

Fonden F&P formidling  
Peder Herbo  
Philip Heymans Allé 1  
2900 Hellerup

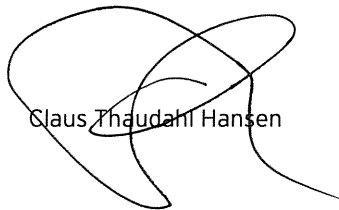
24. marts 2015

Jour.nr.	Akt. nr.	
25 MRS. 2015		
Sagsb.	Kopi til	Afd.

### ISAE 3000-erklæring for 2014 om generelle it-kontroller relateret til WebEDI-systemet

Vedlagt sendes som aftalt underskrevet ISAE 3000-erklæring.

Med venlig hilsen  
ERNST & YOUNG P/S



Claus Thaudahl Hansen



Christian H. Riis

Bilag:  
Underskrevet erklæring

# Fonden F&P formidling

ISAE 3000-erklæring for 2014 om  
generelle it-kontroller relateret til  
WebEDI-systemet



Building a better  
working world



## Indhold

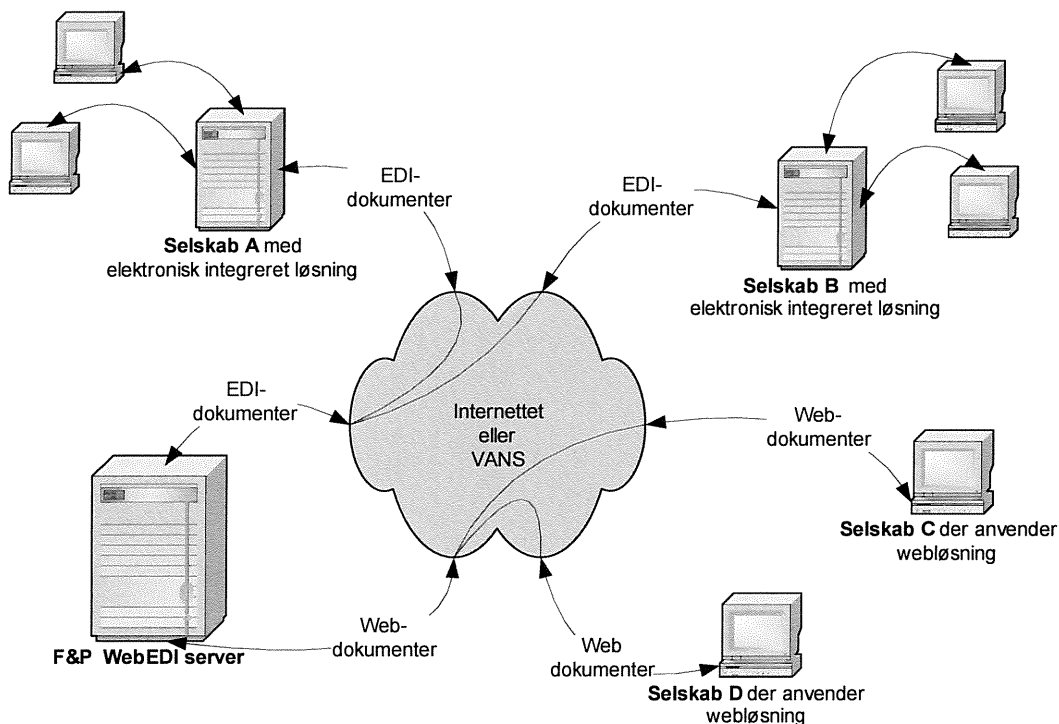
<b>1</b>	<b>Beskrivelse af F&amp;P's WebEDI-system</b>	<b>2</b>
1.1	Risikostyring	3
1.2	Organisering af sikkerheden i it-miljøerne	3
1.3	Væsentlige ændringer i it-miljøerne	4
1.4	Komplementerende kontroller hos brugerne	4
<b>2</b>	<b>Erklæring fra ledelsen</b>	<b>6</b>
<b>3</b>	<b>Den uafhængige revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet</b>	<b>8</b>
<b>4</b>	<b>Tests udført af EY</b>	<b>10</b>
4.1	Formål og omfang	10
4.2	Udførte tests	10
4.3	Resultater af tests	10

## 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-plattform 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, pensionselskaber samt banker og leasingselskaber, og alle oplysninger vedrørende ordningerne Opsigelser, Regres, Panthaverdeklarationer, SP-ordninger, LD-ordninger, § 41 mellem pensionselskaber og § 41 mellem bank og pensionselskaber distribueres gennem serveren. Miljøet kan skitseres således:



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

System	It-komponenter
Servere	3 produktionsservere + 2 2nd site servere
Operativsystem	Windows 2012 Standard
Databasesystem	SQL

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. Brugere 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 beskrevet i ISAE 3402 og omfatter således både kontrolmål og kontroller hos F&P og hos vores serviceunderleverandører CSC og Jaynet.

Erklæringen omhandler ikke applikationskontroller i WebEDI-systemet.

Erklæringen dækker perioden 1. januar 2014 - 31. december 2014.

## 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.

F&P har outsourcet it-drift vedrørende WebEDI-systemet til Jaynet med virkning fra den 9. september 2014. Det er derfor væsentligt, at F&P's informationssikkerhedspolitik også implementeres og efterleveres i forbindelse med drift af WebEDI-systemet hos Jaynet. Med henblik på at sikre dette har F&P indgået en aftale med Jaynet, som indeholder en række sikkerhedsmæssige krav, der skal overholdes af Jaynet. It-driften blev indtil den 8. september 2014 varetaget af CSC, som ligeledes skulle overholde en række sikkerhedsmæssige krav, som var indarbejdet i kontrakten med CSC.

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

### 1.3 Væsentlige ændringer i it-miljøerne

I 2014 foretog F&P en transition af driftsleverandør fra CSC til Jaynet, hvor hele it-miljøet gennemgik en modernisering af både hardwareplatform og software. Løsningen startede hos Jaynet den 9. september 2014. Herudover er der ikke gennemført væsentlige ændringer i it-miljøerne, der anvendes til driftsafvikling af WebEDI-systemet, i perioden 1. januar - 31. december 2014.

### 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
Medarbejdere hos F&P	x <sup>1</sup>	

<sup>1</sup> 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 Jaynet	x	
Sikkerheden i netværksforbindelser mellem Jaynet og brugere		x

## 2 Erklæring 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 CSC, som har varetaget driften af WebEDI-systemet frem til den 8. september 2014. Driften af WebEDI-systemet blev flyttet til Jaynet med virkning fra den 9. september 2014. Denne erklæring er udarbejdet efter helhedsmetoden, og beskrivelsen i kapitel 1 omfatter kontrolmål og tilknyttede kontroller hos både CSC og Jaynet.

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 2014. Kriterierne for dette udsagn 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 2014
  - (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 2014. 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





- (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 2014.

Hellerup, den 23. marts 2015

  
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 2014 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

F&P har anvendt serviceunderleverandøren CSC, som har varetaget driften af WebEDI-systemet frem til den 8. september 2014. Driften af WebEDI-systemet blev flyttet til Jaynet med virkning fra den 9. september 2014. Ledelsens beskrivelse af generelle it-kontroller omfatter kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Denne erklæring er udarbejdet efter helhedsmetoden, og vores handlinger omfatter kontroller hos serviceunderleverandørerne.

#### *F&P's ansvar*

F&P er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i kapitel 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet 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.

#### *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 den internationale standard om andre erklæringsopgaver (ISAE 3000 DK) og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi overholder etiske krav samt 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 kontrollerens 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.

#### *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 hos F&P med relevans for WebEDI-systemet, således som de var udformet og implementeret i perioden 1. januar - 31. december 2014, 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 2014
- (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 2014.


### **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 2015  
ERNST & YOUNG  
Godkendt Revisionspartnerselskab



Claus Thaudah Hansen  
statsaut. revisor



Christian H. Riis  
senior manager

## 4 Tests udført af EY

### 4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3000 DK, Andre erklæringsopgaver med sikkerhed.

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 2014.

### 4.2 Udførte tests

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

<b>Inspektion</b>	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 2014. Dette omfatter bl.a. vurdering af patchningsniveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
<b>Forespørgsler</b>	Forespørgsel af passende personale. Forespørgsler har omfattet, hvordan kontroller udføres.
<b>Observation</b>	Vi har observeret kontrollens udførelse.
<b>Genduføre kontrollen</b>	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 - 8. september 2014 var outsourcet til CSC, har vi instrueret CSC's uafhængige revisor - KPMG - om at rapportere til os, baseret på ISRS 4400, aftalte arbejdshandlinger, om design og funktionalitet af kontroller, som fremgår af oversigten i afsnit 4.3. Instruktionen omfatter kontroller, der er relevante for den outsourcete aktivitet. Vi har vurderet rapporteringen og indarbejdet resultatet i denne erklæring.

For den del af it-miljøerne, der i perioden 9. september - 31. december 2014 har været outsourcet til Jaynet, har vi foretaget test af design, implementering og effektivitet af kontrollerne hos Jaynet.

### 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	Kontrollens hyppighed	Udførte tests	Resultater af tests
A5	<b>It-sikkerhedspolitik</b>  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.	Årlig	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	Årlig	Vi har forespurgt om proces og kontroller i relation til evaluering af it-sikkerhedspolitik.  Vi har inspiceret dokumentation for, at it-sikkerhedspolitikken løbende evalueres, og at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A6	Organisering af informationssikkerhed			
	<b>Kontrolmål:</b> At styre informationssikkerhed i virksomheden og at sikre opretholdelse af sikkerheden vedrørende virksomhedens informationer og informationsbehandlingsstyr, som eksterne parter har adgang til, eller som be- arbejdes, kommunikeres til eller håndteres af eksterne parter.			
A6.1	Der er etableret en sikkerhedsafdeling/sikkerhedsfunktion.	Kontinuerlig	Vi har forespurgt om orga- niseringen af sikkerheds- funktionen. Inspiceret dokumentation for, at sikkerhedsfunctio- nen er hensigtsmæssigt etableret.	Ingen afvigelser konstateret.
A6.2	Der foretages løbende sikkerhedsundersøgelser som kontrol for, at det aftalte sikkerhedsniveau overholdes.	Månedlig	Vi har forespurgt om pro- ces og kontroller i relation til løbende sikkerheds- undersøgelser, herunder hvorledes det sikres, at det aftalte sikkerhedsniveau overholdes. Vi har inspiceret, at det se- neste driftsmøde indehol- der dokumentation for drøftelse af sikkerheds- forhold. Vi har inspiceret på stik- prøvebasis, at dokumenta- tion for drøftelse af sikker-	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A6.3	Ansvar for informationssikkerhedsaktiviteter er klart defineret og planlagt.	Kontinuerlig	Vi har forespurgt om, hvorledes it-sikkerhedsaktiviteter defineres og ansvarsmæssigt placeres.  Vi har inspiceret, at it-sikkerhedsaktiviteter og ansvar herfor er klart defineret i aftalehåndbogen mellem F&P og serviceleverandører.	Ingen afvigelser konstateret.
A6.4	Der afgives tavshedserklæringer fra konsulenter og medarbejdere hos samarbejdspartnere.	Når hændelsen indtræder	Vi har forespurgt om processer 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.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A7	<b>Styring af aktiver</b> <b>Kontrolmål:</b> At opnå og opretholde passende beskyttelse af virksomhedens aktiver.			
A7.1	Der er hos serviceudleverandørerne udpeget en ansvarlig for sikkerheden i WebEDI-systemerne.	Kontinuierlig	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 serviceudleverandørerne, samt at der er udpeget en ansvarlig.	Ingen afvigelser konstateret.
A8	<b>Sikkerhed vedrørende menneskelige ressourcer</b> <b>Kontrolmål:</b> 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.			
A8.1	Identitet og kompetence verificeres for medarbejdere, konsulenter og vikarer inden aftaleindgåelse (ansættelse).	Kontinuierlig	Vi har forespurgt om proces for verifikation af identitet og kompetence for medarbejdere, konsulenter og vikarer inden aftaleindgåelse.	Ingen afvigelser konstateret.





Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A8.2	Medarbejdere, konsulenter og vikarer rapporterer væsentlige sikkerheds-hændelser til it-afdeling/it-sikkerhedsansvarlig.	Kontinuerlig	<p>Vi har inspiceret, at der foretages kontrol af identitet og kompetence i overensstemmelse med retningslinjer herfor.</p> <p>Vi har forespurgt om processer for rapportering af væsentlige sikkerhedshændelser til den sikkerhedsansvarlige.</p> <p>Vi har inspiceret, at der findes en procedure for rapportering af væsentlige sikkerhedshændelser samt på stikprøvebasis inspiceret, hvorvidt der er foretaget rapportering af væsentlige sikkerhedshændelser.</p>	Ingen afvigelser konstateret.
A8.3	Serviceudleverandører rapporterer væsentlige sikkerhedshændelser til systemejer/it-sikkerhedsansvarlig hos Fonden F&P formidling.	Månedlig	<p>Vi har forespurgt om processer og kontroller i relation til rapportering af væsentlige sikkerhedshændelser til systemejer/it-sikkerhedsansvarlig hos F&amp;P.</p> <p>Vi har inspiceret, at det seneste driftsmøde indeholder dokumentation for drøftelse af sikkerhedsforhold.</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A9	<b>Fysisk og miljømæssig sikkerhed</b>			
	Kontrolmål:			
	At forhindre uautoriseret fysisk adgang til, beskadigelse og forstyrrelse af virksomhedens lokaler og informationer.			
A9.1	Såvel ansatte som ikke-ansatte hos serviceunderleverandører skal kunne identificere sig, eksempelvis med personligt adgangskort med billede eller med gæstekort.	Kontinuerlig	Vi har forespurgt om proces og kontrol til sikring af, at alle personer identificerer sig med personligt adgangskort med billede eller med gæstekort.	Ingen afvigelser konstateret.
			Vi har inspiceret, at der findes en procedure til sikring af, at alle personer identificerer sig med personligt adgangskort med billede eller med gæstekort.	
			Vi har observeret, at alle personer synligt bærer personligt adgangskort med billede eller gæstekort i overensstemmelse med retningslinjer herfor.	



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A9.2	Bygning er sikret med passende brandslukningsudstyr, eksempelvis håndslukkere.	Kontinuerlig	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.	Kontinuerlig	Vi har forespurgt om og inspiceret dokumentation for den etablerede sikring af bygninger og serverrum.  Vi har observeret, at bygninger og serverrum er sikret efter gældende retningslinjer.	Ingen afvigelser konstateret.
A9.4	Der er etableret et fysisk adgangskontrolsystem, hvor enhver adgang logges.	Kontinuerlig	Vi har forespurgt om og inspiceret dokumentation for, at enhver fysisk adgang til bygninger og serverrum logges. Vi har inspiceret dokumentation for logning på adgangskontrolsystemer samt på stikprøvebasis inspiceret, at fysisk adgang til bygninger og serverrum logges.	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A9.5	De tildelte fysiske adgange gennemgås og revideres årligt.	Årlig	<p>Vi har forespurgt om proces og kontrol for årlig gennemgang og revidering af fysisk adgang.</p> <p>Vi har inspiceret dokumentation for, at der er etableret en proces for årlig revidering af fysisk adgang samt på stikprøvebasis inspiceret, at revideringen er gennemført.</p>	Ingen afvigelser konstateret.
A9.6	Adgangskontrollog gennemgås efter behov for at afkræfte eller bekræfte mistanke om en mulig sikkerhedshændelse.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til gennemgang af adgangskontrollog for at afkræfte eller bekræfte mistanke om en mulig sikkerhedshændelse.</p> <p>Vi har forespurgt, om der har været mistanke om en mulig sikkerhedshændelse, som har medført en gennemgang af adgangskontrolloggen i 2014.</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A9.7	Der er etableret branddetektering.	Kontinuerlig	Vi har forespurgt om og inspiceret dokumentation for den etablerede brandsikring.  Vi har observeret, at der forefindes branddetektering på relevante lokationer.	Ingen afvigelser konstateret.
A9.8	Der er installeret automatisk brandslukning.	Kontinuerlig	Vi har forespurgt om og inspiceret dokumentation for den etablerede brandsikring.  Vi har observeret, at der forefindes branddetektering på relevante lokationer.	Ingen afvigelser konstateret.
A9.9	Sikkerhedskopier opbevares i sikker afstand fra det primære anlæg.	Kontinuerlig	Vi har forespurgt om opbevaring af sikkerhedskopier i sikker afstand fra det primære anlæg.  Vi har inspiceret dokumentation for dublering af WebEDI-løsningen på to fysiske lokationer.  Vi har inspiceret dokumentation for opbevaring af sikkerhedskopier på den anden lokation end den lokation, hvorpå det primære anlæg er placeret.	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A9.10	Der er vanddetektering eller overvågning af fugtighed.	Kontinuerlig	<p>Vi har forespurgt om og inspiceret dokumentation for den etablerede løsning for vanddetektering eller overvågning af fugtighed.</p> <p>Vi har observeret, at der forefindes vanddetektering eller overvågning af fugtighed på relevante lokationer.</p>	Ingen afvigelser konstateret.
A9.11	Elforsyning er sikret mod udfald, eksempelvis via 2 uafhængige elforsyninger (transformatorer).	Kontinuerlig	<p>Vi har forespurgt om og inspiceret dokumentation for den etablerede løsning for sikring af elforsyning.</p> <p>Vi har inspiceret dokumentation for, at der er etableret to separate elforsyninger samt nødstrømsforsyning på relevante lokationer.</p>	Ingen afvigelser konstateret.
A9.12	Der er installeret nødstrømsbatteri (UPS).	Kontinuerlig	<p>Vi har forespurgt om og inspiceret dokumentation for, at der er etableret nødstrømsbatteri (UPS-anlæg).</p> <p>Vi har observeret, at der er etableret nødstrømsbatteri (UPS-anlæg).</p>	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A9.13	Der er nødstrømsgenerator.	Kontinuerlig	Vi har forespurgt om og inspiceret dokumentation for, at der er etableret nødstrømsgenerator.  Vi har observeret, at der er etableret nødstrømsgenerator.	Ingen afvigelser konstateret.
A9.14	Nødstrømsanlæg testes regelmæssigt.	Halvårlig	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.	Kontinuerlig	Vi har forespurgt om og inspiceret dokumentation for den etablerede løsning for sikring af kommunikationsveje.  Vi har inspiceret dokumentation for, at kommunikationsveje er dublerede.	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
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.	Kontinuerlig	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 inspiceret på stikprøvebasis, 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.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
------	---------------------------	-----------------------	---------------	---------------------

**A10 Styring af kommunikation og drift**

**Kontrolmål:**

- At sikre korrekt og sikker drift af informationsbehandlingsudstyr.
- 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 afsøring, 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.	Kontinuerlig	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.	Ingen afvigelser konstateret.
-------	---	--------------	--	-------------------------------

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.2	Planlægning og gennemførelse af ændringer foretages i henhold til godkendt forretningsgang for ændringsstyring.	Kontinuerlig	<p>Vi har forespurgt om proces og kontrol for planlægning og gennemførelse af ændringer.</p> <p>Vi har inspiceret på stikprøvebasis, at ændringer gennemført i 2014 er planlagt og gennemført i overensstemmelse med den godkendte forretningsgang for ændringsstyring.</p>	<p>Vi har konstateret behov for styrkelse af beskrivelserne af forretningsgangen for ændringsstyring hos driftsleverandøren Jaynet, som har varetaget driften af WebEdi-systemet siden den 9. september 2014.</p> <p>Bortset herfra har vi ikke konstateret afvigelser.</p>
A10.3	Systemejer godkender skriftligt ændringer før implementering.	Kontinuerlig	<p>Vi har forespurgt om proces og kontrol for, at systemejer skriftligt godkender ændringer før implementering.</p> <p>Vi har inspiceret på stikprøvebasis, at systemejer har godkendt alle ændringer gennemført i 2014 før implementering.</p>	<p>Ingen afvigelser konstateret.</p>
A10.4	Der er udarbejdet fallbackprocedure til brug ved fejlslagne ændringer.	Kontinuerlig	<p>Vi har forespurgt om proces og kontrol for fallback til brug ved fejlslagne ændringer.</p> <p>Vi har inspiceret på stikprøvebasis, at fallback-procedurer er beskrevet for ændringer gennemført i 2014 før implementering.</p>	<p>Ingen afvigelser konstateret.</p>

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.5	Ændringer fra serviceleverandør er godkendt af Fonden F&P formidling, hvis de foregår uden for aftalt servicevindue.	Kontinuerlig	<p>Vi har forespurgt om proces og kontrol for godkendelse af idriftsættelse af ændringer, som foregår uden for aftalt servicevindue.</p> <p>Vi har inspiceret på stikprøvebasis, at systemejer har godkendt ændringer gennemført i 2014.</p>	Ingen afvigelser konstateret.
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.	Kontinuerlig	<p>Vi har forespurgt om proces og kontrol for godkendelse af idriftsættelse af ændringer, som foregår uden for aftalt servicevindue.</p> <p>Vi har inspiceret på stikprøvebasis, at systemejer og serviceleverandører har godkendt ændringer gennemført i 2014.</p>	Ingen afvigelser konstateret.
A10.7	Der er etableret funktionsadskillelse.	Kontinuerlig	<p>Vi har forespurgt om proces og kontrol for fysisk adskillelse af udviklings-, test- og driftsaktiviteter.</p> <p>Vi har inspiceret på stikprøvebasis, at der er etableret funktionsadskillelse for udviklere mellem udviklings-, test- og produktionsmiljø.</p>	<p>Der er ikke etableret logisk funktionsadskillelse mellem udviklings-, test- og produktionsmiljø for udviklere.</p> <p>F&amp;P har besluttet, at udviklere skal have adgang til produktionsmiljøet af hensyn til muligheden for at kunne foretage hurtig afhjælpning af eventuelle driftsproblemer.</p>



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.8	Udviklings-, test- og driftsaktiviteter er logisk eller fysisk adskilt.	Kontinuerlig	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.	Bortset herfra har vi ikke konstateret afvigelser.  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.	Månedlig	Vi har forespurgt om proces og kontroller i relation til måling og rapportering af driftseffektivitet.  Vi har inspiceret, at det seneste driftsmøde indeholder dokumentation for måling af aftalt driftseffektivitet.  Vi har inspiceret på stikprøvebasis, at dokumentation for måling af aftalt driftseffektivitet er indeholdt i de månedlige driftsmøder.	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.10	Der afholdes regelmæssigt møder med serviceleverandør med gennemgang af driftsrapport, herunder sikkerhedshændelser, opfølgning på sikkerhedshændelser, driftsproblemer, fejl og nedbrud.	Månedlig	<p>Vi har forespurgt om proces og kontroller i relation til afholdelse af møder mellem serviceunderleverandører og F&amp;P vedrørende driftsrapportering.</p> <p>Vi har inspiceret, at det senest afholdte møde indeholder dokumentation for gennemgang af driftsrapportering.</p> <p>Vi har inspiceret på stikprøvebasis, at afholdte møder indeholder dokumentation for gennemgang af driftsrapportering, herunder sikkerheds- og driftsproblemer samt fejl og nedbrud.</p>	Ingen afvigelser konstateret.
A10.11	Alle servere er sikret med on-access og on-demand antivirussoftware som løbende opdateres.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til sikring af servere med antivirus-software og løbende opdatering heraf.</p> <p>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.</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.12	Der tages sikkerhedskopier, herunder eksempler af parameteropsætninger og anden driftskritisk dokumentation.	Daglig	<p>Vi har forespurgt om proces og kontroller i relation til sikkerhedskopiering af systemer og data.</p> <p>Vi har inspiceret på stikprøvebasis, at sikkerhedskopiering sker i overensstemmelse med den af-talte konfiguration.</p>	Ingen afvigelser konstateret.
A10.13	Sikkerhedskopier afprøves regelmæssigt.	Kvartalvis	<p>Vi har forespurgt om proces og kontroller i relation til kvartalvis test af sikkerhedskopier.</p> <p>Vi har inspiceret, at der er foretaget kvartalvis test af sikkerhedskopier.</p>	Ingen afvigelser konstateret.
A10.14	Gendannelsesprocedurer (restore) afprøves regelmæssigt.	Årlig	<p>Vi har forespurgt om proces og kontroller i relation til gendannelse (restore-test).</p> <p>Vi har inspiceret dokumentation for, at der er foretaget årlig test af gendannelsesprocedurer (restore-test).</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.15	<p>Interne kommunikationsforbindelser er krypterede eller på anden måde beskyttet mod aflytning og uautoriseret adgang.</p> <p>Trådløse netværk er krypteret og beskyttet mod uautoriseret adgang.</p>	Kontinuerlig	<p>Vi har forespurgt om kontroller i relation til beskyttelse af interne kommunikationsforbindelser og trådløse netværk.</p>	Ingen afvigelser konstateret.
A10.17	<p>Regler for kommunikation og dokumentudveksling via elektronisk post er aftalt med samarbejdspartnere, som forestår it-systemudvikling, it-drift og/eller it-support/administration for Fonden F&amp;P formidling.</p>	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til kommunikation og dokumentudveksling via elektronisk post, herunder aftale herom med F&amp;P.</p>	Ingen afvigelser konstateret.
A10.18	<p>Websider er beskyttet mod uautoriserede ændringer via "stærke" sikkeringsforanstaltninger.</p>	Kontinuerlig	<p>Vi har forespurgt om kontroller til beskyttelse af websider mod uautoriserede ændringer.</p>	Ingen afvigelser konstateret.
A10.20	<p>Brugeraktiviteter, afvigelser og sikkerhedshændelser logges i en opfølgningslog.</p>	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til logning af brugeraktivitet, afvigelser og sikkerhedshændelser.</p> <p>Vi har inspiceret på stikprøvebasis, at logning er implementeret på relevante servere og databaser.</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.21	Logning omfatter som minimum succesfulde og fejlslagne logons, oprettelse/nedlæggelse af bruger-ID, ændring af brugeres adgangsrättigheder samt ændring af sikkerhedsmæssige parametre og adgangskontroller.	Kontinuerlig	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 adgangsrättigheder samt ændring af sikkerhedsmæssige parametre og adgangskontroller.  Vi har inspiceret på stikprøvebasis, at logning er implementeret på relevante servere og databaser.	Ingen afvigelser konstateret.
A10.22	Opfølgingslog gennemgås efter behov.	Kontinuerlig	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 2014.	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.23	Aktiviteter udført af systemadministratorer og andre med særlige rettigheder logges.	Kontinuerlig	<p>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.</p> <p>Vi har inspiceret på stikprøvebasis, at logning af aktiviteter udført af systemadministratorer og andre med særlige rettigheder er implementeret på relevante servere og databaser.</p>	<p>For perioden 1. januar - 8. september 2014 har der ikke været logning af aktiviteter udført af systemadministratorer og andre med særlige rettigheder på database-niveau (SQL). Kompenserende herfor var dog, at der blev foretaget logning på operativsystemniveau (Windows).</p> <p>Bortset herfra har vi ikke konstateret afvigelse.</p>
A10.24	Log med aktiviteter udført af brugere med særlige rettigheder gennemgås efter behov.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til gennemgang af logs med aktiviteter udført af brugere med særlige rettigheder.</p> <p>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&amp;P i 2014.</p>	<p>Ingen afvigelse konstateret.</p>

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A10.25	Automatiske fejlregistreringsfunktioner (fejllag) er aktiv. Fejllag gennemgås efter behov.	Kontinuerlig	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 2014.	Ingen afvigelser konstateret.
A11	<b>Adgangsstyring</b>			
<b>Kontrolmål:</b>				
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.				
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.	Kontinuerlig	Vi har forespurgt om proces og kontroller i relation til tildeling, ændring og nedlæggelse af brugere,	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.2	Samme person benytter samme bruger-ID på tværs af alle systemer. Bruger-ID følger en beskrevet navnestandard.	Kontinuerlig	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.	Ingen afvigelser konstateret.
			Vi har forespurgt om proces og kontroller i relation til sikring af overholdelse af navnestandard på tværs af systemer.	
			Vi har inspiceret på stikprøvebasis, at der foreligger dokumentation for overholdelse af navnestandard på tværs af systemer.	

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.3	Brugerrettigheder er tildelt efter et arbejdsmæssigt behov.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til, om tildeling af brugerrettigheder til F&amp;P og serviceleverandørbrugere sker efter et arbejdsmæssigt behov.</p> <p>Vi har inspiceret på stikprøvebasis, at der foreligger dokumentation for tildeling af brugerrettigheder til F&amp;P og serviceleverandørbrugere efter et arbejdsmæssigt behov.</p>	Ingen afvigelser konstateret.
A11.4	Tildeling af udvidede rettigheder til administration af brugerprogrammer og styresystemer er begrænset.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til tildeling af udvidede rettigheder.</p> <p>Vi har inspiceret på stikprøvebasis, at der foreligger dokumentation for tildeling af udvidede rettigheder til F&amp;P og serviceleverandørbrugere efter et arbejdsmæssigt behov.</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.5	Tildelte adgange og rettigheder gennemgås regelmæssigt.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til gennemgang af tildelte adgange og rettigheder.</p> <p>Vi har inspiceret på stikprøvebasis, at der foretages dokumentation for periodisk gennemgang af tildelte adgange og rettigheder.</p> <p>Vi har inspiceret på stikprøvebasis, at den foretagne gennemgang af tildelte adgange og rettigheder har medført nedlæggelse og tilretning af brugernes adgang efter et arbejdsmåsiget behov.</p>	<p>Vi har konstateret behov for styrkelse af processen for regelmæssig gennemgang af tildelte adgangrettigheder hos driftsleverandøren Jaynet, som har varetaget driften af WebEdi-systemet siden den 9. september 2014.</p> <p>Bortset herfra ingen afvigelser konstateret.</p>
A11.6	Adgang gives kun efter afgivelse af et unikt bruger-ID og password.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller, som sikrer, at adgang alene gives efter afgivelse af et unikt bruger-ID og password.</p> <p>Vi har inspiceret på stikprøvebasis, at der foretages dokumentation for, at adgang til servere og databaser kræver afgivelse af bruger-ID og password.</p>	<p>Ingen afvigelser konstateret.</p>

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.7	Password skal være strengt personligt og må ikke videregives.	Kontinuerlig	<p>Vi har forespurgt om process og kontroller, som sikrer, at passwords er personlige og ikke videregives.</p> <p>Vi har inspiceret dokumentation for, at sikkerhedsprocedurer omfatter regler for håndtering af passwords, samt at disse er tilgængelige for alle personer.</p> <p>Vi har forespurgt om begrundet mistanke om, at brugere har videregivet personlige passwords i 2014.</p>	Ingen afvigelse 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.	Kontinuerlig	<p>Vi har forespurgt om process og kontroller i relation til sikring af anvendelse af stærke passwords.</p> <p>Vi har inspiceret på stikprøvebasis, at krav til passwords kompleksitet er aktiveret på de relevante servere og databaser.</p>	<p>Vi har konstateret behov for styrkelse af krav til passwords hos driftsleverandøren Jaynet, som har varetaget driften af WebEDI-systemet siden den 9. september 2014.</p> <p>Bortset herfra ingen afvigelser konstateret.</p>

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.9	Password fornyes efter 90 dage eller ved mistanke om, at password er kendt af andre. Kravet til fornyelse efter 90 dage gælder ikke systembrugere-ID'er, jf. pkt. 11.10.	Kontinuerlig	<p>Vi har forespurgt om processer og kontroller i relation til sikring af periodisk skift af passwords.</p> <p>Vi har inspiceret på stikprøvebasis, at krav til tvunget skift af password er aktiveret på de relevante servere og databaser.</p>	Ingen afvigelse 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.	Kontinuerlig	<p>Vi har forespurgt om processer og kontroller i relation til sikring af periodisk skift af passwords for systembruger-ID.</p> <p>Vi har inspiceret på stikprøvebasis, at krav til årlig skift af passwords for systembruger-ID er overholdt på de relevante servere og databaser.</p>	Ingen afvigelse konstateret.
A11.11	Initielle (1. gangs) password samt nulstillede password er unikke (sikre) og skiftes ved første logon. Password kommunikerer til brugere på en sikker måde.	Kontinuerlig	<p>Vi har forespurgt om processer og kontroller i relation til sikring af sikker kommunikation af initiale passwords samt tvunget skift af password ved første log-on.</p> <p>Vi har inspiceret dokumentation for, at serviceleverandørernes sikkerhedsprocedurer omfatter regler</p>	Ingen afvigelse konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.12	Adgang spærres senest efter 5 mislykkede logon-forsøg.	Kontinuerlig	<p>for håndtering af initiale passwords, samt at disse er tilgængelige for alle personer.</p> <p>Vi har inspiceret på stikprøvebasis, at krav til sikker kommunikation af initiale passwords samt tvunget skift af password ved første log-on er overholdt.</p>	Ingen afvigelser konstateret.
A11.13	BrugerID låst som følge af for højt antal forgæves logon-forsøg genåbnes kun af autoriseret administrator efter henvendelse fra brugeren selv.	Kontinuerlig	<p>Vi har inspiceret på stikprøvebasis, at det er overholdt på de relevante servere og databaser, at adgang spærres senest efter fem mislykkede log-on.</p>	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.14	Pauseskærm med password aktiveres automatisk (senest efter 30 minutter)	Kontinuerlig	<p>for genåbning af adgang, samt at disse er tilgængelige for alle personer.</p> <p>Vi har inspiceret på stikprøvebasis, at krav om genåbning af adgang er overholdt.</p>	Ingen afvigelser konstateret.
			<p>Vi har forespurgt om processer og kontroller i relation til sikring af, at pause-skærm med password aktiveres automatisk (senest efter 30 minutter) for alle brugere.</p>	
			<p>Vi har inspiceret dokumentation for, at sikkerhedsprocedurer omfatter regler for anvendelse af automatisk aktivering af pause-skærm, samt at disse er tilgængelige for alle personer.</p>	
			<p>Vi har inspiceret på stikprøvebasis, at krav om automatisk aktivering af pause-skærm med password er overholdt for alle brugere.</p>	

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.15	Password lagres og transmitteres i krypteret form.	Kontinuerlig	Vi har forespurgt om process 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.	Ingen afvigelser konstateret.
A11.16	Remote-adgang sker kun vha. VPN (IPsec eller SSL).	Kontinuerlig	Vi har forespurgt om process 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.
A11.17	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).	Kontinuerlig	Vi har forespurgt om process 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	Kontrollens hyppighed	Udførte tests	Resultater af tests
A11.18	Fonden F&P formidlings data lagres på dedikerede servere (database- og filservere).	Kontinuerlig	Vi har forespurgt om kontroller i relation til sikring af, at F&P-data lagres på dedikerede servere (database- og filservere).  Vi har inspiceret på stikprøvebasis, at F&P-data lagres på dedikerede servere (database- og filservere).	Ingen afvigelse konstateret.
A12	<b>Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer.</b>			
	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.			
A12.2	Styresystemer og brugersystemer er altid opdateret til et versionsniveau, der rapporteres af leverandøren/anbefales af producenten.	Kontinuerlig	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 rapporteres af leverandøren.	Ingen afvigelse konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A12.3	Der benyttes en beskrevet og aftalt procedure for programudvikling	Kontinuerlig	<p>Vi har forespurgt om process og kontroller i relation til overholdelse af aftalt procedure for programudvikling.</p> <p>Vi har inspiceret på stikprøvebasis, at aftalt procedure for programudvikling er overholdt.</p>	Ingen afvigelser konstateret.
A12.4	Kravspecifikationer godkendes af forud aftalte personer i Fonden F&P formidling før udvikling iværksættes.	Kontinuerlig	<p>Vi har forespurgt om process og kontroller i relation til F&amp;P's godkendelse af kravspecifikationer, før udvikling iværksættes.</p> <p>Vi har inspiceret på stikprøvebasis, at kravspecifikationer/ændringsbeskrivelser er godkendt af F&amp;P.</p>	Ingen afvigelser konstateret.
A12.5	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	Kontinuerlig	<p>Vi har forespurgt om process og kontroller i relation til F&amp;P's godkendelse af design og løsningsbeskrivelser, før udvikling iværksættes.</p> <p>Vi har inspiceret på stikprøvebasis, at design og løsningsbeskrivelser er godkendt af F&amp;P, herunder beskrivelse af implemente-</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A12.6	Ændringer i forhold til den aftalte programudvikling godkendes formelt af forud aftalte personer i Fonden F&P formidling.	Kontinuerlig	ring af sikkerhedskrav og krav til inddatakontroller.  Vi har forespurgt om process 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.
A12.7	Resultat af test godkendes formelt af forud aftalte personer i Fonden F&P formidling.	Kontinuerlig	Vi har forespurgt om process 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	Kontrollens hyppighed	Udførte tests	Resultater af tests
A12.8	System, platform, forretningsgange for drift, er udarbejdet før systemer sættes i drift og holdes efterfølgende løbende ajour.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til ajourføring af system-, platform- og forretningsgange ved ændringer.</p> <p>Vi har inspiceret på stikprøvebasis, at system-, drifts- og brugerdokumentation ved ændringer er udarbejdet/ajourført og overgivet til F&amp;P.</p>	Ingen afvigelser konstateret.
A13	<b>Styring af informationssikkerhedshændelser</b>			
<b>Kontrolmål:</b>				
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.	Kontinuerlig	<p>Vi har forespurgt om proces og kontroller i relation til rapportering af væsentlige sikkerhedshændelser til systemejer/it-sikkerhedsansvarlig hos F&amp;P.</p> <p>Vi har inspiceret, at det seneste driftsmøde indeholder dokumentation for drøftelse af sikkerhedsforhold.</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A13.2	I forbindelse med fejlrettelse er der aftalt en procedure for rapportering og eskalering.	Kontinuerlig	<p>Vi har inspiceret på stikprøvebasis, at dokumentation for drøftelse af sikkerhedsforhold er indeholdt i de månedlige driftsmøder.</p> <p>Vi har forespurgt om processer og kontroller i relation til rapportering og eskalering ved fejlretning.</p> <p>Vi har inspiceret, at det næste driftsmøde indeholder dokumentation for drøftelse af fejlretning.</p> <p>Vi har inspiceret på stikprøvebasis, at dokumentation for drøftelse af fejlretning er indeholdt i de månedlige driftsmøder.</p>	Ingen afvigelser konstateret.
A13.3	Fejlretning sker i henhold til aftalt procedure for ændringsstyring.	Kontinuerlig	<p>Vi har forespurgt om processer og kontroller i relation til håndtering af fejlretninger i henhold til aftalt procedure for ændringsstyring af platform.</p> <p>Vi har inspiceret, at det næste driftsmøde indeholder dokumentation for drøftelse af fejlretning.</p> <p>Vi har inspiceret på stikprøvebasis, at dokumenta-</p>	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A13.4	Der følges periodisk op på registrerede fejl med henblik på analyse og identifikation af årsager til fejl og planlægning af korrigerende tiltag.	Kontinuerlig	<p>tion for godkendelse af fejlretninger foretages efter den aftalte procedure for ændringsstyring af platform.</p> <p>Vi har forespurgt om proces og kontroller i relation til periodisk opfølgning på registrerede fejl og fejlårsager.</p> <p>Vi har inspiceret, at det seneste driftsmøde indeholder dokumentation for drøftelse af registrerede fejl og fejlårsager.</p> <p>Vi har inspiceret på stikprøvebasis, at dokumentation for drøftelse af registrerede fejl og fejlårsager er indeholdt i de månedlige driftsmøder.</p>	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.	Kontinuerlig	Vi har forespurgt om proces og kontroller i relation til håndtering af konstaterede brud på fortrolighed eller integritet i systemer. <p>Vi har forespurgt, om der er konstateret brud på fortrolighed eller integritet i systemer i 2014.</p>	Ingen afvigelser konstateret.



Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
A14	Beredskabsstyring			
	<p>Kontrolmål:</p> <p>At modvirke afbrydelser af forretningsaktiviteter og at beskytte kritiske forretningsprocesser mod virkningerne af større nedbrud af informationssystemer eller katastrofer og at sikre rettidig reetablering.</p>			
A14.1	Der er krav om udarbejdelse af beredskabsplaner og regelmæssige test af disse i outsourcingaftale.	Kontinuerlig	Vi har inspiceret, om beredskabsplanen er opdateret og testet i henhold til krav.	Vi har konstateret behov for udarbejdelse af en specifik beredskabsplan for F&P hos driftsleverandøren Jaynet, som har været taget driften af WebEdi-systemet siden den 9. september 2014.
				Bortset herfra ingen afvigelse konstateret.
A14.2	Beredskabsorganisation er specificeret.	Kontinuerlig	Vi har inspiceret beredskabsaftalen og verificeret, at beredskabsorganisationen er specificeret.	Ingen afvigelse konstateret.
A14.3	Kravet til den maksimale reetableringstid efter en katastrofe er 1 døgn.	Kontinuerlig	Vi har inspiceret rapport fra test af beredskabsplanen og verificeret, at reetableringstiden har været under et døgn.	Ingen afvigelse konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Udførte tests	Resultater af tests
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.	Kontinuerlig	Vi har observeret, at kopier af beredskabsplanen og andre aktiver bliver opbevaret i sikker afstand fra driftsstedet.	Ingen afvigelser konstateret.
A14.5	Beredskabsplaner testes regelmæssigt (minimum årligt).	Årlig	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.	Vi har konstateret behov for styrkelse af dokumentation for test af F&P's beredskab hos driftsleverandøren Jaynet, som har været taget driften af WebEdi-systemet siden den 9. september 2014. Bortset herfra ingen afvigelser konstateret.
A14.6	Resultatet af hel eller delvis test af beredskabsplanen dokumenteres og godkendes af den it-sikkerhedsansvarlige.	Årlig	Vi har inspiceret udleveret dokumentation og vurderet procedurer for dokumentation og godkendelse af beredskabsbest.	Ingen afvigelser konstateret.
A14.7	Der iværksættes tiltag til udbedring af identificerede svagheder ved beredskabet.	Kontinuerlig	Vi har inspiceret rapporter fra test og verificeret, at de er godkendt af både F&P og serviceleverandøren.	Ingen afvigelser konstateret.

Pkt.	Kontrolområder/kontroller	Kontrollens hyppighed	Resultater af tests
A15	<b>Overensstemmelse</b>		
	Kontrolmål:		
	At undgå brud på love, lovbestemte, forskriftsmæssige eller kontraktlige forpligtelser og på sikkerhedskrav.		
A15.4	Data opbevares på betryggende vis i løbende år +5 medmindre andet skriftligt er aftalt.	Kontinuerlig	Ingen afvigelser konstateret.  Vi har forespurgt om proces og kontroller i relation til opbevaring af data.  Vi har inspiceret på stikprøvebasis, at data opbevares betryggende i løbende år + 5.
A15.5	Forretningsgang for sletning af data er beskrevet og godkendt.	Kontinuerlig	Ingen afvigelser konstateret.  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 2014.