www.pwc.dk

Outforce A/S

Erklæring fra uafhængig revisor vedrørende generelle it-kontroller i tilknytning til Outforce A/S' it-drift og hosting-aktiviteter

Januar 2017

Indhold

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Outforce 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. Outforce A/S bekræfter, at:

(a) den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af Outforce A/S' driftsydelser, der har behandlet kunders transaktioner i hele perioden fra 1. februar 2016 – 31. januar 2017. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) redegør for, hvordan systemet var udformet og implementeret, herunder redegør den 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. februar 2016 – 31. januar 2017

(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 for vigtigt efter dennes 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. februar 2016 – 31. januar 2017. Kriterierne for denne udtalelse var, at:

(i) de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(ii) de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. februar 2016 – 31. januar 2017.

Middelfart, den 31. januar 2017

Outforce A/S

Enrico Augustinus
Managing director

2. Outforce A/S' beskrivelse af generelle it-kontroller for driftsydelser i Danmark

Indledning – kort om Outforce A/S

Virksomheden udspringer af den verdensomspændende USTC-koncern i Middelfart.

Indtil 2003 var vi intern it-afdeling for koncernens mange selskaber inden for bl.a. rederi, shipping og bunker-olie. I 2003 blev Outforce A/S udskilt som et særskilt selskab, og i 2007 flyttede vi til et nyt hovedkontor med vores eget moderne datacenter. I 2014 udvides med ekstra hosting-kapacitet på 120 m2, fundet i nyt datacenter.

Outforce A/S rådgiver, designer, servicerer, implementerer og drifter it-løsninger med fokus på følgende:

- Vi er leverandør af dedikerede hostede it-løsninger med 24x7 drift
- Vi er leverandør af it-infrastrukturprojekter
- Vi er kvalitetsbevidste – leverer altid efter "best practice"
- Vi leverer til aftalt tid
- Vi er lette at indgå aftaler med under devisen "keep it simple"

Beskrivelse af ydelser

Outforce A/S' primære ydelser er følgende:

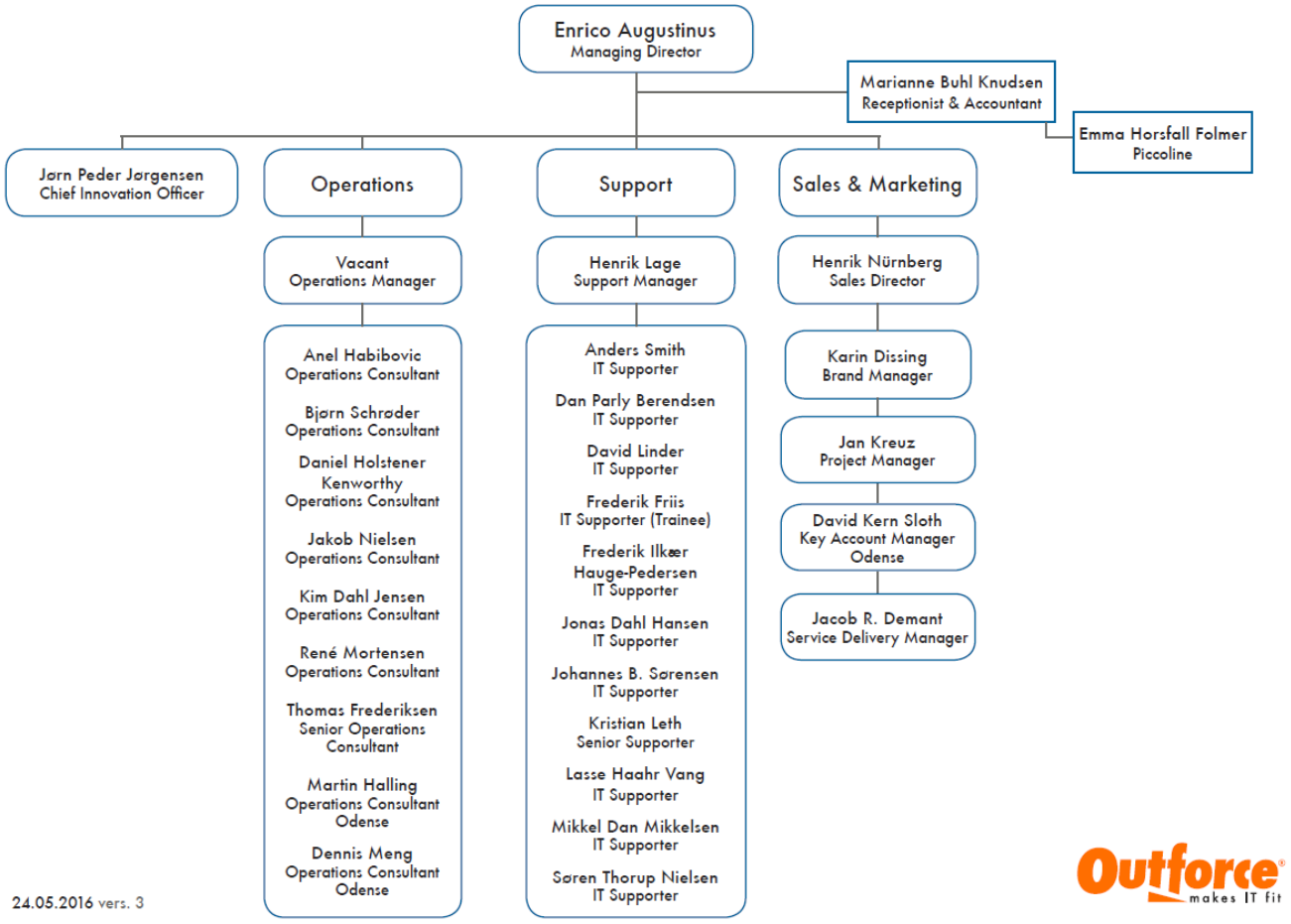
- Levering af dedikerede hosted services
- Levering af remote backup
- Hosted desktop og Citrix
- Microsoft Exchange
- First level brugersupport inkl. support af MAC
- Anskaffelse, ændringsstyring og vedligeholdelse af "hosted" hardware
- Microsoft MS Windows operativ systemer

Outforce A/S har i øjeblikket 2 datacentre på egen matrikel i Middelfart og co-location i Kolding, der er ca. 24 km adskillelse mellem de 2 datacentre og co-location. Herfra fortages overvågning og drift af ca. 1.000 servere.

Outforce A/S' support team kører i 2. holdskift, så de er fysisk bemandet fra kl. 6-21. Alle medarbejdere kan supportere på dansk og engelsk, enkelte kan også på tysk. Outforce A/S leverer first level brugersupport til mere end 5.000 brugere.

Beskrivelsen omfatter drift og overvågning pr. 1. februar 2016 – 31. januar 2017 og er udelukkende til brug for de virksomheder, der anvender Outforce A/S' it-drift og hosting-aktiviteter, og disse virksomheders revisorer og må ikke anvendes til andre formål.

Organisatorisk opbygning i Outforce A/S



Ledelsen har det overordnede ansvar for Outforce A/S' sikkerhedsarbejde.

Outforce A/S har som styrende element at informationssikkerheden er baseret på de reelle risici, som Outforce A/S er udsat for. Derfor har vi med ISO27005 som rammeværktøj, vurderet risikostyringen som beskrevet nedenfor.

Etablerede forhold i risikostyring er vurderet geografisk, it-mæssigt og politisk med udgangspunkt i en kvalitativ konsekvens- og sandsynlighedsvurdering, og med respekt for at Outforce A/S' omverden forandres, vil Outforce A/S kontinuerligt vurdere behovet for tilretning af virksomhedens risikostyring

	Forebyggende tiltag	Udbedrende tiltag
Administrative tiltag	• Politikker og vejledning • Awareness • Change management • CAB-board • Technical Management • Compliance-kontroller • Leverandør-kontrakter • Service- og supportaftaler • System-dokumentation	• Beredsskabsplaner • Logning • Disaster Recovery procedures • Procedure for Major incidents
Fysiske og tekniske tiltage	• Firewalls • Antivirus • Alarmsystemer • Test-miljøer • Monitorering • Intrusion Prevention • Redundans • Brugerstyring • Clusters • Password-politik	• Standby-udstyr • Backup/restore • Virtualisering • StandbySite • Server snapshots • Intrusion detection • Brandslukning • Nødstrøm

Outforce A/S benytter løbende eksterne partnere som HP, IBM og Arrow ECS, således at vi sikrer, at vores installation er udført og vedligeholdt efter best pratice i forhold til teknik og sikkerhed.

Det er op til kunden at gøre krav på specifikke sikkerhedsrutiner eller tekniske installationer, såfremt best pratice i forhold til teknik og sikkerhed, jf. Outforce A/S' standard ikke lever op til dette.

I Datacenter 1 benytter vi iris-scanner og i Datacenter 2 ansigtsgenkendelse som fysisk godkendelse for at komme ind i vores hosting-center. Vore datacentre er også beskyttet af eget alarmanlæg, som er direkte koblet op til Dankontrol. For at komme til vore datacentre skal man ligeledes passere husets alarmsystem og være i besiddelse af en chip.

Kontrolmiljø

Outforce A/S har valgt at bruge ISO27000-serien som framework for etablering af kontrolmiljøet, dette betyder at komponenter fra ISO27000-serien er gennemset og vurderet i forhold til implementering i virksomheden. Outforce A/S anser ISO-27000 som værende en væsentlig sikkerhedsstandard i bestræbelserne op at oparbejde og adressere en compliant og konsistent tilgang til kontrolmiljø og IT-sikkerhedspolitikkerne i Outforce A/S.

Vores metodik for implementering af kontroller er defineret med reference til ISO27002 (regelsæt for styring af informationssikkerhed), og Outforce A/S har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger:

- Overordnede retningslinjer
- Organisering af informationssikkerhed
- Styring af informationsrelaterede aktiver
- Medarbejdersikkerhed
- Fysisk sikkerhed
- Styring af netværk og drift
- Adgangsstyring
- Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer
- Styring af sikkerhedshændelser
- Beredskabsstyring
- Overensstemmelse med lovbestemte og kontraktlige krav

Outforce A/S er opdelt i funktionelle forretningsenheder (se organisationsplan under punktet

Risikostyring) og har derigennem gunstige muligheder for at arbejde struktureret med såvel vejledende og normative krav i ISO27000-serien. Derudover giver den strukturelle opbygning gode betingelser for at tilvejebringe og opretholde et højt serviceniveau overfor Outforce A/S' kunder. Outforce A/S anser højt serviceniveau og høj kundetilfredshed som værende essentielle i minimering af risici for Outforce A/S.

Outforce A/S ledes i dag af Managing Director Enrico Augustinus som referer til USTC koncernen. Outforce A/S har i øjeblikket ansat 31 medarbejdere.

Support teamet har i øjeblikket 11 ansatte. Den primære funktion for denne afdeling er at levere brugersupport til de hostede løsninger, herunder også support af Pc'er og MAC, samt afhjælpe alm. spørgsmål fra kunder.

Operations teamet har i øjeblikket 11 ansatte. Den primære funktion for denne afdeling er at sikre stabil drift, maksimal oppetid og håndtere planlagte service vinduer på infrastrukturen i datacenter. Teamet håndterer også overvågning af servere, netværk, storage samt WAN forbindelse, herunder VPN og layer 2 forbindelser til kunder. Yderligere varetager teamet installation og tilpasning af Windows OS, Exchange og Citrix. Teamet er ansvarlig for implementeringen af nye kunder, herunder styring af tidsplan. Teamet har også eksterne opgaver hos onsite kunder uden for datacenter. Licensrapportering håndteres ligeledes af teamet.

Organisering af informationssikkerhed

Outforce A/S har med udgangspunkt i ISO27001, kvalitativt vurderet hvilke sikkerhedsforanstaltninger og kontrolprocedurer som Outforce A/S tager eller vil tage i anvendelse. Vi er opmærksomme på det forhold at dette vigtige arbejde er en dynamisk proces og tager hensyn til dette i virksomhedens daglige virke samt i eksisterende og kommende strategiarbejde.

Outforce A/S har strategisk tilvalgt at tilbyde kunderne høj oppetid samt høj og lokal tilgængelighed, dette fordrer et kontinuerligt fokus på forhold, der fastholder og forbedrer driftssikkerheden i Outforce A/S.

Outforce A/S er fokuseret på et lavt men væsentligt antal kunder (under 150 stk.) og har formuleret tydeligt i eksisterende 3 årige strategi, at være mere for disse og større kunder.

Outforce A/S har formuleret mål og handlinger i den nuværende strategi, som har til formål at adressere udefrakommende faktorer, som kan udgøre en risiko for informationssikkerheden.

På de indre linjer, har vi formuleret en Informationssikkerhedspolitik, som er forankret i virksomhedens Personalehåndbog. Personalehåndbogen er lettilgængelig for alle medarbejdere på virksomhedens intranet og alle medarbejdere tilgår vilkår og rammer ved ansættelse i Outforce A/S.

Alle brugere bliver logget i AD. Disse logs bliver gennemgået ved begrundet mistanke. Dokumentationen fra gennemgang forelægges virksomhedens ledelse og underskrives af udførende medarbejdere og ledelse samt arkiveres i virksomheden.

I Outforce A/S foretages den interne administrative sikkerhedsfunktion af Operations Manager. Ansvaret for den tekniske sikkerhed er placeret i Operations. Funktionen sikrer implementering og ajourføring af sikkerheds- og kvalitetsprocedurer, forestår den primær kontakt til revisorer/auditorer, sikrer udførelse af egenkontroller, sikrer løbede vedligeholdelse af risikovurderingen, samt sikrer at der findes en beredskabsplan og at denne bliver løbende ajourført.

Herudover er der en organisation til håndtering Salg & Marketing, Innovation, en sekretær og piccoline (se nedenstående organisationsdiagram).

Det påhviler den enkelte medarbejder til stadighed at følge den faglige udvikling inden for sit område samt holde sit uddannelsesniveau ajour. Medarbejderen er berettiget og forpligtet til relevant videreuddannelse, som aftales med nærmeste overordnede. Outforce A/S afholder alle omkostninger til denne uddannelse. To gange årligt følges i MUS-samtaler op på uddannelse - for enkelte medarbejdere er der lavet en plan for et år ad gangen. Dette står i referatet fra MUS-samtalerne, hvor andre personlige forhold også er beskrevet.

Outforce A/S' generelle politikker og forretningsgange er beskrevet i dokumentet " Generelle forretningsgange og driftsrutiner".

Ansvaret for sikkerhedspolitik, beredskabsplaner, driftsrutiner og beskrivelse af forretningsgang ligger hos ledelsen. Det er ledelsen, der kommunikere eksternt med f. eks. pressen. Ansvaret for formidling af forretningsgang og interne rutiner ligger hos ledelsen. Ved opdatering/rettelser er det ledelsens ansvar at formidle disse og forankre disse.

Styring af informationsrelaterede aktiver

Vi har kontrakter på aftalte ydelser for alle vores kunder. Særlige forhold er beskrevet heri som de var ved aftaleindgåelse. Ændringer hertil er beskrevet i bilag i kontrakt, og vedlagt kundens godkendelse implementeret i Outforce A/S' økonomisystem.

Medarbejdersikkerhed

Ledelsen i Outforce A/S vil sikre at alle medarbejdere er bekendt med deres roller og ansvar, og alle er kvalificerede og egnede til at udføre deres rolle.

Alle medarbejdere skal leve op til deres rolle som er tilegnet dem, samt følge vores procedure. Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold eskaleres og håndteres, for herigennem at passe særligt godt på vore kunders data og udstyr og dermed vores eksistensgrundlag.

Vi har en procedure og tjekliste for ansættelse af medarbejdere og etablering af samarbejde med ledere, hvor vi sikrer at vi ansætter den rigtige kandidat ift. baggrund og kompetence.

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold er beskrevet i hver medarbejders ansættelseskontrakt hvor forhold omkring alle sider af ansættelsen, herunder ophør er angivet.

Fysisk sikkerhed

Adgangskontrol eksterne:

Alle besøgende skal indskrives i logbogen der findes i receptionen. Ud over dette skal alle besøgende bære synligt gæstekort.

Adgangskontrol til Datacentre.

Outforce A/S råder over 2 driftscentre som foruden at være beskyttet af et normalt alarmsystem, der sidder i huset, også har et ekstra alarmsystem som kun dækker driftcentrene. Der skal indtastes en 4 cifret kode for at slå alarmsystemet fra og til. Koden er personlig for den enkelte medarbejder og Operations varetager og vedligeholder disse.

Foruden en kode, benyttes der IRIS scanner til kontrol til datacenter 1, og til datacenter 2 benyttes ansigtsgenkendelse. Dvs. begge centre har foruden en kode også fysisk adgangskontrol.

Begge datacentre kan tilgås af medarbejdere 24/7-365. Begge datacentre er overvåget med video, og det er begge kølegrave også.

Datacenteret i Kolding er styret af Global Connect, og Outforce A/S medarbejdere har adgangskort for at tilgå Datacenter i Kolding, er kortet ikke brugt i 3 måneder, bliver det automatisk spærret og skal genåbnes.

Styring af netværk og drift

Overordnet beskrivelse af Datacentre

Outforce A/S Datacenter 1 & 2 er placeret på samme matrikel, men er 2 separate datacentre med redundante fremførte datalinjer fra bl.a. TDC og med hver sin infrastruktur, køl, nødstrømsgenerator, UPS etc.

Datacentrene er forbundet med flere fiberforbindelser og driftes uafhængigt af hinanden - således at kundernes IT installationer fordeles henover begge datacentre og nedbringer derved risiko for nedetid. Vi bruger datacenter 3 i Kolding for image backup, kaldet Disaster Recovery VEEAM.

Bygningen er beskyttet af udvendig videoovervågning samt adgangskontrol på døre. Der er installeret iris-scanner til datacenter. Desuden er der kodebeskyttelse for af komme ind til scanneren.

Beskrivelse af datacenter 1:

- UPS nødstrøm med batteri backup
- Nødstrømsgenerator
- Brandsikring med dysedæmpere
- Frikøle anlæg
- Fysisk adgangskontrol ved hjælp af en irisscanner
- 24 timers overvågning af serverrummet tilkoblet Dankontrols alarmcentral med alarmer for fugt, temperatur, brand, ups og nødstrømsgenerator.
- Fysisk reservedelslager
- Irisskanner

Beskrivelse af vores datacenter 2:

- UPS nødstrøm med batteri backup
- Nødstrømsgenerator
- Brandsikring med dysedæmpere
- Frikøleanlæg
- Fysisk adgangskontrol ved hjælp af en ansigtsscanner
- 24 timers overvågning af serverrummet tilkoblet Dankontrols alarmcentral med alarmer for fugt, temperatur, brand, ups og nødstrømsgenerator.
- Fysisk reservedelslager
- Ansigtsgenkendelse

Backup & Disaster recovery

Data er sikret i begge af Outforce A/S' datacentre med fysiske rammer som lever op til et topmoderne driftscenter med fysisk adgangskontrol. I datacenter 1 og datacenter 2 sker den primære datadrift.

Mindst én gang i døgnet eller efter aftale tages der backup. Backup af servere er delt i 2 – én backup i Disaster Recovery Backup og gemmes i datacenter 3 i Kolding. Den anden backup er en databackup, som gemmes i datacenter hos Frontsafe A/S i Århus.

Disaster Recovery Backup

Disaster Recovery Backup benyttes til at genetablere virtuelle servere meget hurtigt under en hypervisor, således at serverens operativsystem er operationsdygtigt men uden data. Dette kan udføres i begge vores datacentre eller alternativt i datacenter 3, som er lokaliseret i Kolding 27 km fra Outforce A/S' datacenter 1 og 2. Til at foretage Disaster Recovery Backup benyttes der VEEAM. Data opbevares i Danmark. Alle datacentre er forbundet med 10Gbit fiber for højeste hastighed. Data validering af Disaster Recovery Backup sker én gang pr. måned og der laves rapport på dette. En kunde udvælges i rækkefølge pr. kvartal for test af restore-proceduren.

Under en supervisor benyttes Veeam image-baseret backup samt IBM TSM til databackup. Data er eksempelvis SQL databaser og filer.

Veeam er sat op til at tage såkaldte snap shots/images af alle servere. Veeam løsning er placeret på Datacenter 3 i Kolding. Datacenter 3 kan derudover benyttes som almindelig backup2disk eks. en SQL server eksempelvis hvor man kan dumpe logfiler og databaser.

Outforce A/S' formåen til genetablering af et IT miljø bygger både på Disaster Recovery Backup og Data backup som tilsammen sikre at serverne meget hurtigt kan genskabes i et vilkårligt datacenter, således at servernes operativsystem kan starte, efterfølgende startes backup agenten og virksomhedes data genetableres på serveren.

Data backup

Til databackup bruges IBM TSM teknologi og placeres i 2 separate datacentre 98 km væk fra Outforce A/S driftscenter hos Front-Safe i Århus. Vi har specialister på alle niveauer og inden for alle områder der har tværgående kompetencer inden for de brugte teknologier.

Data backup foretages med produktet IBM Tivoli Storage Manager. Servere, både fysiske og virtuelle benytter denne backup, og alle data bliver krypteret og er ikke læsbar for andre end kunderne. Der benyttes fil og database agenter. Database agenter til eks. SQL kan sikre at der tages helt ned til time backup af SQL data, hvis det ønskes.

Data backup foretages mindst én gang i døgnet og data opbevares krypteret. For hurtig tilgang er data opbevaret på disk, men sikres yderligere ved at ældre versioner flyttes til tape i et andet datacenter.

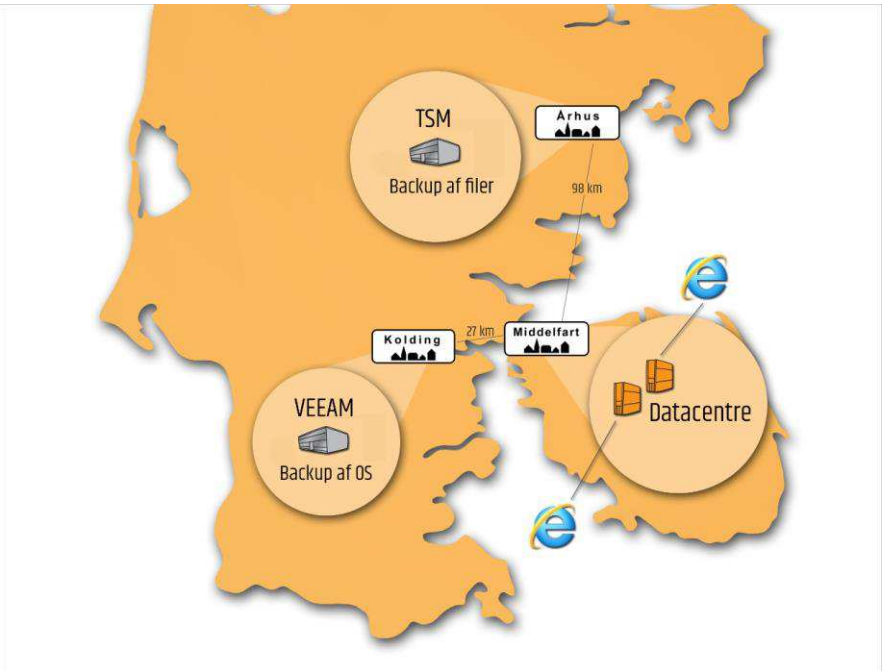
Såfremt at der fremkommer forhold i afklaringsfasen, der tilstræber yderligere tiltag for sikring af datavaliditet, kan backup kan udvides med ARC Automatic Restore Control. Dette sikrer at de data, der er taget backup af er valide. Dette giver sikkerhed for at de data vi har backup af, også er brugbare i tilfælde af de skal genetableres. Automatic Restore Control sker én gang pr. måned med henblik på validering af data.

De to teknologier Veeam og Tivoli Storage Manager (TSM) er hver for sig førende inden for deres felt og sammen sikrer de at man kan reetablere og genskabe tabte data effektivt og hurtigt således eventuel nedetid på baggrund af mistet data minimeres.

Outforce A/S modtager hver dag en rapport hvor alle virtuelle servere der tages filbackup af indgår. Denne rapport viser eventuelle fejl i backup fra dagen før og dette bruges proaktivt til at kunne lave nogle handlinger som sikrer at valid backup foretages næste gang.

Der henvises desuden til Outforce A/S' 3402-erklæring.

Principskitse, Backup og Disaster Recovery



Vedligeholdelse af systemer:

Patch Management – strategi

Der installeres opdateringer i kategorierne Security Updates, Critical Updates og Optional Updates. Hermed kan patchninger klassificeres i forhold til relevans og vigtighed for hver kunde. Outforce A/S tilbyder løbende patchning af alle versioner af Windows Server, som er under aktiv maintenance fra Microsoft. Ud

fra den enkelte kundes krav til løsningens tilgængelighed, defineres frekvens for opdatering, som standardiseret udgangspunkt anbefaler Outforce A/S at der installeres opdateringer hver uge.

Kunden har desuden mulighed for at tilvælge automatisk patching af standardapplikationer som eks. Java, Adobe Reader, Adobe Flash, hvis disse er installeret på kundens løsninger. For at sikre mod kendte sårbarheder i disse standardapplikationer, anbefales Outforce A/S' kunder at benytte sig af dette.

Outforce A/S validerer løbende at opdateringer til operativsystemer såvel som applikationer installeres korrekt i nyeste tilgængelige version.

Change Management-strategi

Outforce A/S' strategi på dette område tilsikrer at ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgang og processer. Dette sker bl.a. via disse midler:

- At der sker registrering og beskrivelse af ændringsanmodninger
- At alle ændringer er underlagt formel godkendelse inden idriftsætning
- At ændringer er underlagt formelle konsekvensvurderinger
- At der beskrives fall-back planer hvor det er muligt
- At der sker identifikation af systemer der påvirkes af ændringer
- At der sker en dokumenteret test af ændringer inden idriftssætning
- At dokumentation opdateres så den i al væsentlighed afspejler de påførte ændringer
- At procedurer er underlagt styring og koordination i Outforce A/S' "change board" – CAB-boardet

Changes opgøres på 2 måder, der tager udgangspunkt i vurdering af impact og sandsynlighed. Derved foretages en egentlig klassifikation af changes. Der udfærdiges dog altid en Change form.

Hvis denne change form er LOW i impact, sandsynlighed og klassifikation kan den udføres uden CAB-board godkendelse, af den enkelte teknikker. Changes som har en anden klassifikation end beskrevet skal forelægges CAB-board bestående af technical management gruppen i Outforce A/S som herefter godkender med mindst 2 personer. Det er Outforce A/S' SDM funktion der sørger for korrekt udfyldning og arkivering af Change form som skal godkendes af CAB-boardet.

Adgangsstyring

Tilgang til IT systemer:
Den logiske sikkerhed omfatter logisk beskyttelse af elektroniske systemer og information, der vedrører serviceydelsen. Fx fastlægger den, at kun autoriserede personer har adgang hertil.

Outforce A/S' strategi på området tilsikrer at medarbejderne får stillet tilstrækkelige arbejdsredskaber til rådighed, og at disse redskaber kontinuerligt sikres i takt med sikkerhedstiltag. Outforce A/S ønsker at fremstå som en fleksibel og attraktiv arbejdsplads, hvorfor at der tilbydes muligheder for remote opkobling til såvel egne som kundernes IT-systemer – og for at sikre disse er nedenstående elementer taget i anvendelse.

Adgangsmuligheder (logon med 2-vejs validering via SMS)

Adgang til vores netværk og adgang uden vores interne netværk, systemer og data, skal ske for kun autoriserede personer.

Der er mulighed for at logge på via krypteret VPN-forbindelse med 2-vejs validering via SMS.

Outforce A/S har givet tilladelse til at der kan benyttes mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Adgang til disse data styres via AD-opsætning. Alle enheder, der synkroniseres låses med kode efter 15 minutter og dette er ikke muligt at ændre for den enkelte medarbejder.

Krav til password – alle brugere med adgang til Outforce A/S' systemer, anvender password med mindst 7 karakterer, hvor både tal og bogstaver indgår

Password politik for en standard bruger er at Password skal skiftes hver 60. dag.
Der er 2 vejs identifikation ved bruger logon udenfor Outforce A/S.
Adgange til kundesystemer er tildelt ud fra arbejdsrelateret behov og styres via en administrator konto for den enkelte medarbejder. Password politikken er den samme som på en standard bruger.
Ved behov for at en ekstern skal logge på oprettes denne med bruger og midlertidig adgang som lukkes efter opgaven er afsluttet.

Krav til pauseskærm – pauseskærm er påkrævet så snart at arbejdspladsen forlades i kortere tid.

For alle medarbejder i Outforce A/S benyttes der 2 vejs kode godkendelse med den ansattes mobil telefon.

Begge Datacentre er overvåget af Dankontrol elektronisk. Dvs. hver aften kigger de på om der er koblet alarm til kl, 20:30 senest. Hvis ikke ringes der til vagten, og på denne måde tilsikres tilkobling af alarm.

Alle PC er beskyttet af en harddisk lås så ved tyveri eller anden bortkomst, så kan data ikke tilgås.

Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer

Outforce A/S vil sikre at alle nyanskaffelser om implementering af servere, systemer, services og software håndteres på struktureret og sikker vis.

Opgaver af en vis størrelse, som kan være væsentlige ændringer i vores generelle driftssystem på tværs af kunder, eller implementering af kundeløsninger, har vi en procedure for, enten håndteres det via vores CAB-board eller vores project manager (projektstyringsmodel).

Vores projektstyringsmodel er baseret på vores egen og praktiske metodik, men er inddelt i en rækker faser: foranalyse, design, test, implementering, test og evaluering. Hver fase indeholder accept fra interessent.

Styring af sikkerhedshændelser

Vore medarbejdere indgår i vagtordning således at vi kan reagere 24 timer i døgnet. Opstår en hændelse udenfor normal arbejdstid, er det den vagthavende medarbejder, der vurderer hvilken reaktion der skal ske. Herefter foretages det fornødne for orientere kunder og omverden. Dette sker efter konsultation af ledelse og kollegaer.

Sker en hændelse indenfor normal arbejdstid, vil medarbejderne håndtere og eskalere sagen på samme vis som andre sager, og med den prioritering som er nødvendig.

Ledelse har ansvaret for at overvåge sikkerhedsbrister samt opfølgninger på disse. Det er endvidere ledelsen, der igangsætter udbedring af eventuelle sikkerhedsbrister. Ledelsen har ansvaret for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Det er medarbejderens ansvar at rapportere sikkerhedsbrister eller mistanke herom til ledelsen omgående. Ligeledes vil virksomhedens overvågningssystem være opsat til at identificere udvalgte sikkerhedsbrister.

Vi holder os fagligt opdaterede vha. producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.

Via vores medlemskab af Brancheforeningen for IT-hostingvirksomheder i Danmark, er vi forpligtet til at sikre, at kritiske sikkerhedsopdateringer implementeres indenfor 2 måneder efter frigivelse. Dette sikrer vi ved, at alle væsentlige opdateringer afvejes og implementeres inden for tidsrammen.

Beredskabsstyring

Information og kommunikation

Det er den enkelte teamleders ansvar at kommunikere internt i Outforce A/S. Det er ledelsen, der er ansvarlig for kommunikationen ud til kunder og presse. Rapportering udarbejdes af de enkelte enheder og godkendes af ledelsen, inden den sendes til kunden.

Måden som der kommunikeres på, er afspejlet i Outforce A/S' vejledning til håndering af Major Incidents, heri fremstår telefonisk kontakt, SMS-kommunikation og mails i en struktureret kommunikationsplatform, som Outforce A/S benytter. Det er ligeledes i proceduren, defineret hvem der i Outforce A/S kommunikerer hvad, hvordan og til hvem. Proceduren er defineret ud fra roller og ikke enkeltpersoner i Outforce A/S.

Beredskabsplaner

Identifikation af kritiske processer

Indsatsen med at udarbejde forretningsnødplaner er identificeret og arbejdet vil i takt med identificeret behov blive udarbejdet. I sammenhæng med de tekniske beredskabsplaner vil disse håndteres af den samlede ledelse i Outforce A/S.

Kommunikation i situationen

Et af hovedelementerne til en succesfuld styring af en beredskabssituation er at sikre en passende kommunikation til alle relevante interessenter, i rette tid og med det rette indhold. Kommunikation skal sikre, at organisationens interessenter informeres så godt om situationen, at forvirring minimeres mest muligt.

I Outforce A/S er der kortlagt en ønsket kommunikationsform og rolle, fordeling berammet i et framework, omhandlende Major Incidents. Ansvaret for vedligeholdelse af denne proces og rollefordeling, påhviler ledelsen i Outforce A/S. Proceduren for håndtering af Major Incidents er tilgængelig for alle medarbejdere på virksomhedens intranet og forefindes ligeledes i hardcopy i virksomheden.

Den effektive kommunikation forventes at forebygge et unødigt stort antal henvendelser om hændelsen og unødig forbrug af tid og kræfter frem for at håndtere selve situationen. Kommunikation skal også sikre, at interessenterne får de fornødne oplysninger til at minimere eventuelle følgevirkninger og til at kunne etablere eventuelle alternative løsninger.

Beredskab for kommunikation skal i lighed med teknisk beredskab afprøves, hvilket sker når der indtræffer en hændelse – derudover revurderes processen kvalitativt løbende.

Minimumskrav for god hosting anser Outforce A/S som væsentligt, og Outforce A/S sikrer gennem procedure at Outforce A/S til enhver tid lever op til de gældende krav til god hosting, som Brancheforeningen for IT-hostingvirksomheder måtte kræve.

Teknisk beredskab

Outforce A/S' tekniske beredskabsplaner er sammenfattet i procedurebeskrivelse omhandlende Generelle procedurer og driftsrutiner 1.12, og omhandler bl.a.

FrozenZone, nødstrøm- og test heraf, backup, brandslukning, Denial-of-Service, oprettelse- og sletning af medarbejdere

Kontrolaktiviteter

Outforce A/S anvender kun standardsystemer. Katastrofeplan, der tilgængelig på intranettet. Desuden findes en kopi på Datacenter 3. Detaljerne fremgår af kontrolmål og kontrolaktiviteter, i følge skema med oplistning og test heraf.

Overensstemmelse med lovbestemte og kontraktlige krav

Vi lader os årligt revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelse af kontrollerne nævnt i denne beskrivelse. I kraft af at vi er medlemmer af BFIH, skal vi årligt attestere at vi følger rammerne indenfor ISO27002. Omtalte revisorerklæring sikrer dette, ligesom BFIH ønsker ekstern revisors bekræftelse på vores overholdelse af foreningens øvrige krav omhandlende forsikringsforhold, gennemsigtighed i forretningsvilkår, selskabsretlige forhold for vores virksomhed mv. Disse bekræftelser fra revisor er hjælp til BFIH's certificering af vores virksomhed.

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

Til ledelsen i Outforce A/S samt kunder af Outforce A/S' it-drift og hosting-aktiviteter i perioden 1. februar 2016 til 31. januar 2017 og disses revisorer.

Omfang
Vi har fået som opgave at afgive erklæring om Outforce A/S' beskrivelse, afsnit 2, af it-kontroller i tilknytning til Outforce A/S' it drift og hosting-aktiviteter i perioden 1. februar 2016 til 31. januar 2017, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Outforce A/S' ansvar
Outforce A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring
Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Vores ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Outforce 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 planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive 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 Outforce A/S har specificeret og beskrevet.

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

Begrænsninger i kontroller hos en serviceleverandør
Outforce A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos Outforce A/S' kunder af Outforce A/S' it-drift og hosting-aktiviteter og disses revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved generelle it-kontroller, som kunderne måtte anse for vigtige 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 Outforce A/S kan blive utilstrækkelige eller svigte.

Konklusion
Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i afsnit 1. Det er vores opfattelse,

(a) at beskrivelsen af de generelle it-kontroller, således som det var udformet og implementeret i perioden 1. februar 2016 til 31. januar 2017, i alle væsentlige henseender er retvisende, og

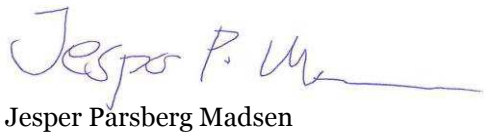
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden 1. februar 2016 til 31. januar 2017, og

(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 perioden 1. februar 2016 til 31. januar 2017.

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, samt arten 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 Outforce A/S' it-drift og hostingaktiviteter i perioden 1. februar 2016 til 31. januar 2017, og deres 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.

Aarhus, den 1. februar 2017
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab



Jesper Parsberg Madsen
statsautoriseret revisor

Iraj Bastar
senior manager

4. Kontrolmål, kontrolaktiviteter, test og resultat heraf

Kontrolmål A: 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.

Kontrolmål/Kontrol	PwC-test	Resultat af test
Skriftlig politik for informationssikkerhed Outforce A/S har udarbejdet en sikkerhedspolitik. Denne er til rådighed for medarbejdere på intranettet. Den revideres mindst én gang årlig. Den er godkendt af ledelsen	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at ledelsen har godkendt sikkerhedspolitikken, samt at den som minimum er revurderet én gang årligt. Endvidere har vi påset, at den forefindes let tilgængelig for medarbejderne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: 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.

Kontrolmål/Kontrol	PwC-test	Resultat af test
Ledelsens forpligtelse i forbindelse med informationssikkerhed Den enkelte afdelingsleder er ansvarlig for, at nye medarbejdere gøres bekendt med retningslinjerne som en del af introduktionen til virksomheden. I takt med at der sker opdatering af retningslinjerne, vil der blive givet besked herom via mail og USTC-nettet, hvor man også kan finde den ajourførte og gældende version af sikkerhedspolitikken.	Vi har overordnet drøftet styring af informationssikkerheden med ledelsen. Vi har påset, at det organisatoriske ansvar for informationssikkerheden er dokumenteret og implementeret. Endvidere har vi foretaget inspektion af, at rapportering om informationssikkerhedshændelser samt fortegnelse over aktiver er udarbejdet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Eksterne parter Outforce A/S beder samarbejdspartnere og eksterne leverandører om at sende revisorerklæring vedrørende de aftalte serviceydelser eller underskriver en kontrakt, der beskriver fortrolighed og sikkerhedsforanstaltninger. Outforce A/S sikrer, at eksterne partnere er bekendt med Outforce A/S' sikkerhedspolitik.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at der er etableret betryggende procedurer for samarbejdet med eksterne leverandører. Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter, og vi har påset, at der er modtaget revisorerklæring fra backupleverandører for den relevante periode.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader, forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Kontrolmål/Kontrol	PwC-test	Resultat af test
Fysisk sikkerhedsafgrænsning Alle medarbejdere hos Outforce A/S har adgang til lokalerne ved hjælp af alarmsystemer. Kontorerne låses automatisk kl. 16.30 og åbnes kl. 7.30. Uden for åbningstiden skal medarbejdere bruge kode og brik for at få adgang til bygningen Datacentre er adgangsreguleret ved hjælp af kode på døren til værkstedet og iris-scanner til datacenter. Adgang til datacenter bliver tildelt efter arbejdsmæssigt behov. Datacenteret er videoovervåget. Outforce A/S kan herved dokumentere handlinger i datacenteret. Gæster bliver ledsaget af en medarbejder med adgang til datacenter.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har observeret, under besøg i Outforce A/S' datacentre, at adgang til sikre områder er begrænset ved anvendelse af adgangssystem. Vi har ved stikprøvevis inspektion gennemgået procedurerne for fysisk sikkerhed vedrørende de sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt om personer uden godkendelse til de sikrede områder skal registreres og ledsages af en medarbejder med behørig godkendelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Sikring af kontorer, lokaler og faciliteter Datacentre er adgangsreguleret ved hjælp af kode på døren til værkstedet og iris-scanner til datacenter. Bygningen er videoovervåget og besøges uden for arbejdstid af et vagtselskab minimum fire gange pr. døgn.	Vi har forespurgt ledelsen om de anvendte procedurer. Vi har gennemført inspektion af alle serverrum og påset, at alle adgangsveje er sikret med kortlæser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Placering og beskyttelse af udstyr I datacentre er installeret Inergen-anlæg, temperaturmåling og videoovervågning. Inergen-anlæg testes én gang om året ifølge gældende lovgivning, og testen udføres af RMG-Inspektion A/S, og der foreligger en godkendt erklæring. Ledelsen og driftsvagten modtager alarmer både på sms og mail ved eventuelle hændelser.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved inspektion gennemgået driftsfaciliteterne og har påset, at der er etableret de fornødne kontroller i form af: • Brandbekæmpelsessystemer • Fugtsikring • UPS og generatorforsyning • Fysisk adgangskontrolsystem • Overvågning af indeklima. Vi har ved stikprøvevis inspektion gennemgået dokumentationen for vedligeholdelse af udstyr til bekræftelse af, at dette løbende vedligeholdes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader, forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Kontrolmål/Kontrol	PwC-test	Resultat af test
Understøttende forsyninger (forsyningssikkerhed) Datacentre er beskyttet mod strømafbrydelse ved anvendelse af UPS. Dieselgenerator overtager strømforsyning efter beskrevet tidsplan. Dette testes hver måned. Brændstofniveau aflæses løbende.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har observeret, under vores besøg i datacentrene, at der foretages monitorering af UPS eller nødstrømsanlæg. Vi har ved stikprøvevis inspektion gennemgået dokumentationen for vedligeholdelse til bekræftelse af, at UPS eller nødstrømsanlæg løbende vedligeholdes og testes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Sikring af kabler Kabler og elforsyning ligger i kabelbakker. Krydsfelt og tilhørende netværksenheder forefindes alle i datacentre.	Vi har ved inspektion observeret, at kabler til elektricitetsforsyning og datakommunikation er sikret mod skader og uautoriserede indgreb.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder monitorering, registrering 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, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolmål/Kontrol	PwC-test	Resultat af test
Dokumenterede driftsprocedurer Outforce A/S har beskrevet driftsprocedurerne for driftsmiljøet. Der gennemføres et dagligt tjek af serverrum. Efterfølgende bliver der bliver udarbejdet en daglig rapport, der bliver godkendt af ledelsen hver dag. Outforce A/S har tre forskellige typer medarbejdere; support, drift og konsulent (storage, firewall og adgangskontrol ligger hos drift). Adgang til fællesdrev er tildelt i forhold til funktion. Til hver stilling findes en stillingsbetegnelse. Outforce A/S har ingen udviklings- eller applikationsvedligehold.	Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenteret. I forbindelse med revision af de enkelte driftsområder er det ved inspektion kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. Vi har endvidere ved inspektion påset, at der foretages tilstrækkelig overvågning og opfølgning herpå.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Funktionsadskillelse Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i it-afdelingen. Disse politikker og procedurer omfatter krav til, • at ansvar for udvikling og opdateringer til produktionsmiljøet er adskilte • at it-afdelingen har ikke adgang til applikationer og transaktioner • at udviklings- og driftsaktiviteter er adskilt.	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 og ikke kompromitterer funktionsadskillelsen mellem udviklings- og produktionsmiljøer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Foranstaltninger mod virus og lignende skadelig kode Der er installeret antivirusprogrammer, som bliver opdateret regelmæssigt. Outforce A/S benytter anerkendt værktøj til antivirus med automatisk versionskontrol.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion gennemgået den tekniske opsætning til bekræftelse af, at der er installeret antivirusprogrammer, samt at disse er opdaterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder monitorering, registrering 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, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolmål/Kontrol	PwC-test	Resultat af test
Sikkerhedskopiering af informationer Backup og validering fortages til Front-Safe A/S En kunde udvælges i rækkefølge pr. kvartal for test af restore-proceduren. Der benyttes VEAM til back-up/restore af virtuelle servere. VEAM benyttes som disaster recovery-backup, der kun skal sørge for at bringe systemdrev i drift, hvorefter data på andre drev genetableres med TSM. VEAM benyttes til hurtig backup og reetablering og bruges løbende i driften efter aftale med kunden. Dermed testes det løbende, om backup er valid.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, gennemgået backupprocedurer, samt påset, at de er tilstrækkelige og formelt dokumenteret. Vi har gennemgået aftalen med Front-Safe A/S samt påset, at proceduren for backup er i overensstemmelse med de i kontrakten beskrevne oppetidsmål. Vi har ved stikprøvevis inspektion gennemgået log vedrørende backup til bekræftelse af, at backupper er gennemført fejlfrit, alternativt at der foretages afhjælpning i tilfælde af mislykkede backupper.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Monitorering af systemanvendelse og auditlogning Der er implementeret logning ved adgang på kritiske systemer. Disse logge bliver gennemgået i tilfælde af mistanke om misbrug eller fejl. Outforce A/S har ikke ansvaret for opsætning og drift af databaserne. Alle brugeres rettigheder bliver kontrolleret mindst én gang om året eller ved til-/afgang af medarbejdere. Alt hardware er overvåget. Der afsendes rapport i tilfælde af fejl. Endvidere er der sat infotavle op, der giver overblik over installationen. Overvågningssystem sender sms og mail i tilfælde af fejl. **Administrator- og operatørlog** Outforce A/S logger transaktioner og handlinger, der er gennemført af brugere og administratorer via domain	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, 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 ved stikprøvevis inspektion påset, at der er etableret overvågning og alarmering for nedsat tilgængelighed samt for forsøg på brud på den etablerede sikringsforanstaltning Vi har endvidere ved stikprøvevis inspektion kontrolleret, at der foretages tilstrækkelig opfølgning på logs fra kritiske systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder monitorering, registrering 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, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.*

Kontrolmål/Kontrol	PwC-test	Resultat af test
controllers (AD) audit log. Brugerkontis rettigheder på AD gennemgås halvårligt. Logs fra AD og andre væsentlige systemer bliver gennemgået løbende og ved begrundet mistanke om uautoriserede handlinger.		

Kontrolmål E: 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.*

Kontrolmål/Kontrol	PwC-test	Resultat af test
Brugerregistrering og administration af privilegier Oprettelse og nedlæggelse af brugere er ledelsesgruppens (LG) ansvar. Brugerne oprettes i forhold til arbejdsrelaterede behov. Proceduren er godkendt af ledelsen. Alle brugeres rettigheder bliver kontrolleret mindst én gang om året eller ved til-/afgang af medarbejdere. Adgang til kundernes systemer er kundens ansvar. Derfor har Outforce A/S ikke beskrevet dette. Brugere oprettes i grupper. Det er disse grupper, der har rettighederne til, hvad den enkelte medarbejder har adgang til. Det er LG, der beslutter, hvilke grupper en medarbejder skal være medlem af. LG vurderer løbende, om Outforce A/S' medarbejdere har de rigtige rettigheder. Samtlige brugere i Outforce A/S' AD og disses rettigheder bliver gennemgået minimum fire gange årligt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion påset, at det er LG, der godkender tildeling af adgang til systemerne, samt stikprøvevis kontrolleret, at forretningsgangene er overholdt for oprettede brugere på Outforce A/S' systemer. Vi har foretaget stikprøvevis kontrol af, at årlige gennemgange foretages.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Administration af brugeradgangskoder (password) Der er implementeret programmerede kontroller, der sikrer, at password har den fornødne kvalitet, jf. sikkerhedspolitikkens bestemmelser. Password skal bestå af minimum otte karakterer, og karaktererne skal være en blanding af tal og bogstaver. Password er gyldigt i maks. 60 dage og bør ikke genbruges.	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 ved inspektion kontrolleret, at der anvendes en passende passwordkvalitet i Outforce A/S' driftsmiljø, ved stikprøvevis test af, at adgang til virksomhedens systemer sker ved brug af brugernavn og password.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Evaluering af brugeradgangsrettigheder Outforce A/S foretager periodisk review af brugerret-	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: 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.*

Kontrolmål/Kontrol	PwC-test	Resultat af test
tigheder til sikring af, at disse er i overensstemmelse med brugernes arbejdsbetingede behov. Uoverensstemmelser undersøges og rettes rettidigt.	Vi har ved stikprøvevis inspektion kontrolleret, at der foretages periodiske gennemgange til bekræftelse af, at disse har fundet sted, samt påset, at identificerede afvigelser afhjælpes. Vi har endvidere stikprøvevis kontrolleret, at forretningsgangene er overholdt for oprettede brugere i Outforce A/S' systemer.	
Inddragelse af adgangsrettigheder Brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver deaktiveret ved disses medarbejderes fratrædelse. Ledelsen godkender inddragelse af rettigheder og nedlæggelse af brugere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, for at inddragelse af adgangsrettigheder sker efter betryggende forretningsgange, og at der foretages opfølgning i henhold til forretningsgangene på de tildelte adgangsrettigheder. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugere på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Politik for anvendelse af netværkstjenester, herunder autentifikation af brugere med ekstern forbindelse Al trafik til og fra internettet styres via en firewall. Opsætning af denne er elektronisk dokumenteret. Adgang fra fx hjemmearbejdsplads sker ved hjælp af VPN. Kunder har deres egen DMZ-zone. Ekstern adgang fra hjemmearbejdsplads eller eksterne samarbejdspartnere valideres ved hjælp af "SSL-VPN".	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, og vi har påset, at der anvendes en passende autentificeringsproces for driftsmiljøet. Vi har ved stikprøvevis inspektion kontrolleret, at brugere identificeres og verificeres, inden adgang gives, samt at fjernadgangen er beskyttet af VPN. Vi har ved inspektion konstateret, at netværket er segmenteret i mindre net ved hjælp af VLAN og DMZ for at reducere risikoen for uautoriseret adgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Styring af netværksforbindelser Netværksforbindelser testes sammen med kunden, såfremt kunden ønsker dette. Outforce A/S gennemgår firewallopsætning for at sikre unødig penetration. Som udgangspunkt er der lukket for trafik udefra. Ønsker	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at styre netværksforbindelser. Vi har ved inspektion konstateret, at der er foretaget periodiske penetrationstest, samt kontrolleret, at der er taget stilling til konstaterede svagheder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: 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.*

Kontrolmål/Kontrol	PwC-test	Resultat af test
kunder dette ændret, sker dette efter skriftlig anmodning.	Vi har ved stikprøvevis inspektion gennemgået firewall konfigurationen og påset, at reglerne i firewallen er sat hensigtsmæssigt op.	
Begrænset adgang til informationer Kun personer med behov for adgang til kundespecifikke systemer har adgang. Alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med Outforce A/S' politikker, til sikring af at rettigheder tildeles 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 kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion kontrolleret, at tildeling af adgang til data og systemer udføres ud fra et arbejdsrelateret behov og er godkendt i overensstemmelse med forretningsgangene.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

Der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer

Kontrolmål/Kontrol	PwC-test	Resultat af test
Styring af software på driftssystemer Outforce A/S har separate udviklings-, test- og produktionsmiljøer. Outforce A/S udvikler ikke software. It-miljøet for kundernes systemer er adskilt fra det interne it-miljø. Outforce A/S benytter patch management til at styre fx OS-opgraderingen. Patchning af kundeservere aftales og accepteres i samarbejde med den enkelte kunde. Patchning udføres i aftalt servicevindue. Proceduren omfatter kun OS, da kunden selv har ansvar for applikationerne.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, for at adskillelse mellem de enkelte miljøer opretholdes. Desuden har vi forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at holde kritiske systemer opdateret, og vi har gennemgået opdateringsprocedurernes tilstrækkelighed, forsåvidt angår Outforce A/S' egne væsentlige systemer samt kundernes systemer i henhold til kontraktlige aftaler. Vi har ved stikprøvevis inspektion gennemgået ændringerne i perioden, og påset at disse er dokumenteret. Vi har endvidere stikprøvevis efterprøvet kontrollerne, herunder at: • der er tilstrækkelig kommunikation med leverandørerne med henblik på, at modtage nødvendige informationer om kritiske og vigtige opdateringer, samt at der foretages de fornødne risikovurderinger af de enkelte opdateringer. • de kritiske systemer er blevet opdateret hensigtsmæssigt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ændringsstyring Outforce A/S bruger change management til at styre ændringer. Ændringer af daglige arbejdsopgaver er beskrevet i standard change, som er forhåndsgodkendt. Ingen ændringer i produktion implementeres, før change er godkendt af kunden og ledelsen samt testet, og fall back-plan er udformet. Nødændringer uden om den normale forretningsgang testes og godkendes efterfølgende. Ingen ændring må udføres uden godkendelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter der udføres, og gennemgået change management-procedurernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur. Vi har ved stikprøvevis inspektion 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 ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål G: Katastrofeplan

Outforce A/S er i stand til at fortsætte servicering af kunder i en katastrofesituation.

Kontrolmål/Kontrol	PwC-test	Resultat af test
Opbygning/Struktur af katastrofeberedskab Outforce A/S har udarbejdet en katastrofeplan. Denne beskriver sandsynligheder samt de nødvendige tiltag. Planen er godkendt af ledelsen og revideres årligt. **Test af katastrofeberedskab** Der sker årlig test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier. Såfremt testen afslører uhensigtsmæssigheder, opdateres planen umiddelbart herefter.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået det udleverede materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.