www.pwc.dk

Athena IT-Group

Erklæring fra uafhængig revisor vedrørende generelle it-kontroller for Athena IT-Group A/S' driftsydelser

April 2012

pwc

Indhold

athena
let's free your potential

1. Ledelsens erklæring

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Athena IT-Group A/S' driftsydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber. Athena IT-Group A/S bekræfter, at:

(a) Den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af Athena IT-Group A/S' driftsydelser, der har behandlet kunders transaktioner i hele perioden fra 1. januar til 31. december 2011. Kriterierne for dette udsagn var, at den medfølgende beskrivelse:

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

- de typer af ydelser, der er leveret, når det er relevant
- de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

(ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. januar til 31. december 2011

(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 kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold

(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar til 31. december 2011. 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

Athena IT-Group
Hovedafdeling
Søndergård Alle 4
DK-6500 Vojens
Tlf.: +45 74 53 15 14
Fax: +45 74 53 14 81

Athena IT-Group
Fyn
Munkerisvej 1
DK-5230 Odense M
Tlf.: +45 70 25 30 30
Fax: +45 66 13 93 85

mail@athena.dk
www.athena.dk

athena
let's free your potential

(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 til 31. december 2011.

Odense, den 19. april 2012
Athena IT-Group A/S

Direktionen

Peter Kroul

Poul Sindberg

Athena IT-Group
Hovedafdeling
Søndergård Alle 4
DK-6500 Vojens
Tlf.: +45 74 53 15 14
Fax: +45 74 53 14 81

Athena IT-Group
Fyn
Munkerisvej 1
DK-5230 Odense M
Tlf.: +45 70 25 30 30
Fax: +45 66 13 93 85

mail@athena.dk
www.athena.dk

2. *Athena IT-Group A/S' beskrivelse af generelle it-kontroller for driftsydelser*

Indledning – kort om Athena IT-Group A/S

Athena IT-Group A/S (Athena), der blev stiftet i 1995, tilbyder totale løsninger inden for it-outsourcing og it-drift med fokus på mindre og mellemstore virksomheder og offentlige organisationer. Virksomheden er beliggende i henholdsvis Vojens og Odense og har i alt 31 ansatte. I 2007 blev virksomheden børsnoteret på NASDAQ OMX First North.

Athena tager det fulde ansvar for kundens it-drift herunder support, licenser, overvågning og backup. Athena sætter en ære i at overholde deadlines, har en udpræget kvalitetsbevidsthed og holder samtidig fokus på en høj grad af fleksibilitet i løsningerne. For Athenas kunder betyder det effektivisering, besparelser og konkurrencemæssige fordele – leveret til den aftalte tid.

Athenas driftsløsninger er karakteriseret ved høj oppetid, stabilitet og stor kundetilfredshed, og via højt uddannet personale med solid erfaring og forretningsforståelse indgår rådgivning, strategisk planlægning og stærk ansvarsfølelse som helt naturlige, implicitte ydelser i alle vores indgåede aftaler.

Det primære datacenter er placeret i Nationalbankens tidligere pengedepot under jorden i Odense, som giver helt optimale og sikre fysiske forhold til it-drift.

Med fokus på kundens behov leverer vi de samlede ydelser, herefter omtalt som driftsydelser, der dækker driften af kundens it-systemer, herunder følgende produkter:

- Managed hosting – leveret som dedikerede og virtuelle servere
- it-outsourcing
- Co-location
- IBM TSM-baserede fjernbackup.

I forhold til nærværende erklæring er grundydelsen i de forskellige produkter identiske og omfatter internetforbindelse, adgangskontrollere, strøm, køling, overvågning, sikkerhed og backup.

Internetforbindelse

For internetforbindelser, stillet til rådighed i forbindelse med hostede ydelser, gør følgende sig gældende:

Athena benytter sig af separat fremførte fiberforbindelser til internet, fremført i samarbejde med to af de største udbydere på det danske marked. Athenas interne opsætning understøtter failover ved fejl på fysisk forbindelse eller hos udbyder.

Ud over internetforbindelser, stillet til rådighed af Athena, kan kunder selv fremføre samt stille forbindelse til rådighed for deres specifikke hostede løsning. Type og implementering afhænger her af den enkelte opsætning.

Adgangskontroller

Athenas hosting-center er som nævnt indrettet i Nationalbankens tidligere pengedepot i Odense. Der er etableret elektronisk adgangskontrol, foruden at oprindelig skalsikring er bibeholdt.

Køling

Hosting-centeret er udstyret med et redundant glykolbaseret køleanlæg. Temperatur og luftfugtighed monitoreres 24/7/365.

Sikkerhed

Hosting-centret er placeret i Nationalbankens tidligere pengedepot under jorden, indkapslet i beton og sikret mod tyveri, vand og brand. I tilfælde af brand aktiveres et Argonite-brandslukningsanlæg, som kvæler branden uden beskadigelse af data, udstyr eller inventar.

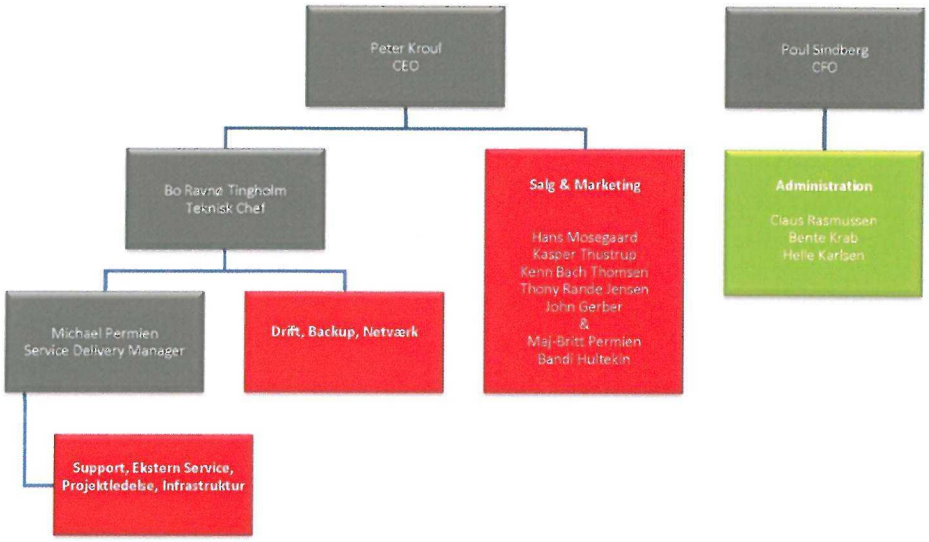
Backup

Athena benytter IBM's TSM-baserede backupsystem. Data opbevares i det særligt sikrede miljø – dubleret på fysisk adskilte lokationer og beskyttet mod både tyveri, brand, strømafbrydelser og oversvømmelse.

Kontrolmiljø

Med udgangspunkt i virksomhedens overordnede strategiplan er virksomhedens sikkerhedspolitik og informationssikkerhedspoliti defineret. Det er ledelsen, der har defineret politikkerne, og ledelsen som tilsikrer, at de efterleves.

Organisation – Athena IT-Group



Det overordnede ansvar ligger hos virksomhedens CEO, der er øverste ansvarlig for det tekniske område. Den tekniske chef implementer indholdet af politikkerne på de forskellige tekniske niveauer og tilsikrer, at der løbende sker en evaluering af hele det tekniske miljø for til stadighed at kunne opfylde vores interne krav og målsætninger. Sideløbende hermed foretages der en evaluering af det tekniske personale med henblik på at opgradere dets tekniske kvalifikationer, således at vi fortsat kan tilbyde kunderne den allernyeste og bedste teknologi.

Den tekniske chef har det overordnede ansvar for implementering af nye teknologiske tiltag, ligesom det er hans ansvarsområde at udfærdige uddannelsesplaner for den enkelte medarbejder.

Risikostyring

Der foretages løbende en evaluering af de til enhver tid ønskede sikkerhedsniveauer, som det er defineret i informationssikkerhedspolitikken og i sikkerhedspolitikken, set i forhold til den risiko der ligger på de enkelte områder. Det er ledelsen, herunder den tekniske chef, der foretager den løbende evaluering og implementerer ændringer, såfremt det er hensigtsmæssigt.

Information og kommunikation

Hele informationsflowet i virksomheden er bygget op i et sagsstyringssystem, der dokumenterer og følger en sags forløb fra vugge til grav. Den tekniske chef har derved hele tiden det samlede overblik over igangværende sager, anvendte ressourcer, tidsfrister mv.

Medarbejderne følger virksomhedens retningslinjer omkring håndtering af følsomme data samt udfærdiget sikkerhedspolitik.

Den direkte kundekontakt er afgørende for et konstruktivt samarbejde, hvilket betyder, at vi ud over den løbende kontakt tilbyder ydelser, der til stadighed dokumenterer, at de aftalte ydelser er udført uden bemærkninger. Øvrig relevant information, relateret til virksomheden, udsendes via vores nyhedsbrev.

Kontrolaktiviteter

Til understøttelse af vores interne forretningsgange har vi iværksat en række kontrolaktiviteter, der sikrer, at vi efterlever den kvalitetsnorm, vi har sat op i virksomheden.

Til løsninger, hostet af Athena, specificeres logisk adgang i de enkelte indgåede kontrakter, såfremt der er behov for ændringer i forhold til specifikationer i de oprindelige kontrakter, udformes firewallformularer, som godkendes af den enkelte kunde. Alle kunders løsninger er logisk adskilt fra hinanden såvel netværks- som datamæssigt. Kundeadskillelse kan kun afviges ved samtykke fra alle implicerede parter. Såfremt kundens egen løsning består af flere enheder, uden specificeret behov for logisk adgang data- eller netværksmæssigt på tværs, vil enhederne ikke kunne opnå adgang imellem hinanden. Til logisk adskillelse af netværksmæssig adgang benyttes VLAN. Dataadskillelse opnås via anvendelse af den funktionalitet som Storage-systemet og virtualiseringssoftware stiller til rådighed.

Hostede løsninger, indeholdende backupydelse, benytter Athenas TSM-opsætning. Ved løsninger, indeholdende backupydelser, reagerer Athena på eventuelle fejl i backup.

Fysisk adgang til virksomhedens driftscenter kontrolleres nøje. Kun personer med ærinde og autorisation får adgang til driftsområdet. Adgange til driftsområder såvel som kontorområder kameraovervåges 24 timer i døgnet.

Driften i centret, herunder netværket overvåges aktivt 24/7/365. Ved driftsforstyrrelser vil teknisk personale blive tilkaldt, og forstyrrelsen vil blive afhjulpet omgående. Desuden monitorerer Athena kapacitet samt ressourceforbrug på såvel delte som kundespecifikke elementer, for i videst muligt omfang at kunne skalere inden fejl opstår.

Såfremt der foretages ændringer af systemer samt systemopsætninger sker dette altid ud fra kontraktmæssig aftale med denne pågældende kunde eller ud fra en teknisk/driftmæssig vurdering. Ændringer dokumenteres i Athenas opgavesystem.

Athena bærer kun ansvar for kontrol af ydelser/løsninger, specificeret i kontrakt. Athena kan dog bistå med monitorering af kundens/tredjepartens ydelse/løsning, i disse tilfælde vil information tilgå kunden/tredjeparten direkte, og disse har selv ansvar for at reagere ud fra de modtagne informationer.

3. Revisors erklæring om beskrivelse af kontroller, deres udformning og funktionalitet

Til ledelsen i Athena IT-Group A/S samt kunder af Athena IT-Group A/S' driftsydelser i perioden 1. januar 2011 til 31. december 2011 og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Athena IT-Group A/S' beskrivelse, afsnit 2, om udformningen og funktionen af generelle it-kontroller, i relation til Athena IT-Group A/S' driftsydelser, der knytter sig til de kontrolmål, som er anført i beskrivelsen for perioden 1. januar 2011 til 31. december 2011.

Athena IT-Group A/S' ansvar

Athena IT-Group A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn, 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.

Vores ansvar

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

Det er vores og Athena IT-Group A/S' opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør

Athena IT-Group A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og disses revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter dennes 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. Det er vores opfattelse,

(a) at beskrivelsen af Athena IT-Group A/S' driftsydelser, således som det var udformet og implementeret i hele perioden fra 1. januar 2011 til 31. december 2011, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2011 til 31. december 2011, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2011 til 31. december 2011.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt Athena IT-Group A/S' driftsydelser, og disses revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 19. april 2012
PricewaterhouseCoopers
statsautoriseret revisionspartnerselskab

Jess Kjær Mogensen
statsautoriseret revisor

Jan Wright
statsautoriseret revisor

4. Kontrolmål, kontroller, test og resultat heraf

Kontrolmål: Informationssikkerhedspolitik

Ledelsen har udarbejdet en informationssikkerhedspolitik, som udstikker en klar målsætning for it-sikkerhed, herunder valg af referenceramme samt tildeling af ressourcer. Informationssikkerhedspolitikken vedligeholdes under hensyntagen til en aktuel risikovurdering.

Kontrolaktivitet	PwC-test	Resultat af test
Skriftlig politik for informationssikkerhed Sikkerhedspolitikken, som er godkendt af ledelsen, er dokumenteret og vedligeholdes ved gennemgang mindst en gang årligt. Sikkerhedspolitikken er gjort tilgængelig for medarbejdere via intranettet.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har foretaget inspektion af, at ledelsen har godkendt sikkerhedspolitikken, samt at den som minimum er revurderet en gang årligt. Endvidere har vi foretaget inspektion af, at politikken forefindes let tilgængelig for medarbejderne.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Organisering af informationssikkerhed

Det organisatoriske ansvar for informationssikkerhed er passende dokumenteret og implementeret, ligesom håndtering af eksterne parter sikrer en tilstrækkelig behandling af sikkerhed i aftaler.

Kontrolaktivitet	PwC-test	Resultat af test
Ledelsens forpligtelse til informationssikkerhed Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Endvidere er der fastlagt regler for fortrolighedsaftaler og rapportering om informationssikkerhedshændelser samt udarbejdet en fortegnelse over aktiver.	Vi har overordnet drøftet styring af informationssikkerheden med ledelsen. Vi har påset, at det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Vi har endvidere foretaget inspektion af, at fortrolighedsaftaler, rapportering om informationssikkerhedshændelser samt fortegnelse over aktiver er udarbejdet.	Vores test har ikke givet anledning til relevante bemærkninger.
Eksterne parter Der er foretaget identifikation af risici i relation til eksterne parter, herunder håndtering af sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder. Der er fortaget gennemgang af ydelser fra serviceleverandører. Forhold undersøges og løses rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at der er etableret betryggende procedurer for samarbejde med eksterne leverandører. Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader, der er resultatet hændelser som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Kontrolaktivitet	PwC-test	Resultat af test
Fysisk sikkerhedsafgrænsning Adgang til sikrede områder (for såvel nye som eksisterende medarbejdere) er begrænset (f.eks. ved anvendelse af adgangskort) til autoriserede medarbejdere og forudsætter dokumenteret ledelsesmæssig godkendelse. For nuværende består sikrede adgangsområder af nedenstående tre zoner, og kriterierne er som beskrevet. Afvigelser fra de pr. zone beskrevne kriterier kræver godkendelse af den administrerende direktør. Zone 1: kontorområder, alle ansatte i Athena IT-Group A/S (Athena) kan opnå godkendelse. Zone 2: hosting- og produktionsområder kræver ansættelsesforhold i den tekniske del af Athena. Zone 3: ekstern båndlokation kræver ansættelse i den tekniske del af Athena samt backuprelaterede arbejdsopgaver. Personer uden godkendelse til sikrede zone 2-områder skal registreres og ledsages af medarbejder med behørig godkendelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at der er etableret zone-opdeling vedrørende fysisk adgang til forskellige områder. Vi har observeret under besøg i datacentre, at adgang til sikre områder er begrænset ved anvendelse af afgangssystem og er kun tildelt de medarbejdere, der har tilladelse til indgang til den pågældende zone. Vi har stikprøvevis gennemgået procedurer for fysisk sikkerhed vedrørende sikrede områder, for at vurdere om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt om personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse. Vi har stikprøvevis gennemgået medarbejdere med adgang til sikre områder og påset, at relevant dokumenteret ledelsesmæssig godkendelse foreligger.	Vores test har ikke givet anledning til relevante bemærkninger.
Sikring af kontorer, lokaler og faciliteter Der er etableret adgangskontrolsystem til alle serverrum samt kontorområder, som sikrer, at alene ledelsesgodkendte medarbejdere har adgang. Jævnfør punktet "Fysisk sikkerhedsafgrænsning" revideres adgange i forbindelse med ændring i ansættelsesforhold eller opgaver vedrørende adgangsrettigheder, dog mindst en gang årligt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har foretaget inspektion af, at alle serverrum og påset, at alle adgangsveje er sikret med kortlæser. Vi har foretaget stikprøvevis kontrol af, at årlig gennemgang foretages.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader, der er resultatet hændelser som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Kontrolaktivitet	PwC-test	Resultat af test
Placering og beskyttelse af udstyr Datacentre er beskyttet mod f.eks. brand, vand og varme. Der er endvidere installeret udstyr til overvågning af indeklima, herunder luftfugtighed.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået driftsfaciliteterne og har påset at brandbekæmpelsessystemer, monitorering af indeklima og køling i datacentre forefindes. Vi har stikprøvevis gennemgået dokumentation for vedligeholdelse af udstyr, til bekræftelse af at dette løbende vedligeholdes.	Vores test har ikke givet anledning til relevante bemærkninger.
Understøttende forsyninger (forsyningssikkerhed) Datacentre er beskyttet mod strømafbrydelse ved anvendelse af redundant UPS (Uninterruptible Power Supply)-opsætning samt dieselbaseret nødstrømsanlæg. Der køres "live test" månedligt med fuld last på henholdsvis UPS- og dieselgenerator. Brandslukningsudstyr testes af leverandøren under de gældende serviceaftaler.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har under besøg i datacentre observeret, at der foretages monitorering af UPS og nødstrømsanlæg. Stikprøvevis gennemgået dokumentation for vedligeholdelse, til bekræftelse af at UPS eller nødstrømsanlæg løbende vedligeholdes og testes.	Vores test har ikke givet anledning til relevante bemærkninger.
Sikring af kabler Alle netværkskabler er placeret i serverrum.	Vi har observeret, at kabler til elektricitetsforsyning og datakommunikation er sikret mod skader og uautoriserede indgreb.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder overvågning samt registrering af og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift samt brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, som på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolaktivitet	PwC-test	Resultat af test
Dokumenterede driftsprocedurer Der forefindes drift og implementeringsprocedurer på alle væsentlige produktområder. Ansvaret for vedligeholdelse af disse ligger i de enkelte produktområder.	Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenteret. I forbindelse med revision af de enkelte driftsområder er det kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres.	Vi har observeret, at der ikke findes en samling af driftsprocedurer for alle væsentlige produktområder. Beskrivelsen af driftsrutiner for det enkelte område er placeret hos gruppen, der har ansvaret for det pågældende område. Vi har fået oplyst, at Athena er i gang med elektronisk at samle procedurebeskrivelser samme sted for nemmere tilgang. Vores test har ikke givet anledning til yderligere relevante bemærkninger.
Funktionsadskillelse Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i den tekniske afdeling. Disse politikker og procedurer omfatter krav til at: • Adgange er tildelt ud fra arbejdsbetingede behov • Athenas administrative platform er adskilt netværksmæssigt såvel som brugermæssigt fra den tekniske platform • Udelukkende personale, ansat i den tekniske del, har adgang til den tekniske platform, netværksmæssigt såvel som brugermæssigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov. Vi har stikprøvevis kontrolleret, at det tekniske net er adskilt fra det administrative, samt at kun relevante personer har adgang til det tekniske net.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder overvågning samt registrering af og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift samt brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, som på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolaktivitet	PwC-test	Resultat af test
Foranstaltninger mod virus og lignende skadelig kode Der er på både den tekniske og den administrative platform etableret antivirusprogrammer, som bliver opdateret regelmæssigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har stikprøvevis gennemgået teknisk opsætning, til bekræftelse af at der er installeret antivirusprogrammer, samt af at disse er opdateret.	Vores test har ikke givet anledning til relevante bemærkninger.
Sikkerhedskopiering af informationer Der bliver foretaget sikkerhedskopiering af data med passende mellemrum. Periodisk sker der test af, at data kan genskabes fra sikkerhedskopier. Som backupsystem internt samt til hostede løsninger benyttes Athenas fjernbackupprodukt, efter samme SLA som eksterne kunder. For hostede ydelser vil frekvens og versioner være beskrevet i den enkelte kontrakt med udgangspunkt i en minimumssikring, der går tre uger tilbage.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået backupprocedurer samt påset, at de er tilstrækkelige og formelt dokumenterede. Vi har stikprøvevis gennemgået backup-log, for bekræftelse af at backup er gennemført succesfuldt, alternativt at der foretages afhjælpning i tilfælde af mislykkede backupper. Desuden har vi stikprøvevis kontrolleret at restore test er udført.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder overvågning samt registrering af og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift samt brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, som på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolaktivitet	PwC-test	Resultat af test
Overvågning af systemanvendelse og auditlogning Der er implementeret logning på alle kritiske systemer. Log fra kritiske systemer opsamles og gennemgås i tilfælde af mistanke om uautoriserede hændelser og aktiviteter. Aktivitet samt brugere med privilegerede rettigheder (f.eks. superbrugere) bliver overvåget i alle af Athena udviklede systemer, som benyttes til opgavestyring vedrørende ændringsstyring samt vedligehold af abonnementer. Afvigende forhold undersøges og løses rettidigt. Særligt risikofyldte operativsystemer og netværkstransaktioner eller aktivitet samt brugere med privilegerede rettigheder bliver overvåget. Afvigende forhold undersøges og løses rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder, bliver logget. Vi har endvidere stikprøvevis kontrolleret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer.	Vi har observeret, at der ikke findes formaliserede procedurer for håndtering af sikkerhedsrelaterede audit logs fra alle kritiske systemer. Der er dog implementeret automatisk og proaktiv gennemgang af driftssikkerhedsrelaterede logs fra en lang række kritiske systemer. Vi har fået oplyst, at tiltag vedrørende udarbejdelse af formelle procedurer for håndtering af audit logs er igangsat. Vores test giver ikke anledning til yderligere relevante bemærkninger.
Fejllogning Systemer er konfigureret til at opdage fejl i automatiske transaktionsprocesser (batch eller realtime), baseret på foruddefinerede kriterier, og blokere for viderebehandling. Systemgenerede fejlrapporter vedrørende fejl i automatiske transaktionsprocesser bliver undersøgt og registrerede fejl løst rettidigt. Relevant vagtpersonale bliver informeret 24/7/365.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har stikprøvevis kontrolleret konfigurationen af de kritiske systemer og påset, at driftsrelaterede fejl på serverne opdages. Vi har endvidere kontrolleret, at de relevante teknikere informeres via alarmer.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolaktivitet	PwC-test	Resultat af test
Brugerregistrering og administration af privilegier Alle adgange for nye og eksisterende brugere vedrørende operativsystemer, netværk, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med virksomhedens politikker. Endvidere sikring af, at rettigheder er tildelt ud fra et arbejdsbetinget behov, er godkendt og oprettet korrekt i systemer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteter er tilstrækkeligt dækkende. Vi har stikprøvevis kontrolleret, at oprettelse af brugere og tildeling af adgang var dokumenteret og godkendt i overensstemmelse med forretningsgangene.	Vores test har ikke givet anledning til relevante bemærkninger.
Administration af brugeradgangskoder (password) Adgange til operativsystemer, netværk, databaser og datafiler er beskyttet med password. På Microsoftplatform er passwordpolitikken minimum syv karakterer og krav til passwordkompleksitet er aktiveret. Desuden er der implementeret restriktioner for både fysisk og logisk netværksadgang.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordkontroller, og påset, at det sikres, at der anvendes passende autentifikation af brugere på alle adgangsveje. Vi har kontrolleret, at der anvendes en passende passwordkvalitet i Athenas driftsmiljø – ved stikprøvevise test af, at adgang til virksomhedens systemer sker ved brug af brugernavn og password.	Vi har observeret, at passwordet for brugerkonti med administratoradgang til netværksenheder og VMware skiftes lejlighedsvis. Der findes ikke formelle procedurer for regelmæssigt passwordskift af disse brugerkonti. Vi har fået oplyst af ledelsen, at der pågår et projekt med henblik på implementering af automatisk passwordskift af brugerkonti med administratoradgang til netværksenheder og VMware. Vores test giver ikke anledning til yderligere relevante bemærkninger.
Evaluering af brugeradgangsrettigheder Ledelsen foretager periodisk gennemgang af brugerrettigheder, til sikring af at disse er i overensstemmelse med brugernes arbejdsbetingede behov. Uoverensstemmelser undersøges og rettes rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har stikprøvevis kontrolleret, at der foretages periodiske gennemgange, til bekræftelse af at disse har fundet sted. Stikprøvevis gennemgået, at identificerede afvigelser afhjælpes.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolaktivitet	PwC-test	Resultat af test
Inddragelse af adgangsrettigheder Brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver inaktiveret rettidigt. Inddragelse af adgangsrettigheder påbegyndes med nærmeste leders godkendelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at inddragelse af adgangsrettigheder sker efter betryggende forretningsgange, og for at der foretages opfølgning i henhold til forretningsgangene for de tildelte adgangsrettigheder. Vi har endvidere stikprøvevis kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugere på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.	Vores test har ikke givet anledning til relevante bemærkninger.
Politik for anvendelse af netværkstjenester, herunder autentifikation af brugere med ekstern forbindelse Datakommunikationen er tilrettelagt på en hensigtsmæssig måde, og er tilstrækkeligt sikret mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed. Der er endvidere fortaget en opdeling af netværk som følger Athenas funktionsopdeling såvel som opdeling i forhold til hver enkelt kunde. Til dele af den tekniske platform udbydes VPN fra faste IP-adresser samt token. Til den administrative platform benyttes token-system. De nævnte platforme er adskilt ved implementering af adskillige VLANs.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og påset, at der anvendes en passende autentificeringsproces for driftsmiljøet. Vi har stikprøvevis kontrolleret, at brugere identificeres og verificeres, inden adgang gives, samt at fjernadgangen er beskyttet af VPN og opnås ved at anvende faste IP-adresser og tokens. Vi har konstateret, at netværket er segmenteret i adskilte net ved hjælp af VLANs for at reducere risikoen for uautoriseret adgang.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolaktivitet	PwC-test	Resultat af test
Styring af netværksforbindelser Der udføres regelmæssigt gennemgang af firewallregelsæt samt penetrationtests til sikring af netværksforbindelser.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at styre netværksforbindelser. Vi har konstateret, at der er foretaget periodiske penetrationstest, samt kontrolleret, at der er taget stilling til konstaterede svagheder. Vi har stikprøvevis gennemgået firewallkonfiguration og påset, at reglerne i firewallen er sat hensigtsmæssigt op.	Vores test har ikke givet anledning til relevante bemærkninger.
Begrænset adgang til informationer Alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med virksomhedens politikker, til sikring af at rettigheder er tildelt ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at begrænse adgangen til informationer. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteter er tilstrækkeligt dækkende. Vi har stikprøvevis kontrolleret, at tildeling af adgang til data og systemer udføres ud fra et arbejdsrelateret behov og er godkendt i overensstemmelse med forretningsgangene.	Vores test har ikke givet anledning til relevante bemærkninger.

Kontrolmål: Anskaffelse, udvikling og vedligeholdelse af styresystemer *Der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.*		
Kontrolaktivitet	**PwC-test**	**Resultat af test**
Styring af software på driftssystemer Der er etableret separate it-miljøer for udvikling, test og produktion.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, herunder eksistensen af et versionsstyringsværktøj. Vi har stikprøve gennemgået ændringer i perioden, til verifikation af at ændringer er testet i testmiljøet forinden idriftsættelsen og dokumenteret.	Vores test har ikke givet anledning til relevante bemærkninger.
Ændringsstyring Ændringer til operative systemer og netværk bliver testet af kvalificeret personale inden flytning til produktion. Test af ændringer til operativsystemer og netværk godkendes før flytning til produktion. Nødændringer af operativsystemer og netværk uden om den normale forretningsgang bliver testet og godkendt efterfølgende. Kunderelaterede ændringer registreres i opgavesystemet. Interne ændringer (infrastruktur, interne platforme) registreres i opgavesystemet eller i enkelte områders dokumentation. Samme formular anvendes til både kunderelaterede og interne ændringer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået ændringsstyringsprocedurernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur. Stikprøvevis gennemgået ændringsønsker for følgende: • Registrering af ændringsanmodninger i det dertil etablerede system. • Dokumenteret test af ændringer, herunder godkendelse. • Godkendelse skal være opnået før implementering. Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende. • Dokumenteret plan for tilbagerulning, hvor relevant.	Vi har observeret, at der ikke er udarbejdet formelle procedurer for dokumentation af aktivt fravalgte opdateringer på de enkelte servere. Athena har oplyst, at den enkelte tekniker er ansvarlig for både vurdering og godkendelse af de enkelte opdateringer, men resultatet af vurdering og godkendelse af opdateringer dokumenteres ikke. Vi har fået oplyst af ledelsen, at tiltag er igangsat for at sikre, at både de implementerede og fravalgte opdateringer på servere og systemer bliver dokumenteret. Vores test har ikke givet anledning til yderligere bemærkninger.

Kontrolmål: Katastrofeplan

Athena IT Group A/S er i stand til at fortsætte servicering af kunder i en katastrofesituation.

Kontrolaktivitet	PwC-test	Resultat af test
Opbygning/Struktur af Athenas katastrofeberedskab Den samlede katastrofeplan er med udgangspunkt i en risikoanalyse, opbygget af en overordnet katastrofestyringsprocedure samt operationelle katastrofeplaner for de konkrete katastrofeområder. Den operationelle katastrofeplan indeholder beskrivelse af katastrofeorganisationen med de ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser for de nødvendige indsatsgrupper. For de enkelte platforme er udarbejdet detaljerede indsatsgruppeinstrukser for reetablering i forhold til nøddrift. **Test af katastrofeberedskab** Der sker årlig test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået udleveret materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser. Vi har stikprøvevis kontrolleret, at beredskabsplaner testes ved skrivebordstest elle via realistiske testscenarier i det omfang der er muligt.	Vores test har ikke givet anledning til relevante bemærkninger.