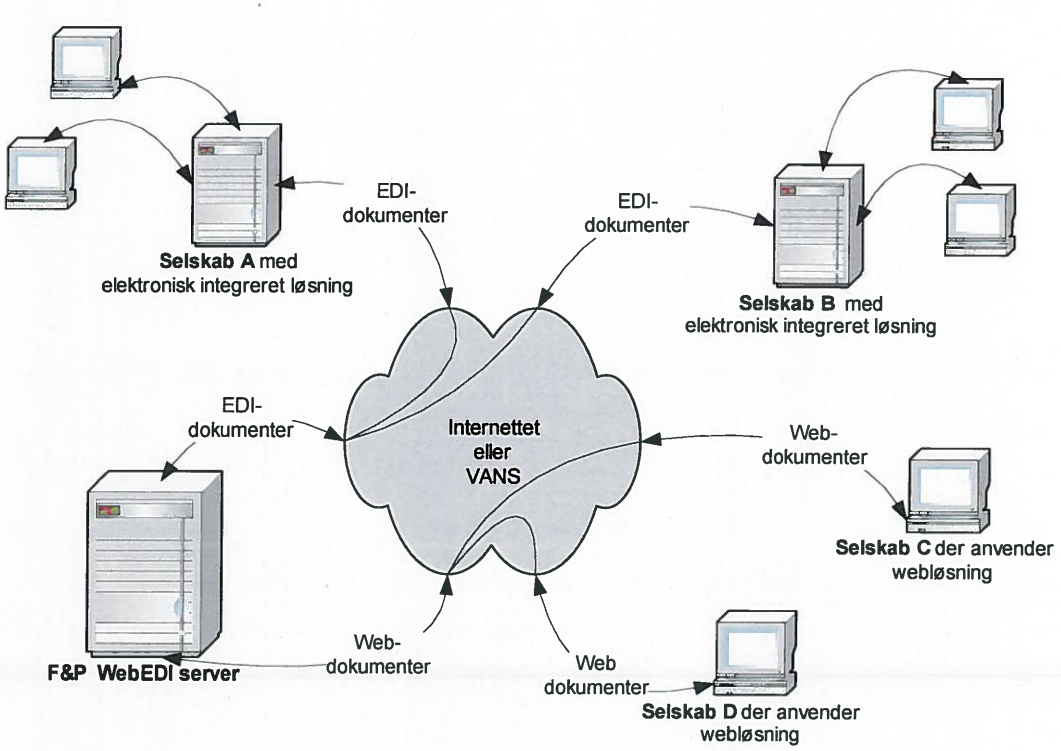
Indhold

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, SP-ordninger, LD-ordninger, § 41 mellem pensionsselskaber og § 41 mellem bank og pensionsselskaber 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 test server 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 2016 - 31. december 2016.

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 27002:2005, 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 ISO27002:2005. Standarden omfatter nedenstående hovedområder.

A.5	**It-sikkerhedspolitik**	A.11	**Adgangsstyring**
A.6	**Organisering af informationssikkerhed**	A.12	**Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer**
A.7	**Styring af aktiver**	A.13	**Styring af informationssikkerhedshændelser**
A.8	**Sikkerhed af menneskelige ressourcer**	A.14	**Beredskabsstyring**
A.9	**Fysisk og miljømæssig sikkerhed**	A.15	**Overensstemmelse**
A.10	**Styring af kommunikation og drift**		

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. Der er i 2016 foretaget enkelte tilpasninger af kontrolteksterne i afsnit 4.3., ligesom enkelte mindre væsentlige kontroller er udgået.

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

Der er ikke gennemført væsentlige ændringer i it-miljøerne, der anvendes til driftsafvikling af WebEDI-systemet i perioden 1. januar - 31. december 2016.

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 managementnetværk 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'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 har anvendt serviceunderleverandøren Sentia. Denne erklæring er udarbejdet efter helhedsmetoden, og beskrivelsen i kapitel 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 2016. 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 2016

(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 2016. 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 2016.

Hellerup, den 23. marts 2017

Carsten Andersen
vicedirektør

Peder Herbo
it-chef

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

Til: Fonden F&P formidling

Omfang

Vi har fået som opgave at afgive erklæring om F&P's beskrivelse i kapitel 1 af generelle it-kontroller vedrørende WebEDI-systemet i perioden fra 1. januar - 31. december 2016 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

F&P har anvendt 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 kapitel 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 kapitel 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 2016, 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 2016

(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 2016.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i kapitel 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 23. marts 2017
ERNST & YOUNG
Godkendt Revisionspartnerselskab

Claus Thaudahl Hansen
statsaut. revisor

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 kapitel 1. Evt. andre kontrolmål, tilknyttede kontroller og kontroller hos de brugere af WebEDI-systemet, der anvender løsningen beskrevet i kapitel 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 2016.

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 2016. 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 2016 - 31. december 2016 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	**It-sikkerhedspolitik**		
	Kontrolmål: At ledelsen viser retning for og understøtter informationssikkerhed i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.		
A5.1	Ledelsen godkender en skriftlig informationssikkerhedspolitik, som offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til godkendelse og kommunikation af it-sikkerhedspolitik. Vi har inspiceret, at ledelsen har godkendt en skriftlig it-sikkerhedspolitik, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.	Ingen afvigelser konstateret.
A5.2	Informationssikkerhedspolitikken evalueres med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til evaluering af it-sikkerhedspolitik. Vi har inspiceret dokumentation for, at it-sikkerhedspolitikken løbende godkendes, og at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A6	**Organisering af informationssikkerhed**		
	Kontrolmål: At styre informationssikkerhed i virksomheden og at sikre opretholdelse af sikkerheden vedrørende virksomhedens informationer og informationsbehandlingsudstyr, som eksterne parter har adgang til, eller som bearbejdes, kommunikeres til eller håndteres af eksterne parter.		
A6.1	Der er etableret en sikkerhedsafdeling/sikkerhedsfunktion.	Sentia: Vi har forespurgt om organiseringen af sikkerhedsfunktionen. Inspiceret dokumentation for, at sikkerhedsfunktionen er hensigtsmæssigt etableret.	Ingen afvigelser konstateret.
A6.2	Der foretages løbende sikkerhedsundersøgelser som kontrol for, at det aftalte sikkerhedsniveau overholdes.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til løbende sikkerhedsundersøgelser, herunder hvorledes det sikres, at det aftalte sikkerhedsniveau overholdes. Vi har inspiceret på stikprøvebasis at driftsstatus rapporteres.	F&P og Sentia: Ingen afvigelser konstateret.
A6.3	Ansvaret for informationssikkerhedsaktiviteter er klart defineret og placeret.	F&P og Sentia: Vi har forespurgt om, hvorledes it-sikkerhedsaktiviteter defineres og ansvarsmæssigt placeres. Vi har inspiceret, at it-sikkerhedsaktiviteter og ansvaret herfor er klart defineret i aftalehåndbogen mellem F&P og serviceleverandører.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A6.4	Der afgives tavshedserklæringer fra konsulenter og medarbejdere hos samarbejdspartnere.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til indhentelse af tavshedserklæringer fra konsulenter og medarbejdere hos samarbejdspartnere. Vi har inspiceret på stikprøvebasis, at der indhentes tavshedserklæringer i overensstemmelse med retningslinjer herfor.	Ingen afvigelser konstateret.
A7	**Styring af aktiver**		
	Kontrolmål: At opnå og opretholde passende beskyttelse af virksomhedens aktiver.		
A7.1	Der er hos serviceunderleverandører udpeget en ansvarlig for sikkerheden i WebEDI-systemerne.	Sentia: Vi har forespurgt om proces for udpegning af medarbejder med ansvar for sikkerheden i WebEDI-systemerne. Vi har inspiceret, at sikkerhedsansvaret er klart defineret i aftalehåndbogen mellem F&P og serviceunderleverandører, samt at der er udpeget en ansvarlig.	Ingen afvigelser konstateret.
A8	**Sikkerhed vedrørende menneskelige ressourcer**		
	Kontrolmål: At sikre, at medarbejdere, kontrahenter og eksterne brugere forstår deres ansvar og er egnede til de opgaver, de er kommet i betragtning til, og at nedsætte risikoen for tyveri, bedrageri eller misbrug af faciliteter.		

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A8.1	Medarbejdere, konsulenter og vikarer rapporterer væsentlige sikkerhedshændelser til it-afdeling/it-sikkerhedsansvarlig.	F&P og Sentia: Vi har forespurgt om proces for rapportering af væsentlige sikkerhedshændelser til den sikkerhedsansvarlige. Vi har inspiceret, at der forefindes en procedure for rapportering af væsentlige sikkerhedshændelser. Sentia: Stikprøvevis inspiceret, hvorvidt der er foretaget rapportering af væsentlige sikkerhedshændelser.	Ingen afvigelser konstateret.
A8.2	Serviceunderleverandører rapporterer væsentlige sikkerhedshændelser til systemejer/it-sikkerhedsansvarlig hos Fonden F&P formidling.	Sentia: Vi har forespurgt om proces og kontroller i relation til rapportering af væsentlige sikkerhedshændelser til systemejer/it-sikkerhedsansvarlig hos F&P. Vi har observeret at serviceleverandør rapporterer væsentlige sikkerhedshændelser til Fonden F&P formidling.	Ingen afvigelser konstateret.
A9	**Fysisk og miljømæssig sikkerhed**		
	Kontrolmål: At forhindre uautoriseret fysisk adgang til, beskadigelse og forstyrrelse af virksomhedens lokaler og informationer.		

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.1	Såvel ansatte som ikke-ansatte hos serviceunderleverandører skal kunne identificere sig, eksempelvis med personligt adgangskort med billede eller med gæstekort.	Sentia: Vi har inspiceret, at der forefindes en procedure til sikring af, at personer identificerer sig med personligt adgangskort med billede eller med gæstekort samt at der skal benyttes adgangskort for at få adgang til bygninger og serverrum.	Ingen afvigelser konstateret.
A9.2	Bygning er sikret med passende brandslukningsudstyr, eksempelvis håndslukkere.	Sentia: Vi har forespurgt om og inspiceret dokumentation for den etablerede brandsikring. Vi har observeret, at der forefindes brandslukningsudstyr på relevante lokationer.	Ingen afvigelser konstateret.
A9.3	Bygning og serverrum er forsynet med lås.	Sentia: Vi har observeret, at bygninger og serverrum er aflåst.	Ingen afvigelser konstateret.
A9.4	Der er etableret et fysisk adgangskontrolsystem, hvor adgang logges.	Sentia: Vi har forespurgt om og inspiceret dokumentation for, at fysisk adgang til bygninger og serverrum logges.	Ingen afvigelser konstateret.
A9.5	De tildelte fysiske adgange gennemgås og revurderes årligt.	Sentia: Vi har forespurgt om proces og kontrol for årlig gennemgang og revurdering af fysisk adgang.	Sentia: Der er ingen dokumenteret proces for periodisk gennemgang af fysiske adgange til datacentre hos Sentia, og der er

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Vi har inspiceret dokumentation for, at der er etableret en proces for årlig revurdering af fysisk adgang samt på stikprøvebasis inspiceret, at revurderingen er gennemført.	ingen skriftlig dokumentation af den foretagne gennemgang af de fysiske adgange. Bortset herfra har vi ikke konstateret afvigelser.
A9.6	Adgangskontrollog gennemgås efter behov for at afkræfte eller bekræfte mistanke om en mulig sikkerhedshændelse.	Sentia: Vi har forespurgt om proces og kontroller i relation til gennemgang af adgangskontrollog for at afkræfte eller bekræfte mistanke om en mulig sikkerhedshændelse. Vi har forespurgt, om der har været mistanke om en mulig sikkerhedshændelse, som har medført en gennemgang af adgangskontrolloggen i 2016.	Ingen afvigelser konstateret.
A9.7	Der er etableret branddetektering.	Sentia: Vi har forespurgt om og inspiceret dokumentation for den etablerede branddetektering.. Vi har observeret, at der forefindes branddetektering på relevante lokationer.	Ingen afvigelser konstateret.
A9.8	Der er installeret automatisk brandslukning.	Sentia: Vi har forespurgt om og inspiceret dokumentation for den etablerede brandsikring. Vi har observeret, at der forefindes brandslukningsudstyr på relevante lokationer.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.9	Sikkerhedskopier opbevares i sikker afstand fra det primære anlæg.	Sentia: Vi har forespurgt om opbevaring af sikkerhedskopier i sikker afstand fra det primære anlæg. Vi har inspiceret at Web-EDI-løsningen er dubleret på to fysiske lokationer. Vi har inspiceret opbevaring af sikkerhedskopier på den anden lokation end den lokation, hvorpå det primære anlæg er placeret.	Ingen afvigelser konstateret.
A9.10	Der er vanddetektering eller overvågning af fugtighed.	Sentia: Vi har forespurgt om og inspiceret dokumentation for den etablerede løsning for vanddetektering eller overvågning af fugtighed. Vi har observeret, at der forefindes vanddetektering eller overvågning af fugtighed på relevante lokationer.	Ingen afvigelser konstateret.
A9.11	Elforsyning er sikret mod udfald, eksempelvis via 2 uafhængige el-forsyninger (transformatorer).	Sentia: Vi har inspiceret dokumentation for, at der er etableret to separate elforsyninger samt nødstrømsforsyning på relevante lokationer.	Ingen afvigelser konstateret.
A9.12	Der er installeret nødstrømsbatteri (UPS).	Sentia: Vi har observeret, at der er etableret nødstrømsbatteri (UPS-anlæg).	Ingen afvigelser konstateret.
A9.13	Der er nødstrømsgenerator.	Sentia: Vi har observeret, at der er etableret nødstrømsgenerator.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A9.14	Nødstrømsanlæg testes regelmæssigt.	Sentia: Vi har forespurgt om proces og kontroller i relation til regelmæssig test af nødstrømsanlæg. Vi har inspiceret dokumentation for, at der er foretaget test af nødstrømsanlæg efter gældende retningslinjer herfor.	Ingen afvigelser konstateret.
A9.15	Kommunikationsveje er dublerede.	Sentia: Vi har forespurgt om og inspiceret dokumentation for den etablerede løsning for sikring af kommunikationsveje.	Ingen afvigelser konstateret.
A9.16	Reparationer og vedligeholdelse udføres kun af sikkerhedsgodkendte personer, eller af virksomheder med hvem der er indgået fortrolighedsaftale. Personer fra virksomheder, som ikke er sikkerhedsgodkendte, får udleveret gæstekort og ledsages ved adgang til serverrum.	Sentia: Vi har forespurgt om proces og kontrol til sikring af, at reparation og vedligeholdelse alene udføres af sikkerhedsgodkendte personer eller af virksomheder, med hvem der er indgået fortrolighedsaftale. Vi har observeret, at personer, som ikke er sikkerhedsgodkendt, synligt bærer gæstekort og er ledsaget i overensstemmelse med gældende retningslinjer herfor.	Ingen afvigelser konstateret.
A10	**Styring af kommunikation og drift**		
	Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsudstyr.		

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
	At implementere og opretholde et passende niveau af informationssikkerhed og serviceydelser i overensstemmelse med aftaler om ydelser fra tredjeparter. At minimere risikoen for systemnedbrud. At beskytte integriteten af software og informationer. At opretholde integritet og tilgængelighed af informationer og informationsbehandlingsudstyr. At sikre beskyttelse af informationer i netværk og beskyttelse af den understøttende infrastruktur. At forhindre uautoriseret afsløring, ændring, fjernelse eller destruktion af aktiver og afbrydelse af forretningsaktiviteter. At afsløre uautoriserede informationsbehandlingsaktiviteter.		
A10.1	Forretningsgange for ændringsstyringer er beskrevet og godkendt af parterne. Ændringsstyring er styret og formaliseret.	F&P og Sentia: Vi har forespurgt om proces og kontrol for, at ændringsstyring er beskrevet, formaliseret og godkendt af parterne. Vi har inspiceret på stikprøvebasis, at programændringer sker i overensstemmelse med de etablerede procedurer.	Sentia: Vi har konstateret behov for styrkelse af beskrivelserne af forretningsgangen for ændringsstyring. Der er pr. 21. marts 2017 udarbejdet en dokumenteret procedure for ændringshåndtering hos Sentia. Bortset herfra har vi ikke konstateret afvigelser.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A10.2	Planlægning og gennemførelse af ændringer foretages i henhold til godkendt forretningsgang for ændringsstyring.	F&P og Sentia: Vi har forespurgt om proces og kontrol for planlægning og gennemførelse af ændringer. Vi har inspiceret på stikprøvebasis, at ændringer er planlagt og gennemført i overensstemmelse med den godkendte forretningsgang for ændringsstyring.	Ingen afvigelser konstateret.
A10.3	Systemejer godkender skriftligt ændringer før implementering.	F&P og Sentia: Vi har forespurgt om proces og kontrol for, at systemejer skriftligt godkender ændringer før implementering. Vi har inspiceret på stikprøvebasis, at systemejer har godkendt ændringer før implementering.	Ingen afvigelser konstateret.
A10.4	Der er udarbejdet fallbackprocedure til brug ved fejlslagne ændringer.	F&P og Sentia: Vi har forespurgt om proces og kontrol for fallback til brug ved fejlslagne ændringer. Vi har inspiceret på stikprøvebasis, at der en beskrevet fallback plan for ændringer i revisionsperioden.	Sentia: Der er konstateret behov for styrkelse af processen for fallback ved fejlslagne ændringer. Bortset herfra har vi ikke konstateret afvigelser.
A10.5	Ændringer fra serviceleverandør er godkendt af Fonden F&P formidling, hvis de foregår uden for aftalt servicevindue.	F&P og Sentia: Vi har forespurgt om proces og kontrol for godkendelse af idriftsættelse af ændringer, som foregår uden for aftalt servicevindue.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Vi har inspiceret på stikprøvebasis, at systemejer har godkendt ændringer gennemført i 2016.	
A10.6	Ændringer fra Fonden F&P formidling er godkendt af serviceleverandør, hvis de foregår uden for aftalt servicevindue og kan have effekt for leverandørens opfyldelse af de aftalte servicemål.	F&P og Sentia: Vi har forespurgt om proces og kontrol for godkendelse af idriftsættelse af ændringer, som foregår uden for aftalt servicevindue. Vi har inspiceret på stikprøvebasis, at systemejer og serviceunderleverandører har godkendt ændringer gennemført i 2016.	Ingen afvigelser konstateret.
A10.7	Der er etableret funktionsadskillelse.	F&P: Vi har forespurgt om proces og kontrol for fysisk adskillelse af udviklings-, test- og driftsaktiviteter. Vi har inspiceret på stikprøvebasis, at der er etableret funktionsadskillelse for udviklere mellem udviklings-, test- og produktionsmiljø.	F&P: 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 yderligere afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A10.8	Udviklings-, test- og driftsaktiviteter er logisk eller fysisk adskilt.	F&P: Vi har forespurgt om proces og kontrol for fysisk adskillelse af udviklings-, test- og driftsaktiviteter. Vi har inspiceret dokumentation for arkitektur af WebEDI-løsningen for at sikre, at udviklings-, test- og driftsaktiviteter er adskilt på separate servere og databaser.	Ingen afvigelser konstateret.
A10.9	Krav til driftseffektivitet samt måling og rapportering af samme er aftalt. Den maksimalt accepterede utilgængelighed afspejles i aftaler om driftseffektivitet.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til måling og rapportering af driftseffektivitet. Vi har inspiceret på stikprøvebasis, at den maksimalt accepterede utilgængelighed er overholdt.	Ingen afvigelser konstateret.
A10.10	Der afholdes regelmæssigt møder med serviceleverandør med gennemgang af driftsrapport, herunder sikkerhedshændelser, opfølgning på sikkerhedshændelser, driftsproblemer, fejl og nedbrud.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til afholdelse af møder mellem serviceunderleverandører og F&P vedrørende driftsrapportering. Vi har inspiceret på stikprøvebasis, at afholdte møder indeholder dokumentation for gennemgang af driftsrapportering, herunder sikkerheds- og driftsproblemer samt fejl og nedbrud.	F&P og Sentia: Ingen afvigelser konstateret.
A10.11	Alle servere er sikret med on-access og on-demand antivirussoftware, som løbende opdateres.	Sentia:	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Vi har forespurgt om proces og kontroller i relation til sikring af servere med antivirus-software og løbende opdatering heraf. Vi har inspiceret på stikprøvebasis, at servere er konfigureret med antivirus-software, samt at der sker løbende opdatering heraf, således at det sikres, at servere er beskyttet på tilstrækkelig vis.	
A10.12	Der tages sikkerhedskopier, herunder eksempelvis af parameteropsætninger og anden driftskritisk dokumentation.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikkerhedskopiering af systemer og data. Vi har inspiceret på stikprøvebasis, at sikkerhedskopiering sker i overensstemmelse med den aftalte konfiguration.	Ingen afvigelser konstateret.
A10.13	Sikkerhedskopier afprøves regelmæssigt.	Sentia: Vi har forespurgt om proces og kontroller i relation til kvartalsvis test af læsbarhed. Vi har inspiceret, at der foretages kvartalsvis test af læsbarhed.	Sentia: Vi har konstateret at test af læsbarhed er foretaget en gang i 2016. Bortset herfra har vi ikke konstateret afvigelser.
A10.14	Gendannelsesprocedurer (restore) afprøves regelmæssigt.	Sentia: Vi har forespurgt om proces og kontroller i relation til årlig gendannelses test (restoretest).	Sentia: Vi har konstateret behov for styrkelse af processen for af-

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
			prøvning af gendannelse (restore). Gendannelse (restore) er ikke afprøvet i 2016. Bortset herfra har vi ikke konstateret afvigelser.
A10.15	Interne kommunikationsforbindelser er krypterede eller på anden måde beskyttet mod aflytning og uautoriseret adgang. Trådløse netværk er krypteret og beskyttet mod uautoriseret adgang.	Sentia: Vi har forespurgt om kontroller i relation til beskyttelse af interne kommunikationsforbindelser og trådløse netværk.	Ingen afvigelser konstateret.
A10.16	Websider er beskyttet mod uautoriserede ændringer via "stærke" sikringsforanstaltninger.	Sentia: Vi har forespurgt om kontroller til beskyttelse af websider mod uautoriserede ændringer. Vi har observeret, at websider er beskyttet af firewalls, logisk adgangskontrol samt SSLkryptering i overensstemmelse med Sentia's retningslinjer herfor.	Ingen afvigelser konstateret.
A10.17	Brugeraktiviteter, afvigelser og sikkerhedshændelser logges i en opfølgningslog.	Sentia: Vi har forespurgt om proces og kontroller i relation til logning af brugeraktivitet, afvigelser og sikkerhedshændelser. Vi har inspiceret på stikprøvebasis, at logning er implementeret på relevante servere og databaser.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A10.18	Logning omfatter som minimum succesfulde og fejlslagne logons, oprettelse/nedlæggelse af bruger-ID, ændring af brugeres adgangsrettigheder samt ændring af sikkerhedsmæssige parametre og adgangskontroller.	Sentia: Vi har forespurgt om proces og kontroller i relation til logning på servere og databaser, herunder at denne omfatter succesfulde og fejlslagne logons, oprettelse/nedlæggelse af bruger-ID, ændring af brugeres adgangsrettigheder samt ændring af sikkerhedsmæssige parametre og adgangskontroller. Vi har inspiceret på stikprøvebasis, at logning er implementeret på relevante servere og databaser.	Ingen afvigelser konstateret.
A10.19	Opfølgningslog gennemgås efter behov.	Sentia: Vi har forespurgt om proces og kontroller i relation til gennemgang af logs. Vi har forespurgt, om der har været begrundet mistanke om sikkerhedshændelser, som skal medføre en gennemgang af logs for F&P i 2016.	Ingen afvigelser konstateret.
A10.20	Aktiviteter udført af systemadministratorer og andre med særlige rettigheder logges.	Sentia: Vi har forespurgt om proces og kontroller i relation til logning af aktiviteter udført af systemadministratorer og andre med særlige rettigheder på servere og databaser. Vi har inspiceret på stikprøvebasis, at logning af aktiviteter udført af systemadministratorer og andre med særlige rettigheder er implementeret på relevante servere og databaser.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A10.21	Log med aktiviteter udført af brugere med særlige rettigheder gennemgås efter behov.	Sentia: Vi har forespurgt, om proces og kontroller i relation til gennemgang af logs med aktiviteter udført af brugere med særlige rettigheder. Vi har forespurgt, om der har været begrundet mistanke om sikkerhedshændelser, som skal medføre en gennemgang af logs med aktiviteter udført af brugere med særlige rettigheder for F&P i 2016.	Ingen afvigelser konstateret.
A10.22	Automatiske fejlregistreringsfunktioner (fejllog) er aktiv. Fejllog gennemgås efter behov.	Sentia: Vi har forespurgt om proces og kontroller i relation til opsætning og gennemgang af fejllogs. Vi har forespurgt, om der har været begrundet mistanke om sikkerhedshændelser, som skal medføre en gennemgang af logs for F&P i 2016.	Ingen afvigelser konstateret.

A11 Adgangsstyring

Kontrolmål:

At styre adgangen til informationer.

At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang til informationssystemer.

At forhindre uautoriseret brugeradgang og kompromittering eller tyveri af information og informationsbehandlingsudstyr.

At forhindre uautoriseret adgang til netværkstjenester.

At forhindre uautoriseret adgang til driftssystemer.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
	At forhindre uautoriseret adgang til information i forretningssystemer. At sikre informationer, når der anvendes mobilt udstyr og fjernarbejdspladser.		
A11.1	Der anvendes en formaliseret forretningsgang for tildeling, ændring og nedlæggelse af brugere, nulstilling af password og tildeling/ændring af autorisationer.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til tildeling, ændring og nedlæggelse af brugere, nulstilling af password og tildeling/ændring af autorisationer. Vi har inspiceret på stikprøvebasis, at der foreligger dokumentation for tildeling, ændring og nedlæggelse af brugere, nulstilling af password og tildeling/ændring af autorisationer.	Sentia: Godkendelse af oprettelse og ændring af brugere hos Sentia dokumenteres ikke. Bortset herfra har vi ikke konstateret afvigelser.
A11.2	Samme person benytter samme bruger-ID på tværs af alle systemer. Bruger-ID følger en beskrevet navnestandard.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af overholdelse af navnestandard på tværs af systemer. Vi har inspiceret på stiprøvebasis, at der foreligger dokumentation for overholdelse af navnestandard på tværs af systemer.	Ingen afvigelser konstateret.
A11.3	Brugerrettigheder er tildelt efter et arbejdsmæssigt behov.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til, om tildeling af brugerrettigheder til F&P og serviceleverandørbrugere sker efter et arbejdsmæssigt behov. Vi har inspiceret på stikprøvebasis, at brugerrettigheder til F&P og serviceleverandørbrugere er tildelt efter et arbejdsmæssigt behov.	Sentia: Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A11.4	Tildeling af udvidede rettigheder til administration af brugerprogrammer og styresystemer er begrænset.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til tildeling af udvidede rettigheder. Vi har inspiceret at udvidede rettigheder er restriktivt tildelt.	Ingen afvigelser konstateret.
A11.5	Tildelte adgange og rettigheder gennemgås regelmæssigt.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til gennemgang af tildelte adgange og rettigheder. Vi har inspiceret på stikprøvebasis, at der foreligger dokumentation for periodisk gennemgang af tildelte adgange og rettigheder. Vi har inspiceret på stikprøvebasis, at den foretagne gennemgang af tildelte adgange og rettigheder har medført nedlæggelse og tilretning af brugernes adgang efter et arbejdsmæssigt behov.	Sentia: Vi har konstateret behov for styrkelse af processen for regelmæssig gennemgang af tildelte adgangsrettigheder. Sentia har pr 21. marts 2017 tilføjet en årlig gennemgang af tildelte adgange og rettigheder til årshjulet for sikkerhedsgennemgange. Bortset herfra ingen afvigelser konstateret.
A11.6	Adgang gives kun efter afgivelse af et unikt bruger-ID og password.	Sentia: Vi har forespurgt om proces og kontroller, som sikrer, at adgang alene gives efter afgivelse af et unikt bruger-ID og password.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Vi har observeretat adgang til servere og databaser kræver afgivelse af bruger-ID og password.	
A11.7	Password skal være strengt personligt og må ikke videregives.	Sentia: Vi har forespurgt om proces og kontroller, som sikrer, at passwords er personlige og ikke videregives. Vi har inspiceret dokumentation for, at sikkerhedsprocedurer omfatter regler for håndtering af passwords, samt at disse er tilgængelige for alle personer. Vi har forespurgt om begrundet mistanke om, at brugere har videregivet personlige passwords i 2016.	Ingen afvigelser konstateret.
A11.8	Der skal benyttes et stærkt password, dvs. passwordlængde skal mindst være 8 tegn og skal sammensættes af store og små bogstaver, tal og specialtegn.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af anvendelse af stærke passwords. Vi har inspiceret på stikprøvebasis, at krav til passwords kompleksitet er aktiveret på de relevante servere og databaser.	Sentia: Vi har konstateret et mindre antal systembrugere på databasesystemet med behov for styrkelse af krav til password. Bortset herfra ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A11.9	Password fornys efter 90 dage eller ved mistanke om, at password er kendt af andre. Kravet til fornyelse efter 90 dage gælder ikke systembruger-ID'er, jf. pkt. 11.10.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af periodisk skift af passwords. Vi har inspiceret på stikprøvebasis, at krav til tvunget skift af password er aktiveret på de relevante servere og databaser.	Ingen afvigelser konstateret.
A11.10	Systembruger-ID kan tillades til brug i forbindelse med kørende services og kan efter godkendelse, som de eneste bruger-ID, undtages fra systemmæssige krav om passwordskift. Sådanne services dokumenteres, spærres mod interaktivt logon via netværket, og deres password skiftes minimum årligt.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af periodisk skift af passwords for systembruger-ID. Vi har inspiceret på stikprøvebasis, at krav til årligt skift af passwords for systembruger-ID er overholdt på de relevante servere og databaser.	Sentia: Der er ikke en procedure for skift af password til systemkonti hos Sentia. Vi har observeret systemkonti der ikke har skiftet password i 2016. Bortset herfra ingen afvigelser konstateret.
A11.11	Adgang spærres senest efter 5 mislykkede logon-forsøg.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af, at adgang spærres senest efter fem mislykkede logon-forsøg. Vi har inspiceret på stikprøvebasis, at det er overholdt på de relevante servere og databaser, at adgang spærres senest efter fem mislykkede logon.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A11.12	Pauseskærm med password aktiveres automatisk (senest efter 30 minutter)	F&P og Sentia: Vi har inspiceret på stikprøvebasis, at krav om automatisk aktivering af pauseskærm med password er overholdt.	Ingen afvigelser konstateret.
A11.13	Password lagres og transmitteres kun over internettet i krypteret form.	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af krypteret lagring og transmission af password. Vi har inspiceret på stikprøvebasis, at krypteret lagring og transmission af passwords er overholdt på de relevante servere og databaser.	Sentia: Ingen afvigelser konstateret.
A11.14	Remote-adgang sker kun ved hjælp af VPN (IPsec eller SSL).	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af, at remote-adgang til systemerne er krypteret. Vi har inspiceret på stikprøvebasis, at remote-adgang til systemer sker via en krypteret VPN-adgang.	Ingen afvigelser konstateret.
A11.15	Remote-adgang sker kun via to-faktor-identifikation ("Noget man ved, og noget man har", eksempelvis hardware-token og/eller certifikat - med tilhørende PIN-kode).	Sentia: Vi har forespurgt om proces og kontroller i relation til sikring af, at remote-adgang til systemerne er baseret på to-faktor-identifikation. Vi har inspiceret på stikprøvebasis, at remote-adgang til systemer sker baseret på to-faktor-identifikation.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12	**Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer.**		
	Kontrolmål: At sikre, at sikkerhed er en integreret del af informationssystemer. At forhindre fejl, tab, uautoriseret ændring eller misbrug af informationer i forretningssystemer. At nedsætte risici, der skyldes udnyttelse af kendte tekniske sårbarheder.		
A12.1	Styresystemer og brugersystemer er altid opdateret til et versionsniveau, der supporteres af leverandøren/anbefales af producenten.	Sentia: Vi har forespurgt om proces og kontroller i relation til opdatering af styresystemer og brugersystemer. Vi har inspiceret på stikprøvebasis, at servere og databaser er opdateret til et versionsniveau, der supporteres af leverandøren.	Sentia: Vi har konstateret at styresystem på servere ikke patches regelmæssigt. Bortset herfra ingen afvigelser konstateret.
A12.2	Der benyttes en beskrevet og aftalt procedure for programudvikling	F&P: Vi har forespurgt om proces og kontroller i relation til overholdelse af aftalt procedure for programudvikling. Vi har inspiceret på stikprøvebasis, at aftalt procedure for programudvikling er overholdt.	Ingen afvigelser konstateret.
A12.3	Kravspecifikationer godkendes af forud aftalte personer i Fonden F&P formidling, før udvikling iværksættes.	F&P: Vi har forespurgt om proces og kontroller i relation til F&P's godkendelse af kravspecifikationer, før udvikling iværksættes.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Vi har inspiceret på stikprøvebasis, at kravspecifikationer/ændringsbeskrivelser er godkendt af F&P.	
A12.4	Design, løsningsbeskrivelse godkendes af forud aftalte personer i Fonden F&P formidling, før udvikling iværksættes, herunder beskrivelse af implementering af sikkerhedskrav og krav til inddatakontroller	F&P: Vi har forespurgt om proces og kontroller i relation til F&P's godkendelse af design og løsningsbeskrivelser, før udvikling iværksættes. Vi har inspiceret på stikprøvebasis, at design og løsningsbeskrivelser er godkendt af F&P, herunder beskrivelse af implementering af sikkerhedskrav og krav til inddatakontroller.	Ingen afvigelser konstateret.
A12.5	Ændringer i forhold til den aftalte programudvikling godkendes formelt af forud aftalte personer i Fonden F&P formidling.	F&P: Vi har forespurgt om proces og kontroller i relation til, at F&P's godkendelse af programudvikling alene sker af forud aftalte personer i F&P. Vi har inspiceret på stikprøvebasis, at godkendelse af programudvikling er foretaget af personer hos F&P med rette bemyndigelse.	Ingen afvigelser konstateret.
A12.6	Resultat af test godkendes formelt af forud aftalte personer i Fonden F&P formidling.	F&P: Vi har forespurgt om proces og kontroller i relation til, at F&P's godkendelse af test af ændringer sker af forud aftalte personer i F&P. Vi har inspiceret på stikprøvebasis, at godkendelse af programudvikling er foretaget af personer hos F&P med rette bemyndigelse.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A12.7	System, platform, forretningsgange for drift, er udarbejdet, før systemer sættes i drift og holdes efterfølgende løbende ajour.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til ajourføring af system-, platforms- og forretningsgange ved ændringer. Vi har inspiceret på stikprøvebasis, at system-, drifts- og brugerdokumentation ved ændringer er udarbejdet/ajourført og overgivet til F&P.	Ingen afvigelser konstateret.
A13	**Styring af informationssikkerhedshændelser**		
	Kontrolmål: At sikre, at informationssikkerhedshændelser og svagheder i forbindelse med informationssystemer kommunikeres på en sådan måde, at der kan iværksættes korrigerende handlinger rettidigt. At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud.		
A13.1	Sikkerhedshændelser, dvs. tab af service, udstyr og funktioner, fejl ved software eller hardware, brud på Forsikring & Pensions it-sikkerhedspolitik og retningslinjer skal rapporteres af medarbejdere, konsulenter og vikarer til den it-ansvarlige/it-sikkerhedsansvarlige.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til rapportering af væsentlige sikkerhedshændelser til systemejer/it-sikkerhedsansvarlig hos F&P. Vi har inspiceret på stikprøvebasis, at sikkerhedshændelser rapporteres.	Ingen afvigelser konstateret.
A13.2	I forbindelse med fejlrettelse er der aftalt en procedure for rapportering og eskalering.	Sentia: Vi har forespurgt om proces og kontroller i relation til rapportering og eskalering ved fejlretning.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
		Vi har inspiceret på stikprøvebasis, at dokumentation for drøftelse af fejlretning er indeholdt i driftsmøder.	
A13.3	Fejlretning sker i henhold til aftalt procedure for ændringsstyring.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til håndtering af fejlrettelser i henhold til aftalt procedure for ændringsstyring af platform. Vi har inspiceret på stikprøvebasis, at dokumentation for godkendelse af fejlretninger foretages efter den aftalte procedure for ændringsstyring af platform.	Ingen afvigelser konstateret.
A13.4	Der følges periodisk op på registrerede fejl med henblik på analyse og identifikation af årsager til fejl og planlægning af korrigerende tiltag.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til periodisk opfølgning på registrerede fejl og fejlårsager. Vi har inspiceret på stikprøvebasis, at dokumentation for drøftelse af registrerede fejl og fejlårsager er indeholdt i driftsmøder.	Ingen afvigelser konstateret.
A13.5	Ved mistanke om eller konstaterede brud på fortrolighed (lækage af oplysninger) eller brud på integritet i systemer skal den it-sikkerhedsansvarlige omgående kontaktes med henblik på aftale om reaktioner herpå.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til håndtering af konstaterede brud på fortrolighed eller integritet i systemer. Vi har forespurgt, om der er konstateret brud på fortrolighed eller integritet i systemer i 2016.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A14	**Beredskabsstyring**		
	Kontrolmål: At modvirke afbrydelser af forretningsaktiviteter og at beskytte kritiske forretningsprocesser mod virkningerne af større nedbrud af informationssystemer eller katastrofer og at sikre rettidig reetablering.		
A14.1	Der er krav om udarbejdelse af beredskabsplaner og regelmæssige test af disse i outsourcingaftale.	Sentia: Vi har inspiceret, om beredskabsplanen er opdateret og testet i henhold til krav.	Sentia: Ingen afvigelser konstateret.
A14.2	Beredskabsorganisation er specificeret.	Sentia: Vi har inspiceret beredskabsplanen og verificeret, at beredskabsorganisationen er specificeret.	Ingen afvigelser konstateret.
A14.3	Kravet til den maksimale reetableringstid efter en katastrofe er 1 døgn.	Sentia: Vi har inspiceret kravspecifikation og verificeret, at krav reetableringstid er 1 døgn.	Sentia: Ingen afvigelser konstateret.
A14.4	Kopier af beredskabsplanen og andre aktiver, der er nødvendige for at gennemføre beredskabsplaner, opbevares i sikker afstand fra stedet, hvor de enkelte it-systemer driftes.	Sentia: Vi har observeret, at kopier af beredskabsplanen og andre aktiver bliver opbevaret i sikker afstand fra driftsstedet.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A14.5	Beredskabsplaner testes regelmæssigt (minimum årligt).	Sentia: Vi har inspiceret beredskabsplanen og verificeret, at krav til årlig test er beskrevet. Vi har inspiceret rapporter fra test af beredskabsplanen og verificeret, at test foretages minimum årligt.	Sentia: Vi har konstateret at beredskabsplanen ikke er testet. Bortset herfra ingen afvigelser konstateret.
A14.6	Resultatet af hel eller delvis test af beredskabsplanen dokumenteres og godkendes af den it-sikkerhedsansvarlige.	F&P og Sentia: Vi har inspiceret udleveret dokumentation og vurderet procedurer for dokumentation og godkendelse af beredskabstest.	Sentia: Vi har konstateret at beredskabsplanen ikke er testet. Bortset herfra ingen afvigelser konstateret.
A14.7	Der iværksættes tiltag til udbedring af identificerede svagheder ved beredskabet.	Sentia: Vi har inspiceret udleveret dokumentation og vurderet procedurer for iværksættelse af tiltag til udbedring af svagheder identificeret ved test. Vi har inspiceret beredskabsplan og verificeret at denne gennemgås og godkendes minimum årligt.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Udførte tests	Resultater af tests
A15	**Overensstemmelse**		
	Kontrolmål: At undgå brud på love, lovbestemte, forskriftsmæssige eller kontraktlige forpligtelser og på sikkerhedskrav.		
A15.1	Data opbevares på betryggende vis i løbende år +5 medmindre andet skriftligt er aftalt.	F&P og Sentia: Vi har forespurgt om proces og kontroller i relation til opbevaring af data.	Ingen afvigelser konstateret.
A15.2	Forretningsgang for sletning af data er beskrevet og godkendt.	Sentia: Vi har forespurgt om proces og kontroller i relation til sletning af data for F&P. Vi har forespurgt, om der er foretaget sletning af data for F&P i 2016.	Ingen afvigelser konstateret.