www.pwc.dk

Rackhosting ApS

ISAE 3402-erklæring fra uafhængig revisor vedrørende generelle it-kontroller i tilknytning til driften af kunders it-miljøer for perioden 1. januar 2016 til 31. december 2016 med udgangspunkt i standardvilkår

Juni 2017

pwc

Indhold

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Rackhosting ApS' generelle driftsydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunder selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i den enkelte kundes regnskab. Rackhosting ApS bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af de generelle kontroller i tilknytning til Rackhosting ApS' generelle driftsydelser, der er anvendt af kunder i perioden fra 1. januar 2016 til 31. december 2016. Kriterierne for denne udtalelse 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 2016 til 31. december 2016

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som kunder måtte anse for at være 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 perioden fra 1. januar 2016 til 31. december 2016. 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 perioden fra 1. januar 2016 til 31. december 2016.

Taastrup den 28. juni 2017
Rackhosting ApS

Martin Helms
Adm. direktør og ejer

2 Rackhosting ApS' beskrivelse af generelle it-kontroller i tilknytning til driften af kunders it-miljø med udgangspunkt i standardvilkår for 2016

2.1 Indledning

Rackhosting har eksisteret siden 1998 og er i dag en velkonsolideret virksomhed med en god track record hos kunderne.

Virksomheden har siden 2006 haft kontor med salg, administration og teknisk overvågningscentral (NOC) samt primære datacenter faciliteter, på samme adresse i Tåstrup.

Rackhosting har på et meget tidligt tidspunkt anerkendt at Serverdrift og Datacenter drift er to vidt forskellige ting og har derfor valgt ikke at drive egne datacentre. Det giver en større valgfrihed i forbindelse med systemdesign, og undgår at låse kundens løsninger og vores services til ét datacenter eller én DC leverandør.

Vi har kun ét kerneprodukt som vi kalder for CloudCore™ ENTEPRISE. Det er en Cloud platform der driver stort set alle kunder og services. Platformen består af er 3 anerkendte producenter nemlig Cisco netværk og Cisco UCS servere, Nimble Hybrid Flash SAN og VMware vCloud Air™ og kaldes en Smartstack™ under et. Platformen udemærker sig ved høj performance, driftssikkerhed, let administration og ikke mindst backup af alle data hver kvartér til et søster SAN i sekundært datacenter.

CloudCore™ er ydermere medlem af verdens største Content Delivery Network eller populært kaldet et CDN, som gør os i stand til at udnytte kræfterne fra over 170 Datacentre verden over, hvis kunden har behovet og hvis den enkelte løsning og data er egnet dertil.

Kunderne spænder vidt fra SMB segmentet til velrenommerede virksomheder som SBS/Discovery, Ingeniøren A/S, Sweco A/S (tidl. Grontmij/Calbro), Plandent A/S, D'Angleterre & Hilton, offentlige institutioner som Forsknings ministeriet, Statens IT, Energistyrelsen, og en stribe velkendte medie- og reklamebureauer.

Vores produkter og forretningsmodel henvender sig primært til virksomheder med egen eller ekstern IT organisation.

Rackhosting har ét erklæret ambitionsniveau; at blive en af Danmarks foretrukne cloud-udbydere til dansk erhvervsliv. Det vil vi opnå gennem second to none support og en mærkbart bedre performance end vores nærmeste konkurrenter.

2.2 Beskrivelse af ydelser

I dag afvikles stort set alle Rackhostings ydelser fra kun én platform nemlig VMware vCloud Air. Produkterne sælges både som standardprodukter på almindelige vilkår eller specialtilpasset til en kundes specifikke behov og på særskilt kontrakt, udarbejdet individuelt i samarbejde med kunden.

Til driftsydelserne tilbydes forskellige optioner, som domæneregistrering, SSL-certifikater, backup, antivirus og ikke mindst overvågning. Alle driftsydelser understøttes af differentierede serviceaftaler (SLA'er), professionel servicedesk og personlig konsulentbistand.

CloudCore™ ENTERPRISE	
Serviceydelse	CloudCore ENTERPRISE er baseret på VMware Enterprise og sælges som puljer med et fast sæt ressourcer til en fast månedlig pris. Kunden betaler altså for et aftalt sæt ressourcer i pakker, fx 24 GB RAM og 1 TB SAN og 12 vCPU'er. Pakkerne har en blød ressourcegrænse med et tilladt 10 % overforbrug indbygget, således at kunden kan skride ressource-grænsen uden at komme i vanskeligheder og uden at skulle opgradere. Rackhosting kan oprette servere for kunden, hvis dette er særskilt aftalt. Kunden kan vælge at have administrative rettigheder over de oprettede servere eller lade RH håndtere til og med operativlaget. Firewall og backupfunktion håndteres på baggrund af aftale. Rackhosting tager snapshot-backup til brug for egne katastrofescenarier. Kunden bør indgå særskilt aftale omkring backup. Aftaler er som regel indgået efter særskilt proces og krav. Hvis kunden har valgt Rackhosting som administrator af kundens operativsystemlag er der typisk lavet særskilt aftale omkring patchning og opdatering.

2.3 Kontrolmiljø

Teknisk personale sidder i vores NOC (Network Operations Center) i Tåstrup, hvor drift og kundeservice drives fra.

NOC'en indeholder storskærme til et generelt og samlet overblik over primære driftsparametre, incidents, og servicedesk-sager for alle tekniske medarbejdere.

De primære værktøjer er:

- Nagios til overvågning af KPI'er og eventhåndtering med SMS-alarmering til personale og kunder.
- Kayako Servicedesk til sagshåndtering og kundekommunikation
- Cacti til MRTG statistikker herunder performance og trafik
- ControlManager™ til dokumentation og procedurer samt kontrol og risikostyring herunder udarbejdelse af risikovurderinger.

Strategien for 2014-16 kan læses i virksomhedens separate 2014-2017 it-strategi.

Løsninger drives på baggrund af én standardaftale, hvis kunden ikke har fundet anledning til at forhandle den eller ikke har individuelle behov til løsning, omfang, budget og aftalevilkår.

Ansvarsfordelingen hos personalet er præciseret gennem vores kontrolkatalog, ControlManager™, hvor primære og sekundære personer er knyttet til aktiver, processer og kontroller. ControlManager styrer og adviserer ligeledes om opfølgende kontrolaktiviteter og risikostyring.

Som en del af ansættelsesaftalen skriver medarbejderne under på en fortrolighedsaftale. En tavshedspligt som også er gældende efter ansættelsesforholdets ophør.

Alle primære servere er placeret i et dedikeret serverrum som kun Rackhosting administrerer og kontrollerer, i et datacenter der drives af en ekstern leverandør. Der indhentes årlige revisorerklæringer dækkende dette område.

2.4 Risikostyring

Virksomhedens risikostyring håndteres af ledelsen gennem kontrolkataloget og tages op til revision hvert halve år eller oftere hvis noget fordrer det.

2.5 Information & Kommunikation

Rackhostings kommunikation med kunder baserer sig primært på vores servicedesk, Kayako. Kunderne sender mail til support@rackhosting.com og får et sagsnummer tilbage som kvittering på at sagen er modtaget korrekt.

Sager prioriteres af kunden, passes automatisk ind i kundens SLA-niveau og eskaleres eventuelt manuelt eller automatisk efter foruddefinerede principper. Sager tildeles ligeledes manuelt eller automatisk. Sager styres til og besvares af det rette personale alt efter type. Driftsrapportering sker i det omfang, det er aftalt separat med den enkelte kunde. Kunder på CloudCore vil i løbet af 2017, i et vist omfang selv mulighed for at følge drift-performance, i kundeportalen.

2.6 Overvågning

ControlManager™ overvåger og adviserer automatisk ansvarlige personer om udførelse eller manglende udførelse af prædefinerede kontroller. Der er netop ansat en ny person der skal varetage Awarenes i hele virksomheden således at alle medarbejdere informeres om og fastholder deres kontrolopgaver og ikke mindst bliver bevidst omkring ændringer og nye tiltag. Ledelsen følger med i, at udførelsen foregår og at medarbejderne prioriterer sikkerheden.

I ControlManager foreligger informationssikkerhedspolitikken, som løbende opdateres, og ændringer godkendes af ledelsen. Medarbejderne har adgang til sikkerhedspolitikken via ControlManager™ og alle ændringer eller tiltag vil blive uddelt og gennemgået på ugentlige morgenmøder hver tirsdag.

2.7 Kontrolaktiviteter

- Kontrol af proceduren: "Kapacitetsstyring og overvågning"
- Kontrol af proceduren: "Overvågning – VMware"
- Kontrol af proceduren: "Overvågning – CloudCore"
- Kontrol af proceduren: "Overvågning – Hardware"
- Kontrol af proceduren: "Tildeling af brugeradgang"
- Kontrol af proceduren: "WSUS opdateringer"
- Kontrol af proceduren: "Roll-Back efter fejlet WSUS opdatering"
- Kontrol af proceduren: "Backup/Restore politik og procedure".

Nærværende erklæring vedrører alene ydelser leveret og fysisk placeret i Danmark. Kundespecielle forhold er ikke omfattet.

2.8 Kundens ansvar

Kunder er selv ansvarlige for anskaffelse, udvikling og vedligeholdelse af applikationssystemer.

Kunden er ansvarlig for at melde tilbage inden for den fastsatte frist ved leverancer, såfremt en ydelse ikke modsvarer bestillingen, eller såfremt der er fejl eller mangler ved leverancen. Endvidere er det kundens ansvar løbende at sikre opdatering af adgange til kundens systemer, når der sker ændringer.

Det er ligeledes kundens ansvar at sikre behørig backup, det være sig en ydelse som Rackhosting leverer eller noget kunden selv har installeret. Når og hvis der er backup, er det især kundens ansvar at sikre jævnlige genskabelsestest af backuppens beskaffenhed. Hvis Rackhosting skal udføre det på vegne af kunden er det som udgangspunkt en betalt serviceydelse.

2.9 Detaljeret kontrolmål og egenkontroller

Detaljeret beskrivelse af kontrolmål og kontrolaktiviteter fremgår af afsnit 4.

.

3 Uafhængig revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet

Til ledelsen i Rackhosting ApS, kunder og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Rackhosting ApS' beskrivelse i afsnit 2 af it-kontroller for perioden 1. januar 2016 til 31. december 2016 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende beskrivelse omfatter ikke kundespecifikke forhold.

Rackhosting ApS ansvar

Rackhosting ApS er ansvarlig for udarbejdelse 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 Rackhosting ApS' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i beskrivelsen. 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, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om 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, egnetheden af de heri anførte mål samt egentheden af de kriterier, som Rackhosting ApS har specificeret og beskrevet.

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

Begrænsninger i kontroller hos en serviceleverandør

Rackhosting ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som kunder måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover

er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

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

(a) at beskrivelsen af Rackhosting ApS' generelle driftsydelser, således som de var udformet og implementeret i perioden fra 1. januar 2016 til 31. december 2016, 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 2016 til 31. december 2016, 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. januar 2016 til 31. december 2016.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder og disses revisorer, som har en tilstrækkelig forståelse til at overveje disse sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i kunders regnskab.

København, 28. juni 2017
PricewaterhouseCoopers
statsautoriseret revisionspartnerselskab

Michael Clement
statsautoriseret revisor

4. Kontrolmål, kontroller, test og resultat heraf

Outsourcing af fysisk sikkerhed, som er hostet hos Nianet med GlobalConnects datacenter i Taastrup som backup lokation, er begge indarbejdet i nærværende erklæring efter partielmetoden.

Kontrolmål og kontroller er opbygget efter ISO 27002:2013.

4. Risikovurdering

Kontrolmål 4.1: Risikovurdering

At virksomheden har en procedure for risikovurdering og der er udarbejdet en aktuel risikoanalyse, som er godkendt af ledelsen.

	Rackhosting-kontrol	PwC-test	Resultat af test
4.1.1	**Risikovurdering** Rackhosting gennemfører risikovurdering af kritiske interne informationsaktiver. Risikovurderingen er systematiseret ved anvendelse af værktøj. Risikovurdering foretages minimum én gang årligt. Ansvaret for risikovurdering er placeret hos ledelsen, der initierer igangsætning af vurdering i samarbejde med en vurderingsansvarlig.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret udleveret risikovurdering fra ControlManageren. Vi har desuden inspiceret, at risikovurderingen er foretaget inden for det sidste år.	Området er testet uden væsentlige bemærkninger

5. Informationssikkerhedspolitikker

Kontrolmål 5.1 Retningslinjer for styring af informationssikkerhed

At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

	Rackhosting-kontrol	PwC-test	Resultat af test
5.1.1	**Politikker for informationssikkerhed** Rackhostings informationssikkerhedspolitik er dokumenteret og vedligeholdes via ControlManageren ved regelmæssige gennemgange og opdateringer. Informationssikkerhedspolitikken er godkendt af ledelsen. Informationssikkerhedspolitikken er gjort tilgængelig for medarbejdere via ControlManageren.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at ledelsen har godkendt sikkerhedspolitikken, samt at den opdateres løbende. Endvidere at den forefindes let tilgængelig for medarbejderne.	Området er testet uden væsentlige bemærkninger

6. Organisering af informationssikkerhed

Kontrolmål 6.1: Intern organisering

At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen

	Rackhosting-kontrol	PwC-test	Resultat af test
6.1.1	**Roller og ansvarsområder for informationssikkerhed** Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Endvidere er der fastlagt regler for fortrolighedsaftaler, rapportering om informationssikkerhedshændelser samt udarbejdet dækkende fortegnelser over væsentlige aktiver.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, 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.	Området er testet uden væsentlige bemærkninger
6.1.2	**Funktionsadskillelse** Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i Rackhosting. Disse politikker og procedurer omfatter krav til at: • Administratorer med ansvar for produktion ikke har adgang til applikationer og transaktioner. • Backupadministratorer har ikke administrative rettigheder til både primær og sekundær backuplokation.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. It-medarbejderne er under interview blevet forespurgt til kompetencer, arbejdsområder og ansvar. Vi har inspiceret, at der er funktionsadskillelse mellem økonomi og it-drift. Vi har inspiceret, at der er funktionsadskillelse mellem primær og sekundær backuplokation.	Området er testet uden væsentlige bemærkninger

9. Adgangsstyring

Kontrolmål 9.1 Forretningsmæssige krav til adgangsstyring

At begrænse adgangen til information og informationsbehandlingsfaciliteter

	Rackhosting-kontrol	PwC-test	Resultat af test
9.1.1	***Adgang til netværk og netværkstjenester, datakommunikation*** Datakommunikationen er tilrettelagt på en hensigtsmæssig måde og er tilstrækkelig sikret mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed. Der er endvidere fortaget en opdeling af netværk, hvor dette er fundet nødvendigt eller aftalt med kunden.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter der udføres, og inspiceret at der anvendes en passende autentificeringsproces for driftsmiljøet. Vi har ved stikprøvevis inspiceret, at brugere identificeres og verificeres, inden adgang gives, samt at fjernadgangen er beskyttet af VPN. Vi har inspiceret at der gøres brug firewall-konfigurationen intrusion detection-system, som løbende og aktivt giver oplysninger om mulige ændringer, som kan påvirke "fortroligheden, integriteten og tilgængeligheden i data. Vi har inspiceret, at netværket er opsat med separate VLAN.	Området er testet uden væsentlige bemærkninger

Kontrolmål 9.2 Administration af brugeradgang

At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester

	Rackhosting-kontrol	PwC-test	Resultat af test
9.2.2	***Tildeling af brugeradgang*** Alle brugere skal være registreret med unikt bruger-id, og deres rettigheder til netværk og systemer skal være i overensstemmelse med Rackhostings politikker. Endvidere skal det sikres at rettigheder er betinget af et arbejdsbetinget behov, og er godkendt og oprettet korrekt i systemerne.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret procedure for brugeradministration samt, at kontrolaktiviteterne er tilstrækkeligt dækkende for Rackhostings behov. Vi har indhentet oversigt over brugerkonti på systemer og netværk. Vi har stikprøvevis inspiceret, at anmodning om adgang fra disse var dokumenteret og godkendt i overensstemmelse med relevant sikkerhedspolitik, og at der gøres brug af unikke og personhenførbare bruger-id'er.	Området er testet uden væsentlige bemærkninger
9.2.6	***Inddragelse eller justering af adgangsrettigheder*** Ved medarbejderes fratrædelse bliver alle brugerrettigheder til systemer, netværk, databaser og datafiler inaktiveret.	Vi har forespurgt ledelsen om de procedurer og 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 inspiceret at fratrådte medarbejdere var slettet fra AD og at brugere ikke fremgik af oversigt over aktuelle brugerkonti.	Området er testet uden væsentlige bemærkninger

Kontrolmål 9.4 Styring af system- og applikationsadgang
At forhindre uautoriseret adgang til systemer og applikationer

	Rackhosting-kontrol	PwC-test	Resultat af test
9.4.2	***Procedurer for sikker log-on*** Adgange til systemer, netværk, databaser og datafiler, er beskyttet med password. Der er opsat kvalitetskrav til passwords, således at der kræves en minimumslængde, kompleksitet og maksimal løbetid ligesom password-opsætninger medfører, at password ikke kan genbruges. Endvidere bliver brugeren lukket ude ved gentagne fejlagtige forsøg på login.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres i forbindelse med passwordkontroller, og inspiceret at der anvendes passende autentifikation af brugere på alle adgangsveje. Vi har inspiceret, at der anvendes en passende passwordkvalitet i Rackhostings driftsmiljø. Endvidere har vi stikprøvevis inspiceret at adgang til virksomhedens systemer sker ved brug af brugernavn og password.	Området er testet uden væsentlige bemærkninger

11. Fysisk sikring og miljøsikring

Kontrolmål 11.1 Sikre områder

At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter**.**

	Rackhosting-kontrol	PwC-test	Resultat af test
11.1.2	**Fysisk sikkerhedsafgrænsning** Adgang til sikrede områder (for såvel nye som eksisterende medarbejdere) er begrænset (bl.a. ved anvendelse af sikkerhedsbrik og personlig kode) til autoriserede medarbejdere. Personer uden godkendelse til sikrede områder, skal ledsages af en medarbejder med behørig godkendelse.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at der er modtaget ISAE 3402-erklæringer fra relevante serviceleverandører for relevant periode. Vi har endvidere foretaget en fysisk inspektion og konstateret, at sikkerheden er uændret i forhold til tidligere år.	Området er testet uden væsentlige bemærkninger

Kontrolmål 11.2 Udstyr

At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen**.**

	Rackhosting-kontrol	PwC-test	Resultat af test
11.2.2	**Placering og beskyttelse af udstyr** Datacentre er beskyttet mod fysiske forhold som brand, vand og varme. Der er endvidere installeret udstyr til overvågning af indeklima, herunder luftfugtighed og temperatur. Kabelføringen er sikret mod uautoriseret adgang. Datacentre er beskyttet mod strømafbrydelse ved anvendelse af UPS (Uninterruptible Power Supply) og nødstrømsanlæg.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at der er modtaget ISAE 3402-erklæringer fra relevante serviceleverandører for relevant periode. Vi har endvidere foretaget en fysisk inspektion og konstateret, at sikkerheden er uændret i forhold til tidligere år.	Området er testet uden væsentlige bemærkninger

12. Driftssikkerhed

Kontrolmål 12.1: Driftsprocedurer og ansvarsområder

At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter

	Rackhosting-kontrol	PwC-test	Resultat af test
12.1.1	**Dokumenterede driftsprocedurer** Der foreligger dokumenterede og ledelsesgodkendte driftsprocedurer for alle væsentlige områder i Rackhostings kvalitetsstyringssystem.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. I forbindelse med revision af de enkelte driftsområder har vi inspiceret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres.	Området er testet uden væsentlige bemærkninger
12.1.2	**Ændringsstyring** Nye systemer og væsentlige opgraderinger bliver testet, herunder brugeraccepttest af kvalificerede medarbejdere før implementering i produktionsmiljøet. Der udføres endvidere efterfølgende test af implementeringer. Problemer identificeret under udvikling og implementering af nye systemer og væsentlige opdateringer bliver løst tilfredsstillende. Test/vurdering af ændringer til systemer og netværk godkendes før flytning til produktion. Nødændringer af systemer og netværk uden om den normale forretningsgang bliver testet og godkendt efterfølgende.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter der udføres, samt ændringsstyringsprocedurernes tilstrækkelighed. Vi har inspiceret, at der er etableret et passende ændringshåndteringssystem, der er understøtter den tekniske infrastruktur. Vi har stikprøvevis inspiceret ændringsønsker for følgende: • Dokumenterede tests af ændringer herunder godkendelse • Godkendelse skal være opnået før implementering. Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende. • Plan for tilbagerulning, via snapshot hvor relevant.	Vi har observeret, at test af ændringer ikke i tilstrækkelig grad dokumenteres, samt at ledelsesmæssig godkendelse eller anden review i flere tilfælde ikke er formelt dokumenteret.

Kontrolmål 12.2: Malwarebeskyttelse

At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware

	Rackhosting-kontrol	PwC-test	Resultat af test
12.2.1	**Kontroller mod malware** Der er implementeret antivirusprogrammer, som bliver opdateret regelmæssigt.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har stikprøvevis inspiceret, at antivirusprogrammer er installeret, hvor det er relevant, og at disse er opdateret.	Området er testet uden væsentlige bemærkninger

Kontrolmål 12.3: Backup

At beskytte mod tab af data

	Rackhosting-kontrol	PwC-test	Resultat af test
12.3.1	**Backup af information** Der bliver foretaget sikkerhedskopiering af data med passende mellemrum. Periodisk sker der test af, at data kan genskabes fra sikkerhedskopier.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret at, backupprocedurer er opdaterede og formelt dokumenterede. Vi har ved stikprøvevis inspiceret, at backups er gennemført succesfuldt, alternativt at der foretages afhjælpning i tilfælde af mislykkede backups. Desuden har vi stikprøvevis inspiceret, at restore-test er udført.	Området er testet uden væsentlige bemærkninger

Kontrolmål 12.4: Logning og overvågning

At registrere hændelser og tilvejebringe bevis.

	Rackhosting-kontrol	PwC-test	Resultat af test
12.4.3	***Administrator- og operatørlogge*** Transaktioner eller aktivitet samt brugere med privilegerede rettigheder (fx superbrugere) bliver logget. Dette inkluderer også databaser. Afvigende forhold undersøges og løses rettidigt.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har stikprøvevis inspiceret at systemopsætningen af parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder på servere og væsentlige netværksenheder bliver logget. Vi har endvidere stikprøvevis inspiceret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer.	Området er testet uden væsentlige bemærkninger

13. Kommunikationssikkerhed

Kontrolmål 13.1: Styring af netværkssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter

	Rackhosting-kontrol	PwC-test	Resultat af test
13.1.1	***Sikring af netværkstjenester*** Der gennemgås regelmæssigt penetrationstests til sikring af netværket.	Vi har inspiceret, at der er foretaget periodisk penetrationstests samt, at der er taget stilling til konstaterede svagheder og iværksat tiltag til udbedring.	Området er testet uden væsentlige bemærkninger

15. Leverandørforhold

Kontrolmål 15.2: Styring af leverandørydelser

at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne

	Rackhosting-kontrol	PwC-test	Resultat af test
15.2.1	***Overvågning og gennemgang af leverandørydelser*** Der er fortaget gennemgang af ydelser fra serviceleverandører, herunder taget stilling til indhentning af revisionserklæringer fra disse fx 3402-erklæring. For type 2-erklæringer gennemgås brugerkontroller og disse sammenholdes med eksisterende kontroller og processer. Nye erklæringer bliver periodisk gennemgået til sikring af, at disse dækker korrekt periode. Endvidere gennemgås identificerede kontrolsvagheder. Forhold undersøges og løses rettidigt.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres, Vi har inspiceret, at der er modtaget ISAE 3402-erklæringer fra relevante serviceleverandører for relevant periode. Vi har desuden ved stikprøvevis inspiceret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter.	Området er testet uden væsentlige bemærkninger

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Kontrolmål 17.1: Informationssikkerhedskontinuitet

Informationssikkerhedskontinuitet bør være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

	Rackhosting-kontrol	PwC-test	Resultat af test
17.1.1	**Planlægning af Informationssikkerhedskontinuitet** Den samlede katastrofeplan er 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.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Området er testet uden væsentlige bemærkninger
17.1.2	***Verificer, gennemgå og evaluer* Informationssikkerhedskontinuiten** Der sker årligt test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret at beredskabsplaner testes ved skrivebordstest eller via realistiske testscenarier, i det omfang det er muligt.	Området er testet uden væsentlige bemærkninger